SWYX CONTROL CENTER

Administrator Documentation

As of: January 2024

Legal information

© 1/24 Enreach GmbH. All rights reserved.

Trademarks: Swyx, Swyxlt! 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

Emil-Figge-Str. 86

D-44227 Dortmund

office@enreach.de

enreach.de/en

CONTENTS

About this documentation ... 6

Introduction ... 8

Logging in and logging out ... 9
2.1 Resetting your password ... 10
2.2 Minimum requirements for passwords ... 11
2.3 Limited number of log-in attempts ... 11

User interface and menu navigation ... 12
3.1 Navigating and defining settings ... 13
3.2 Searching and filtering in lists ... 14
3.3 Starting calls from lists ... 14
3.4 Connectivity information ... 15

Editing General Settings ... 16
4.1 Defining login and number range settings ... 16
4.2 Retrieving license information ... 17
4.3 Entering a license activation key ... 19
4.4 Assigning Feature Profiles ... 19
4.5 Connection to Cloud Services ... 20
4.5.1 SwyxWare/SwyxWare for DataCenter (licensed via license key) ... 20
4.5.2 SwyxWare (Online Licensing) ... 21
4.5.3 SwyxON ... 21
4.5.4 Check the status of the connection ... 21
4.6 Configuring the provisioning of SIP phones ... 21
4.6.1 Displaying the administrative password for Desk Phones ... 22
4.7 Defining the log in settings ... 22
4.8 Defining an email server ... 24
4.9 Setting technical contact ... 25
4.10 Set RemoteConnector settings ... 26
4.11 Synchronizing intersite connections ... 27
4.12 Edit files ... 27
4.13 Setting music on hold ... 29
4.14 Intersite connections ... 30
4.15 Distributing software to clients or devices ... 30
4.15.1 Distributing firmware to devices ... 32
4.16 Defining client settings for all Users ... 32
4.17 Accessing SwyxWare Administration ... 33
4.17.1 Downloading trunk recordings ... 34
4.18 Defining codec filters ... 34
4.19 Federated authentication via identity provider ... 35
4.19.1 Create identity provider configuration ... 36
4.19.2 Edit identity provider configuration ... 37
4.20 Expert settings ... 37
4.21 Synchronize user status with Microsoft Teams ... 41
4.21.1 Requirements ... 42
4.21.2 Registration on your Microsoft Teams tenant ... 42
4.21.3 Configuration in Swyx Control Center ... 44
4.21.4 Checking the functionality ... 44

Online Licensing ... 46
5.1 Subscribe or Purchase ... 46
5.2 Feature Profile ... 46
5.3 Additional functions ... 49
5.4 Evaluation Installation ... 51
5.5 Billing ... 51

Licensing via license key ... 52
6.1 Licensing Procedure ... 52
6.1.1 Swyx Update Service (SUS) ... 53
6.1.2 SwyxWare for DataCenter Licensing procedure ... 53

6.1.3 User license ... 53
6.1.4 Licenses for Clients ... 54
6.1.5 Licensing of data channels ... 55
6.1.6 Options and Option Packs ... 55
6.1.7 SwyxWare Option packs at a glance ... 58
6.1.8 Licensing of the SwyxWare variants at a glance ... 60

Creating and editing Locations ... 62
7.1 Creating Locations ... 62
7.2 Editing the Location settings ... 63
7.3 Limiting the number of calls between Locations ... 63
7.4 Deleting Locations ... 64

Trunks ... 65
8.1 Create trunk groups ... 65
8.2 Edit trunk groups ... 67
8.3 Create trunks ... 70
8.4 Edit trunks ... 75
8.5 Delete trunk groups ... 78
8.6 Delete trunks ... 78
8.7 Forwarding and number substitution ... 79
8.7.1 Defining call number substitutions for a trunk group ... 81

Creating and editing Users ... 83
9.1 Administration profiles ... 83
9.1.1 Administrators in SwyxWare for DataCenter and SwyxON ... 84
9.2 Authentication for clients ... 84
9.3 Creating Users ... 86
9.4 Editing Users' general settings ... 89
9.5 Editing the authentication settings ... 89
9.6 Editing the SIP settings ... 90
9.7 Editing the encryption settings ... 90
9.8 Defining call and status signaling ... 91
9.9 Creating Remote Connector client certificates ... 92
9.10 Defining rights ... 92
9.11 Defining a relation between manager and secretariate ... 93
9.12 Setting the telephony settings ... 94
9.13 Set name keys and line keys ... 98
9.14 Editing shortcut keys ... 100
9.15 Import/export key assignments ... 101
9.16 Editing numbers for Groups ... 101
9.17 Defining client settings for selected Users ... 102
9.17.1 Defining status signaling via device ... 102
9.17.2 Defining settings for lists and buttons ... 103
9.17.3 Activating conversation recordings ... 104
9.18 Editing user-specific files ... 104
9.19 Defining the skin ... 106
9.20 Editing the call signaling settings ... 107
9.21 Defining ring tones ... 107
9.22 Display Swyx Mobile configuration ... 108
9.23 Deleting Users ... 109

Creating and editing Groups ... 110
10.1 Creating Groups ... 110
10.2 Editing the general settings for Groups ... 113
10.3 Editing the assignment of Users to Groups ... 113
10.4 Editing numbers for Groups ... 113
10.5 Adding alternative numbers for Groups ... 113
10.6 Set voice box for groups ... 114
10.7 Editing the signaling settings for Groups ... 115
10.8 Deleting Groups ... 115

Creating and editing conference rooms ... 116
11.1 Creating Conference Rooms ... 116

11.2 Editing numbers for Conference Rooms ... 117
11.3 Deleting Conference Rooms ... 117

Devices ... 118
12.1 Certified SIP phones ... 118
12.1.1 Customer-specific configuration of multiple phones ... 118
12.1.1.1 Application example: ... 120
12.1.1.2 Provisioning file upload ... 121
12.1.1.3 Remove customer-specific settings ... 121
12.1.2 802.1X authentication of Yealink devices in the SwyxWare environment ... 122
12.1.3 Creating Desk Phones ... 124
12.1.3.1 Importing Desk Phones ... 124
12.1.4 Activating Desk Phones ... 125
12.1.5 Log in/out Desk Phones ... 125
12.1.6 Editing settings for certified Desk Phones ... 126
12.1.7 Deleting Desk Phones ... 129
12.2 DECT telephones ... 129
12.2.1 DCF DECT system put into operation ... 130
12.2.1.1 Prepare hardware ... 130
12.2.1.2 Create DECT system ... 131
12.2.1.3 create DECT base station(s) ... 131
12.2.1.4 Creating DECT handsets ... 132
12.2.1.5 Activating DECT system ... 133
12.2.1.6 Configure subnet base stations (optional) ... 135
12.2.1.7 Check commissioning ... 136
12.2.2 Editing the DECT systems ... 136
12.2.2.1 Edit DECT systems ... 136
12.2.2.2 Edit DECT base station ... 137
12.2.2.3 Edit DECT handsets ... 137
12.2.2.4 Assigning function keys on the DECT handset ... 138
12.2.3 Perform factory reset ... 139
12.2.4 Activate administration menu on a DECT 800 handset ... 139
12.2.5 Error messages from DECT handsets ... 140
12.3 Swyx Phones ... 140
12.3.1 edit SwyxPhones ... 141

Editing phonebooks ... 142
13.1 Creating phonebook entries ... 142
13.2 Editing phonebook entries ... 143
13.3 Exporting phone books ... 143
13.4 Importing phonebook entries ... 144

Data Storage ... 145
14.1 Storage location configuration ... 146
14.2 Trunk Recording ... 147
14.3 Voice messages ... 151
14.4 Call Detail Records (CDR) ... 152
14.4.1 File Format ... 154
14.4.2 Examples for CDR ... 157

Numbers and Number Mappings ... 161
15.1 Number Types ... 161
15.1.1 Internal numbers ... 161
15.1.2 External numbers ... 161
15.1.3 SIP-URIs ... 162
15.2 Number concept ... 163
15.3 Mapping of numbers ... 164
15.4 Examples of number mappings ... 165
15.5 Placeholder ... 167
15.5.1 General Placeholders ... 167
15.5.2 Special placeholders ... 168
15.5.2.1 Placeholders in the Call Permission ... 168
15.5.2.2 Placeholders for number replacement ... 168
15.6 Supplied Configuration Data ... 170
15.6.1 NumberFormatProfiles.config ... 170

15.6.2 ProviderProfile.config 174

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 documentation is primarily directed at Users.

Conventions for the descriptions

Operating steps

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

Menu operation

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

My profile | Password

refers to the menu item **Password** which you will find in the **My Profile** menu.

Special design elements

STOP

This indicates a security notice: ignoring the notice can lead to material damage or loss of data.

This indicates a security notice 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 indicates helpful tips that can make using the software easier.

Instructions are designed as follows,

...which prompt the User to perform an action requiring several steps (**1.**, **2.** etc.)

Online help

To access the help system, click on ? on the top right on a page.

Further information

- For current information on the products, please see our Internet homepage:
  enreach.com
- The latest documentation for all products can be found in the support area of the homepage:
  enreach.de/en/products/support/documentation.html

1 INTRODUCTION

What is Swyx Control Center?

Swyx Control Center is a web-based administration tool with which you can carry out the basic configuration of your SwyxWare conveniently via browser. With Swyx Control Center you can set server and user properties, manage desk phones, the global phonebook, trunks, proxy settings and much more.

Further configuration options are provided via SwyxWare Administration. For requirements and installation of Swyx Control Center and information about SwyxWare Administration see help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/index.html.

2 LOGGING IN AND LOGGING OUT

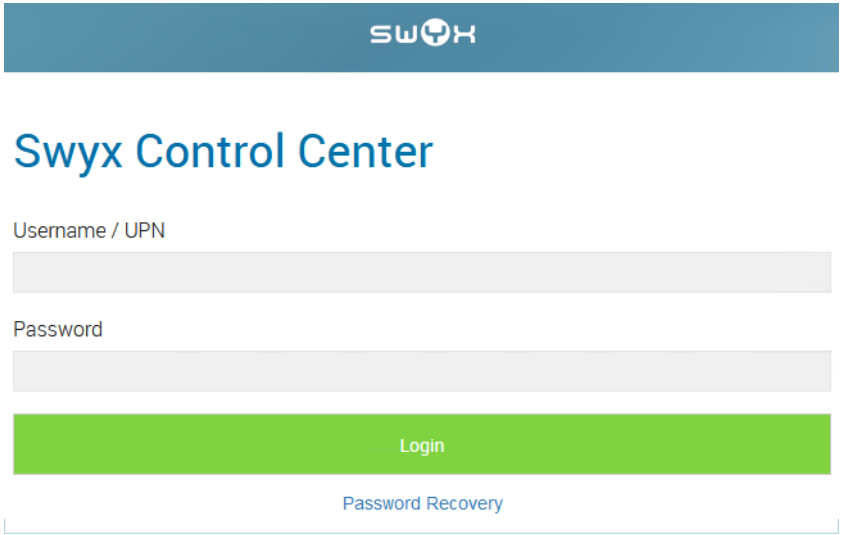
You must authenticate yourself to gain access to Swyx Control Center.

You receive the homepage address and the login data via email or directly from your Administrator.

When saving and processing personal data, observe the appropriate applicable legal data protection regulations.
If you have any questions especially regarding data protection in SwyxWare, please contact your administrator.

How to log in

1 Enter the Swyx Control Center address to your web browser.
✓ The login window appears.



2 Enter your SwyxWare login name and password.
Depending on the system and user configuration, the following login names can be used:
Display name: "Jones, John"
E-mail address: "john.jones@mailserver.com
User Principal Name (UPN): "john.jones@exapmle.com"
or
If necessary, click **Password Recovery**, see **2.1 Resetting your password**, page 9

3 Click on **Log in**.
✓ When you first log in, you are requested to set up two-factor authentication via an app on your smartphone.
For this purpose, the following steps are necessary:

1 Click on **Next**.
✓ The **Configure Two-Factor authentication** configuration wizard appears.

If a user has two-factor authentication enabled, their password can only be changed by the administrator.

2 Load one of the apps displayed onto your smartphone with internet access.

3 Set up the app on your smartphone and start the QR code scan.

4 In Swyx Control Center, click on **Next**.
✓ A QR code appears in the Swyx Control Center for 30 seconds.

5 Point your smartphone camera at the screen to scan the QR code.

If you do not scan the QR code within 30 seconds, you must restart the process. To do this, click on **Finish** and return to the login page.

✓ A 6-digit PIN appears in the app on your smartphone.

For security reasons, the PIN is regenerated every 30 seconds. A PIN is only valid one-off and appropriately for 6 minutes.

6 Enter the PIN on the Swyx Control Center within 6 minutes.

If you do not enter the PIN for setting up two-factor authentication within 6 minutes or enter it incorrectly, you must restart the process. To do this, click on **Finish** and return to the login page.

- ✓ You are logged in.
- ✓ The Swyx Control Center home page appears.
- ✓ For all subsequent logins, you must enter the current PIN in the app on your smartphone in Swyx Control Center.

If you cannot access the app, please contact your Administrator.

To log off from Swyx Control Center

1 Click on your display name in the title bar.

✓ The sub-menu **My Profile** appears.

2 Click on **Logout**.

For security reasons, you are automatically logged out after 60 minutes' inactivity.

2.1 RESETTING YOUR PASSWORD

Your password can be reset by the administrator, see **Reset user passwords (password reset service)**, page 85.

Your password is deleted. Login at SwyxWare is no longer possible. Your current login session will expire within an hour.

You will receive an email from Enreach with the password reset link to the Swyx Control Center dialog. Access the link and proceed to **To reset your password**, page 9.

You can only reset your password if an email address has been configured for you in Swyx Control Center.

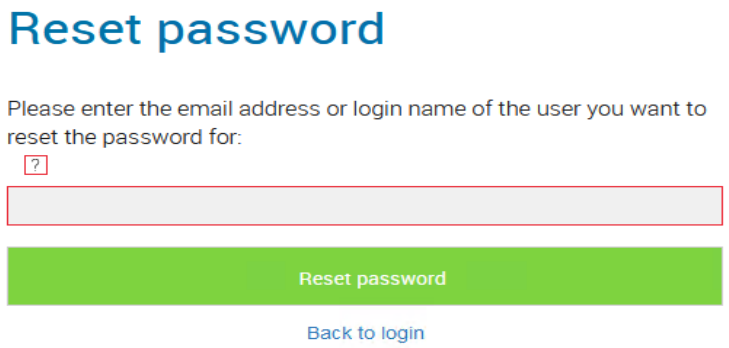
You can change your password

- on the login page, click on **Password Recovery**.
- after a failed login attempt in SwyxIt! login dialog. Click **Forgot password**.

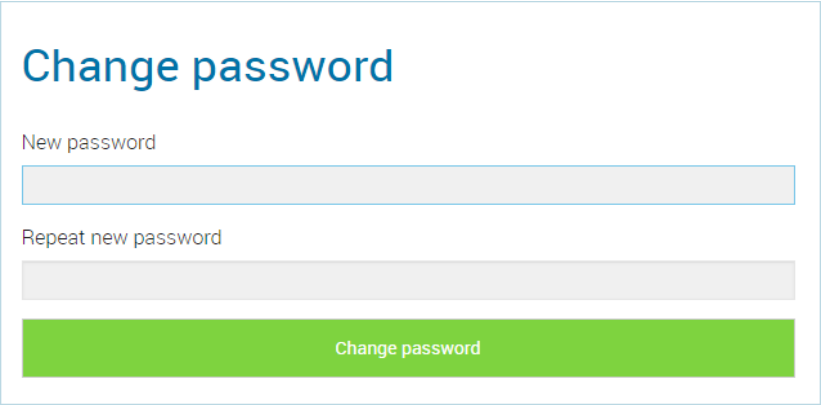
To reset your password

You have followed the link to reset the user password.

✓ The corresponding web page in Swyx Control Center opens:



1 Click on **Reset password**.



2 Enter your new password in the **New password** field and confirm the entry in the **Repeat new password** field, see section **2.2 Minimum requirements for passwords**, page 10.

It is not possible to use the current password again when changing a password. It is not possible to reuse the three previous passwords if **Force complex user passwords and password history** is enabled for the user.

You can change your complex password anytime you are logged on to the system, see section **Title bar**, page 12.

2.2 MINIMUM REQUIREMENTS FOR PASSWORDS

Passwords 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: full-stops, commas, brackets, blanks, hash tags (#), question marks (?), percent signs (%), ampersands (&).

Alphabetic characters (such as: ß, ü, ä, ẽ, ô) and non-Latin characters (such as: Ω, π, μ) are not special characters and are regarded as letters.

2.3 LIMITED NUMBER OF LOG-IN ATTEMPTS

The number of log in attempts can be limited.

When the maximum number of failed log in attempts has been reached, the account is locked and a message appears with an instruction to contact the Administrator.

You can no longer log in, neither via Swyx Control Center nor client nor end device, until the Administrator has reactivated your account.

See also **4.7 Defining the log in settings**, page 21.

The number of failed logins is set to zero after a successful login.

The number of failed log in attempts is irrelevant, when the Administrator has established a forced password change, and the User attempts to log in with his/her previous password.

3 USER INTERFACE AND MENU NAVIGATION

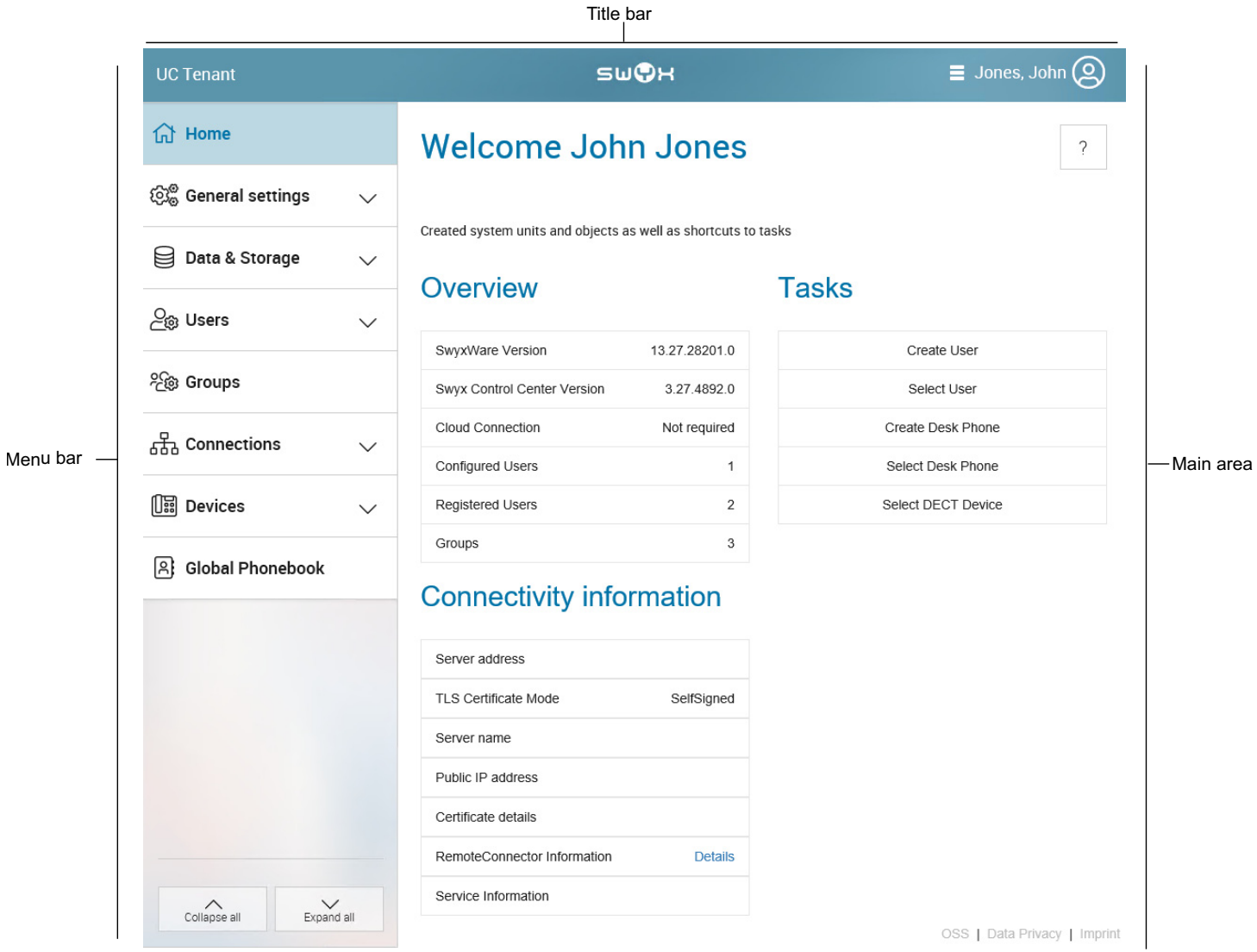


Abb. 3-1: Home page (example for visualization)

See also **3.4 Connectivity information**, page 14

You can only use the full functionality of Swyx Control Center cookies and pop-ups are permitted in your browser settings.

The elements displayed on the user interface are context- and/or profile-related, i.e. different for each user.

Title bar

Your name and User picture are displayed on the title bar.

With a click on your name, you move to your profile information, language selection and can log out.

Further information about your current settings is displayed under the title bar. Click on ✕ to hide the information.

Menu bar

On every page, you will see the menu that provides you with access to settings and information.

Use the arrow keys to hide or unhide submenu items.

Button	Explanation
⌄	Show sub-menu items
⌃	Hide sub-menu items
‹	Fully hide menu (only appears if you remain above the menu bar with the mouse pointer)
›	Fully display menu

Main area

An overview of your created system units (e.g. Users, Desk Phones) appears on the start page with buttons for fast access to your tasks - a single click suffices to reach the appropriate menu item. In addition, the contact details of your reseller may appear.

On the menu pages, various settings appear as well as buttons providing access to configuration wizards. Additionally, some main menu items provide buttons for the quick access to settings which are available in sub menu items.

Navigating and defining settings

Searching and filtering in lists

Starting calls from lists

Connectivity information

3.1 NAVIGATING AND DEFINING SETTINGS

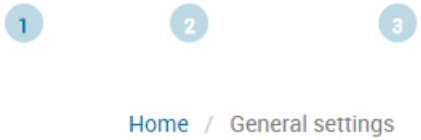
The setting options on menu pages and in configuration wizards depend on your administration profile and your SwyxWare solution.

Configuration wizards are available on the corresponding menu pages for creating system units and specifying basic settings. Use the **Next**, **Back** and **Cancel** buttons to navigate within the configuration wizard. In general, you are offered additional optional settings in step before last.

On the menu pages you can find further settings under various tabs; these can be defined after creation.

If inputs are incorrect or missing, ? and a red margin around the corresponding field are displayed. An explanatory error message appears if you remain over the field with the mouse pointer.

With the help of the navigation path in configuration wizards and on menu pages, you can orientate yourself and return to a past step or a superordinate menu item with a single click.



3.2 SEARCHING AND FILTERING IN LISTS

In lists you can click on in a table column heading to filter lists by search items.

Button	Explanation
	Enter string
	No active filter
	Filter active
Filter	Apply filter
Remove	Remove filter

Click on a column heading and an arrow is displayed which shows whether the column is sorted alphabetically backwards or forwards. Click again to reverse sorting or to hide the arrow again.

Click on to display further information.

Click on **Elements per page** to define how many list elements are displayed per page.

3.3 STARTING CALLS FROM LISTS

In lists you can start calls via SwyxIt! to this user by clicking on in the line of the corresponding user.

For this purpose you need to set SwyxIt! in your control panel as the default program for tel: Set URL.

As a User without administrator rights, you can call the Administrator on the start page by clicking or send him or her an email from your standard email program.

3.4 CONNECTIVITY INFORMATION

SwyxWare is equipped with an automatically generated (SelfSigned) TLS certificate by default. If your system was equipped with an official trusted TLS certificate and optionally with a unique public server name (Fully qualified Domain Name, FQDN), the following information appears on the start page:

Label	Explanation
Server address	The registered FQDN of your network. This FQDN may have been randomly generated by the SwyxON DNS service and assigned to the public IP address.
TLS certificate mode	**Manually:** You use your own certificate. or **Automatically:** TLS certificate was obtained from Let's Encrypt.
Server name	Name of the SwyxServer Clients must use this name to communicate with the SwyxServer.
Public IP address	The public IP address of your network.
Certificate validity	The time and date when the validity of the certificate expires. You must update the certificate before the expiration date.
Certificate information	Click on **View**. **Name** TLS certificate name is defined by Let's Encrypt, if applicable, and usually contains the FQDN and creation date for information. **Issuer** A certificate authority (CA) that issues digital certificates. **Thumbprint** Digital thumbprint of the certificate. **Valid until** The date on which the validity of the certificate expires. You must update the certificate before the expiration date.
RemoteConnector information	Click on **Details** See **4.10 RemoteConnector for SwyxIt! Define settings**, page 25
Server information	Click on **Details** This page displays information about the current state of the SwyxServer. See also **4.20 Expert settings**, page 37

See also https://help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/SCST

4 EDITING GENERAL SETTINGS

Under **General Settings** you can define settings which are valid for all Users, Locations, Desk Phones on the same server etc.

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

The setting options on menu pages and in configuration wizards depend on your administration profile and your SwyxWare solution.

Defining login and number range settings

4.1 DEFINING LOGIN AND NUMBER RANGE SETTINGS

Proxy server

For online licensing with license query by the Swyx license server, there must be a permanent internet connection to your SwyxServer, see also help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/online_licensing_$.

If you use a proxy server for this purpose, you must specify the required settings either during installation or in Swyx Control Center, see also help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/configure_swyxware_$.

To define a proxy server

1 In the menu, select **General Settings | System**.

Designation	Explanation
Connection test	Click on the button to test the connection to the Swyx license server.
Activating proxy	Activate the checkbox to activate the proxy settings.
Proxy address	Enter the IP address or the DNS server of the proxy server.
Proxy port	Enter the port of the proxy server.
Proxy username	Enter a username for the authentication on the proxy server.
Proxy password	Enter a password for the authentication on the proxy server.

2 Click on **Save**.

Internal number range

Under internal phone numbers, users can be reached by other users who are assigned to the same or a different networked location. For this purpose, a call number range must be defined from which the internal call numbers can be dialed, see also **15 Numbers and Number Mappings**, Seite 164.

The following specifications apply to internal call numbers:

- Several internal phone numbers can be assigned to one User.
- Internal phone numbers may differ from the extension number of the external phone number.

  Example: External phone number +49 231 5666 227 -> Internal phone number 5227
- The maximum number of digits for internal numbers is 10.
- The lowest and highest numbers in the number range must have the same number of digits.

  Example: 111-999
- Internal phone numbers must not overlap with other phone numbers or codes used in the system.

  Example: An internal call number may not begin with a "0" if this is used for the outside line access of the location.

- An internal call number must not be contained in an internal call number that has already been assigned.

  Examples:

  User 1 has the internal number 12345; User 2 must then not have the internal number 1234, 1235 would, however, be possible.

Designation	Explanation
Lowest internal number	Enter the lowest of the phone numbers that can be assigned to the users at SwyxServer.
Highest internal number	Enter the highest of the phone numbers that can be assigned to the users at SwyxServer.

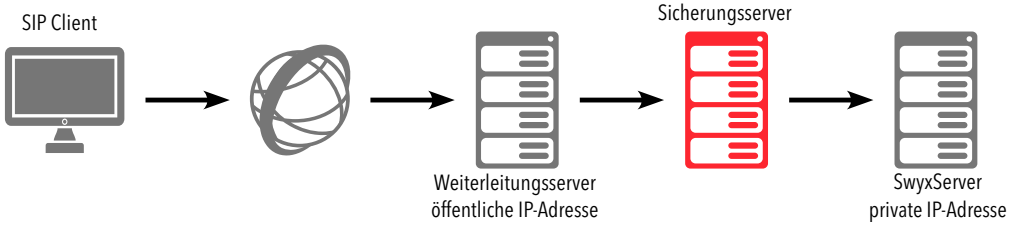
Prevent registrations and calls

For the maintenance of SwyxServer it may be necessary to block registrations and calls via SwyxServer. Once the options are enabled, users can no longer log in and/or make calls. Existing calls are not interrupted. So you can wait until all calls are finished and then stop the server after activating this option.

Designation	Explanation
Disable login	Select the checkbox to prevent logon to SwyxServer.
Disable calls	Activate the checkbox so that no calls can be made via SwyxServer.

Public IP address for SIP

In SwyxWare for DataCenter, 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. Direct communication from the outside into the private network behind the firewall is not allowed, but all data traffic passes through a backup server. The SwyxServer, which is located in the private network, is addressed from outside (Internet) via a forwarding server. This forwarding server has a public IP address and forwards the communication to SwyxServer, which only has a private IP address within the network.



SIP clients such as SwyxIt! that want to log on as SwyxWare users via the Internet must configure the public IP address of the forwarding server as SwyxServer (=SIP Registrar/Proxy). This forwarding server forwards the logon and also all other CallControl messages to SwyxServer.

When communicating with the SIP clients that connect to SwyxServer via the Internet, SwyxServer needs this public IP address to indicate it as the sender. For this reason, SwyxServer must be made known via which public IP address it can be reached from outside.

In a standard SwyxWare installation, specifying a public IP address of the forwarding server does not work. Here, internal clients (within the company network) and external clients (on the Internet) are typically mixed. In such a case, an SwyxServer access via VPN must be set up for the external clients.

See also help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/SIP_$.

Designation	Explanation
Public IP address for SIP	Enter the public IP address that can be used to reach SwyxServer from the outside if the server is running behind a firewall. Leave the field empty if no public IP address is required.

4.2 RETRIEVING LICENSE INFORMATION

You can get information about the scope of your licenses from the Swyx Flex license server, see also **5 Online Licensing**, Seite 46 or **6 Licensing via license key**, Seite 52.

For provisioning of Yealink Desk Phones in SwyxWare for DataCenter it is necessary that you connect once to the Swyx license server under . Click on **Activate** to do this.
See also **4.15.1 Distributing firmware to devices**, Seite 31, and **12 Devices**, Seite 118.

If your licensing is about to expire or is insufficient, a warning will appear in the title bar.

To retrieve license information

1 In the menu, select **General Settings | Licenses and Features**.
- ✓ For online licensing and SwyxON a list appears with all of your licensed Feature Profiles.
- ✓ For licensing via license key, the list of your registered licenses appears.

For license information on licensing via license key see **License information on licensing via license key**, Seite 18.

For information on feature profiles in SwyxWare see also help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/profiles_$.

License information on online licensing

Designation	Explanation
Name	Feature Profile name
Licensed	Number of licensed Feature Profiles
Used	Number of currently used Feature Profiles
Free	Number of licensed, unused Feature Profiles
Expiration date	Date from which the license loses its validity, i.e. the corresponding Feature Profiles are deactivated

2 Click on **User specific features**.
- ✓ A list appears with your licensed additional features which are assigned to certain Users.

Designation	Explanation
Name	Name of the feature
Licensed	Number of licensed features
Used	Number of currently used features
Free	Number of licensed, unused features
Expiration date	Date from which the license loses its validity, i.e. the corresponding functions are deactivated

3 Click on **Customer system specific features**.
- ✓ A list of your licensed features appears, which are billed per SwyxWare system and are available to all Users.

Designation	Explanation
Name	Name of the feature
Licensed	Number of licensed features
Used	Number of currently used features
Free	Number of licensed, unused features
Expiration date	Date from which the license loses its validity, i.e. the corresponding functions are deactivated

Click on **Update license information** to retrieve the current information from the licensing server.

In SwyxON your function profiles, conference rooms and fax channels including the maximum number available appear as license information, see also help.enreach.com/swyxon/1.00/Partner/Swyx/en-US/#context/help/ordering_contingents_$ and help.enreach.com/swyxon/1.00/Partner/Swyx/en-US/#context/help/ordering_conference_rooms_$.

4.3 ENTERING A LICENSE ACTIVATION KEY

If your system has been licensed online, you can enter a new activation key in Swyx Control Center, e.g. in case of a functional enhancement or after the evaluation period has expired.

You can obtain the activation key from your service provider, see **5 Online Licensing**, Seite 46

To enter an activation key

1 In the menu, select **General Settings | Licenses and Features**.

2 Click on **Enter activation key**.
✓ The input field **Activation key** appears.

3 Enter the activation key.

4 Click on **Activate**.
The activation may take a while.

5 Click on **Update license information** to check the licensing.
✓ The activation is completed and the ordered features are available for you.

4.4 ASSIGNING FEATURE PROFILES

You can assign Feature Profiles to Users.

If the assignment is not possible, there is no license for the Feature Profile.

To assign Feature Profiles to Users

1 In the menu, select **General Settings | Licenses and Features**.

2 Click on **Feature Profiles**.
✓ A list appears with all of your licensed Feature Profiles.

Designation	Explanation
Name	Name of the feature
Licensed	Number of licensed features
Used	Number of currently used features
Free	Number of licensed, unused features

The infinity symbol means that the number is unlimited.

3 Drag and drop one of the users on the right to a Feature Profile in the table on the left. To cancel the assignment, assign another profile to the user.

Use the search bar above the list of all users to search for users. Click on **View All** to end the search.

✓ The User can use the included features as soon as he or she logs in to SwyxServer

License information on licensing via license key

Designation	Explanation
Product	Name of the product
Permanent	Number of permanent licenses for the product
Temporary	Number of licenses for a time-limited installation

4 To access further information, click on ⌄.

Designation	Explanation
Product details	Exact designation of the product
Type	Permanent or temporary

Designation	Explanation
Number	Number of licenses for the product

Make sure to acquire a sufficient amount of user licenses for an Option Pack since 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.

In SwyxWare for DataCenter this tab is not available if you have activated the option "Use license server" in SwyxWare. If you administer the licensing server yourself, you will find only one license here. See also https://help.swyx.com/cpe/13.30/Client/Swyx/en-US/index.html#context/help/office_communication_$.

For information on assigning users to Feature Profiles see **4.4 Assigning Feature Profiles**, Seite 18.

4.5 CONNECTION TO CLOUD SERVICES

To ensure the functionality of Swyx Meeting and Swyx Messenger you need to connect your installation with appropriate Swyx Cloud Services.

The connection to cloud services is registered to the domain name you set in Logpn settings, see **Domain (not in SwyxON and SDC)**, Seite 23.
Once the connection is established, you cannot change the domain name.
If you have not entered a domain name, a random name, such as "5wmoue.swyx.net" will be generated when connecting to cloud services.

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.

Cloud service delivery may differ depending on your SwyxWare variant:

SwyxWare/SwyxWare for DataCenter (licensed via license key)

SwyxWare (Online Licensing)

SwyxON

4.5.1 SWYXWARE/SWYXWARE FOR DATACENTER (LICENSED VIA LICENSE KEY)

Requirements:

- Valid permanent licenses
- "New Swyx Messenger" is activated via Konfigurationsassistent, see help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/configure_swyxware_$

If the requirements are not met, contact your Swyx partner or distributor to manually activate Swyx Messenger and Swyx Meeting for installation.

To connect your system to cloud services

1. In the menu, select **General Settings | Licenses and Features**.
2. Click on **Connect to cloud services** and confirm the procedure.
   ✓ An automatic order request is forwarded to the technical staff.

It may take up to 24 hours before you can use the new features.

4.5.2 SWYXWARE (ONLINE LICENSING)

Requirements:

- The installation was done with a valid activation key
- "New Swyx Messenger" is activated via Konfigurationsassistent, see step 26 under help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/configure_swyxware_$

To connect your system to cloud services

1 In the menu, select **General Settings | Licenses and Features**.

2 Click on **Connect to cloud services** and confirm the procedure.
✓ The message **You have connected to cloud services successfully** appears. Swyx Messenger and Swyx Meeting are activated for your SwyxWare and can be used immediately.

4.5.3 SWYXON

No further steps are necessary. Swyx Messenger and Swyx Meeting are provided by default.

4.5.4 CHECK THE STATUS OF THE CONNECTION

In case of problems with the cloud services, you can quickly check the current connection state between the UC Tenant and the cloud services.

To check the connection to cloud services

1 In the menu, select **Homepage**.
✓ In the **Overview** section, in the line **Cloud connection** you will see one of the following states:

Designation	Explanation
Not required	Use of the Cloud services is not requested by you.
Not connected	Use of the cloud services has been ordered. You must connect your system to the cloud services, see *Connection to Cloud Services*.
Established	Connection has been established, cloud services are being used.
Established (Services pending...)	Connection has been established, but the automatic setup of the services is not yet complete.
Produced (Waiting for confirmation...)	Connection has been established. A manual confirmation by the provider is expected. Please contact support if this condition lasts more than 24 hours.
Interrupted	Connection is interrupted.
Deactivated	The cloud services are deactivated

4.6 CONFIGURING THE PROVISIONING OF SIP PHONES

You can configure DCF provisioning of certified SIP phones and DECT systems in the local network, see also chapter **12 Devices**, Seite 118.

To configure SIP phone provisioning

1 In the menu, select **General Settings | System**.

2 Click on **Provisioning**.

Designation	Explanation
Reset SIP credentials of the device	Click on the button if the DECT handsets should automatically log on for the corresponding assigned users after a SwyxWare/NetPhone database restore, see **12.3.2.3 Edit DECT handsets**, Seite 139

Designation	Explanation
Activation required for certified phones	If you activate this option, all certified SIP phone users must authenticate themselves once before they can use the relevant device.
URL auto detect (not in SwyxON and SDC)	Activate the checkbox if the IP address of the SwyxServer can be resolved automatically in the local network.
Host name for the provisioning URL	If you deactivate the "URL auto detect" option, you can enter the IP address or the appropriate provisioning server's host name.
Provisioning URL (not in SwyxON and SDC)	URL for provisioning phones. Click on to copy the path to your clipboard.
Update RPS IP (only SwyxON and SDC)	Click on the button to update the IP address of the provisioning server.
Administrative device password for certified phones	See **4.6.1 Displaying the administrative password for Desk Phones**, Seite 21.

3 Click on **Save**.

4.6.1 DISPLAYING THE ADMINISTRATIVE PASSWORD FOR DESK PHONES

For certified Yealink SIP phones and SwyxPhone L6x, you can define manufacturer-specific settings via the manufacturer's web interface. The IP address can be found on the device under **Menu | Status**. You can log in with the user name "admin". Alternatively, you can define the settings directly on the device under **Menu | Settings | Advanced Settings**.

To access the settings, you need the administrative password. The password is automatically set during the installation of your customer system and applies to provisioned phones on your network. The password cannot be changed.

To display the administrative password

1 In the menu, select **General Settings | System**.

2 Click on **Provisioning**.

3 In the **Administrative device password for certified phones** field, click .

✓ The password is displayed.

or

4 Click on .

✓ The password is stored in your clip board.

4.7 DEFINING THE LOG IN SETTINGS

You can define server-wide password settings and the UPN suffix as part of the username that all users can use to log on to SwyxServer. You can use the domain name or an alias for the UPN suffix.

These settings are fixed for SwyxON and cannot be changed.

Two-factor authentication is deactivated by default, except in SwyxON. For SwyxON the option cannot be deactivated.

Logins to end devices and SIP registrations as well as authentication via Windows user accounts are not affected by these password settings.

Force complex user passwords

In SwyxON the guideline for complex passwords is forced by default and cannot be removed by any administrator.

This server setting can be changed for individual users, see **Authentication with user name and password**, Seite 84:

When this policy is enabled, passwords must 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: full-stops, commas, brackets, blanks, hash tags (#), question marks (?), percent signs (%), ampersands (&).

Alphabetic characters (such as: ß, ü, ä, ẽ, ô) and non-Latin characters (such as: Ω, π, μ) are not special characters and are regarded as letters.

If the **Force complex user password and password history** option is enabled, the user's last three passwords will be taken into account during the change. The user cannot reuse the last three passwords.

If the **Force complex user password and password history** option is enabled in the server configuration and/or in the user configuration, the user can continue to use his previous password until he changes his password himself or is forced to do so by the administrator, see **Authentication with user name and password**, Seite 84

Independent of the password settings, any attempt to re-use the current password is checked by the system and not permitted.

To define the login settings

1 In the menu, select **General Settings | System**.

2 Click on **Login**.

Designation	Explanation
Force complex user passwords and password history	Activate the checkbox if you want users to use a complex password. The user's last three passwords are taken into account and cannot be reused. Existing user accounts are not affected by this policy until a user changes their password themselves or the administrator forces a password change.
Two-factor authentication	Activate the checkbox so that administrators must authenticate themselves via PIN to Swyx Control Center in addition to the user name and password, see also **2 Logging in and logging out**, Seite 8.
Deactivate user after max. number of failed logins	Select this checkbox if you want the system to lock user accounts after a specified number of failed logins, such as entering the password incorrectly more than once. The appropriate users will be deactivated and will not be able to use terminal devices or clients. System administrators are not locked.
Maximum number of failed logins	Enter after how many failed logins a user account will be locked. The number of failed login attempts will be reset for the appropriate 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 in attempts is irrelevant, when the Administrator has established a forced password change, and the User attempts to log in with his/her previous password.

Designation	Explanation
Domain (not in SwyxON and SDC)	Enter the SwyxServer domain. This serves as the UPN suffix for the username used to log in to SwyxWare Administration and clients. For logging in to SwyxIt! currently only the display name can be used. In addition, the domain name is used for registration with Swyx Cloud services, see **4.5 Connection to Cloud Services**, Seite 19.
SCC URL	Enter the address where the Swyx Control Center should be reachable for users. The SCC URL is used as a base to generate password reset URLs for welcome emails and password reset emails. *E.g. https://swyxware-admin.local:9443/swyx-controlcenter/* If you use a local DNS record or a private IP address, the link will work only as long as the user is logged into your local network. See also **Reset user passwords (password reset service)**, Seite 85. In SwyxON this setting is set automatically and cannot be changed.

If two-factor authentication is activated for a user, their password can only be changed by the administrator.

Other requirements for sending password reset URLs are the following settings of the SwyxServer and the SwyxWare user:
1st Configured email server, see **4.8 Defining an email server**, Seite 23
2. Configured email address of the user, see **9.3 Creating Users**, Seite 86

To allow users secure access to Swyx Control Center via the Internet, the SCC URL must be reachable via the public IP address of your network and protected by a TLS certificate, see help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/SCST

3 Click on **Save**.

4.8 DEFINING AN EMAIL SERVER

All welcome and password reset emails are delivered to the SwyxWare users via the email server you specify.

To define the settings for the email server

1 In the menu, select **General Settings | System**.
2 Click on **Mail Server**.

Designation	Explanation
Activate SMTP	Activate the checkbox to activate the SMTP settings.
SMTP mail server	Enter the unique address of the email server you are using. Allowed format: Symbolic name, DNS name, IP address
SMTP port	Enter the SMTP port for connecting the mail server.

Designation	Explanation
Sender address	Enter the email sender address for all voicemails, welcome and password reset emails delivered via SwyxServer to SwyxWare users (e.g. SwyxServer@company.com). The address must be chosen in correlation to the email server used. Some email servers support any choice of originating address, others require that the address be in the same format as the address which as already been stored for you. In any case, the domain name (e. g. "@company.com") should be identical to one of the domains managed by the mail server.
Enable SMTP authentication	Activate the checkbox to activate authentication on the e-mail server according to the RFC 2554 specification. Supported methods: "LOGIN", "PLAIN", "CRAM-MD5"
User name	Enter a Username for authentication of SwyxServer on the email server.
Password Authentication	Enter a password for authentication of SwyxServer on the email server.
Use SSL	Activate the checkbox to encrypt the connection to the email server.

3 Click on **Send test email** to send a test email via the specified mail server to the specified originating address.

4 Click on **Save**.

4.9 SETTING TECHNICAL CONTACT

You can store the contact details for a person who should be available to assist SwyxWare users with technical questions.

When the SwyxWare installation is updated, the corresponding e-mail notification is sent to the technical contact.

On the tab **Partner Information** you can view the contact information of the partner. You can contact your partner for licensing-related questions.

To set the technical contact

1 In the menu, select **General Settings | Technical contact**.

Label	Explanation
Select technical contact based on an existing user Activate this option if you want to set a configured user as the contact person.	
Users	Select a desired user, e.g. an SwyxWare administrator.
Create technical contact Activate this option if you want to enter the contact data yourself.	
Name	Enter a display name for the contact person.
E-mail	Enter the e-mail of the contact person.
Internal number	Enter the internal phone number of the contact person.
Public number	Enter the Public number of the contact person.

2 Click on **Save**.
✓ The configured contact details are used for technical support.

4.10 REMOTECONNECTOR FOR SWYXIT! DEFINE SETTINGS

The RemoteConnector for SwyxIt! You can define settings in the Swyx Connectivity Setup Tool from v. 13.20, see help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/SCST

You can display these settings.

See also **9.22 View Swyx Mobile configuration**, Seite 108.

To display the RemoteConnector settings

1 In the menu, select **General Settings | System**.

2 Click on **RemoteConnector**.

Designation	Explanation
Activate remote access	Indicates whether connections to clients via the Internet are allowed.
Authentication server	Public server address (FQDN or public IP address) for accessing the authentication service. This address must be configured within the respective settings on the Client computers. See also help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/mobile_clients_$.
Authentication port	If you use a port other than the default 9101, this port must be explicitly entered in the client settings.
Remote Connector server	Public server address of the Remote Connector server. See also https://help.swyx.com/cpe/13.30/CRM/Swyx/en-US/index.html##context/help/internet_connection_remotecontroler_$.
Remote Connector port	The port of the RemoteConnector server. The default port is 16203.

3 Click on **Save**.

To display the Swyx Mobile configuration for all Users

1 In the menu, select **General Settings | System**.

2 Click on **RemoteConnector**.

3 Click on or .

Designation	Explanation
Internal server	SwyxServer address
External server	RemoteConnector address
Server type	Determined automatically by the installation
Connection mode	**Auto (default)** The available network is automatically set **Standard** Internet
Connection type	**Business (default)** Data transmission via VoIP **Private** Data transmission via mobile network **Request** You are asked before each telephone call which connection type is to be used.
Remote Connector mode	**Auto** An automatic attempt will be made to establish a direct connection to SwyxServer. If the connection fails, e.g. because you are outside your company network, you are connected to SwyxServer via Remote Connector. **Always** The connection to SwyxServer is always made via RemoteConnector for SwyxIt! If no connection via RemoteConnector is possible, no attempt will be made to establish a connection via your company network.

Select **Users** from the menu, select the appropriate User and click on **Client Settings** and **RemoteConnector** to view the Swyx Mobile configuration for a selected User.

4.11 SYNCHRONIZING INTERSITE CONNECTIONS

By setting up a SwyxLink it is possible to implement a connection between two or more SwyxServers. By configuring this link, status information (available, away etc.), collaboration, video and instant messaging capabilities are available across servers. Similarly, the users of one site will be displayed in the Global Phonebook of the other site, and vice versa. See also help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/intersite_presence_$. In Swyx Control Center you can synchronize intersite connections or delete existing intersite connections.

To synchronize intersite connections

1 In the menu, select **General Settings | System | Intersite Connections**.

2 Click on **Start sync**.
✓ All listed SwyxWare sites are synchronized with each other.

3 In the line of the appropriate SwyxWare site, click on 🗑 to delete the intersite connection.
✓ The intersite connection is deleted. The site is no longer part of the synchronization process.

4.12 EDIT FILES

During the SwyxWare installation, global files are created for all users. These files include, for example, all ringtones, music on hold, announcements and scripts, as well as a customizable template for welcome emails, etc. These user-specific files can be edited by the administrator. User-specific files can also be edited for individual users, see **9.18 Editing user-specific files**, Seite 104

The files are displayed according to their assignment on the following tabs:

- Users
  User files are assigned to a single user. Only the user himself, an administrator or SwyxServer, if he e.g. executes scripts of the Call Routing Manager, has access to these files. All files created with a SwyxIt! or 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.
- User Standard
  User default files are stored as default files in the database for a specific user (e.g. central office) during installation. This user can use these files unchanged.
- Global
  Global files (such as skins or Call Routing Manager rules) can be used by any user.
  For example, the global files allow the administrator to create templates for all SwyxWare users. A company-wide uniform skin can be stored here, which the users can further customize according to their wishes, or a call routing script, which the users personalize with their personal announcement and number.
  Global files with the same name as a system file are preferred, you should save a new global greeting with the name "Standardansage.wav" like the supplied system standard file of the same name.
- System standard
  System default files are stored in the database during the SwyxWare installation and are renewed if necessary during an update.

If a user standard or global file is modified by the user, the modified file is displayed under **Users** and will not be changed by a later SwyxWare update. Global files always remain unchanged during a SwyxWare update.

You can add, delete or save files under a different name. The total size of all files created for this user (except fax files) is specified.

- Trunk recording

Conversations on Trunks can be recorded, see **14.2 Trunk Recording**, Seite 150

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

Deleting or downloading trunk recordings is being logged, see **Log** under the list of trunk recordings.

Not all personal data can be automatically deleted from the database. In order to meet the valid data protection regulations, it may be necessary to delete the corresponding entries manually.

To manage the files

1 In the menu, select **General Settings | Files**.

2 Select the desired tab **User** or **User default** etc.
✓ The list of files appears.

3 Select the checkbox in the line of the file you want to select, then click one of the following buttons:

Designation	Explanation
	Click on the button to download the file.
	Click on the button to delete the file. You can select multiple files to be deleted.
	Click the button to edit the file properties, see **To add a file**, Seite 27.
	Click on the button to display more detailed information about the file (size, date of last modification).
Delete multiple files	Select the desired files and click the button to delete these files.

To add a file

1 In the menu, select **General Settings | Files**.

2 Select the desired tab **User** or **User default** etc.
✓ The list of files appears.

3 Select the checkbox in the line of the file you want to select, then click one of the following buttons:

4 Select the desired tab **User** or **User default** etc.
✓ A list appears with all user specific files.

5 Click on **Upload file**.
✓ The configuration wizard **Upload file** appears.

Designation	Explanation
...	Click the button to upload a file from your hard disk.
Name	Specify the name under which the selected file should be stored in the database.
Scope	**Users** This file should be assigned directly to the user. It is only available to the selected user. **User Standard** This file is available to all users who are logged on to this SwyxServer.

Designation	Explanation
Category	Specify the category to which this file belongs. The following categories are available: • Ringtones • Fax cover page graphics • Fax cover page • Fax Letterhead • Call Routing Scripts • Example Call Routing Scripts • Bitmaps • User pictures • Templates • Announcements • System announcements • Example announcements • Music on hold • Recordings • Skins • Other
Users	From the drop-down list, select a user to whom the file should be assigned.
Description	Enter a description, if applicable.
File Properties	**Private** This file is only accessible to the user himself, e.g. in one of his scripts. *Example: Call routing script with password.* Hidden This file does not appear in the selection dropdown lists. *Example: The file '20m.wav' (twenty minutes) belongs to the time greeting and does not appear when you select a greeting message.* **System** This file was created during installation and is always read-only (this option cannot be changed)

6 Click on **Save**.
✓ The new file appears in the **User** or **User default** list.

4.12.1 ACCESS VISUALGROUPS AND VISUALCONTACTS ON A SEPARATE SERVER VIA REMOTECONNECTOR

You have Swyx VisualGroups or Swyx VisualContacts **not** installed on the 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: service.swyx.net/hc/en-gb/articles/360017729619.
- For SwyxWare versions 13.30 and higher, the configuration is done via a configuration file. This is described below for Swyx Control Center.

How to add a RemoteConnector access via configuration file via Swyx Control Center

1 In the menu, select **General Settings | Files**.
2 Select the **System default** tab.
3 Search for the **CPE_ippbx_cpe.rcconfig** file under the **RemoteConnectorConfigFile** category.

If necessary, display more elements per page and search for the entry with ctrl+f.

4 Download the file, see **To manage the files**, Seite 27.
5 Open the file (with Notepad++) and navigate to the VisualContacts or VisualGroups area.
6 In the desired area, enter the required destination address in the line **DestinationSocket(...)** for **0.0.0.0**.

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>
```

7 Save the file.

8 Upload the edited file to the Swyx Control Center using the **Upload file** button, see **To add a file**, Seite 27.

9 Confirm with **Save**.
✓ The new configuration file is uploaded and used. You can find them under the **Global** tab.

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.

4.13 SETTING MUSIC ON HOLD

You can upload a file that contains on-hold music or an announcement that plays while calls are on hold.

The music on hold delivered with SwyxWare was composed and made available by "corporatemusic". For more information on professional music and speech solutions, visit www.corporate-music.de and www.gema.de

To set the music on hold

1 In the menu, select **General Settings | System**.

2 Click on **Music on hold**.

Designation	Explanation
File with music on hold	All announcement files saved in the database appear in the drop-down list, see also help.enreach.com/cpe/13.30/Administration/Swyx/en-EN/#context/help/tab_files_$. The files have the audio format "16 kHz 16 Bit PCM mono".
	Click the button to search for files in any wav format on the network. After selecting a WAV file, it is converted to the above format and stored in the database. The Windows functions used in this conversion process may degrade the audio quality. In this case, use a professional conversion program instead of Windows conversion to create WAV files in the above format.
	Click on the button to delete the selected announcement. You can only delete files you have created yourself.
	Click on the button to test play the currently selected greeting.
	Click the button to adjust the volume for test playback.
	Click on the button to download the currently selected file.

Designation	Explanation
Codec used for Recordings	Audio attachments are sent as wav files (Microsoft Wave Audio GSM) by default. As an alternative, additional built-in or custom compressions can be used to reduce the size of attachments. The compression to be used can be set for all Users, or individually for each User. **Microsoft wav Audio G711** wav file, G.711 compressed **Microsoft wav Audio GSM** WAV file, GSM compressed (Default setting after installation) **Microsoft wav Audio PCM** Standard WAV file, uncompressed

4.14 INTERSITE CONNECTIONS

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 start a manual synchronization of the connected SwyxServer via **Start synchronization**. 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.

4.15 DISTRIBUTING SOFTWARE TO CLIENTS OR DEVICES

You can distribute more recent clients or firmware versions. Version control is performed via Swyx version server.

If a more recent version is available, you have the following options to release the version data from the Swyx version server for distribution to the registered users or endpoints on your network:

- Manually: Check if a more recent version is available on the Swyx versions server and confirm the distribution
- Automatically: As soon as a more recent version is on the Swyx versions server let it be distributed without further confirmation (Auto sync)

To release a version manually

1 In the menu, select **General Settings | Versions**.

2 Select the desired tab:

Designation	Explanation
Enreach GmbH	SwyxIt! Clients
Deutsche Telekom AG	NetPhone Clients
Yealink AG	Firmware for Certified SIP phones
Ascom AG	Firmware for DECT 800 systems

✓ A list appears with all logged on Desk Phones.

Designation	Explanation
Manufacturer	Software vendor
Variant	Name of the software
Recommended	Version of the software available on the Swyx version server (FIS) and recommended by the service provider
Currently distributed	Version available on your SwyxServer or NetPhone server and currently distributed in the local network
Distribution	✓ = the distribution of the software is activated

3 In the line of the corresponding software, click on to download a more recent software version to the database.
✓ The URL available on the server is copied over which the version can be distributed.

4 Click to make the software available on your network, or

Click to stop the share, or

Click to review and edit the update information if necessary, see **To edit the update information**, Seite 30.

If you want to change the URL of the local version, e.g. to provide the software via local FTP server, make sure that the entered local version matches the version of the software package.

To release versions automatically

1 In the menu, select **General Settings | Versions**.

2 Select the desired tab
✓ The list of available versions appears.

3 Click to release the version for automatic distribution.

No further steps are necessary on your part.

To edit the update information

1 In the menu, select **General Settings | Versions**.

2 Select the desired tab
✓ The list of available versions appears.

3 Click in the row of the corresponding version.
✓ The dialog window **Update version** opens.

Designation	Explanation
VendorID	Firmware vendor
DeviceTypeID	Terminal device model
Variant	Name of the firmware
Recommended	Software version available on the Swyx versions server.
Accept	Click the button to accept this version for eventual distribution.
Empholene (URL)	The address of the server version
Currently distributed	Version available on your SwyxServer or NetPhone Server
Currently distributed (URL)	The address of the local version
Distribute version	Activate the check box to make the version available to clients/end devices. (Only possible if the version has been accepted for distribution)
Auto-Sync	Activate the check box to release the version for automatic distribution. (Only possible if the version has been accepted for distribution)
Reset	Click the button if you want to revert to the old version that was available at the time of SwyxWare installation. (Only possible if **Distribute version** is enabled.)

4 Click on **Save**.

4.15.1 DISTRIBUTING FIRMWARE TO DEVICES

When providing end devices, the current firmware is transferred. If a newer firmware is available you can distribute it to the corresponding devices.

To update the firmware

1 In the menu, select **General Settings | Versions**.

2 Click on the tab with the appropriate manufacturer name.

3 In the line of the corresponding firmware, click on to download a more recent firmware version to the database.
✓ The URL available on the server is copied over which the version can be distributed.

4 Click on ✓ to distribute the firmware in your network.

If you click on in the second step, will be released for automatic distribution. No further steps are necessary on your part.

Click on to deactivate automatic distribution.

Click on to check the firmware URL, edit it if necessary and click on **Save** after that.

4.16 DEFINING CLIENT SETTINGS FOR ALL USERS

You can define settings that apply server-wide to all SwyxWare telephony clients.

To define settings for SwyxIt!

1 Select in the menu **General Settings | Client Settings | SwyxIt! Settings**.

Designation	Explanation
Standard SwyxIt! Skin file for MS Teams	Select a skin that will be used server-wide as default skin for SwyxIt! Connector for Microsoft Teams is to be used.
Standard skin (SwyxIt!)	Select a skin to be used server-wide as the default skin for SwyxIt. The setting is adopted by all users who have defined the "Default Skin" in the User configuration.
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). You can use placeholders: **Environment variable %APPDATA%** %APPDATA% is defined on the client computer and denotes the directory of this user's application data. *e. g. %APPDATA%\Recordings* **SwyxWare User name [username]** The dummy [username] is replaced by SwyxIt! with the current SwyxWare- user name. The recordings can thus be stored in a directory within the domain *e. g. \\fileserver\callrecordings\[username]* By default, the path is: *%APPDATA%\Swyx\Recording* This stores all recordings locally under the application data of the user account under which SwyxIt! 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. For customizing a different directory, see **9.17.3 Activating conversation recordings**, Seite 104.

The Windows user account under which SwyxIt! was started is used to save SwyxIt! recordings.

SwyxPhone users can only listen to recordings if they log on to SwyxServer with SwyxIt!, see also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/#context/help/login_$.

2 Click on **Save**.

To define SIP client settings

1 In the menu, select **General Settings | Client Settings**.

2 Click on **SIP client settings**.

Designation	Explanation
Standard log-in mode for SIP devices	Select whether or not a SIP terminal device must be authenticated when logging in.
Standard log-in mode for SIP devices	Define the standard realm (FQDN or IP address) for all users at this SwyxServer.
STUN server	Enter the STUN server to be used by the SIP devices.
STUN-Port	Enter the associated port for the STUN server (standard value: 3478).

3 Click on **Save**.

4.17 ACCESSING SWYXWARE ADMINISTRATION

Some of the settings for UC Tenants or SwyxServer are only available via SwyxWare Administration. The following is required for remote administration:

- Installation of SwyxWare Administration on the computer from which access is to be made
- Installation of the remote access tool Remote Admin Connector on the computer from which access is to be made.
- Authentication token (SwyxON) or SwyxWare login data
- IP address and port or the UC Tenant's or SwyxServer's FQDN

Remote Admin Connector must be installed before the installation of the SwyxWare Administration. If there is already a SwyxWare Administration installation on your system, you must uninstall the program and reinstall it after the installation of Remote Admin Connector.

To install Remote Admin Connector

Remote Admin Connector is included in the SwyxWare installation package, however it must be installed via command line parameters.

1 Navigate to the folder where the installation package is saved.

2 Execute the following command in the command line:

```
msiexec /i Admin64.msi RemoteAdminConnector=1
```

✓ The SwyxWare setup appears.

3 Select **Remote Admin Connector** from the list, click on **Next >** and confirm your input.

You can uninstall Remote Admin Connector via the Windows Control Panel.

To log in to Remote Admin Connector

1 Open **Remote Admin Connector**.
✓ A window appears and displays the current connection status.

2 Click on **Select UC Tenant**.
✓ "Remote Admin Connector" appears, if applicable, with the UC Tenants list for which you last defined the settings via SwyxWare Administration.

3 Select an UC Tenant from the list, click on **Connect** and enter the appropriate authentication token
or
click on **Add Tenant Address** and enter the UC Tenant's or SwyxServer's IP address and port or FQDN for which you wish to determine settings in the SwyxWare Administration.

You can find the IP address and port as well as the authentication token in the SwyxON Portal under the appropriate UC Tenant | General settings | UC administration.

✓ A window appears and displays the current connection status.

4 Start SwyxWare Administration.

5 Select from the SwyxWare Administration **RemoteComputer** and enter 127.0.0.1 in the field as the target address.
✓ The SwyxWare Administration login dialog appears.

6 Select **Login with authentication token** and enter the authentication token in the corresponding field
or
click on **User Name Authentication** and, if applicable, enter the PIN that appears in the two-factor authentication app on your smartphone in the corresponding field.

User Name Authentication is only available if you have SwyxWare credentials and if you have set up two-factor authentication, see also **2 Logging in and logging out**, Seite 8.

✓ The appropriate SwyxWare Administration appears.

7 Click in the **Remote Admin Connector** status window, if applicable, on **Select UC Tenant** to select a different UC Tenant.

8 In the **Remote Admin Connector** status window, click if applicable, on **Download trace files** to download SwyxWare trace files.
or
click **Download trunk recordings** to download the recorded calls, see **4.17.1 Downloading trunk recordings**, Seite 33

9 Select the appropriate checkbox to select a component for which you want to download traces.

If necessary, click the plus sign to show subcomponents.

4.17.1 DOWNLOADING TRUNK RECORDINGS

1 Follow steps 1 to 7 at **To log in to Remote Admin Connector**, Seite 33.

2 Click **Download Trunk Recordings**.

3 Select the file directory where the trunk recordings are to be saved.

4 Select a trunk and set a time restriction if necessary. Then click **Search** to display the desired recordings.

5 Select the recordings you want to download and click **OK**.
✓ The recordings are saved in the previously selected directory.

Only the recordings that are displayed in the list can be marked are downloaded. To download more recordings, scroll to the next page and highlight the next entries you want to download.

4.18 DEFINING CODEC FILTERS

You can define codec filters server-wide for all users and edit them in the user settings of each User.

Via codec filter you define the allowed codecs for calls. Codecs define how much voice data is compressed, i.e. how high the voice quality is for calls. In addition, you can filter out the T.38 protocol when establishing a fax connection in the user settings to ensure compatibility with IP adapters that do not support certain variants of the protocol.

Incoming calls with non-permitted codecs are rejected and an error message appears.

If you do not allow a codec, no phone calls are possible.

For new SwyxWare installations and updates, the codec filter is deactivated by default, i.e. all codecs are allowed.

To define a codec filter for all Users

1 In the menu, select **General Settings | System**.

2 Click on **Default codec filter**.

Designation	Explanation
Use server default	Only available in the user settings: Select the checkbox if you want the default codec filter defined under **General Settings** to be applied for the selected User.
Allow the following codecs	Activate the checkbox to select individual codecs that are allowed to be used. If the checkbox is deactivated, all codecs are automatically allowed. If you activate the checkbox and do not select a codec, no phone calls are possible.
G.722 (around 84 kbit/s per call)	Activate the checkbox to allow this codec. Speech, high bandwidth. If possible, the voice data is transferred in HD audio quality.
G.711a (around 84 kbit/s per call)	Activate the checkbox to allow this codec. Voice, high bandwidth. The voice data is hardly compressed.
G.711µ (around 84 kbit/s per call)	Activate the checkbox to allow this codec. Voice, high bandwidth. The voice data is hardly compressed.
G.729 (around 24 kbit/s per call)	Activate the checkbox to allow this codec. Speech, low bandwidth. The voice data is optimally compressed.
Fax over IP (T.38, around 20 kbit/s per call)	Activate the checkbox to allow this protocol. Fax - the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration.
Action on fax receipt	Only available in the user settings: When a fax connection is established, the T.38 protocol is negotiated between the devices involved. Certain variants of this negotiation may not be supported by some IP adapters. Use the following fax/T.38 options to establish compatibility with such devices.
Remove T.38 codec from initial invite	Activate the checkbox to activate this option. T.38 is removed from the first 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	Activate the checkbox to activate this option. • The receiving fax machine switches to T.38 after detecting the fax tone (CED tone, 2100Hz). Alternatively, switching to T.38 can be done by the signal of the sending fax machine. Some IP adapters do not support switching by the sender. If this option is activated, 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.

4.19 FEDERATED AUTHENTICATION VIA IDENTITY PROVIDER

The user of a client has to authenticate himself when logging on to SwyxServer, see **9.2 Authentication for clients**, Seite 84

If your company uses Identity Provider services, you can configure federated authentication (OAuth 2.0 and OpenID Connect) for SwyxServer and enable it for the desired users.

As of SwyxWare version 3.15 only the following identity providers are supported: Auth0 and Microsoft Azure (as a beta test).

Identity Provider	URL to the user documentation
Auth0	https://auth0.com/docs

Identity Provider	URL to the user documentation
Microsoft Azure	https://docs.microsoft.com/azure/active-directory/hybrid/whatis-fed

Requirements:

- You must have an account with an identity provider that you can manage yourself.
- The SwyxWare application must be configured in your identity provider account.
- You need to enable the "google-oauth2" protocol in the account settings.
- All SwyxWare users which should use federated authentication must be configured in the user directory at your identity provider and mapped to SwyxWare application.
- The user names (UPN) at the identity provider must correspond to the email addresses of the SwyxWare users.

Configuration in the local network:

Clients must have direct access to the identity provider service.
Make sure that port 443 is open to the outside.

Configuration in Swyx Control Center:

- You need to create an identity provider configuration in Swyx Control Center, see **4.19.1 Create identity provider configuration**, Seite 36
- For all desired SwyxWare users federated authentication has to be allowed (via the option **Allow federated authentication**), see **To edit the authentication settings for a User**, Seite 89

Configuration in SwyxIt!

- For **Auth0** option must be enabled during the SwyxIt! installation **Auth0 authentication** option must be enabled.

4.19.1 CREATE IDENTITY PROVIDER CONFIGURATION

You can preconfigure different supported identity providers.

To use one of the configured identity providers, you must enable the corresponding configuration.

If you enable an identity provider configuration, SwyxServer will offer federated authentication for selection instead of authentication via the Windows user account.
Disable all identity provider configurations to reuse Windows authentication.

To create an identity provider configuration

1 Select in the menu **General Settings | Federated Authentication**.

2 Click on **Create configuration**.
✓ The configuration wizard appears **Create identity provider configuration**.

Label	Explanation
Activated	Select the check box if the identity provider from this configuration should be used for federated authentication.
Name	Name the configuration with a unique name. The name of the configuration is displayed to the user in the client login dialog box.
Identity Provider	Choose an identity provider. Only identity providers for which no configuration has been created yet are available.

Label	Explanation
Application ID, Domain ID	Enter the application ID and domain ID. You can find this data in your identity provider account: • For Auth0 you find the data under **Applications | <SwyxWare App> | Settings | Basic Information | Domain, Client-ID**. • For Microsoft Azure you can find the data under **App registrations | <SwyxWare App> | Overview | Directory (tenant) ID, Application (client) ID**
Document metadata	Enter the URL to the identity provider metadata document: • For Auth0 you can find the URL at **Applications | <SwyxWare App> | Advanced Settings | Endpoints | OpenID Configuration**. • For Microsoft Azure, you can find the URL at **App registrations | <SwyxWare App> | Endpoints | OpenID Connect metada document**
User name, Password (Microsoft Azure only)	Enter the account credentials you have set for synchronization between Active Directory and SwyxWare.

3 Click on **Create**.
✓ The new configuration is created and appears in the list **Composite authentication**.

4.19.2 EDIT IDENTITY PROVIDER CONFIGURATION

You can enable/disable an identity provider configuration, delete it, and customize the configuration data.

Only one identity provider configuration can be activated. The corresponding identity provider is used for federated authentication.

To edit identity provider configurations

1 Select in the menu **General Settings | Federated Authentication**.
✓ The activated configuration is marked with ✓.

2 If necessary, click ⊘ to deactivate the configuration.

3 If necessary, click ✎ to adjust the configuration to the configuration data.

4 If necessary, click 🗑 to delete the configuration.

4.20 EXPERT SETTINGS

Under the menu item **Expert settings** you have the possibility to change some specific settings for different SwyxWare components.

"Expert settings" are only intended for experienced SwyxWare administrators and can have a serious impact on the SwyxWare configuration. Please refrain from making any changes in this area if you are unsure about the possible consequences of your settings.

In earlier SwyxWare versions these settings were defined via registry keys. During a system update to v12.30 or newer, parameters defined via registry keys are not changed and transferred to the database. All future changes must be made in the "Expert Settings". This also applies to a new installation of the software.

Which expert settings are displayed?

The expert settings are grouped on tabs in different/multiple topics. The individual tabs are visible under the following conditions:

Tab name	Display requirements
IpPbxIMAP4	Visible when SwyxServer is successfully started.
IpPbxSrv	Visible when • at least one client or device is connected, • at least one call is made.
LinkMgr	Visible when at least one SIP trunk has been registered.
PhoneMgr	Visible when • at least one device (HFA) is connected and configured, • at least one firmware update is available for one of the connected devices.

Which administrators can see and edit the expert settings?

As SwyxWare administrator you have full access to the expert settings.

The expert settings can only be edited or viewed by the following SwyxON administrators:

SwyxON Administrator profile	PlatformExpertSettingsRW	ServerExpertSettingsRW	ServiceExpertSettingsRW	ExpertSettingsRO
Advanced Platform Administrator	✓	✓	✓	✓
Platform Administrator	-	✓	✓	✓
Advanced Partner Administrator	-	✓	✓	✓
Support Administrator	-	-	-	✓
Partner Administrator	-	-	-	✓
UC Tenant Administrator	-	-	-	✓

legend: ✓ = allowed for this administration profile

To set the expert settings

1 Open Your user profile in the title bar on the right.

2 Select **View | Enable Expert Mode**.
✓ The Expert Mode is activated. The warning triangle icon appears in the title bar.

3 In the menu, select **General Settings | Expert Settings**.

4 Select the appropriate tab and define the required settings.

You can define following settings:

In the fields with Boolean values ("True" or "False"), "0" means the option is disabled. "1" means the option is active.

Tab	Designation	Explanation
IpPbxSMTP	SecurityLevel	Degree of mail server certificate verification: 0 = none - not secure 4 = check exhibitor - almost secure 5 = check exhibitor, check hostname - secure • Default value = 5
IpPbxSMTP	ConnectTimeout	Maximum time to connect to the e-mail server, For TLS connections, including the time for the STARTTLS phase. • Default value = 15 seconds
	MailSendTimeout	Maximum transaction time for sending an e-mail to the email server in seconds • Default value = 300 seconds (5 min.)
	MinutesBeforeMailWarning	Time in minutes after which a warning message is sent if the attempt to send an email fails repeatedly. • Default value = 2880 minutes (2 days)
	HoursBeforeMailGiveup	Time in hours after which a repeated attempt to send an e-mail is aborted. • Default value = 120 hours (5 days)
IpPbxSMTP	MailMaxLinesToCite	Number of text lines to be quoted in a warning message from the failed email. • Default value = 15 lines
IpPbxSMTP	MaxBase64LineLength	Maximum length of a Base64-encoded line (for binary attachments) • Default value = 898 characters
	MinutesBetweenMailRetrys	Time in minutes after which an email send attempt should be repeated if the previous attempt failed. • Default value = 30 minutes
	CreateNewSessionForEachMail	Establish a new connection to the email server for each email to be sent: 0 -false | 1 -true • Default value = 0 - false

Tab	Designation	Explanation
	TimeBetweenMailTransactions	Time interval in seconds between email transmissions (can lead to a denial by the email server if the time interval is too short) • Default value = 5 seconds
IpPbxSrv	CallNotificationOn2ndCallDisabled	Specify whether the call notification should still be displayed on the second line if the second call is deactivated. • Default value = 1 (call notification is NOT displayed)
IpPbxSrv	CDRForAuxiliaryCallsDisabled	Specify whether CDR entries should also be written for CTI+ auxiliary calls (calls from/to the CTI+ controlled terminal). • Default value is 0 (CDRs for additional calls are NOT written).
	EnableTrunkCallEarlyMedia	Specify whether to use the media bridging functionality. • Default value = 1 (media bridge is used.)
	ExclusiveMediaFileEP	Specify whether to use the Media Manager exclusive mode for playfile endpoints. This mode should be activated if the waiting announcement is always to be played from the beginning in calls on hold. • Default value = 1 (Exclusive mode is enabled).
	PhoneCallListEntryCallForIsFirstRedirector	Specify whether the call display in the client should also include the original call destination before forwarding. • Default value = 1 (The original call destination is NOT displayed).
	RFC2833DTMFPayloadType	Set the RTP payload type for marking DTMF signals according to RFC2833. • Default value = 101 (DTMF)
	SkipGroupCallMembersWithActiveAway	Specify whether group members with the status "Away" are to be disregarded during a group call. • Default value = 0 (group members with "Away" receive the calls).

Tab	Designation	Explanation
	SkipGroupCall-MembersWit-hActiveDoNotDis turb	Specify whether group members with the status "Do not disturb" are to be disregarded during a group call. • Default value = 0 (group members with "Do not disturb" receive the calls).
IpPbxSrv	**SuppressInter-nalNumbers**	Specify whether the display of the call number should be suppressed for an internal call if the user has activated the "Hide number" function. • Default value = 0 (The number for internal calls is always displayed).
	SuppressNames	Specify whether the contact name display should be suppressed for an internal call. • Default value = 0 (The contact name is displayed for internal calls)
	TrunkCallRetry-OnBusyOrReject	Specify whether call repetition should also be performed for a call over the trunk that was disconnected by "Busy" or "Reject". • Default value = 0 (no call repetition)
	TrunkCallRetry-OnTonesAvaila-ble	Specify whether to suspend call repetition when a 183 session progress is received with SDP for this line. When stopped, the caller hears "early" tones (alert, etc.) generated by the attendant. • Default value = 0 (call repetition is NOT interrupted).
	TrunkRecording-ForAuxiliary-CallsDisabled	Specify whether to record trunk recordings for auxiliary calls (calls to/from the CTI+ controlled terminal). • Default value = 1 (recordings are recorded)
	WritePhoneCall-ListEntryOnG-roupCall	Specify whether group calls are registered in the call journal. • Default value = 1 (group calls are registered).

Tab	Designation	Explanation
	PlayRecording-NotificationS-ound	Set whether to enable (1) or disable (0) the notification tones at the beginning and end of a trunk recording. Default value = 1 (activated).
LinkMgr	**StunRefresh**	Set the refresh time in milliseconds for the STUN connection. • Default value = 10000 (corresponds to 10 seconds).
	SIPNetworkPro-videdNumber	Set a fixed trunk-specific NPN (netowrk provided number) here, which overwrites the number transmitted by the server if necessary.
	ForwardAOC-Messages	Specify whether AOC (Advice of Charge) messages are to be transmitted via trunk. • Default value =1 (AOC messages are transmitted).
	AddExchange-HistoryInfo	Specify whether to add the "SIP History-Info" header field to the INVITEs for MS Exchange support on the trunk. • Default value = 0 (no "SIP History-Info" fields)
PhoneMgr	**AutoFirmwa-reUpdate**	Set whether the firmware update is performed by all phones without prompting. • Default value = 0 (The prompt appears).
MsTeamsPresence-Sync	See **4.21 Synchronize user status with Microsoft Teams**, Seite 40.	
Tele-metry	This page displays information about the current state of the SwyxServer. You cannot make any settings.	

4.21 SYNCHRONIZE USER STATUS WITH MICROSOFT TEAMS

The presence status as well as some activities of a SwyxWare user can be displayed to other participants registered at the same SwyxServer. You can define this option for the user, see **9.8 Defining call and status signaling**, Seite 91

If a SwyxWare user also has a Microsoft Teams account, his/her Microsoft Teams status can be forwarded to SwyxServer and synchronized with the SwyxWare status information.

The system recognizes which Microsoft Teams user is assigned to the SwyxWare user based on the matching email addresses. Make sure that the e-mail address entered in the user configuration matches the account name (name.surname@company.com) of the corresponding MS Teams user account, see **9.3 Creating Users**, Seite 86.

- Learn more about Microsoft Teams user statuses: https://docs.microsoft.com/en-us/microsoftteams/presence-admins#presence-states-in-teams
- Further information about the SwyxWare user status: help.enreach.com/cpe/latest.version/Client/Swyx/en-US/#context/help/status_signalling$

The data from Microsoft Teams to SwyxWare is transmitted encrypted in the network traffic.

This function is not supported in the standby scenario.

SwyxWare Synchronize status "Speaking" with MS Teams

From SwyxWare version 13.25 you can activate an additional option.

Any SwyxWare user who is on a call with a device or a client app on the SwyxServer will receive the status "Speaking". This status will be forwarded to Microsoft Teams and the status of the MS Teams user will change to "In a call" accordingly.

The MS Teams "In a call" status, which is triggered by the SwyxWare "Speaking" status, has no effect on the Microsoft Teams "Busy-on-Busy" call policy.
This is a confirmed bug of MS teams, see https://feedbackportal.microsoft.com/feedback/idea/31f4ed87-5253-ec11-a819-000d3a7bc845 and https://techcommunity.microsoft.com/t5/teams-developer/ms-graph-setpresence-problems/m-p/2798805/highlight/true#M3957
While speaking via SwyxServer, incoming calls via MS Teams can still be signaled to users and are not rejected with a busy signal.

Changing status in Microsoft Teams can take up to three seconds.

Additional configuration

The additional configuration steps **in Azure AD** are:

- Presence.ReadWrite.All, User.Read.All, User.ReadBasic.All - add permissions,
- create a secret client key (Client secret)

see *Registration on your Microsoft Teams tenant*

The additional configuration steps **in Swyx Control Center** are:

- enter secret client key in **MsTeamsClientSecret** field,
- enter the value "2" in the **MsTeamsStatusSyncMode** field

see also *Configuration in Swyx Control Center*, step **(4)**.

Requirements

4.21.1 REQUIREMENTS

Before configuration in Swyx Control Center the following requirements must be met:

Installation on SwyxServer

The function "MS Teams User Status" must have been activated during the SwyxServer installation. As a result the corresponding SwyxServer service "SwyxMsTeamsPresenceSync" will be installed. help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/run_setup_$

The "MS Teams User Status" feature is not installed by default during the first installation or update.

If the service has not yet been installed, run the SwyxServer installation file again: In the first step, select the **Modify** option and in the next step, activate the **MS Teams User Status** function under **Telephony**. Then run the configuration wizard again.

Installation of the Solution AddOn (Only for SwyxON)

Note that this is only valid if you have installed a SwyxWare version 12.xx.

If your SwyxWare system is installed in a SwyxON environment, an additional step has to be done via SwyxON Administration: Install the MS Teams Sync service as a Solution AddOn on your UC Tenant, see https://help.enreach.com/swyxon/1.00/Partner/Swyx/en-US/#context/help/solution_addOn_$

4.21.2 REGISTRATION ON YOUR MICROSOFT TEAMS TENANT

On your Microsoft Teams Tenant in the Azure Active Directory you have to register the "SwyxMsTeamsPresenceSync" service:

The service runs under the account of a Microsoft Teams User. We recommend that you create a special user for this purpose.

To register the "SwyxMSTeamsPresenceSync" service in Azure AD

1 Follow the initial steps of the following instruction:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

2 Specify the following settings under **App registrations | Add registration**:

Designation	Explanation
Name	Enter a name for the service registry. *e.g.:SwyxMSTeamsPresenceSync*
Supported Account Types	Select the option "Accounts in this organizational directory only (YOURDOMAIN only - Single tenant)".
Redirect URI	Select **Public client/native** from the drop-down list and enter "https://localhost/".

3 Click on **Register** to save your changes.
✓ Your registration appears in the corresponding list under **App registrations**.

4 Open the registration of the "SwyxMSTeamsPresenceSync" service.
✓ The **Application (client) ID** and the **Directory (tenant) ID** are displayed at the top.

5 Copy the above IDs to Swyx Control Center for the further configuration steps, see *To enter the Azure AD registration data under the expert settings*.

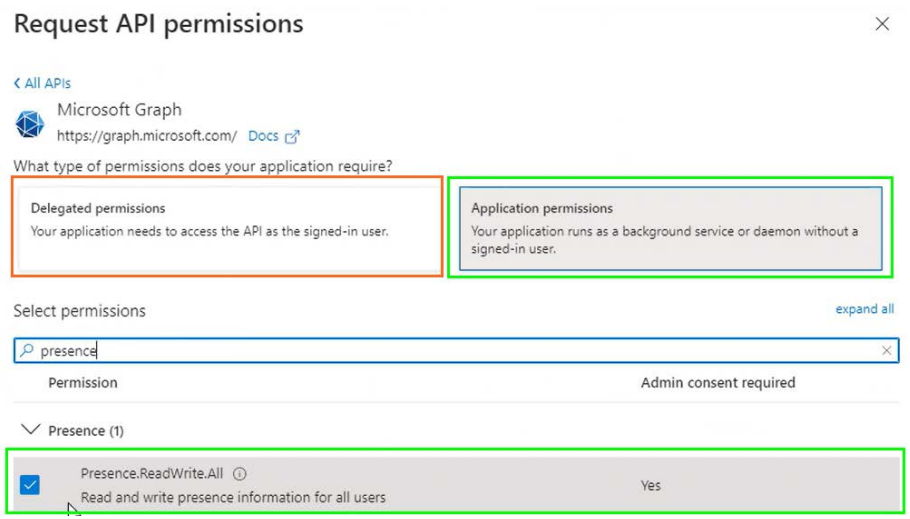
6 Select **Authentication | Advanced settings** and set **Allow public client flows** to **Yes**.

7 Add the following API permissions under **API permissions | Add permissions**, see "Adding permissions to access Microsoft Graph" under:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis#more-on-api-permissions-and-admin-consent
You must add the following permissions:

- Presence.Read (Type: Delegated)
- Presence.Read.All (Type: Delegated)
- Presence.ReadWrite (Type: Delegated)
- User.Read (Type: Delegated)
- User.Read.All (Type Delegated)
- User.ReadBasic.All (Type: Delegated)
- User.ReadWrite.All (Type: Delegated)

You may need to add the following permissions if you want the SwyxWare status "Speaking" to be forwarded to MS Teams:

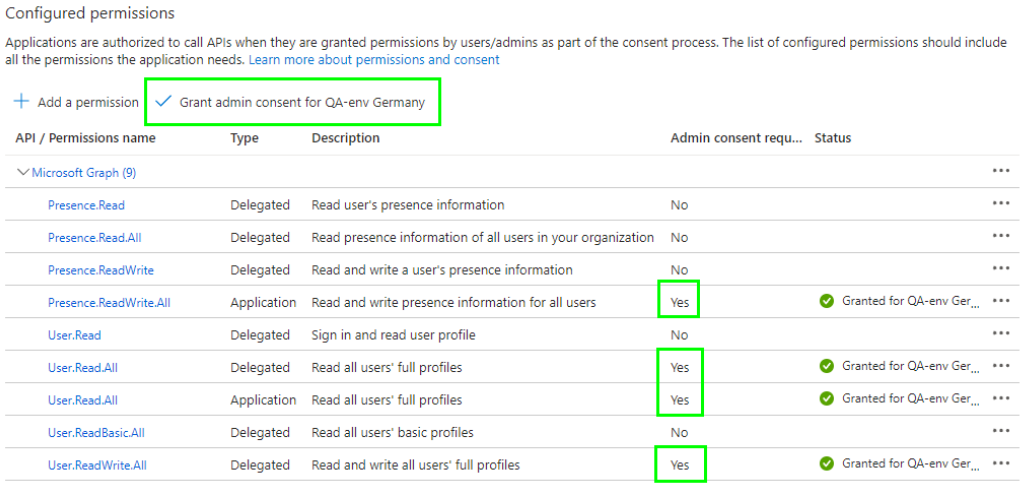
- Presence.ReadWrite.All (Type: Application)
- User.Read.All (Type: Application)



8 Assign each API permission to your registered domain, see "Application Permission for Microsoft Graph" at https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis#more-on-api-permissions-and-admin-consent

It is required that Administrator Consent is granted for each Application API permission, see "'Administrator Consent' Button" at https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis#more-on-api-permissions-and-admin-consent

✓ Each required API permission is assigned to your domain:



9 (Only for synchronization towards MS Teams:) If necessary, create a secret key under **Certificate and secrets | Client secrets**, see "To generate additional client secrets" under:
https://learn.microsoft.com/en-us/azure/marketplace/create-or-update-client-ids-and-secrets#update-the-client-secret-associated-with-your-client-id
For the validity of the client secret, we recommend selecting the maximum duration.

The value of the secret client key is subsequently hidden by "***...". Save the key (**Value** column) immediately after creating it in a protected file to enter it in Swyx Control Center afterwards.

10 Follow the next steps under *Configuration in Swyx Control Center*

4.21.3 CONFIGURATION IN SWYX CONTROL CENTER

You must enter the Azure AD registration data in the expert settings:

To enter the Azure AD registration data under the expert settings

1. Open Your user profile in the title bar on the right.
2. Select **View | Enable Expert Mode**.
   ✓ The Expert Mode is activated. The corresponding warning triangle icon appears in the title bar.
3. In the menu, select **General Settings | Expert Settings**.
4. Select the tab **MsTeamsPresenceSync** and enter the required data:

Designation	Explanation
Activated	After SwyxWare/NetPhone installation the service "MSTeamsPresenceSync" is disabled by default. Enter the value "1" in the field to enable the service. • 0 - MSTeams Presence Sync is disabled (default value) • 1 - MSTeams Presence Sync is activated
MsTeamsAppGuid	Enter the "Application (client) ID" that was generated when you registered the service, see *To register the "SwyxMSTeamsPresenceSync" service in Azure AD*, step **(4)** *e.g. 33733f45-cfce-4d1e-9d17-0xxxxx0xx000*
MsTeamsAzureAdInstanceUrl	Enter the URL of your Microsoft Teams tenant, including the "Directory (tenant) ID" generated when you registered the service, see *To register the "SwyxMSTeamsPresenceSync" service in Azure AD*, step **(4)** *e.g. https://login.microsoftonline.com/33733f45-cfce-4d1e-9d17-0xxxxx0xx000*
MsTeamsUserName	Enter the login details of your Microsoft Teams user account with the appropriate access rights.
MsTeamsPassword	
MsTeamsClientSecret	If necessary, enter the client secret key that you created in Azure AD. You need to add this permission if you want the SwyxWare status "Speaking" to be forwarded to MS Teams:
MsTeamsStatusSyncMode	After SwyxWare/NetPhone installation the mode "MSTeamsStatusSyncMode" is set to "1" by default: Only Microsoft Teams status is synchronized towards SwyxWare. Enter the value "2" in the field to additionally forward the Swyx status "Speaking" to Microsoft Teams.

5. Save Your entries.
   ✓ The new configuration is deactivated.

4.21.4 CHECKING THE FUNCTIONALITY

You can check the functionality of the application at SwyxIt!.

Microsoft Teams Status --> SwyxWare

The status of the Microsoft Teams users is transferred to SwyxWare in the following way after five seconds at the latest:

In MS teams (set by the user)	In MS teams (automatically set, based on activity)	The consequent SwyxWare status
Available	Available	Available
	Available out of office	Available
Busy	Busy	Away
	In a call	Speaking
	In a meeting	Away
	On a call, out of office	Speaking
Do not disturb	-	Do not disturb
	Presenting	Speaking
	Focussing	Do not disturb
Away	Away	Away
	Away Last Seen <time>	Away
Be right back	-	Away
Appear offline	-	Away
	Offline	No synchronization with Microsoft Teams
	Status unknown	
	Out of office	

The status text that a SwyxWare user has set in a client remains unaffected by the synchronization.

SwyxWare Status --> Microsoft Teams

The status "Speaking" is transferred to Microsoft Teams after three seconds at the latest.

If the MS Teams user has set his status manually, this status remains unchanged. The exceptions are "Available" and "Busy". Under the influence of "Speaking", these statuses change to "In a call".

5 ONLINE LICENSING

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

There are following technical ways to licence your software:

- **6 Licensing via license key**, page 52 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 **5.2 Feature Profile**, page 46 and **5.3 Additional functions**, page 49

Using activation key

You must enter the activation key, which you received from your provider, in the configuration wizard during the SwyxWare installation.

In Swyx Control Center you can enter the activation key afterwards, e.g. in case of a function extension, see **4.3 Entering a license activation key**, page 18.

License server

The validity of the licenses is constantly checked by the Swyx license server. If, for example, the connection between SwyxServer and the Swyx 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.

5.1 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.

5.2 FEATURE PROFILE

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:

Features	Feature Profile		
	Basic	Profes-sional	Premium
Telephony system and UC functional-ity (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		✓	✓
SwyxCTI+			✓
SwyxMonitor			✓
Swyx VisualContacts			✓
Swyx Connector for Skype			✓

Functions in Detail: Performance features

Name of the function	Explanation
SwyxAdHocConference	Dial-in conferences with 3 internal and/or exter-nal participants
SwyxBCR (Basic Call Routing)	Use of the Call Routing Managers. This is an additional component of SwyxIt!, which allows the user to define simple call forwarding.
SwyxECR (Extended Call Routing)	This function contains the full usage of the Graph-ical 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 Managers.
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! in CTI mode), the conver-sations can be recorded directly on the trunk connection.
SwyxFax	Use of central, server-based fax services with the Windows client. Transmission of fax messages from all applications 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.

Name of the function	Explanation
SwyxMonitor	Permanent call recording of incoming or outgoing external calls, silent connection to calls (Silent Call Intrusion).
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.

You must consider the following information when ordering feature profiles:

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.

SwyxConference

For using conferences you may have to appropriately extend the number of calls to a location.

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.

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.

STOP

When dialing an emergency number (e.g. 112), a voice channel cannot be released automatically, when all voice channels are already occupied by external phone calls.
Configure enough voice channel licenses, so that sufficient capacities for external connections are guaranteed.

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 use SwyxIt! 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.

5.3 ADDITIONAL FUNCTIONS

In addition to the ordered feature profiles, you can order additional functions and assign them separately to the desired users.

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	✓	✓	✓
Swyx Connector für 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

Name of the 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 für Notes	Integration in Lotus/IBM/HCL Notes, calendar-based forwarding, dialing from any contact databases, number identification
Swyx Meeting	WebRTC-based web conference service Maximum 25 participants: 1 host + 24 guests
Swyx Analytics by aurenz	Extension for the analysis of corporate communication on the basis of the generated call data

Name of the function	Explanation
Swyx VisualGroups Standard	With Swyx VisualGroups, departments with a high caller volume receive an optimal queue solution with seamless integration into the SwyxIt! user interface.
Swyx VisualGroups Enhanced	Additionally, VisualGroups Enhanced offers a statistics function.
Swyx Connector für DATEV	Integration of Swyx telephony functions in DATEV applications
Swyx Connector for Microsoft Teams	Integration of SwyxIt! telephony functions into the Microsoft Teams user interface

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) 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 (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 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.

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 Visual-Groups	Swyx Visual-Groups 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 Swyx Flex model and must be purchased separately.

Swyx Analytics by aurenz

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

5.4 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	Number
Feature Profile "Premium"	5
System Phone	5
Feature Pack for Certified SIP phones	5
Swyx Connector für 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

5.5 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 desired 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, billing will continue to take place.

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.

6 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.

6.1 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 **6.1.3 User license**, page 53.

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 **6.1.1 Swyx Update Service (SUS)**, page 53.

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)..

6.1.1 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.

6.1.2 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.

6.1.3 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 logon 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 52.

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 assign 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 function profile "Deactivated" to the new users and order later if required.

6.1.4 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 (devices 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.

6.1.5 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.

STOP

When dialing an emergency number (e.g. 112), a voice channel cannot be released automatically, when all voice channels are already occupied by external phone calls.
License a sufficient number of voice channels, so that enough capacities for external connections are guaranteed.

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).

6.1.6 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 Managers.

SwyxECR (Extended Call Routing)

This option pack 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.

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 vir-

tual 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 58.

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 use SwyxIt! 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 für Notes

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

- Direct dialing from Swyx Connector für Notes
- Display Swyx Connector für Notes contacts (for incoming call, from lists)
- The search function in the SwyxIt! input field and the phonebook also searches Swyx Connector für Notes contacts
- Name resolution from Swyx Connector für Notes for incoming calls and for list search
- Swyx Connector für 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! functions directly in 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 Visual-Groups	Swyx Visual-Groups 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 Enreach website.

Swyx Analytics by aurenz

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

This Option Pack 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.

6.1.7 SWYXWARE OPTION PACKS AT A GLANCE

The following option packs are available:

Option Pack	SwyxWare Variant	Explanation
SwyxProfes-sional	• 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.

Option Pack	SwyxWare Variant	Explanation
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 the Call Routing Managers. 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

Option Pack	SwyxWare Variant	Explanation
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, ad-hoc conference feature
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

User functions	Description
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 für Notes	Integration in Lotus/IBM/HCL Notes, dialing from any contact databases, number identification
Swyx Connector for Microsoft Teams	Integration with Microsoft Teams
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.

6.1.8 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	pro User
SwyxFax	5 licenses	Option	pro User
SwyxPhone	2 licenses	Option per phone	pro phone/pro User
SwyxRecord	5 licenses	Option Pack	pro User
SwyxConference	5 licenses	Option Pack	-
SwyxMonitor	5 licenses	Option Pack	pro User/-
SwyxStandby	included	Option Pack	-
SwyxAdHocConference	included	included	pro User
Swyx Option Pack for Swyx Connector für Notes	5 licenses	Option Pack	pro 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
Swyx Connector for Microsoft Teams	5 licenses	Option	pro User
Swyx Connector for DATEV	5 licenses	Option	pro User

	Evaluation Installation	SwyxWare	SwyxWare for DataCenter/ SwyxON
Feature Pack for Certified SIP Phones	5 licenses	Option	pro User
Swyx Visual-Groups Enhanced	1 queue or 5 licenses	Option	-
SwyxVoicemail	included	included	pro User
SwyxCTI	included	included	pro User
SwyxCTI+	5 licenses	Option	pro 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

7 CREATING AND EDITING LOCATIONS

Location is a User and Trunk Group property, which Groups together site-dependent parameters.

The setting options on menu pages and in configuration wizards depend on your administration profile and your SwyxWare solution.

Creating Locations

Editing the Location settings

Further information can be found at:

help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/893

7.1 CREATING LOCATIONS

To create a Location

1 In the menu, select **Connections | Locations**.
✓ A list appears with all Locations.

2 Click on **Create Location**.
✓ The **Create a Location** configuration wizard appears.

3 Define the Location settings.

Designation	Explanation
Location	Enter a name for the Location. The name must be unambiguous within SwyxWare.
Description	Enter a description, if applicable.
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 6p.m. to 8p.m. If a User in England now calls at 7:15p.m. local time a number in Germany (German local time 8:15p.m.), the ISDN Trunk Group is disabled for this call.*
Standard Location	Activate the check box, if you want the Location to be used as the default for all subsequently created Users and Trunk Groups.
Number of concurrent calls	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.

When making later changes to settings, click **Save** to save the settings.

4 Click on **Next**.

5 Define the number settings for the Location.

Designation	Explanation
Country code	Enter the country code of the location. *Example:'44' for Germany*
Area code	Enter the location code of the site without leading '0'. *Example: '20' for London or '161 for Manchester*
Public line access codes (separated by ";"):	Enter the code for external calls, e.g. 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.

Designation	Explanation
Prefix for long distance calls	Enter the code for long distance calls. *Example:'44' for Germany*
Prefix for international calls	Enter the code for international calls. *Example:'44' for Germany*
Number for undeliverable calls	Select from the Global Phonebook a User to whom calls will be forwarded which are in the SwyxServer number range but are not assigned to a User. The number for undeliverable calls can also be assigned to a User at a linked SwyxServer.

When making later changes to settings, click **Save** to save the settings.

6 Click on **Create**.
✓ The entry is displayed in the list of all Locations.

7.2 EDITING THE LOCATION SETTINGS

You can also edit Locations, e.g. by adding further public line access prefixes.

To edit a Location

1 In the menu, select **Connections | Locations**.
✓ A list appears with all Locations.

To access further information, click on ⌄.

2 In the line of the appropriate Location, click on ✎.

See also step **3Define the Location settings.**, page 62

7.3 LIMITING THE NUMBER OF CALLS BETWEEN LOCATIONS

To limit the number of calls between Locations

1 In the menu, select **Connections | Locations**.
✓ A list appears with all Locations.

2 In the line of the appropriate Location, click on ✎.

Designation	Explanation
Restricting calls between the Locations	Activate the checkbox, if you want to allow only a certain number of calls from/to this Location. You can limit the number of possible connections between 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 24kbit/s (compressed) and 84kbit/s (uncompressed) bandwidth is needed per call.
Maximum number of calls from/to this Location and other Locations	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.

3 Click on **Save**.

4 Click on **Numbers**.
See also step **5Define the number settings for the Location.**, page 62

7.4 DELETING LOCATIONS

How to delete a Location

1 In the menu, select **Connections | Locations**.
✓ A list appears with all Locations.

2 In the line of the appropriate Location, click on 🗑.

3 Click on **Yes** to confirm the process.
✓ The Location is deleted and is not available anymore.

8 TRUNKS

A Trunk is a connection to another network and a property of Users and Trunk Groups in which site-dependent parameters are combined.

A Trunk must always be a member of a Trunk Group. The trunks in a trunk group then have the same properties (such as the same connection protocol, the same location, or the same authorization parameters).

In SwyxWare there are the following Trunk types:

- ISDN Trunk (SwyxGate lines)
- SIP Trunk
- SIP Gateway Trunk
- ENUM Trunk
- SwyxLink Trunk (Server-server coupling)

See https://help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/Trunks_TrunkGroups_$.

See also **15 Numbers and Number Mappings**, page 164

The setting options on menu pages and in configuration wizards depend on your administration profile and your SwyxWare solution.

In Swyx Control Center you can:

Create trunk groups

Edit trunk groups

Create trunks

Edit trunks

Delete trunk groups

Delete trunks

8.1 CREATE TRUNK GROUPS

A trunk must be assigned to a trunk group. Create a trunk group of the required type (SIP, SIP gateway, etc.) to be able to subsequently create trunks of the corresponding type.

To create a trunk group

1. In the menu, select **Connections | Trunks**.
2. Select **Trunk groups**.
3. A list appears with all Trunk Groups.
4. Click on **Create Trunk Group** .resp **Create SwyxLink group** .
   ✓ The configuration wizard appears **Create trunk group**.
5. Set general settings for the trunk group.

Label	Explanation
Name	Enter a name for the trunk group. The name must be unambiguous within SwyxWare.
Descrip-tion	Enter a description, if applicable.
Trunk group type	Choose a trunk type: The trunks subsequently created in this trunk group will have the property of the selected type.
	SIP Trunk SIP trunks enable the use of VoIP services. The service provider usually assigns a number range or SIP URIs. If the service provider in question also offers gateway services, numbers in the public telephone network can also be reached via a SIP trunk and the provider's gateway behind it.
	SIP Gateway Trunk SIP gateway trunks are used to control gateways that are themselves reached by SwyxServer via a SIP connection. This makes it possible, for example, to operate telephones in small branches and branch offices, each with a local gateway and with a local direct connection to the public telephone network. Only gateways for which profiles are included in the delivery are supported at present.

Label	Explanation
	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.
	Trunk (Server-server coupling) SwyxServers at different locations are connected to each other via an IP link using a SwyxLink Trunk. The SwyxLinkManager takes over the control of the connection. Within the configuration of a SwyxLink Trunk the connection to further SwyxWare sites can be defined, so that status information (logged off, available, currently speaking) can also be exchanged between users who are logged on to different servers. See also **4.14 Inter-site connections**, page 30
Location	Select one of the locations, see *Creating and editing Locations*. The location defines prefixes and time zone for the trunk group
Provider profile (not for SwyxLink group)	Select a 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. The phone number format is defined for each of these profiles. For SIP Trunks in particular, the profile specifies the provider and the necessary SIP parameters. See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/sip_trunkgroup_$ Currently, only one profile exists for each of the SwyxLink and ENUM trunk types.
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 **14.2 Trunk Recording**, page 150

6 Click on **Next**.

7 If necessary, set the SIP registration for the trunk group (SIP type only).

The registrar port must match the selected transport protocol. Leave the filed empty if you did not receive information on the port by your Service provider. The port is determined via DNS query.

Label	Explanation
SIP Registration	Check the box if SIP registration is to be used.
Registrar	Enter the server address of the registrar. REGISTER messages are sent to this address.
Registrar Port	Set the port on which the configured registrar will accept the registration request.
Re-registration interval (seconds)	Set the frequency of re-registration. *e.g. 120 (seconds)* 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.

8 Click on **Next**.

9 Set the forwarding.

Label	Explanation
Trunks of this trunk group use...	Specify for which calls this Trunk Group should be used. You can use wildcards (*) when entering phone numbers or URIs, see **15.5 Placeholder**, page 170 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

10 Click on **Create**.
✓ The trunk group is created and appears in the list of trunk groups.

You can define further settings for the trunk group, see *Edit trunk groups*

8.2 EDIT TRUNK GROUPS

You can customize the settings you specified when you created the trunk group. You can also specify other settings.

To edit a trunk group

1 In the menu, select **Connections | Trunks**.
2 Select **Trunk groups**.
3 A list appears with all Trunk Groups.

Label	Explanation
Name	Name of the Trunk Group
Description	Description of the Trunk Group
Type	Type of Trunk Group
Profile	Trunk Group Profile
Location	Location of Trunk Group
Calling Rights	Defines where incoming calls of this trunk group may be forwarded to if the call destination is not a user at the same SwyxServer See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/Trunks_TrunkGroups_$.

4 In the row of the desired trunk group, click ✎.
✓ The following tab appears **General**.
5 You can edit name, description, location and profile, see *Create trunk groups*. You can also edit the following Settings:

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 allowing the possibility to route incoming calls back to the outside via a trunk only in exceptional cases.

The string for the selection prefix must not begin with the outside line access code and must not begin with an existing internal telephone number. It is recommended to let the selection prefix start and end with * or # to achieve a better differentiation to the destination number.

If a user has used the selection prefix to specify a trunk group through which the call should be routed, no forwarding rules are applied to that call.

If a project code number is used in addition to the selection prefix, enter it first. The project code always begins with * and ends with #.

If a selection prefix has been entered by the user, only trunks in this trunk group will be selected and no further attempt will be made to route the call through other trunks.

Label	Explanation
Calling Rights	Select where incoming calls received via this trunk group may be forwarded to. This way you define if and which other trunk groups the call may use to leave this SwyxWare installation if its destination is not a user of this SwyxServer: • Internal connections only (default value) • International connections • Calls within Europe • National connections • local calls • Deny all calls If a user has been called on this SwyxServer and the call is forwarded by his Call Routing, the call gets the permissions of the called user.

Label	Explanation
Selection prefix for the trunk group	Set a prefix that allows a user to route the call specifically through this trunk group. The selection prefix must be uniquely assigned to a trunk group, it cannot be assigned more than once, it may only consist of the characters '01234567890#*' and may not begin with '##'. *Examples:* *In the following, the project code *1234# and the selection prefix **34#* *<*Project code#><Selection prefix><Canonical call 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*
Public line access of the superior PBX	If SwyxWare is configured as a sub PBX, enter the outside line access of the parent PBX.

6 Click on **Save**.

7 Select the tab **Phone number formatting**.

Label	Explanation
Conversion for outgoing calls	Procedures for converting outgoing numbers and interpreting incoming numbers are defined within a trunk group. In the properties of a trunk group, the selected profile is used to specify in detail which phone number (outgoing or incoming and calling or called number) is converted into which format. This mapping of formats can be modified subsequently by administrators. For the available phone number formats, see section "Supplied configuration files" under **15.6.1 NumberFormatProfiles.config**, page 173
Conversion for incoming calls when number type is unknown	

8 Click on **Save**.

9 If necessary, select the tab **SIP** (SIP and ENUP types only).

10 You can change the SIP registration data for a SIP trunk group, see *Create trunk groups*. You can also specify other settings:

Label	Explanation
STUN support	Check the box to enable STUN support. STUN can be used to determine the current public IP address of the connection so that the remote station can address and return its call data correctly.
STUN server	If your SIP provider supports STUN, enter the name or IP address of your provider's STUN server and the corresponding port. Alternatively, you can use the free STUN server "stunserver.org" with port "3478".
STUN server port	
Outbound proxy (SIP only)	Some providers have an outbound proxy before the SIP proxy. If necessary, enter these parameters according to your provider's specifications.
Outbound proxy port (SIP only)	

Label	Explanation
Proxy (SIP only)	Enter the address and port of the proxy server. 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. Upon request, the subscriber then receives the current IP address of the subscriber and can thus deliver the call to this address.
Proxy port (SIP only)	
Realm (SIP only)	If necessary, enter the realm area 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 not specified, the Registrar or Proxy value is used.
DTMF method: (SIP only)	Select a DTMF method if necessary. This mode is used to specify how the provider handles keystrokes from the user (DTMF signaling). **None.** DTMF signalling is deactivated. **RFC2833_Event:** DTMF signaling is used based on the event mechanism described in RFC2833. **Info Method DTMF Relay** DTMF signaling is used as suggested by Cisco (applicationtype DTMFRelay).

11 Click on **Save**.

12 If necessary, select the tab **Encryption** (SIP type only).

Make sure that the selected transport protocol is supported by your provider.

When "Encryption mandatory" is selected, voice data encryption is obligatory. This means that encryption is either always performed or the call is terminated with the reason "Destination does not support encryption".

The encryption mode for a SIP trunk group has no influence on the SRTP encryption configuration for SwyxServer.

Label	Explanation
Transport protocol	Select the transport protocol to be assigned 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	Select the encryption mode. This setting is enabled only 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** The voice data is encrypted between SIP provider and SwyxLinkManager.

13 Click on **Save**.
✓ The trunk group settings have been updated.

See also **8.7 Forwarding and number substitution**, page 79

8.3 CREATE TRUNKS

A trunk must be assigned to a trunk group. To be able to create a trunk of the required type (SIP, SIP gateway, etc.), a trunk group of the corresponding type must have been created first, see **8.1 Create trunk groups**, page 65

To create a trunk

1 In the menu, select **Connections | Trunks**.
2 A list appears with all Trunks.
3 Click on **Create trunk**.
✓ The configuration wizard appears **Create Trunk** or **Create SwyxLink**.
4 Set the general settings for the trunk.

Label	Explanation
Name	Enter a name. The name must be unambiguous within SwyxWare.
Descrip-tion	Enter a description, if applicable.
Trunk Group	Select a trunk group of the required type to which the trunk is to be assigned: The trunk assigned to this trunk group gets the property from the corre-sponding type. If no matching trunk group or SwyxLink group exists yet, click on **Create Trunk Group** or **Create SwyxLink group**.
	SIP Trunk SIP trunks enable the use of VoIP services. The service provider usually assigns a number range or SIP URIs. If the service provider in question also offers gateway services, it is also possible to reach numbers in the public telephone network via a SIP trunk and the provider's gateway behind it.
	SIP Gateway Trunk SIP gateway trunks are used to control gateways that are themselves reached by SwyxServer via a SIP connection. This allows, for example, telephones in small branches and branch offices to be operated with a local gateway in each case and with a local direct connection to the public telephone network. Only gateways for which profiles are included in the delivery are supported at present.
	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 automati-cally 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.
	Trunk (Server-server coupling) SwyxServers at different locations are connected to each other via an IP link using a SwyxLink Trunk. The SwyxLinkManager takes over the control of the connection. Within the configuration of a SwyxLink Trunk the con-nection to further SwyxWare sites can be defined, so that status informa-tion (logged off, available, currently speaking) can also be exchanged between users who are logged on to different servers. See also **4.14 Inter-site connections**, page 30

5 Click on **Next**.

6 If necessary, set the **SwyxLink trunk** (SwyxLink type only).

Label	Explanation
Locally managed SwyxLink Trunk	Each cross-site connection is managed by exactly one SwyxLinkManager. If you want to manage the SwyxLink on this side of the connection, choose **Locally managed SwyxLink trunk**. This SwyxLink must then be set up "remotely managed" on the other side.
Remotely managed SwyxLink Trunk	

7 Click on **Next**.

8 If necessary set the **Remote SwyxServer** (SwyxLink type only).

Label	Explanation
Remote server	Enter the name (FQDN) or IP address of the SwyxServer to which this SwyxLink trunk should be configured. Make sure that there is a transparent TCP/IP connection between the server running the LinkManager service (local SwyxLink) and all remote clients and the SwyxServer.
Remote standby server	If a standby scenario is used on the other side, enter the name of the standby server as well.
Test Link	Click the button to test the connection to the remote SwyxServer.

9 Click on **Next**.

10 If necessary, set the **SIP account** data (SIP gateway type only).

Label	Explanation
SIP User ID	Enter here the SIP account data with which the SIP gateway should log on to SwyxServer via this trunk. This logon data must be entered in the same format as when was configured. SIP User ID is the user ID that together with the realm forms the SIP address (URI).
Authentication method	Select whether the gateway should authenticate itself.
User name	The user name and password are required for user authentication.
Password Authentication	
Repeat password	

11 Click on **Next**.

12 If necessary, set the **SIP trunk provider / user data** (SIP type only).

Label	Explanation
SIP provider	SIP Provider Profile. This property is inherited from the assigned trunk group.
SIP User ID	Enter the user data you obtained from your SIP provider: SIP User ID is the user ID that together with the realm forms the SIP address (URI).
SIP user name	The user name and password are required for user authentication.
Password Authentication	
Repeat password	

13 Click on **Next**.

14 Define the numbers.

Enter the public numbers (or range of numbers) to be used by this trunk.

External calls to these numbers go over this trunk. Calls with a calling party number assigned to this trunk are routed via this trunk.

If you get several individual phone numbers or several phone number ranges set up by your provider, specify only one range and add the others later, see **8.4 Edit trunks**, page 75

Country and area codes are specified by the location of the trunk group.

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

The existing phone number entries are automatically extended by the new "Subscriber number" input field when updating to v. 13.20. Make sure that the automatic allocation is correct and adjust the corresponding entries manually if required.

Label	Explanation
Country code	If necessary, enter the country code. *example:'44' for Germany*
Area code	If necessary, enter the area code. *z. E. g. 30 (for Berlin)*
Subscriber number	Enter the part of the phone number that follows the area code and precedes the extension (internal phone number).
First extension	Enter the first extension (internal phone number) of the phone number range.
Last extension	Enter the Last extension extension (internal phone number) of the phone number range.

15 Click on **Next**.

16 Set the SIP URIs if necessary (SIP and ENUM type only).

Label	Explanation
Username	If necessary, enter the SIP addresses (URIs) that this trunk should manage. A SIP has the following format: SIP:<Username>@<Realm> For simplification, you can use '*' as a placeholder here, *E.g. '*@company.com' represents all users with the realm 'company.com'.*
Realm	The realm is already specified by the selection of the trunk group, but can be overwritten.

17 Click on **Next**.

18 Set **Codecs** set.

Label	Explanation
Codec priority and filter	Select the type of compression to be used on this trunk: **Prefer quality** The codecs are provided in the order G.722, G.711a, G.711µ, G.729, Fax over IP. **Prefer low bandwidth** The codecs are provided in the order G.729, G.722, G.711a, G.711µ, Fax over IP. It is important to use as little bandwidth as possible. You can disable unwanted codecs:
G.711µ (around 64 kbit/s per call)	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.
G.711a (around 64 kbit/s per call)	
G.722 (around 84 kbit/s per call)	Voice, highest bandwidth (G.722) HD quality
G.729 (around 24 kbit/s per call)	Voice, low bandwidth. High compression.
Fax over IP (T.38, around 20 kbit/s per call)	The special fax protocol T.38 takes into account the conditions of an IP network.

19 Click on **Next**.

20 Set **Number of channels** set.

Label	Explanation
Number of channels	If necessary, enter how many calls may be made simultaneously via this trunk. Basically, the maximum number of channels depends on the available bandwidth, as well as the codec setting, i.e. the bandwidth per call. Using a SIP Trunk, the provider will define how many connections at the same time will be possible.

21 Click on **Next**.

22 Select if necessary **Connection type for Intersite Presence** (SwyxLink type only).

Label	Explanation
No status information	Specify whether status information ("Logged off", "Away", "Do not disturb", "Currently speaking" etc.) should be exchanged between users of different SwyxServers. Furthermore, users are shown in the Global Phonebook of the connected servers. Select this option if you do not want user status information to be published via this link.
Remote SwyxServer in the same organization	Select this option if the remote SwyxServer is in the same organization as the SwyxServer you are currently administering. 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.

Label	Explanation
Remote SwyxServer in another organization	Select this option if the remoteSwyxWare is located in a different organization than the SwyxServer you are administering. With this type of connection you can define individual groups of your SwyxServer which should be visible on 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 do this accordingly in the opposite direction, so that groups of his SwyxServer become visible on your side. 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.

23 Click on **Next**.

24 Select if necessary **Settings for Intersite Presence** (SwyxLink type only).

Configuring intersite connections within the SwyxLink trunk does not automatically activate status signaling between the different SwyxWare sites. 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 **9.8 Defining call and status signaling**, page 91

Label	Explanation
Internal numbers only	Activate this option to display only the internal phone number of the users in the Global Phonebook on both pages.
Public numbers only	Enable this option to display only the public phone number of the users in the Global Phonebook on both pages.
Internal and public call numbers	Enable this option to display only the public phone number of the users in the Global Phonebook on both pages.

Label	Explanation
Data synchronization	• User pictures Specify whether the user images stored by the user should also 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 do not allow calls, the Video, Collaboration and SwyxIt! meeting features are automatically disabled. If you deactivate the status information button, you are not able to choose Instant Messaging

25 Set **Computer name** set.

Label	Explanation
Computer name	Apply the default computer name. SwyxLink type: Enter the name of the computer where the SwyxLink-Manager is managed. Use the name of the computer as it appears in the computer properties.

26 Click on **Create**.
✓ The trunk is created and appears in the list of trunks.

You can define further settings for the trunk, see *Edit trunks*

8.4 EDIT TRUNKS

You can adjust the settings you specified when you created the trunk. You can also specify other settings.

The existing phone number entries are automatically extended by the new "Subscriber number" input field when updating to v. 13.20. Make sure that the automatic allocation is correct and adjust the corresponding entries manually if required.

To edit a trunk group

1 In the menu, select **Connections | Trunks**.
2 A list appears with all Trunks.

Label	Explanation
Name	Trunk name
Type	Type of Trunk
Number of concurrent calls	Number of calls which may be routed via this Trunk at the same time
Activated	✓ = The trunk is activated and can be used for incoming and outgoing calls. ⊘ = The trunk is locked, e.g. for maintenance.
Logged in	✓ = Trunk is logged in

3 In the row of the desired trunks, click ✎.
✓ The following tab appears **General**.
4 You can change the name, description, computer name, see *Create trunks*. You can also specify other settings:

Whether a trunk has been enabled or disabled is not recorded in the change log.

Label	Explanation
Trunk is activated	Check the box to unlock the trunk for incoming and outgoing calls.

5 Click on **Save**.

6 Select the tab **SIP registration** (SwyxLink, SIP, SIP Gateway type only).

You can change the SIP registration data, see **8.3 Create trunks**, page 70

7 Click on **Save**.

8 Select the tab **Phone numbers**.
✓ The list of all call number ranges assigned to this trunk appears.

You can edit or delete the corresponding phone number ranges.

9 If necessary, click **Add phone number range** to assign additional phone numbers or phone number ranges to this trunk, see also **15 Numbers and Number Mappings**, page 164.

10 Click on **Save**.

11 Select the tab **Codecs**.

12 You can change the codec priority and filters, see *Create trunks*. You can also specify other settings:

Label	Explanation
Behavior during fax transmission	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 first 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 switching 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.

During a new installation of SwyxWare or during an update the option "Use server default" is activated by default. 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.

13 Click on **Save**.

14 Select the tab **Channels**.

You can change the total number of simultaneous calls or set the number for each incoming and outgoing call.

15 Click on **Save**.

16 Select the tab **Call number signaling**:

Label	Explanation
Always suppress number	Select whether and how the phone number for outgoing calls should be signaled via this trunk. Select this option if the called party is not to be signaled (XXX), regardless of the phone number configured for this trunk.
Always Use This Number:	Enter a call number in canonical format or a SIP URI that is always signaled to the called party (e.g., the number of the central office), regardless of the call number configured for this trunk.
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	Specify which phone number this trunk uses. You can define the behavior for phone numbers that are assigned to this trunk as well as for phone numbers that have not been assigned, see the table:

Use	When assigned to this trunk	If assigned to this trunk, otherwise:	Required input
Origination Number	Number of the transferor		
	Hide number		
	Don't use this trunk		
	Use the following number		Enter the desired phone number
Number of the transferor	Origination Number	Hide number	
		Don't use this trunk	
		Use the following number	Enter the desired phone 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

17 Click on **Save**.

18 Select the tab **Encryption** (SIP Gateway, ENUM type only).

If "No encryption" was set within the server properties, the mode here is also set to "No encryption"; if "Encryption mandatory" was configured, the setting "Encryption mandatory" can also be found here. In both cases, the mode cannot be changed. The field is then deactivated.

Label	Explanation
Encryption mode	**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 user is 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.
Key Repeat key	To ensure a secure communication via SRTP between SwyxServer and remote station a shared key (PreSharedKey) has to be defined and exchanged between them. For all components using the SwyxWare database (e.g. SwyxIt!, PhoneMgr, ConferenceMgr, Gateway) this key is automatically generated by SwyxServer and distributed encrypted to the respective component. For SIP gateway, ENUM type, the key must be entered manually. In addition, the stored key must also be entered at the remote terminal.

19 Click on **Save**.

20 Select the tab **SIP URIs** (SIP type only).
✓ The list of all SIP URIs assigned to this trunk appears.

21 You can edit or delete the corresponding SIP URIs.

22 If necessary, click **Add SIP URI** to assign additional SIP URIs to this trunk.

23 Select the tab **Link settings** (SwyxLink type only).

You can change the link settings for the SwyxLink trunk, see **8.3 Create trunks**, page 70

24 Click on **Save**.
✓ The trunk settings have been updated.

8.5 DELETE TRUNK GROUPS

You can delete trunk groups.

To delete a trunk group

1 In the menu, select **Connections | Trunks**.

2 Select **Trunk groups**.
✓ A list appears with all Trunk Groups.

3 In the trunk group row, click 🗑 to delete this trunk group.
✓ The trunk group is deleted and no longer appears in the list.

8.6 DELETE TRUNKS

You can delete trunks.

To delete a trunk

1 In the menu, select **Connections | Trunks**.
✓ A list appears with all Trunks.

2 Click 🗑 in the trunk line to delete this trunk.
✓ The trunk is deleted and no longer appears in the list.

8.7 FORWARDING AND NUMBER SUBSTITUTION

Outgoing calls can be made depending on

- the phone number of the calling SwyxWare user,
- of the dialed number,
- of group membership,
- the location of the user and/or
- the time conditions,

be forwarded via various routes.

A forwarding entry is always assigned to a specific trunk group.

You can also use placeholders when defining rules, see **15.5 Placeholder**, page 170.

Example:

You have an ISDN trunk to the public telephone network in Hamburg and a SwyxLink connection to a branch office in Berlin. All calls to Berlin (+4930) should be routed via SwyxLink.*

You set up a forwarding for the trunk group SwyxLink is a member of (destination number/URI: +4930), 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 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).*

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 according to priority order, i.e. in this case the SwyxLink connection is selected first, then the SIP connection and then the connection via ISDN.*

If a user has used the selection prefix to specify a trunk group through which the call should be routed, no forwarding rules are applied to that call.

Priority

Forwarding entries can be set with different priority (0-1000) for each trunk group individually.

A sequence is created, e.g. "Try first on trunk group A, then on trunk group B".

A forwarding entry is automatically created for a SwyxLink trunk with configured Intersite settings. This entry is not editable.

If a trunk group contains several trunks, the trunk to which the caller's phone number is assigned is selected preferentially. If no trunk matching the caller number is found within the selected trunk group, the trunk that signals the most information regarding the caller is selected.

Example:

You have two SIP connections. 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.

When one of the two users calls an external number, a trunk group is selected based on the dialed number and priority. If no preferred trunk group can be selected by these criteria, the trunk group is selected randomly. i.e. trunk group 1 can also be selected for user 2.

If caller ID suppression is configured on the trunk groups for unassigned caller IDs, then - unintentionally by the user - his caller ID is displayed on one call and not on another call. To avoid this, if the trunks are similar, you can manage both in one trunk group, regardless of the fact that two different ports are represented by it.

SwyxWare can repeat connection attempts to external numbers via different trunk groups.

If no connection is established with the first selected trunk, the next forwarding entry is taken after the priority. Depending on the configuration, this can be the same trunk group again.

In the following example, first an attempt is made to dial a call via the trunk group TG2 (priority 600), then three attempts are made (once + two

retries) to establish a connection via TG1 (priority 500). 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.

Trunk Group	Priority	Number	Prefix	Repetitions
TG1	500	+*	01013	2
TG2	600	+*	-	0
TG3	400	+*	01033	0
TG4	300	+*	-	0
TG5	200	+*	-	0

Extended Least Cost Routing

With the extended least-cost routing, the use of remote access to the public telephone network (SwyxGate) is possible.

Example:

When a SwyxWare user at the Dortmund site connects to a subscriber near the London site, the SwyxServer at the Dortmund site can now determine based on the parameters of the trunk assigned to London that the dialed subscriber can be reached via the corresponding trunk. 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.

Of course, for the connection via SwyxGate in London to the external subscriber, the least-cost routing of SwyxServer in London and the corresponding service provider is then used again.

It is often desired that the calls from Dortmund can also signal a Dortmund number. On the "Call numbers" tab of the corresponding trunk, you define which call number is signaled to a call partner. The trunk in London must then be able to use foreign (i.e. Dortmund) numbers on the outgoing call. The "CLIP no Screening" function is used for this purpose and must be requested separately from your provider.

To set a forwarding entry

1 In the menu, select **Connections | Trunks**.

2 Select **Trunk groups**.

3 A list appears with all Trunk Groups.

4 Click on ✎ in the line of the speed dial selected.

5 Select in the menu **<Trunk group name> | Forwarding & Replacement**.
✓ The tab **Forwarding entries**.

6 Click on **Add forwarding entry**.
✓ The configuration wizard appears **Forwarding entries**.

7 Enter a short description if necessary.

8 If the forwarding rule should be applied immediately, activate the checkbox **Forwarding entry is activated**.

9 Click on **Next**.
✓ The following tab appears **Forwarding**.

10 Specify which criteria regarding the phone number or URI should be used for forwarding:

Label	Explanation
Use this trunk group for the following calls Enable this option if you want the calls to be routed through this trunk group that meet the following conditions:	
Destination number/ URI	Enter the public phone number or URI to be routed over this trunk. You can use placeholders for this.
With call-by-call prefix	If necessary, enter a sequence of digits to be placed in front of each destination number that is forwarded via this trunk group, *z. E.g., a call-by-call prefix: 01013*
Number of repetitions	Specify how often a connection attempt should be repeated (standard: 0). If no LCR is used, but the call-by-call prefix of a low-cost but heavily congested provider is dialed directly, these repetitions can be useful to try a low-cost provider several times.
DO NOT use this trunk group for the following calls Enable this option if the calls with certain destinations should NOT be routed through this trunk group.	

Label	Explanation
Destination number/ URI	Enter the public phone number or URI that should NOT be routed via this trunk. You can use placeholders for this.
Record Priority	Specify the priority with which this forwarding is applied to a Call. You can use a value between 0 (lowest) and 1000 (highest).

11 Click on **Next**.
✓ The tab appears **Source**.

12 If necessary, specify whether the origin of the call is taken into account. If nothing is configured, the forwarding rule applies to all calls.

You can use the two options **Members of the group** as well as **Users of the location** (e.g. All users of the "Support" group at the "Munich" site). The **Phone number** option can be combined with either the **User** or **Members of the group** and/or **Users of the location** options.

Label	Explanation
Phone number	Activate the option and enter an internal phone number or URI. The forwarding applies to all calls signaling this phone number or URI (internal SwyxWare user or group). If the calls coming in through this trunk are to be forwarded according to this rule, enter the phone number or URI in canonical format. The number is matched from the beginning onward. If you enter "21", for example, the forwarding rule applies to all callers whose own phone number begins with "21".
Users	Enable the option and select a user for whom the forwarding should apply.
Members of the group	Activate the option and select a group. The forwarding applies to all members of the group.
Users of location	Activate the option and select a location. The forwarding applies to all Users.

13 Click on **Next**.
✓ The tab **Time limit**.

14 Set time conditions (days of the week, time) for forwarding.

Label	Explanation
Apply forwarding entry on specific day(s)	Enable the option if you want the forwarding to apply on certain days of the week. Then activate the desired days of the week.
Use Routing Record on specific Time of Day	Enable the option if you want the forwarding to apply at specific times. Then select the desired times (From and To) to define a time section.

15 Click on **OK**.
✓ The forwarding is created and appears in the list of forwarding entries.

You can adjust or delete the redirects using the buttons and .

8.7.1 DEFINING CALL NUMBER SUBSTITUTIONS FOR A TRUNK GROUP

For individual phone numbers or SIP URIs, you can define a special, automatic phone number substitution. You can create number substitutions for

- outgoing caller numbers,
- outgoing Target numbers,
- incoming Caller numbers and
- incoming destination numbers

Example:

Original number +4923112345 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.

Numbers that are to reach the public telephone network must be entered in canonical format.

You can also use place holders when defining rules, see **15.5 Placeholder**, page 170.

"Apply also in reverse" option

If you activate the option **Also apply in reverse** option, this replacement applies in both directions, i.e. the incoming caller number is replaced and vice versa 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:

Original number +44 is replaced by 0044**

If "Also apply in reverse" is activated, then for incoming calls the 0044 in the caller number is replaced by +44.

To set a call number substitution

1 In the menu, select **Connections | Trunks**.

2 Select **Trunk groups**.

3 A list appears with all Trunk Groups.

4 Click on in the line of the speed dial selected.

5 Select in the menu **Trunk group name | Forwarding & Replacement**.
✓ The tab **Forwarding entries**.

6 Select the desired tabs
Outgoing caller number
Outgoing destination number
Incoming caller number
Incoming destination number

7 Click Add phone number replacement.
✓ The configuration wizard appears **Add phone number replacement**.

8 Define the replacement for a phone number or a SIP URI.

Label	Explanation
Original call number:	Enter the original phone number or URI.
Replacement:	Enter a replacement for the original phone number.
Also apply in reverse	Enable the option to apply the replacement to both directions.

9 Click on **OK**.
✓ The phone number replacement is added and appears in the list.

You can adjust or delete the number replacements using the buttons and .

9 CREATING AND EDITING USERS

To log into SwyxServer Users need a SwyxWare account which they can create in Swyx Control Center.

When saving and processing personal data, observe the appropriate applicable legal data protection regulations.
If you have any questions especially regarding data protection in SwyxWare, please contact your administrator.

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

Administration profiles
Authentication for clients
Creating Users
Editing Users' general settings

9.1 ADMINISTRATION PROFILES

The administrator profile defines what rights this User has when he connects to a SwyxServer via SwyxWare Administration or Swyx Control Center. Depending on the profile, he can, for example, create or change Users or edit Phonebooks.

Administration profile	Description
System Administrator	This administrator has unrestricted access to SwyxWare.
Backoffice Administrator	This administrator has all the rights required to configure SwyxServer. Primarily, this administrator can create or change feature profiles.
User Administrator (User Administrator)	This administrator can make all configurations for Users and Groups. In particular, he can carry out number allocation, Group configuration and the allocation of administration profiles. The exception to this is Trunks, Trunk Groups and Feature Profiles.
User Operator (User Operator)	This administrator can change all User properties and enter or delete Users. These rights are typically necessary for an administrator who should not change the system configuration.
Call Status Operator (Call Status Operator)	This administrator can recognize the current call status in the administration, e.g. whether calls are currently being made.
Phonebook Operator (Phonebook Operator)	This administrator can edit the Global Phonebook, i.e. for example the addition of or changes to further important company-wide telephone numbers.
No Administrator (No Administrator)	This profile is allocated to every newly entered User as a default. With this, the User can log in via SwyxWare Web Administration as a User and change his own data.

Please note that in a standby scenario the Users must be set up on both PCs where SwyxServer is installed. A User must, e.g. have the administration profile "User Administrator" on both computers in order to be able to edit Users, regardless of which of the two SwyxServers is currently active.

9.1.1 ADMINISTRATORS IN SWYXWARE FOR DATACENTER AND SWYXON

In SwyxWare for DataCenter and SwyxON we normally distinguish between provider and reseller or partner level administrators on the one hand and a customer's own administrators on the other hand.

Customer level administrators are entered by the provider or reseller or partner in order to provide the customer the option to administrate his telephone system himself.

In detail, the following options are provided:

Administration profile	Solution	Description
Advanced UC Tenant Administrator	SwyxON	This administrator manages his own UC Tenant as well as the objects created with it, including Trunk Groups and Trunks.
UC Tenant Administrator	SwyxON	This administrator manages his own UC Tenant except Trunk Groups and Trunks.
Customer Administrator	SwyxWare for DataCenter	This administrator has the maximum possible rights for a customer. He can make all necessary configurations for his front end server. The only exception to this is Trunks, Trunk Groups and Feature Profiles.
User Administrator	SwyxWare for DataCenter	This administrator can make all configurations for Users and Groups. In particular, he can carry out number allocation, Group configuration and the allocation of administration profiles. The exception to this is Trunks, Trunk Groups and Feature Profiles.
Call Status Operator	SwyxWare for DataCenter	This administrator can recognize the current call status in the administration, e.g. whether calls are currently being made.
Phonebook Operator (editing the Global Phonebook)	• SwyxWare for DataCenter • SwyxON	This administrator can edit the Global Phonebook, i.e. for example the addition of or changes to further important company-wide telephone numbers.

The setting options on menu pages and in configuration wizards depend on your administration profile and your SwyxWare solution.

9.2 AUTHENTICATION FOR CLIENTS

The user of a client has to authenticate himself when logging on to SwyxServer. Basically, the following authentication types are available:

Authentication with user name and password

Authentication with Windows user account

Federated authentication via identity provider

You can define for each user which of the three authentication types they may use, see **To edit the authentication settings for a User**, page 89

When logging in, the user is offered two authentication types; even if one or even all of them are not allowed for the user:
- Windows account or composite authentication
- Name/Password Authentication

Ensure that the user can authenticate via at least one of these options.

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 **4.7 Defining the log in settings**, page 21.

The user name is used to create a SIP user ID.

See also SIP user name and SIP user ID; SIP password.

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.

Force complex user password

As an administrator, you can force or deactivate the use of complex passwords as a general rule for SwyxServer in server configuration (**Force complex user passwords**, page 21)

This rule can be configured individually for each user.

In the **Force complex password and password history** setting you can choose between the following three options:

- 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 user passwords (password reset service)

The Swyx Control Center offers the possibility to reset a user password:

- By the administrator
  An administrator can reset the password of individual users under **User | <Username> | Authentication**, see **9.5 Editing the authentication settings**, page 89.
  The user's password will be deleted and the user will not be able to log in to SwyxServer. The user's existing login session will be automatically terminated within one hour. The user receives an email with the URL to the special Swyx Control Center dialog (SCC URL) where he has to reset his password, see **2.1 Resetting your password**, page 9

The link to reset 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 expiry date, reset the user's password to send a new email with the link or send the generated SCC URL with the user token directly to the user.

- Initiated by user
  The user can click the **Forgot password** button in the login window of SwyxIt! 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 **2.1 Resetting your password**, page 9

The following settings for SwyxServer and the SwyxWare user are required to reset user passwords:

1. E-mail server, see **4.8 Defining an email server**, page 23
2. Email address of the user, see **9.3 Creating Users**, page 86
3. SCC URL, see **4.7 Defining the log in settings**, page 21

If two-factor authentication is activated for a user, their password can only be changed by the administrator.

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 to place calls.

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 enable an identity provider configuration, SwyxServer will offer federated authentication for selection instead of authentication via the Windows user account.
Disable all identity provider configurations to reuse Windows authentication.

See **4.19 Federated authentication via identity provider**, page 35

9.3 CREATING USERS

To create a User

1 In the menu, select **User**.
✓ A list appears with all Users.

2 Click on **Create a User**.
✓ The **Create a User** configuration wizard appears.

3 Define the general settings.

Designation	Explanation
Display name	Enter a name for the User that is displayed in Swyx Control Center. The display name should correspond to the User's first and last name. *Example:* *John Jones*
E-mail address	Enter a unique email address for the SwyxWare integration in Microsoft Office (SwyxIt! function "Office Communication AddIn"). The email address must be provided which is set-up as the User's primary SMTP email address on the company's E-mail server (e.g. Microsoft Exchange Server). This email address is also used by default for voice message delivery. The voice box address can be configured by the user or under **Call forwarding | Voice Box**, see section **9.12 Setting the telephony settings**, page 94. Additionally, you can send the User via this address welcome emails with his registration data and configurations.
Description	Enter a description, if applicable.
Administration profile	Select an Administration Profile for the User (Standard: No Administrator), see also section **9.1 Administration profiles**, page 83.
Feature Profile	Select a Feature Profile for the User. The feature profile determines which SwyxWare features a User can use. The "Default" profile is pre-configured and contains all licensed options.
Activated	Check the box to activate the user account immediately after creating it. Deactivated Users cannot log into SwyxServer. Deactivate the checkbox to temporarily deactivate a User account.

When making later changes to settings, click **Save** to save the settings.

4 Click on **Next**.

5 Define the numbers.

The numbers 110 and 112 are reserved for emergency calls in Germany. As of SwyxWare V13.30, these numbers are always interpreted as emergency calls, even if they are assigned to an internal user.

Designation	Explanation
Internal number	Enter the number under which the User is available site internally. May be preset by default: Next free number *Example: 101*
Public number	If necessary, enter a phone number where the user can be reached publicly. Allowed format: canonical (+<country code><area code><number>) *Example: +49 231 1234100*
Show in Phonebook	Activate the checkbox if you want the numbers to appear in the Global Phonebook.
Location	Select the Location for the User.
Calling Rights	Select the Calling Right for the User: **Deny all calls** The User may not make any calls. This Calling Right is useful or Users who will only receive calls, e.g. Script Users. **Internal destinations** Only calls to internal SwyxWare participants may be started. **Local destinations** Only calls within the area code may be started. **National destinations** Only calls within the country code may be started. **European destinations** Only calls within Europe can be started, i.e. the country code may only start with a 3 or a 4. **No call restrictions** There are no call restrictions.

When making later changes to settings, click **Save** to save the settings.

6 Click on **Next**.

Designation	Explanation
User account for Call Routing	Activate the check box, if the User should only be used for call forwarding. In this case, the User cannot log in with a device.

7 Click on **Next**.

8 Define the authentication settings for logging into SwyxServer. (See also **9.2 Authentication for clients**, page 84)

Designation	Explanation
Enable federated authentication	Select the check box if the user should be allowed to use federated authentication when logging in to SwyxWare. An identity provider configuration must be configured and activated for, see **4.19 Federated authentication via identity provider**, page 35
Windows account (not for SwyxON)	Select the check box if the user should be allowed to log in with his Windows (domain) user account, see **Authentication with Windows user account**, page 85
Assigned Windows user accounts (not for SwyxON)	If the User has Windows user accounts, you can find and add them. You can assign several accounts to the User. It is necessary that the computer of the SwyxIt! user or the Swyx Control Center installation is a member of the same domain as SwyxWare. Windows user accounts cannot be used to log on to Swyx Control Center.
SwyxWare Login data	Check the box if you want the user to log in with SwyxWare user name and password, see **Authentication with user name and password**, page 84

Designation	Explanation
Continue without password	Select the check box if you want the user to set their initial password independently using the link in the welcome email or password reset email, see **Reset user passwords (password reset service)**, page 85. You can send an email to make the user to reset his password, see **9.5 Editing the authentication settings**, page 89
User name	The User name is configured automatically from the data you have entered. You can edit the Username.
TenantDomain	The UPN suffix is part of the Username and is automatically generated from your entered data, see also **4.7 Defining the log in settings**, page 21.
Password Authentication	Enter a password for the User.
Repeat password	Enter the password again to confirm your entry.

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 password to the user by other means.

When making later changes to settings, click **Save** to save the settings.

9 Click on **Next**.

10 Define the SIP settings.

Designation	Explanation
Logon via SIP device	Activate the checkbox to permit the use of third party SIP devices for the User.
SIP User ID	Enter an ID to log into SwyxServer with SIP devices.
SIP Authentication method	Select how the User can log into SwyxServer with SIP devices: **<SwyxServer default>** The server default defines if the User must enter his or her login data for using a SIP device, see also **4.6 Configuring the provisioning of SIP phones**, page 20. **No authentication** The User must never enter his login data for using a SIP device. **Always authenticate** The User must always enter his login data for using a SIP device.
User Name Authentication	Username to log into SwyxServer with SIP devices The SIP User name need not be identical with the SwyxWare User name.
SIP password	Enter a password to log into SwyxServer with SIP devices. The SIP password need not be identical with the SwyxWare password.
Repeat the SIP password	Enter the password again to confirm your entry.
Use SIP devices as system phone	Check the box to allow SwyxCTI+ with a third party phone.

When making later changes to settings, click **Save** to save the settings.

11 Click on **Next**.

12 Define the Desk Phone settings.

If a user wants to make further settings locally on the phone, he needs a minimum 6-digit "user PIN". If the assigned PIN is less than 6 characters, it must be entered twice, e.g. 1234 --> 12341234. This does not apply to the login on the device. It is therefore recommended to assign a PIN with at least 6 digits.

Designation	Explanation
Logon via Swyx-Phone (deactivated)	If you have not created a PIN, the logon via SwyxPhone is disabled.
User-PIN on Desk Phone	Enter a PIN or have a PIN created with which the User can log into SwyxPhone and/or Swyx certified phones.
Logon via certified SIP phone	Activate the checkbox to permit the use of certified SIP devices for the User.
MAC-adress	Enter the MAC address of the certified Desk Phone *e.g. a1:c2:e3:f4:11:12*

13 Click on **Next**.

Designation	Explanation
Send welcome email	Check the box or click the button to send the user a welcome email with their configuration information. If configured, this email can also contain the SCC URL where the user can reset their password, see, **4.7 Defining the log in settings**, page 21. See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/tab_files_$ and https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/tab_advanced_$.

14 Click on **Create**.
✓ The User appears in the list with all Users.

9.4 EDITING USERS' GENERAL SETTINGS

You can edit the general settings for Users, e.g. name and email address.

To edit the general settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.
See also step **3 Define the general settings.**, page 86

9.5 EDITING THE AUTHENTICATION SETTINGS

You can edit the authentication settings for logging into SwyxServer.

For authentication settings specified when the user was created, see **8 Define the authentication settings for logging into SwyxServer.**, page 87.

To edit the authentication settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on **Authentication**.

Label	Explanation
Force complex password:	You can change this server setting for the user, see **Force complex user password**, page 85. In SwyxON this setting cannot be changed.

Label	Explanation
Resetting your password	Click the button to delete the user's password. The user can no longer log on to SwyxServer and receives an email with the URL to the Swyx Control Center dialog where he has to reset his password. See also **Reset user passwords (password reset service)**, page 85

4 If applicable, click **Reset password**.
✓ The **Reset password** dialog box appears with a confirmation whether the e-mail was sent successfully.

Label	Explanation
	Click the icon to copy the URL to the clipboard. As an alternative to the password reset email, you can also send the URL to the user via another communication medium.

The SCC password reset URL is valid only for 24 hours or until the user changes his password.
If the user has not yet changed their password after the expiry date, reset the user's password to send a new email with the link or send the generated SCC URL with the user token directly to the user.

5 If applicable, click **Close**.
6 Click on **Save**.

9.6 EDITING THE SIP SETTINGS

You can edit the settings for logging into SwyxServer with SIP devices.

To edit the SIP settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.
2 As administrator, click on > in the line of the appropriate user.
3 Click on **SIP**.
See also step **10 Define the SIP settings.**, page 88

9.7 EDITING THE ENCRYPTION SETTINGS

You can edit the settings for the encryption of voice data.

To edit the encryption settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.
2 As administrator, click on > in the line of the appropriate user.
3 Click on **Encryption**.

If "No encryption" or "Encryption required" is set in the server-wide settings, you cannot change the setting for individual users, see also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/tab_security_$.

Designation	Explanation
Encryption mode	Select the settings for the encryption of voice data: **No encryption** If "No encryption" is selected, the speech data is not encrypted. **Encryption preferred** If "Encryption preferred" is selected, the speech data is only encrypted if your call partner has configured either the "Encryption preferred" or "Encryption mandatory" mode. If this is not the case, the voice data is not encrypted, but telephony is still possible. **Encryption mandatory** If "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 call partner has configured the "No encryption" mode.
Pre-shared key	Enter a pre-shared key if the User uses SIP devices (with MIKEY support) from a third-party manufacturer. The key must then be stored in the device as well, e. g. via the phone's web interface. The key (PSK) is allocated automatically for Swyx components.
Repeat pre-shared key	Enter the pre shared again to confirm your entry.

4 Click on **Save**.

9.8 DEFINING CALL AND STATUS SIGNALING

You can define the signaling settings for calls and status (available, away etc.) between Users and Groups.

In the current Swyx Control Center version it is not yet possible to add users of different instances (SwyxLink) to the same group.

To define the call and status signaling for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on **Relations**.

4 Click on **Create Relation** or in the line of the appropriate Relation, click on ✎.
✓ The **Create Relation** or **Edit Relation** configuration wizard appears.

Designation	Explanation
Signalize incoming calls to	Activate the check box if you want calls to this User to be signalized to the selected User. A User can pick up calls signaled to him.
Status signaling to	Activate the check box if you want the status to be signalized to the selected User. A User can only call another User via intercom connection or use the messenger if he or she is signaled the status of the other User.
Receiving call signaling from	Activate the check box if you want incoming calls to the selected User to be signalized to the User. A User can pick up calls signaled to him.
Receiving status signaling from	Activate the check box if you want the selected User's status to be signalized to the User. A User can only call another User via intercom connection or use the messenger if he or she is signaled the status of the other User.
	From the dropdown list select the User for whom you want to define signaling settings.

5 Click on **Save**.

Additionally, on the **Relationships** tab you get an overview of all Groups the User is assigned to. Click on 🗑 to remove the User from a Group. Click on **Add to Groups** and activate the checkbox of the appropriate Group to add the User.

✓ The Relationship appears in the list of all Relationships of the User.

9.9 CREATING REMOTE CONNECTOR CLIENT CERTIFICATES

Via Remote Connector you can establish a connection with SwyxServer if you are outside your company network (LAN or VPN). SwyxIt! Users must have a valid client certificate for this purpose, which you can create in Swyx Control Center.

During a new installation or update to SwyxWare V. 13.20 you can have client certificates created automatically for all users, see https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/SCST.

To create a RemoteConnector certificate for a user

1. In the menu, select **User**.
   ✓ For administrators, a list appears with all Users.
2. As administrator, click on > in the line of the appropriate user.
3. Click on **RemoteConnector**.

To use RemoteConnector, you need a server certificate and a root certificate. These are optionally created during the configuration of SwyxWare via the configuration assistant. If you have skipped this step and want to generate the certificates later, you can either start the configuration wizard or the Unattended Setup again or use your own server certificate.

For the creation of the client certificate, have the password of the root certificate ready. This is not necessary in SwyxON.

Designation	Explanation
Thumbprint	The client certificate's digital thumbprint for SwyxRemoteConnector
Create certificate	Click on the button to create a new client certificate for the User.
Root certificate password	Enter the password you have used for the root certificate.

9.10 DEFINING RIGHTS

You can define the following rights for Users:

- Calling Rights
- Feature Profile
- Available features

For further information see https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/index.html#context/help/configure_users_$.

To define the rights for a User

1. In the menu, select **User**.
   ✓ For administrators, a list appears with all Users.
2. As administrator, click on > in the line of the appropriate user.
3. Click on **Rights**.

Designation	Explanation
Calling Rights	Select if and to which destinations the User is allowed to start calls: **Deny all calls** The User may not make any calls. This Calling Right is useful or Users who will only receive calls, e.g. Script Users. **Internal destinations** Only calls to internal SwyxWare participants may be started. **Local destinations** Only calls within the area code may be started. **National destinations** Only calls within the country code may be started. **European destinations** Only calls within Europe can be started, i.e. the country code may only start with a 3 or a 4. **No call restrictions** There are no call restrictions.
Feature Profile	Select the SwyxWare features the User is allowed to use. The "Default" profile is pre-configured and contains all licensed options.
Available features	Activate the checkbox to enable the features for the User.

4 Click on **Save**.

9.11 DEFINING A RELATION BETWEEN MANAGER AND SECRETARIATE

You can specify that all calls to a User are forwarded to another User defined as the secretary.

The feature includes the following settings:

- Immediate and delayed redirection of calls to management to the secretary's office
- No reply forwarding of calls for the Secretariate to the standard Voice Box
- Mutual call and status signaling
- Assigning the other's number to the first Speed Dial
- Assigning the same SwyxIt! Skin

A User can be assigned to several Managements as a Secretariate, but only one Secretariate can be assigned to each Management.

To set a secretarial relationship

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 In the line of the appropriate User, click on >.

4 Click on **Secretariate**.
✓ A list appears with all Secreteriate relations of the selected User.

5 Click on **Add Management** to assign a Management to the selected User or on **Add Secretariate** to assign a Secretariate to the selected User.
✓ The **Create Relation** configuration wizard appears.

Designation	Explanation
Unconditional and no reply forwarding of all calls for the Management to the Secretariate	Activate the check box if you want calls to the Management to be forwarded to the Secretariate. For further call forwarding settings see section **To define the call forwarding settings for a User**, page 94.
Delayed redirection of all calls to the secretary to the standard Voice Box	Select the check box if calls to the secretary are to be diverted to the voice box after a specified time. For further call forwarding settings see section **To define the call forwarding settings for a User**, page 94.

Designation	Explanation
Mutual call and status signaling	Activate the check box if you want calls and status (available, away etc.) are to be signaled mutually between Management and Secretariate. A User can pick up calls signaled to him. A User can only call another User via intercom connection or use the messenger if he or she is signaled the status of the other User.
Speed Dials of Management **Speed Dials of Secretariate**	**Leave the first Speed Dial unchanged** The first Speed Dial of the Management/Secretariate remains unchanged. **Set Management's/Secretariate's Speed Dial as the first Speed Dial** The first Speed Dial of Management/Secretariate is assigned to the other. If the key is already assigned, the previous assignment is moved to the next Speed Dial, as with all other Speed Dials. **Overwrite first Speed Dial** The first Speed Dial of Management/Secretariate is assigned to the other. If the key is already assigned, the assignment is overwritten.
Phone number of Management/Secretariate	Select from the dropdownlist the number of the Management/Secretariate with which the first Speed Dial of the other is to be assigned.

Designation	Explanation
Skin settings	**Leave SwyxIt! Skin for Management and Secretariate unchanged** The Skin of Management/Secretariate remains unchanged. **Transfer SwyxIt! Skin from Management to Secretariate** The Skin of the Management is loaded and used by the Secretariate's SwyxIt! . **Transfer SwyxIt! Skin from Secretariate to Management** The Skin of the Secretariate is loaded and used by the Management's SwyxIt! . The options for transfer are only available if the current Skins of Management and Secretariate differ. Changes made to the Skin by one User will only be adopted by the other User after a new login to SwyxServer.
Same SwyxIt! Skin	Name of the Skin used by Management and secretariate. If the field is empty, the same Skin is not used.

6 Click on **Save**.

7 In the row of the corresponding secretary relationship, click to edit the settings.

8 In the line of the appropriate secretariate relationship, click on to delete the secretariate relationship.

9.12 SETTING THE TELEPHONY SETTINGS

You can define the following telephony settings for Users:

- Call forwarding
- Call properties
- Phone numbers
- Desk Phones
- Client settings

To define the call forwarding settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on ⌄ on the right next to the User name.

4 Click on the sub-menu item **Call Forwarding** that additionally appears.

If you have permitted "Change forwardings" for a User, the User can change the settings you have defined here via Swyxlt!.

When a user is logged out, the default setting is immediate redirection to the default Voice Box.

Designation	Explanation
Forward all calls immediately	Activate the checkbox if you want all calls for the User to be immediately forwarded to the destination defined below.
Forward call to (number)	Enter the corresponding phone number or click on **Select** to select a phone number from the phone book. **Voice Box** All calls will be forwarded to the Standard Voice Box, see also step **12 Click on Standard remote inquiry.**, page 95

5 Click on **Save**.

6 Click **Delayed**.

Designation	Explanation
Forward calls after a defined time if line is idle/User is away (Call forwarding no reply)	Activate the checkbox if you want all calls for the User to be forwarded to the destination defined below after x seconds (e.g. during absence).
Forward call to (number)	Enter the appropriate phone number or click on **Select** to select the number from the phonebook. **Voice Box** All calls will be forwarded to the Standard Voice Box, see also step **12 Click on Standard remote inquiry.**, page 95
After (seconds)	Enter the number of seconds after which the call will be forwarded.

7 Click on **Save**.

8 Click on **Busy**.

Designation	Explanation
Forward calls if the line is busy	Activate the checkbox if you want all calls for this User to be immediately forwarded to the destination stipulated below if the User's line is busy.
Forward call to (number)	Enter the appropriate phone number or click on **Select** to select the number from the phonebook. **Voice Box** All calls will be forwarded to the Standard Voice Box, see also step **12 Click on Standard remote inquiry.**, page 95

9 Click on **Save**.

10 Click on **Voice Box**.

Designation	Explanation
Welcome message	Activate the checkbox to activate the welcome message settings. Select a welcome message from the dropdown list or click on to upload a .wav file.
Record voice message	Check the box to enable recording of voice messages for the user. The date format of the Voice Box depends on the language setting in the Windows operating system, i.e. a computer with the language English (United States) will also provide the American date format (mm/dd/yy) for the Voice messages.
Maximum voice message length in seconds (3-600)	Enter the maximum recording time for voice messages.
Send voice messages to the following email address	Enter the email address to which voice messages are to be sent to the User.
Starting Remote Inquiry via * button	Activate the checkbox to permit the User to start a remote inquiry for his standard Voice Box with the * key.

11 Click on **Save**.

12 Click on **Standard remote inquiry**.

Remote inquiry enables you both to listen to your voice messages and to change immediate call forwarding from any telephone.

If you have permitted "Change forwardings" for a User, the User can change the settings you have defined here via SwyxIt!.

Designation	Explanation
Use PIN for remote query	Activate the checkbox to protect the remote inquiry by a PIN.
PIN	Enter a PIN with which the User can authenticate him or herself for remote inquiry.
Confirm PIN	Enter the PIN again to confirm your entry.

13 Click on **Save**.

To set the call settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on ❮ on the right next to the User name.

4 Click on the submenu item **Call settings**.

Designation	Explanation
Hide number/URI	Activate the checkbox if you want the User's number not to be displayed to the contact person when making external calls.
Disable secondary call	Activate the checkbox if no further calls should be accepted if a line is busy.
Transfer on hook on	Activate the checkbox to permit the User to connect two call partners when hanging up. *Example:* *Subscriber A is called by C. Then subscriber A begins a second call on another line to subscriber B. When A hangs up, B and C are connected with each other.*

To edit the numbers for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on ⌄ on the right next to the User name.

4 Click on the sub-menu item **Numbers** that additionally appears.

5 Click on **Add number**.
✓ The **Add number** configuration wizard appears.
See also step **5 Define the numbers.**, page 86

To define alternative numbers for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on ⌄ on the right next to the User name.

4 Click on the sub-menu item **Numbers** that additionally appears.

5 Click on **Add alternative number**.

6 Click on **Add alternative number**.
✓ The **Select alternative number** configuration wizard appears.

7 Activate the checkbox in the line of the appropriate number and click on **Select**.
✓ The alternative number appears in the list and can be used for outgoing calls.

To define fax numbers for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on ⌄ on the right next to the User name.

4 Click on the sub-menu item **Numbers** that additionally appears.

5 Click on SwyxFax**Numbers**.
✓ The **Add number** configuration wizard appears.

Label	Explanation
Internal number	Enter a fax number under which the User is available site internally. May be preset by default: Next free number *e.g. 102*
Public number	Enter a fax number under which the User is available publicly, if applicable. Allowed format: canonical (+<country code><area code><number>) *e.g. +49 231 1234102*

6 Click on **Save**.
✓ The numbers appear in the list.

To define fax forwarding settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on ⌄ on the right next to the User name.

4 Click on the sub-menu item **Numbers** that additionally appears.

5 Click on **Fax forwarding**.

Label	Explanation
Forward faxes to the User's fax client	Activate the checkbox if incoming fax documents should be forwarded to the User's SwyxFax client.
Add email	Click on the button to add an email address to which the User's incoming faxes will be sent.
E-mail address	Enter the e-mail address of the user.

Label	Explanation
Attachment format	Select the format for fax documents. If "TIFF and PDF" is selected, the e-mail will include two attachments. Click on **Add**.
Add printer	Click on the button to select the printer to be used to print incoming fax documents. Forwarding to a printer takes place via the SwyxFax Printer Gateway.
Printer	Select the printer.
Gateway	Enter the name of the gateway via which the fax documents are forwarded to the printer. Click on **Add**.

6 Click on **Save**.

To define the CTI+ settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the sub-menu item **Numbers** that additionally appears.

4 Click on **CTI+**.

Label	Explanation
Using an external telephone via this number	Enter a number or click on ---, to select one of the User's numbers.
Forward the caller to this number, also if SwyxIt! is terminated" or CTI deactivated	Activate the checkbox if incoming calls should be forwarded to the external telephone, also if the User's computer is switched off or CTI is deactivated.

5 Click on **Save**.

9.13 SET NAME KEYS AND LINE KEYS

If you have permitted "Change User Profile" for a User, the User can change the settings you have defined here via SwyxIt!, see also **9.10 Defining rights**, page 92.

To define the number of buttons for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on ✓ on the right next to the User name.

4 Click on the sub-menu item **Keys** that additionally appears.

If you have permitted "Change User Profile" for a User, the User can change the settings you have defined here via SwyxIt!, see also **9.10 Defining rights**, page 92.

Designation	Explanation
Number of line keys	Enter the number of line keys, which should be available to the User.
Number of speed dial keys	Enter the number of name keys, which should be available to the User.

5 Click on **Save**.

6 Click on **Speed dials**.
✓ The list of speed dial keys configured for the User appears.

7 In the line of the appropriate name key, click on ✎.

If you have permitted "Change User Profile" for a User, the User can change the settings you have defined here via SwyxIt!, see also **9.10 Defining rights**, page 92.

Designation	Explanation
Labelling	Enter the name of the key you want to appear in SwyxIt!.
Number/URI	Enter a phone number or URI for the contact or select a number from the phonebook.
Dialing options	Select the dialing options for the speed dial: **Immediate Dial** Activation of the speed dial starts the call without additional actions (e.g. activation of the line key, taking the handset off the hook). **Deleting the display before dialing** Activation of the speed dial deletes any existing data in the phone number entry field. **Intercom Connection** Activation of the speed dial starts intercom connection.
Picture	Select or upload an image to be displayed on the name button: **- No picture -** No picture is used. **- Automatic -** The appropriate User picture is accessed from the SwyxWare database.
	Click on the button to search for images in your file directory and upload them.
	Click the button to delete the image.

8 Click on **Save**.

9 Click on **Line keys**..

10 In the line of the appropriate line key, click on .

If you have permitted "Change User Profile" for a User, the User can change the settings you have defined here via SwyxIt!, see also **9.10 Defining rights**, page 92.

Designation	Explanation
Labelling	Enter the name of the button you want to appear in SwyxIt!.
Use as default line	Activate the checkbox if all calls started by the User should be made via this line. This setting is only effective if the User has not activated another line key prior to this.
Incoming calls	Select which calls can be made via this line: **All calls** All incoming calls are made via the line. **Only Group calls** Only incoming calls for Groups the User belongs to are made via the line. **Using the number** Incoming calls only for a specific number of the User are made via the line. Click on ..., to select one of the User's numbers.
Outgoing calls	Click on ... to select the User's number which should be signalized when outgoing calls are made via this line. *Example:* *A User has the internal extension "225", which is allocated to the external number "+49 231 55666225" . Moreover, the User has the internal extension "325", which is allocated to the external number "+44 778 88325" . If then only "225" is selected for incoming calls, this User signalizes the number "+49 231 55666225" externally.*

Designation	Explanation
Hide number/URI	Activate the checkbox if the User's number should not be displayed to the contact person when making external calls on this line.
Disable line after call	Activate the checkbox if this line should remain busy for the defined time span following a call, for example for processing customer inquiries.
Wrap up time in seconds (5-1800)	Enter the time span for which the line will be blocked after a call.

11 Click on **Save**.

9.14 EDITING SHORTCUT KEYS

Shortcut keys allow you to access frequently used programs and websites via SwyxIt!. You can edit shortcut keys via SwyxIt! or Swyx Control Center and create additional shortcut keys via the Skin editor. See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/index.html#context/help/tab_files_$ und https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/index.html#context/help/tab_advanced_$.

To edit shortcuts

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on ⌄ on the right next to the User name.

4 Click on the sub-menu item **Keys** that additionally appears.

5 Click on **Shortcuts**.
✓ The list of all shortcut keys appears.

6 Click on the line of the appropriate shortcut key.

The value "Index" is required by the system to assign the link.

Designation	Explanation
Shortcuts	Enter the web address or the name of the program file for the shortcut.
Working directory	Optionally, enter the path to the working directory of the linked program. This specification is required if the linked program must access files that are not stored in the same location as the program.
Picture	Select or upload a picture which will be displayed on the speed dial. **- No picture -** No picture is used.
	Click on the button to search for images in your file directory and upload them.
	Click the button to delete the image.
Labelling	Enter the name of the button you want to appear in SwyxIt!.

7 Click on **Save**.

8 Click in the line of the corresponding shortcut button to delete the shortcut.

To delete several shortcuts at the same time, activate the check box in the line of the appropriate shortcut, click on **Delete several shortcuts** and confirm with **Yes**.

9.15 IMPORT/EXPORT KEY ASSIGNMENTS

The speed dials and shortcuts of individual users can be exported and/or imported.

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

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.

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).

Linked contacts are imported regardless of whether the corresponding applications are connected to SwyxIt!

To import/export key settings

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on ⌄ on the right next to the User name.

Click on the sub-menu item **Keys** that additionally appears.

4 Click on **Import/export configuration**.
✓ The configuration wizard appears **Importing/exporting the configuration**.

5 Choose whether you want to export key bindings **import** or **export** want.

6 Click on **Next**.

7 Select the Key types: Name keys and/or shortcut keys that you want to import or export.

8 When importing, select the desired .key file from your hard disk, if necessary.

9 Click on **Upload** or **Download**.

9.16 EDITING NUMBERS FOR GROUPS

If the option package SwyxMonitor is installed, an SwyxWare user (supervisor) can connect to an existing call of another SwyxWare user (call agent). The prerequisite is that the agent is on the phone with SwyxIt! (not in CTI mode). The supervisor can use any device.

Define which internal telephone numbers can be connected to calls from this agent. You can enter group numbers as well as multiple phone numbers. The permission for call intrusion applies to all call numbers of the agent.

See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/index.html#context/help/SCST

To define the user's internal telephone numbers for call intrusion

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 In the line of the appropriate User, click on >.

4 Click on **Call Intrusion**.
✓ A list of all phone numbers of the selected user enabled for call intrusion appears.

5 Click on +.
✓ A list of all phone numbers of the selected user appears.

6 Activate **internal** to display only the internal phone numbers.

7 Activate the check box next to the desired phone number(s).

8 Click on **Select**.
✓ The selected phone numbers are enabled for call intrusion and appear in the corresponding list.

9.17 DEFINING CLIENT SETTINGS FOR SELECTED USERS

You can define settings which are loaded when a User logs in to SwyxServer via SwyxIt!. The user can thus access the same SwyxIt! settings independently of the computer on which he logs in.

Defining status signaling via device

Defining settings for lists and buttons

Activating conversation recordings

To define the client settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the sub-menu item **Client Settings** that additionally appears.

If you have permitted "Change User Profile" for a User, the User can change the settings you have defined here via SwyxIt!, see also **9.10 Defining rights**, page 92.

Designation	Explanation
Allow Collaboration	Activate the check box so that the User can use Collaboration.
Call notification with tray icon for incoming calls	Activate the check box if you want incoming calls to be signalized via task bar.
Call notification in the taskbar for call signalizations	Activate the checkbox if you want signalized calls to be signalized via task bar.
SwyxIt! always on top	Activate the checkbox if you want SwyxIt! to be displayed permanently before other open applications.
SwyxIt! pop up on ringing	Activate the checkbox if you want SwyxIt! to be displayed in the foreground on an incoming call.
SwyxIt! pop up when in a call	Activate the checkbox if you want SwyxIt! to be displayed in the foreground during a call.
SwyxIt! minimize after call	Activate the checkbox if you want SwyxIt! to close automatically after a call and appear as an icon in the Windows notification area and the Windows taskbar.
Minimize to tray icon	Activate the checkbox if you want SwyxIt! to be displayed only in the Windows notification area and not in the Windows taskbar when minimized.

9.17.1 DEFINING STATUS SIGNALING VIA DEVICE

If Users are logged in to SwyxServer with different devices, you can specify which of the devices defines the status.

Example:
A User has a SwyxPhone installed on his desk and SwyxIt! installed on his workstation computer. The SwyxPhone is always logged in, the computer is only turned on when the User is at his or her workplace. It makes sense to have the login status signaled by SwyxIt! only. If SwyxIt! has not been started, the user is still able to make calls using the SwyxPhone, however, internal employees and the Call Routing receive the status "logged off". If the user is making a call using SwyxPhone, the status "Speaking" is signaled to the employees, the status "logged off" is signaled to Call Routing.

If you have permitted "Change User Profile" for a User, the User can change the settings you have defined here via SwyxIt!, see also **9.10 Defining rights**, page 92.

No more than a total of four devices of any type (SwyxIt!, Desk Phones, SIP phone, DECT device) can be simultaneously logged in to one SwyxWare user account.

The settings are loaded when a user logs on to SwyxServer via SwyxIt!. The user can thus access the same SwyxIt! settings independently of the computer on which he logs in.

To set status signaling via terminal for all users

1 In the menu, select **General Settings | System**.
Click on **Status Signaling**.
2 Activate the checkbox of the appropriate device.

You select can multiple devices.

The "Basic Client" is the Swyx Mobile app for Windows phones.

To define status signaling via device for a selected User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.
2 As administrator, click on > in the line of the appropriate user.
3 Click on the sub-menu item **Client Settings** that additionally appears.
4 Click on **Devices**.
5 Activate the checkbox of the appropriate device or activate **Use server default settings**.

9.17.2 DEFINING SETTINGS FOR LISTS AND BUTTONS

You can define the maximum number of list entries that can be saved and the actions that can be started when certain buttons are clicked.

If you have permitted "Change User Profile" for a User, the User can change the settings you have defined here via SwyxIt!, see also **9.10 Defining rights**, page 92.

To define the lists and buttons settings for a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.
2 As administrator, click on > in the line of the appropriate user.
3 Click on the sub-menu item **Client Settings** that additionally appears.
4 Click on **Lists and Buttons**.

Designation	Explanation
Shortcuts (maximum number)	Enter the number of shortcuts, which should be available to the User.
Caller list (maximum number of entries)	Enter the maximum number of entries in the User's Caller list.
Redial list (maximum number of entries)	Enter the maximum number of entries in the User's Redial list.
Automatic redial timeout in seconds	Enter seconds Enter the number of seconds between two call attempts (0 to 3600 seconds).
Standard behavior of the Voice Box Button	Select which action is started when the Voice Box button is clicked (the other option is still available via the context menu): **Launch email client** The User's standard email program appears. **Voice Box remote enquiry** The User's remote inquiry starts.

Designation	Explanation
Immediate Dial	Activate the checkbox if you want the automatic redial to start when you click the redial button. If the option is deactivated, the phone number is only entered in the input field and the User must click on the receiver or enter button.
Always use Automatic Redial	Activate the checkbox if you always want the automatic redial to start when you click the redial button. If the option is deactivated, the phone number is only entered in the input field and the User must click on the receiver or enter button.

5 Click on **Save**.

9.17.3 ACTIVATING CONVERSATION RECORDINGS

You can specify whether a user is allowed to record conversations or whether all conversations of a user are recorded. The recording files are saved in .opus or .wav format.

If you have permitted "Change User Profile" for a User, the User can change the settings you have defined here via SwyxIt!, see also **9.10 Defining rights**, page 92.

To activate recordings

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the sub-menu item **Client Settings** that additionally appears.

4 Click on **Conversation Recordings**.

Designation	Explanation
Activate Conversation Recording	Select the checkbox to allow the User to record conversations himself.
Record all conversations	Activate the checkbox if you want all of the User's conversations to be recorded.
Use server settings	Activate the check box if you want to save recording files to the server-side specified storage location, see also **14.2 Trunk Recording**, page 150.
Storage location for recordings	Enter the storage location for conversation recordings, if applicable.

9.18 EDITING USER-SPECIFIC FILES

During the SwyxWare installation, global files such as ring tones, announcements, etc. are created for all users. Furthermore, additional files can be created specifically for a user. The user can, for example, record his own greetings or create his own scripts. These user-specific files can be edited by the administrator or the corresponding user.

The files are displayed according to their assignment on the following tabs:

- Users
  User files are assigned to a single user. Only the user himself, an administrator or SwyxServer, if he e.g. executes scripts of the Call Routing Manager, have access to these files. All files created with a SwyxIt! or 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.
- User Standard
  User default files are stored as default files in the database for a specific user (e.g. central office) during installation. This user can use these files unchanged.

When a user standard is changed, the changed file is displayed on the tab **User** and will not be changed by a later SwyxWare update.

You can add, delete or save files under a different name. The total size of all files created for this user (except fax files) is specified.

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

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

To manage the user-specific files

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the submenu item **Files**.

4 Select the desired tab **User** or **User default**.
✓ A list appears with all user specific files.

5 Select the checkbox in the line of the file you want to select, then click one of the following buttons:

Designation	Explanation
	Click on the button to download the file.
	Click on the button to delete the file. You can select multiple files to be deleted.
	Click the button to edit the file properties, see **To add a file**, page 105.
>	Click on the button to display more detailed information about the file (size, date of last modification).

To add a file

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the submenu item **Files**.

4 Select the desired tab **User** or **User default**.
✓ A list appears with all user specific files.

5 Click on **Upload file**.
✓ The configuration wizard **Upload file** appears.

Designation	Explanation
...	Click the button to upload a file from your hard disk.
Name	Specify the name under which the selected file should be stored in the database.
Scope	**Users** This file should be assigned directly to the user. It is only available to the selected user. **User Standard** This file is available to all users who are logged on to this SwyxServer.

Designation	Explanation
Category	Specify the category to which this file belongs. The following categories are available: • Ringtones • Fax cover page graphics • Fax cover page • Fax Letterhead • Call Routing Scripts • Example Call Routing Scripts • Bitmaps • User pictures • Templates • Announcements • System announcements • Example announcements • Music on hold • Recordings • Skins • Other
Users	The user the file is assigned to. (This option cannot be changed.)
Description	Enter a description, if applicable.
File Properties	**Private** This file is only accessible to the user himself, e.g. in one of his scripts. *Example: Call routing script with password.* Hidden This file does not appear in the selection dropdown lists. *Example: The file '20m.wav' (twenty minutes) belongs to the time greeting and does not appear when you select a greeting message.* **System** This file was created during installation and is always read-only (this option cannot be changed)

6 Click on **Save**.
✓ The new file appears in the **User** or **User default** list.

9.19 DEFINING THE SKIN

You can define the standard Skin for Users. To select a server-wide Skin, see **4.16 Defining client settings for all Users**, page 32.

To define the standard Skin

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the sub-menu item **Client Settings** that additionally appears.

4 Click on **Skins**.

Designation	Explanation
Skin	Select the appropriate Skin from the drop-down list or click to upload a .cab file.
	Click the button to search for Skins in any WAV format on the network.
	Click on the button to delete the selected Skin.
Changing of Skins allowed	Activate the check box so that the User can change the Skin via SwyxIt!.
Editing of Skins allowed	Activate the check box so that the User can use the Skin Editor.

5 Click on **Save**.

9.20 EDITING THE CALL SIGNALING SETTINGS

You can define whether second calls and calls to other users or groups are signaled acoustically and on which devices calls are signaled.

To define call signaling settings

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the sub-menu item **Client Settings** that additionally appears.

4 Click on **Signaling**.

Designation	Explanation
Call waiting tone for secondary calls	Activate the check box if you also want call signals to be acoustically indicated by an alerting tone. See also **9.8 Defining call and status signaling**, page 90.
Attention tone for signalled calls (call pickup)	Activate the **Enable acoustic second call signaling** in order to hear the call-waiting tone in the headset when a second call is received.
Ringing of CTI devices	In the **Ringing of CTI devices** dropdown list, you can select which devices ring when SwyxIt! is operated in CTI mode: **Both devices** SwyxIt! in CTI mode and the controlled device (SwyxIt! or SwyxPhone) **Only CTI SwyxIt!** **Only controlled device (SwyxIt! or SwyxPhone)**

5 Click on **Save**.

9.21 DEFINING RING TONES

You can set individual ringing sounds depending on the caller and the User's phone number.

For information on uploading additional ringtones, see https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/index.html#context/help/tab_files_$.

To assign ringtones

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the sub-menu item **Client Settings** that additionally appears.

4 Click on **Sounds**.

Designation	Explanation
Name	Select for which calls the ringing sound is to be used: Internal calls External calls
Number/URI	Call number/URI to which the ringing sound is assigned
Sound	Currently selected ringing sound

5 Click on ✎ to select a different ringing sound.
✓ The **Ringing sound settings** configuration assistant appears.

Designation	Explanation
Call type	Internal calls External calls

Designation	Explanation
Caller's or own number / URI	Define the phone number for which the selected ringing sound is used. You have the following options: You enter the phone number of a specific caller. When this caller calls one of your phone numbers, the selected ringing sound is used. You enter one of your phone numbers. When any caller calls this number, the selected ring tone is used. You can also use placeholders for the phone number (* for multiple digits, ? for one digit).
Sound	Select the appropriate sound from the dropdown list or click on to upload a .wav file.
Pause between ringing	Enter the number of seconds to elapse before the ringing sound is played again.
	Click the button to search for ringing sounds in your file directory and upload them.
	Click the button to delete the ringing sound.
	Click the button to play the ringing sound.
	Click the button to pause the playback.
	Click the button to download the ringtone.
	Move the slider left or right to set the playback volume. The setting does not affect SwyxIt! or the devices used.
Volume	Slide the slider to the left or right to set the volume for SwyxIt! or the User's devices.

Designation	Explanation
Apply volume to all ringing sounds	Activate the checkbox to apply the selected volume to all ringing sounds.

6 Click on **Save**.

9.22 VIEW SWYX MOBILE CONFIGURATION

You can display the Swyx Mobile configuration via Swyx Control Center and call the URL to configure your Swyx Mobile Client (Easy configuration).

To configure Swyx Mobile

1 In the menu, select **User**.
✓ If applicable, a list appears with all Users.

2 In the line of the appropriate User, click on .

3 Click on **RemoteConnector**.

4 Click on or .

5 Scan the QR Code with your smartphone.

6 Android: You may need to install an app for reading QR Codes.

7 Open the link by confirming and select the Swyx Mobile App to open it.

8 Android: Enter your password under **Settings | Password** and log in under **Settings | Sign in**.

9 iOS: Enter your password, save and continue in the wizard.

See also the Swyx Mobile for iOS or Swyx Mobile for Android online help.

To display the Swyx Mobile configuration for a selected User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.
3 Click on **RemoteConnector**.
4 Click on or .

Designation	Explanation
Internal server	SwyxServer address
External server	RemoteConnector address
Server type	Determined automatically by the installation
Connection mode	**Auto (default)** The available network is automatically set **Standard** Internet
Connection type	**Business (default)** Data transmission via VoIP **Private** Data transmission via mobile network **Request** You are asked before each telephone call which connection type is to be used.
RemoteConnector mode	**Auto** An automatic attempt will be made to establish a direct connection to SwyxServer. If the connection fails, e.g. because you are outside your company network, you are connected to SwyxServer via Remote Connector. **Always** Always connects you to SwyxServer via RemoteConnector. If no connection via RemoteConnector is possible, no attempt will be made to establish a connection via your company network.

Select in the menu **General Settings | System** and click on **RemoteConnector** to display the Swyx Mobile configuration for all users.

See also the Swyx Mobile for iOS or Swyx Mobile for Android online help.

9.23 DELETING USERS

This is how you delete a User

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on in the line of the appropriate user.
3 Click on **Yes** to confirm the process.
✓ The User's numbers can be assigned elsewhere again.

10 CREATING AND EDITING GROUPS

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. Creating Groups makes it possible to contact members at a common Group number. There is a configuration wizard available to create Groups

When saving and processing personal data, observe the appropriate applicable legal data protection regulations.
If you have any questions especially regarding data protection in SwyxWare, please contact your administrator.

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

During a standard installation of SwyxServer several Groups and Users are already created.

The setting options on menu pages and in configuration wizards depend on your administration profile and your SwyxWare solution.

Creating Groups
Editing the general settings for Groups

10.1 CREATING GROUPS

To create a Group

1 In the menu, select **Groups**.
✓ A list appears with all Groups.

2 Click on **Create Group**.
✓ The **Create a Group** configuration wizard appears.

3 Define the general settings for the Group.

Designation	Explanation
Name	Enter a name for the Group.
Description	Enter a description, if applicable.
Make this Group the 'Everyone Group'	Activate the checkbox, if you want all new Users to be added to this Group by default. The function can only be activated if you have previously deactivated it in the preconfigured "Everyone" group. As a consequence, new Users no longer have access to the functionalities of the preconfigured "Everyone" group. See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/preconfigured_users_$.

Designation	Explanation
Hunt Group type	Select one of the following hunt Group types: **Parallel** Calls to the Group number are delivered simultaneously to all members. The person who accepts the call first speaks to the caller. **Random** Calls are distributed randomly within the Group, i.e. when the time specified in the **Ringing time** field is over, the next member is selected randomly from the entire Group. **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. **Sequential** The calls to the Group are delivered according to the order of the Group members. always starting with the first Group member.
Call duration (in seconds)	Specify the maximum duration of an individual connection attempt, before the call is routed to the next member of the Group.
Calls to this Group will also be delivered to MEM devices	Activate the check box if you want calls to this Group to be signalized on mobile devices. This option is only available after creating the Group, see also section **10.2 Editing the general settings for Groups**, page 113.

When making later changes to settings, click **Save** to save the settings.

4 Click on **Next**.

5 Define the numbers for the Group.

Designation	Explanation
Internal number	Enter the number under which the Group members are available site internally. May be preset by default: Next free number
Public number	Enter the number under which the Group members are available publicly, if applicable. Allowed format: canonical (+<country code><area code><number>)
Show in Phonebook	Activate the checkbox if you want the Group number to be displayed in the Global Phonebook.

When making later changes to settings, click **Save** to save the settings.

6 Click on **Next**.

7 Assign Users to the Groups:

Click on a User and then on one of the buttons >, <, to select him as a Group member or remove him from the Group.

Click on one of the buttons >> <<, to select or unselect all elements.

Click on one of the buttons ▲ ▼ to position the element higher or lower.

Use the input fields to search for names or phone numbers. Only the user's main phone number is available for the search.

When making later changes to settings, click **Save** to save the settings.

8 Click on **Next**.

9 Specify the signaling settings for calls and status (available, away, etc.).

Please be aware that call and status signaling settings are valid for a User or a Group member, not for Groups themselves. I.e. for example that a Group without members cannot signal calls to other Users or Groups.

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.

Designation	Explanation
Signalize incoming calls to	Activate the check box if you want calls to this Group or Group members to be signalized to the selected User or the members of the selected Group. A User can pick up calls signaled to him.
Status signaling to	Activate the check box if you want the Groups members' status to be signalized to the selected User or the members of the selected Group. A User can only call another User via intercom connection or use the messenger if he or she is signaled the status of the other User.
Receiving calls from	Activate the check box if you want the Group members to receive call signaling from the selected User or the members of the selected Group. A User can pick up calls signaled to him.
Receiving status signaling from	Activate the check box if you want the Group members to receive status signaling from the selected User or the members of the selected Group. A User can only call another User via intercom connection or use the messenger if he or she is signaled the status of the other User.
Dropdown list	Select the User or Group for which you want to define signaling settings.
Mutual call signaling	Activate the check box if you want the selected User or the members of the selected Group to receive call signaling from the Group. This option is only available after creating the Group, see also section **10.7 Editing the signaling settings for Groups**, page 115.
Mutual status signaling	Activate the check box if you want all members of the Group to signal their status to the other members. The Group members can call each other via intercom. This option is only available after creating the Group, see also section **10.7 Editing the signaling settings for Groups**, page 115.

10 Click on **Save**.
✓ The signaling settings for the Group are saved.

Click on one of the buttons to edit or delete signaling settings.

11 Click on **Create**.
✓ The Group appears in the list of all Groups.

10.2 EDITING THE GENERAL SETTINGS FOR GROUPS

To edit the settings for a Group

1 In the menu, select **Groups**.
✓ A list appears with all Groups.

2 In the line of the appropriate Group, click on .
See also step **3 Define the general settings for the Group.**, page 110

10.3 EDITING THE ASSIGNMENT OF USERS TO GROUPS

To edit the assignment of Users to a Group

1 In the menu, select **Groups**.
✓ A list appears with all Groups.

2 Click in the row of the corresponding group.

3 Click on **Members**.
See also step **7 Assign Users to the Groups:**, page 111

10.4 EDITING NUMBERS FOR GROUPS

To edit the numbers for a Group

1 In the menu, select **Groups**.
✓ A list appears with all Groups.

2 In the row of the corresponding group, click .

3 Click on **Numbers**.

4 In the line of the appropriate numbers, click on to edit the numbers or click on to delete the numbers.

5 Click on **Add number** to add numbers.
See also step **5 Define the numbers for the Group.**, page 111

10.5 ADDING ALTERNATIVE NUMBERS FOR GROUPS

You can define alternative numbers, which the Group members 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!/SwyxPhone. Alternative numbers are marked there by the addition Alternative number.

Example:

The administrator can allow every SwyxWare User to signal the operator's number (+492314666100) 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 add alternative numbers for a Group

1 In the menu, select **Groups**.
✓ A list appears with all Groups.

2 Click in the row of the corresponding group.

3 Click on **Add alternative number**.
✓ Click on **Add alternative number**.

Designation	Explanation
Internal number	Enter the number under which the Group members are available site internally. May be preset by default: Next free number

Designation	Explanation
Public number	Enter the number under which the Group members are available publicly, if applicable. Allowed format: canonical (+<country code><area code><number>)
Users	User or Group to whom the number is assigned

4 Click on **Select**.

5 Click on 🗑 to remove the alternative number for the Group.

10.6 SET VOICE BOX FOR GROUPS

A separate Voice Box (answering machine) can be configured for each group.

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. In addition, you can specify whether a recording of the voice message should be possible in principle when the call is routed to the group Voice Box. In addition, It can be set the maximum length of the voice message in seconds and enter the email address to which the recorded voice message should be sent.

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 the 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.

> ⚠ Please make sure that you create a script for group-based call forwarding in the Call Routing Manager (CRM). Otherwise, no group-related voice message will be recorded.

To define the Voice Box Settings for one group

1 In the menu, select **Groups**.
✓ A list appears with all Groups.

2 In the line of the appropriate Group, click on ✎.

3 Click on **Voice Box**.

Label	Explanation
Welcome message	Activate the checkbox to activate the welcome message settings. Select a welcome message from the dropdown list or click on ⇧ to upload a .wav file.
Record voice message	Check the box to enable recording of voice messages for the group. The date format of the Voice Box depends on the language setting in the Windows operating system, i.e. a computer with the language English (United States) will also provide the American date format (mm/dd/yy) for the Voice messages.
Maximum voice message length in seconds (3-600)	Enter the maximum recording time for voice messages.
Send voice messages to the following email address	Enter the email address to which voice messages are to be sent to the group.
Starting Remote Inquiry via * button	Activate the checkbox to permit the group to start a remote inquiry for his standard Voice Box with the * key.

4 Click on **Save**.

5 Click on **Standard remote inquiry**.

Remote inquiry enables you both to listen to your voice messages and to change immediate call forwarding from any telephone.

> ℹ If you have permitted "Change forwardings" for a group, the User can change the settings you have defined here via SwyxIt!.

Label	Explanation
PIN	Enter a PIN with which the User can authenticate him or herself for remote inquiry.
Confirm PIN	Enter the PIN again to confirm your entry.

6 Click on **Save**.

10.7 EDITING THE SIGNALING SETTINGS FOR GROUPS

To edit the signaling settings for a group

1 In the menu, select **Groups**.
✓ A list appears with all Groups.

2 In the row of the corresponding group, click .

3 Click on **Relations**.

4 Click on **Create Relation** or **Edit Relation**.
See also step **9 Specify the signaling settings for calls and status (available, away, etc.).**, page 112

10.8 DELETING GROUPS

To delete a Group

1 In the menu, select **Groups**.
✓ A list appears with all Groups.

2 Click in the row of the corresponding group.

3 Click on **Yes** to confirm the process.
✓ Group related settings for the Users who had been assigned to the Group are deleted.
✓ The Group numbers can be assigned elsewhere again.

11 CREATING AND EDITING CONFERENCE ROOMS

In SwyxWare the prerequisite for using the conference room feature with more than three participants is the licensing of theSwyxConference feature. See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/online_licensing_$ and https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/offline_licensing_$.

The Conference function is implemented with the help of the SwyxConferenceManager service. SwyxConferenceManager can be installed on SwyxServer or on an independent computer. See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/additional_computer_$.

When SwyxConferenceManager is installed, a User is set up that is specifically intended for operating this SwyxConferenceManager. If there is more than one SwyxConferenceManager installed, a User is created for each of them. The conferences are then distributed to the various SwyxConferenceManagers.

If a SwyxConferenceManager is activated, all Users can initiate conferences and add more than two subscribers to conferences. See also https://help.enreach.com/cpe/13.30/Client/Swyx/en-US.

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. See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/tab_rights_$.

You can create rules for this Conference Room via 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/13.30/CRM/Swyx/en-US/#context/help/create_rule_$.

In SwyxWare Advance for DataCenter and SwyxON the configured conference rooms are listed separately in the license report.

The setting options on menu pages and in configuration wizards depend on your administration profile and your SwyxWare solution.

Creating Conference Rooms

Editing numbers for Conference Rooms

11.1 CREATING CONFERENCE ROOMS

To create a Conference Room

1 In the menu, select **General Settings | Conference Rooms**.
✓ A list appears with all Conference Rooms.

2 Click on **Create Conference Room**.
✓ The **Create a Conference Room** configuration wizard appears.

3 Define the numbers for the Conference Room.

Label	Explanation
Internal number	Enter the number under which the Conference Room is available site internally. Default: Next free number
Public number	Enter the number under which the Conference Room is available publicly. Allowed format: canonical (+<country code><area code><number>)
PIN	Enter a PIN which every participant needs to enter the conference room.

When making later changes to settings, click **Save** to save the settings.

4 Click on **Save**.
✓ The Conference Room is displayed in the list of Conference Rooms.

11.2 EDITING NUMBERS FOR CONFERENCE ROOMS

To edit the numbers for a Conference Room

1 In the menu, select **Conference Rooms**.
✓ A list appears with all Conference Rooms.

2 In the line of the appropriate Conference Room, click on .
See also step **3 Define the numbers for the Conference Room.**, page 116

11.3 DELETING CONFERENCE ROOMS

To delete a Conference Room

1 In the menu, select **Conference Rooms**.
✓ A list appears with all Conference Rooms.

2 In the line of the appropriate Conference Room, click on .

3 Click on **Yes** to confirm the process.
✓ The Conference Room is deleted.
✓ The Conference Room numbers can be assigned elsewhere again.

To delete several Conference Rooms at the same time, activate the check box in the line of the appropriate conference room, click on **Delete several conference rooms** and confirm with **Yes**.

12 DEVICES

With SwyxWare you can use the following hardware devices:

Certified SIP phones

DECT phones

SwyxPhones

See also **4.6.1 Displaying the administrative password for Desk Phones**, page 21

12.1 CERTIFIED SIP PHONES

Via Swyx Control Center you can create Swyx certified SIP devices to make them available to the users in your local network. Proceed in the following order:

1 Optional: Prepare user-specific file for Yealink phone provisioning, see **12.1.1 Customer-specific configuration of multiple phones**, page 119

2. Optional: Preparing Yealink devices for the 802.1X authentication, see **12.1.2 802.1X authentication of Yealink devices in the SwyxWare environment**, page 122

3. Create a desk phone object in the system, see section **12.1.3 Creating Desk Phones**, page 124.
   After creation the devices are detected by SwyxServer.

4. Connecting Desk Phones,
   see **12.1.4 Activating Desk Phones once**, page 126,
   see **12.1.5 Log in/out Desk Phones**, page 126,
   see also https://help.enreach.com/docs/quickstarts/english/quickstart_Yealink_T4xS.pdf

5. Optional (SwyxON only): Using Yealink desk phones outside the customer network, see **12.2 Connect desk phones to UC Tenants via the Internet**, page 130

If you connect the device to the network before the desk phone object has been created in Swyx Control Center, the logon prompt may not during the inital operation. The desk phone object is not detected by SwyxServer.
After you have created the desk phone object, you can trigger the restart of the device as well as the logon prompt via "Reboot" or by briefly disconnecting the device from the power supply.

After putting the device into operation, the current firmware and user configuration data are transferred from the server.

See also https://service.swyx.net/hc/en-gb/articles/360000868680-Technical-background-information-about-DCF-Yealink-Phones (you may need to be logged in to Swyx Help Center to view the content).

Certified SIP devices are not supported in the standby scenario (Swyx-Standby). Certified SIP devices cannot log on to the standby server. If Desk Phones are processed on the standby system, this may result in disturbances on the master system.

For the provisioning of the Desk Phones it is necessary that the IP address of SwyxServer can be resolved in the local network.
If there is no name resolution (DNS) in your network, enter the current IP address of SwyxServer in the Windows Registry on the computer where SwyxServer is installed.
(HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Swyx\General\CurrentVersion\Options\LocalIPAddress)

If the provisioning of phones cannot be performed via multicast due to the network infrastructure, you can also distribute the provisioning URL (e. g. http://172.20.1.1:9200/ippbx/client/v1.0/device/provision/) via DHCP Option 66.

The setting options on menu pages and in configuration wizards depend on your administration profile and your SwyxWare solution.

12.1.1 CUSTOMER-SPECIFIC CONFIGURATION OF MULTIPLE PHONES

By default, device settings that are not SwyxWare-specific are not taken into account at the automatic provisioning. In this case, these settings must be made by the user on the phone or via the web interface.

With a provisioning file, you can distribute the desired settings (also for SwyxWare) to multiple Yealink phones immediately at provisioning or at a later time.

Settings can be addressed to all Yealink devices, to selected device types, or to individual devices.

As not all combinations of SwyxWare settings and device manufacturer settings can be tested, only standard functions of SwyxWare can be guaranteed.
Test your settings on a single device first and limit yourself to necessary changes. Make sure your information is correct and use only settings that do not affect the functionality of the system.

Customer-specific provisioning file

You can create a file in the format of a typical Yealink provisioning file.

The data in this file supplements or overwrites the SwyxWare settings. Name the file "common.cfg" or "mac.cfg" and upload it to the SwyxWare. Once the file is uploaded, SwyxWare will distribute the new settings to the targeted phones, see **12.1.1.2 Provisioning file upload**, page 121.

File Format

The file consists of header line(s) and parameter lines. A header controls the application of the subsequent parameters:

Specifications before the first header line have no effect on the phone settings. You can use this area for your comments.
In addition, all lines below the header and beginning with "##" are also considered comment lines.

Here is an example of the file:

```
##+==================================================+
##| ~~~~~~ e.g.: Network: NB45 ~~~~~~~~~~~~~~~~~~~ |
##| ~~~~~~ e. g.: Provisioning on 28.09.24 ~~~~~~ |
##+==================================================+

##< And here are more comments... >

##--boundary---mode:default---models:T53W
## and here another comment
static.my.parameter1=value1
static.my.parameter2=value2
static.my.parameter3=value3
##--boundary---mode:overwrite---models:T57W,T54W
static.my.parameter1=value1
static.my.parameter2=value2
static.my.parameter3=value3
##--boundary---mode:default---devices:805ec07f962a
static.my.parameter1=value1
static.my.parameter2=value2
static.my.parameter3=value3
```

Header value	Explanation
`##--boundary`	Default start of a header
`---mode:`	Application mode: **default** The parameters after this header are only added if they have not already been set by SwyxWare. **overwrite** The parameters after this header will be added and may overwrite the possibly existing parameters from SwyxWare.

`---models:`	Specification of the device type:
	`---models:T57W`
	or, to address multiple models:
	`---models:T54W,T57W`

Header value	Explanation

`---devices:`	MAC address of the device:
	`---devices:805ec07f962a`
	
	or, to address multiple devices:
	`---devices:805ec07f962a,805ec07f962b`

It is recommended to use the "---overwrite" application mode only in exceptional cases.

The options "---models:" and "---devices:" cannot be put together in one header.
If neither "---models:" nor "---devices:" is specified, the setting affects all Yealink phones in your network.

Overlaps in the configuration

If the same parameter is repeated under multiple headers with different values, the value under the most specific header is used for the provisioning phone. This results in the following validity priority:

1 Device-specific header with the lowest number of devices.

```
##--boundary---mode:default---devices:805ec07f962a
static.my.parameter1=value1
##--boundary---mode:default---devices:805ec07f962a,805ec07f962b
static.my.parameter1=value2
```

In this case, "value1" is written on device 805ec07f962a, although this device is listed in the other header along with another device.

2. Type-specific header with the lowest number of device types

```
##--boundary---mode:default---models:T53W,T57W
static.my.parameter1=value1
##--boundary---mode:default---models:T53W
static.my.parameter1=value2
```

In this case, "value2" is adopted on all T53W devices, although this device type is listed in the other header together with another device type.

3. Header without device or type specification

```
##--boundary---mode:default
static.my.parameter1=value3
##--boundary---mode:default---models:T53W,T57W
static.my.parameter1=value2
##--boundary---mode:default---devices:805ec07f962a
static.my.parameter1=value1
```

In this case the device with the MAC address 805ec07f962a receives the value "value1". The device types T53W and T57W receive the value "value 2". All other phones get the value "value3".

The order of the headers and parameters is irrelevant for prioritization. If there are headers with the same applicable device or type number, you should define the headers so that the parameters are uniquely assigned to the phones.

12.1.1.1 APPLICATION EXAMPLE:

The following are examples of configurations that solve a specific task:

Task 1

Using the Estos directory (192.168.178.96:712) as phonebook for all Yealink phones, instead of the global phonebook of SwyxWare.

```
##--boundary---mode:overwrite

## LDAP
ldap.base = CN=Directory,O=estos
ldap.port = 712
ldap.host = 192.168.178.96
ldap.customize_label = Estos Directory
ldap.tls_mode = 2
ldap.ldap_sort = 1
ldap.display_name = %cn
```

```
ldap.numb_attr = ipPhone telephoneNumber otherIpPhone
otherTelephone
ldap.name_attr = cn
ldap.number_filter =
((telephoneNumber=%)(otherIpPhone=%)(otherTelephone=%))
ldap.name_filter =
(|(&(cn=*%)(ipPhone=*))(&(cn=*%)(telephoneNumber=*)))
```

Task 2

Display of the company logo on the display of all phones of type T57W, T53, T53W.

The graphic files must comply with Yealink's format specifications:

- T53(W): 800x480 - 16bit color, file.jpg
- T57W: 360x160 - 2 color grey scale, file.dob

The files must be available on the local network, e.g.:

http://fileserver.example.com/logo_colored.jpg

http://fileserver.example.com/logo_monochrome.dob

```
##--boundary---mode:default---models:T57W
wallpaper_upload.url = http://fileserver.example.com/
logo_colored.jpg
phone_setting.backgrounds = logo_colored.jpg

##--boundary---mode:default---models:T53W,T53
wallpaper_upload.url = http://fileserver.example.com/
logo_monochrome.dob
phone_setting.lcd_logo.mode = 2
```

Task 3

Change URLs for uploading 802.1x certificates, see also **Changing the certificate URL**, page 123.

You can use the following parameters to specify the URLs for 802.1x certificates.

The root certificate and client certificates for each phone must be available on the local network, e.g.:

http://fileserver.example.com/ca_cert.pem

http://fileserver.example.com/client_cert_805ec07f962a.pem

http://fileserver.example.com/client_cert_805ec07f962b.pem

http://fileserver.example.com/client_cert_<MAC Adresse>.pen

etc.

```
##--boundary---mode:default---devices:MAC805ec07f962a
static.network.802_1x.root_cert_url = http://
fileserver.example.com/ca_cert.pem
static.network.802_1x.client_cert_url = http://
fileserver.example.com/client_cert_805ec07f962a.pem

##--boundary---mode:default---devices:MAC805ec07f962b
static.network.802_1x.root_cert_url = http://
fileserver.example.com/ca_cert.pem
static.network.802_1x.client_cert_url = http://
fileserver.example.com/client_cert_805ec07f962b.pem
```

12.1.1.2 PROVISIONING FILE UPLOAD

Uploading the provisioning file starts a new provisioning of the corresponding phones.

Depending on the set parameters, it may happen that the newly configured phone restarts.

You can upload the file in one of the following ways:

- In the SwyxWare administration (MMC), see https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/addFiles_$
  Verify that the **DCF Custom Provisioning** file category is correctly recognized by the system.
- With the following command of the SwyxWare PowerShell module:
  ```
  Import-IpPbxDCFCustomProvisioningFile -FilePath
  C:\<directory>\common.cfg
  ```
- In Swyx Control Center:

How to upload the provisioning file in Swyx Control Center

The provisioning file ("common.cfg" or "mac.cfg") is located in your file system.

1. In the menu, select **General Settings | Files**.
2. Select the **Global** tab.
   ✓ The list of SwyxWare system files appears.

3 Click on **Upload file**.
✓ The configuration wizard **Upload file** appears.

4 Click ... and select the desired provisioning file.
✓ **DCF Custom Provisioning** appears in the **Category** field.

5 Click on **Save**.

12.1.1.3 REMOVE CUSTOMER-SPECIFIC SETTINGS

If you want to remove the provisioning file settings from phones, you must delete the provisioning file in SwyxWare.

Deleting the file starts a new deployment of the phones. The default SwyxWare settings will be restored.

When deleting the file, make sure that the category **DCF Custom Provisioning** is correct. There are files of the same name of other categories.

To delete the provisioning file

1 In the menu, select **General Settings | Files**.

2 Select the **Global** tab.
✓ The list of SwyxWare system files appears.

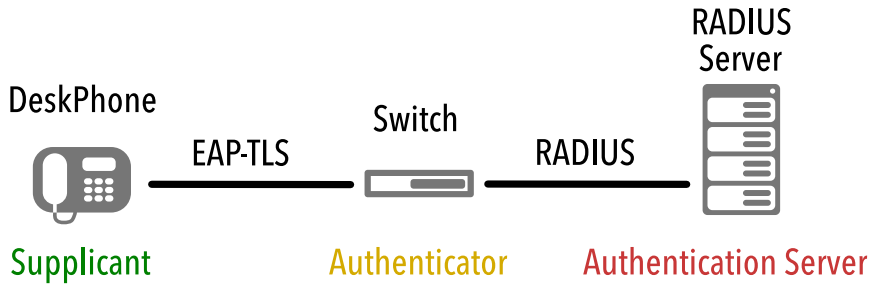
3 In the line of the corresponding .cfg file with the **DCF Custom Provisioning** category, click 🗑.

4 Click on **Yes** to confirm the process.
✓ The file is deleted. The Yealink phones are provisioned with the changed settings.

12.1.2 802.1X AUTHENTICATION OF YEALINK DEVICES IN THE SWYXWARE ENVIRONMENT

If you use certified SIP devices from Yealink, you have the option of further protecting access to your network.

The connected end devices can authenticate themselves via 802.1x protocol. Authentication against the authentication server is performed on Layer 2 (OSI).



Configuration on devices

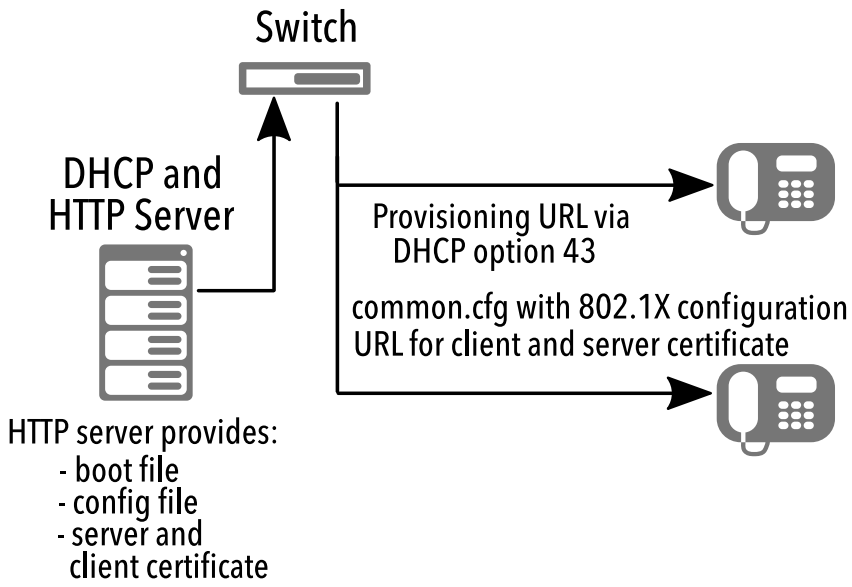
The Yealink devices must be configured to use the IEEE 802.1X protocol.

Refer to the manufacturer's documentation at http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage for details of the appropriate configuration.

Select <Terminal Model> | User & Administrator | Yealink 802.1X Authentication_VX_X.pdf.

Provisional provisioning network

If you are using a certificate-based authentication protocol such as EAP-TLS, you should set up an Initial Provision Network to upload certificates and configuration files to the endpoints. Further information can be found in the manufacturer documentation mentioned above.

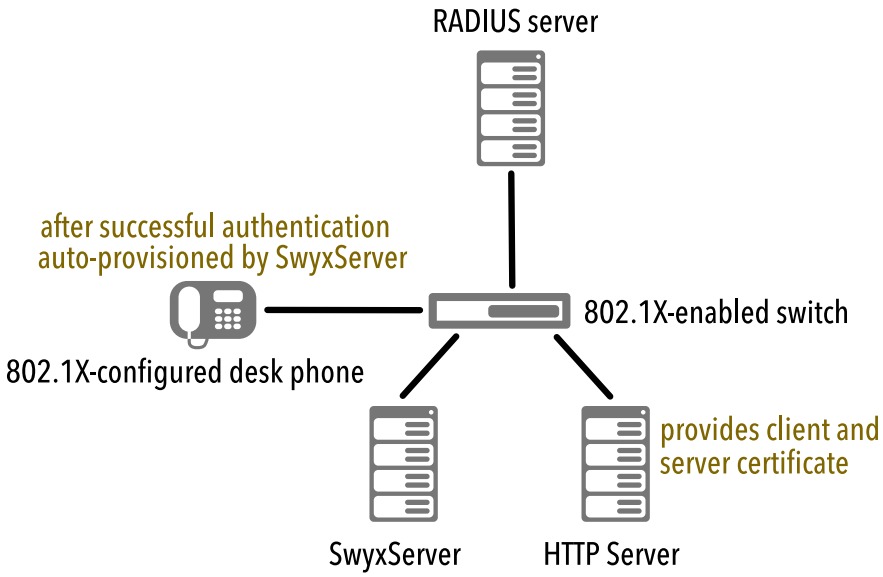


The required configuration files are provided via HTTP server for downloading by the mobile devices. Make sure that the corresponding server URL is made known to the end devices via DHCP option 43.

The URL for root and client certificate is noted in the configuration file, see also **Changing the certificate URL**, page 123.

Company network with 802.1X authentication

After the configuration files have been downloaded to the end devices and the certificates installed, the end devices are ready for authentication in the 802.1X-protected network. After 802.1X network authentication, endpoints are automatically configured via DCF provisioning service to SwyxWare.



Changing the certificate URL

In some cases, e.g. in case of changes in the network infrastructure, it may be necessary to change the certificate URL afterwards.

> While the configuration is being updated, the telephony function on the corresponding Desk Phones is not available for some time.

To change the certificate URL using a provisioning file

See **12.1.1 Customer-specific configuration of multiple phones**, page 119 und **Task 3**, page 121

To change the certificate URL via Swyx PowerShell module

The connection to SwyxServer must be established.

1 Start the Swyx PowerShell module.

2 Extract the existing configuration from the SwyxWare database in a local folder with the following command:

```
Export-IpPbxYealinkConfigFile -Path <your local path>
```

for example

```
Export-IpPbxYealinkConfigFile -Path C:\
```

3 Open the configuration file "common.cfg" in a text editor.

4 Add the following lines to the end of the file:

```
static.network.802_1x.root_cert_url = <URL for the server
certificate>
static.network.802_1x.client_cert_url = <URL for the client
certificate>
```

for example

```
static.network.802_1x.root_cert_url =   http://192.168.2.51/
ca_cert.pem
static.network.802_1x.client_cert_url = http://192.168.2.51/
client_cert.pem
```

5 Save the file.

6 Import the file via Swyx PowerShell module with the following command:

```
Import-IpPbxYealinkConfigFile -FilePath <full path of the modified
configuration file>
```

for example

```
Import-IpPbxYealinkConfigFile -FilePath C:\common.cfg
```

7 Confirm the execution of the command.

According to the autoprovisioning schedule, the new configuration file is uploaded to the end devices.

After the certificates have been downloaded, the end devices are restarted and re-registered.

12.1.3 CREATING DESK PHONES

To allow users of to use certified desktop phones, you must enter the appropriate MAC addresses in Swyx Control Center.

As of SwyxWare V13.30, a certified SIP device (desk phone or DECT) can only be assigned to a user with a system telephone license.
Yealink devices also require the Feature Pack for Certified SIP phones.

Keep the MAC addresses for the corresponding end devices on hand.

To create a Desk Phone

1 In the menu, select **Devices | Desk Phones**.

2 Click on **Create Desk Phone**.
✓ The **Create Desk Phone** configuration wizard appears.

If you have not set a User PIN on Desk Phone for the User, he cannot log on or off independently.

Designation	Explanation
Users	If applicable, select the User for whom the device should automatically be logged on or choose **Unassigned** - a User must log in to use the device and configure it via Swyx Control Center, see **12.1.5 Log in/out Desk Phones**, page 126.
MAC-adress	Enter the MAC address of the Desk Phone *e.g. a1:c2:e3:f4:11:12*
User-PIN on Desk Phone	If applicable, enter a number with which the User can log in to the Desk Phone. (User PIN on Desk Phone)

Designation	Explanation
Notify User	Check the box if you want the user to receive a welcome email with their credentials. Prerequisite: An email address is stored for the User in Swyx Control Center, see also section **9.4 Editing Users' general settings**, page 89.

3 Click on **Create**.
✓ The device appears in the list **Assigned certified phones** or **Unassigned certified phones**.

If you did not activate the option "Notify User" when creating or assigning the Desk Phone objects, you should notify the Users of the required activation and login data by other means:
- The 8-digit activation key can be found in the menu under **Desk Phones | Unassigned certified phones** in the line of the appropriate device.
- The internal number of a user can be found in the user list.
- You can find or set the User-PIN on Desk Phone under **Users | <User Name> | Desk Phones | SwyxPhone**, see **12.4.1 editSwyxPhones**, page 143.

12.1.3.1 IMPORTING DESK PHONES

As an alternative to creating Desk Phone objects in Swyx Control Center, you can import a .CSV file with the MAC addresses of the Desk Phones.

For a User to be able to use a Desk Phone, you must enable its use in his or her user settings, see also **12 Define the Desk Phone settings.**, page 88

MAC addresses must be unique within SwyxWare.

The MAC addresses must be one below the other.

The .CSV file may contain a maximum of 100 entries.

To import Desk Phones

1 In the menu, select **Devices | Desk Phones**.
2 Click on **Import Desk Phones**.
✓ The **Import Desk Phones** configuration wizard.
3 Click on **Select file** and on **Upload** to upload a file from your file system.

Click the cross icon to remove the file from the selection.

4 Click on **Next**.
5 If applicable, select a User to log on to the device, see **12.1.5 Log in/out Desk Phones**, page 126.

Designation	Explanation
MAC-adress	MAC address of the appropriate Desk Phone
Users	If applicable, select the User for whom the device should automatically be logged on or choose **Unassigned** - a User must log in to use the device, see **12.1.5 Log in/out Desk Phones**, page 126.
Assigning Users	Click on the button to import the listed Desk Phones.

6 Check if all entries have been imported.
If the import fails, you can adapt the erroneous lines or create the appropriate Desk Phones separately in Swyx Control Center, see also section **12.1.3 Creating Desk Phones**, page 124.

7 Click **Finish**.
✓ The Desk Phones have been registered in the system according to the import result and appear in the list **Assigned certified phones** or **Unassigned certified phones**.

12.1.4 ACTIVATING DESK PHONES ONCE

If you have activated the **Activation required on certified phones** (see **Activation required for certified phones**, page 21), all certified SIP devices must be authenticated the first time they connect to the network.

The following entries must be made on the device during initial startup:

Activation	Entries on the device
Activation required	• Internal number in the **User Name** field • 8-digit activation key in the **Password** field

If you have not selected the **Activation required** option, certified SIP phones are activated immediately when they are connected to the network.

When a desk phone is activated and connected to the network, it can be in the following states:

You have assigned the desk phone to a user.	The desk phone is registered to the assigned user.
The desk phone in not assigned.	The display shows the message **Logged off**. Press **Log In** to call up the login dialog.

Log in/out Desk Phones

12.1.5 LOG IN/OUT DESK PHONES

Every User can log on to a logged off certified SIP decive (Hot Desking). As an administrator, you can log off the logged in device or assign it to another user; the desk telephone is then automatically logged on for this user.

If you have not set a User PIN on Desk Phone for the User, he cannot log on or off independently.

For Hot Desking, the following steps may be necessary to use the device:

Device status	Configuration in Swyx Control Center	Entries on the device
logged off	Administrator assigns the Desk Phone to the User	none (Desk Phone is logged on automatically)
	none	• Press "Log In" • Internal phone number in the "Internal number" field • User-PIN on Desk Phone in the "PIN" field
logged in	Administrator assigns the user	none (Desk Phone is logged off)
	none	Press "Log Out"
	Administrator reassigns the User	none

To assign a Desk Phone to a User

1 In the menu, select **Devices | Desk Phones**.
2 Click on **Unassigned certified phones**.
3 In the line of the appropriate Desk Phone, click on ⇨|.
✓ The **Assign Desk Phone** configuration wizard appears.
4 Select the User from the dropdown list.
5 If applicable, click on **Create PIN**.
6 If applicable, activate **Notify User** if you want the User to receive a welcome email with his login data.

7 Click on **Assign Desk Phone**.
✓ The Desk Phone is logged on to the desired User and appears in the **Assigned certified phones** list.

To log off a Desk Phone in Swyx Control Center

1 In the menu, select **Devices | Desk Phones**.
✓ The **Assigned certified Desk Phones** list appears.

2 In the line of the appropriate Desk Phone, click on 🗑 .

3 Click on **Move Desk Phone**.
✓ The device is logged off and appears in the list **Unassigned certified phones**.

A User can log on to the device.

To reassign a Desk Phone in Swyx Control Center

1 In the menu, select **Devices | Desk Phones**.
✓ The **Unassigned certified phones** list appears.

2 In the line of the appropriate Desk Phone, click on ⇨|.
✓ The **Reassign Desk Phone** configuration wizard appears.

3 Check the current User's data and select the desired User from the dropdown list **New User**.

4 If applicable, click on **Create PIN**.

5 If applicable, activate **Notify User** if you want the User to receive a welcome email with his login data.

6 Click on **OK**.
✓ The Desk Phone is logged on to the desired User and appears in the **Assigned certified phones** list.

12.1.6 EDITING SETTINGS FOR CERTIFIED DESK PHONES

You can edit the following settings for Desk Phones:

- Assigning functions to function keys (e.g. name keys, number keys)
- Assigning contacts to name keys
- Copying function key assignment from a different Desk Phone

Do not assign the function keys directly on the device. Otherwise, configuration errors may occur.
The configuration may only be done via Swyx Control Center.

The user's settings for a certified Desk Phone can only be edited if the user is logged on to the appropriate device.

NUMBER KEYS

If several internal numbers (including group numbers and alternative numbers) are configured for a User in his SwyxWare account, a corresponding function key with the "Internal numbers" function can be configured for each number.

- Incoming calls to the assigned numbers are highlighted on the key. This function is not available on a key module.
- Outgoing calls from the assigned number can be initiated via this key

Maximum quantity of numbers

On Yealink devices the maximum number of own numbers is limited. Only the first 5 numbers of a user account are supported on the T41S, and the first 9 numbers of a user account on the T42S, T46S and T48S models.

The numbers are used by the system according to the following prioritisation on Desk Phones:

1. All own numbers
2. All group numbers
3. All alternative numbers

The numbers which are outside the maximum quantity cannot be used on devices.

Example

For a User, 101, 102, 103, 104 are defined as own numbers in his user account. He is a member of a group with the number 200. His alternative number is 118. So he has 6 numbers in total.

On Yealink T41S, no number key should be assigned the number 118.

If you have configured call number keys and the user has not selected a specific call number when making a call, the system uses his/her first internal call number.
Exception:
A different default line is configured in the SwyxIt! settings.

You can only edit logged on Desk Phones.
The configuration applies to the logged in user and is stored in his SwyxWare account.
When another user logs on to the device, its key configurations is loaded.

In the list of all certified Desk Phones, the phone's current firmware appears under **Versions**, see also section **4.15 Distributing software to clients or devices**, page 30.

To assign function keys

1 In the menu, select **Devices | Desk Phones**.
✓ A list appears with all Desk Phones.

2 In the line of the appropriate Desk Phone, click on .
✓ The configuration assistant **Edit Desk Phone for User...** appears.

Designation	Explanation
Button no.	Number of the assignable button in accordance with the numbering accepted. The adopted numbering of the function keys runs from the top to the bottom of the Desk Phones, visible marking doesn't exist.
Labelling	Label which appears next to the function key on the LCD
Function	Select the function which you want to assign to the key. If you select **Speed dial**, the appropriate input fields **Index** and **Number** as well as the **Edit option are** activated, see **To assign a Speed Dial**, page 128.

3 Click on **Save all**.
✓ The changes are saved and updated on the Desk Phone.

To assign a number key

If you assign a number key with a number that is outside the maximum quantity of own numbers for this device (see **Maximum quantity of numbers**, page 127), the first number of the user account is used on the key.

1 In the menu, select **Devices | Desk Phones**.
✓ A list appears with all logged on Desk Phones.

2 In the line of the appropriate Desk Phone, click on .
✓ The configuration assistant **Edit Desk Phone for User...** appears.

3 In the line of the appropriate key, select the function **Internal number**.

4 Click on .
✓ All of the user's own (also group and alternative) numbers appear.

5 Activate the checkbox in the line of the number which should be assigned to the key, and confirm with **Select**.

6 Click on **Save all**.
✓ The changes are saved and updated on the Desk Phone.

To assign a Speed Dial

1 In the menu, select **Devices | Desk Phones**.
✓ A list appears with all Desk Phones.

2 In the line of the appropriate Desk Phone, click on ✎.
✓ The configuration assistant **Edit Desk Phone for User...** appears.

3 Select the **Speed dial** option from the dropdown list.

4 Select the number for the intended speed dial under **Index**.

The "Index" number is used to allocate the Speed dial in the User account and does not determine the sequence of speed dial keys on the Desk Phone.

5 Click on ✎ in the line of the speed dial selected.

The settings for the selectable options and the User picture are only relevant for SwyxIt! or SwyxPhone Lxxx.

Designation	Explanation
Labelling	Enter the display name for the appropriate speed dial.
Number/URI	Enter the number which is selected via the speed dial. The corresponding labelling is entered automatically.
...	Or: Select a User from the phonebook via the button.
Dialing options	Activate the appropriate options, if applicable: **Immediate Dial** Confirmation of the speed dial starts the call. **Deleting the display before dialing** The display is deleted before dialing. **Intercom Connection** Confirmation of the speed dial starts intercom connection.
User's picture	Select whether a User picture will be displayed and upload a file from your file system, if applicable. **Automatic** The User picture is ´transmitted by SwyxServer.

To add a key module

1 In the menu, select **Desk Phones**.
✓ A list appears with all Desk Phones.

2 In the line of the appropriate Desk Phone, click on ✎.
✓ The configuration assistant **Edit Desk Phone for User...** appears.

3 Click on **Add key module**.

4 Select the appropriate key module type from the dropdown list.

5 Click on **Add key module**.

6 Select from the appropriate key's dropdown list the appropriate function.

7 Click on **Save all**.

To copy function key assignment from another Desk Phone

Only the function keys will be copied. The user-specific content of the key assignment is not taken into account during the copying process.

For example, user A has assigned the key with the "Index" number #1 as a name key in his user account. The name key #1 has been configured for dialing the phone number 101. On the desk telephone X, the third function key is set up as name key #1. The logged-in user A can dial 101.
The key configuration of desk phone X has been copied to desk phone Y.
The name key #1 has been configured for dialing the phone number 215. He can dial 215 via the third function key of the desk phone Y.

1 In the menu, select **Devices | Desk Phones**.

2 In the line of the appropriate Desk Phone, click on ✎.

3 Click on **Copy settings from another Desk Phone**.

4 Activate the checkbox in the line of the appropriate Desk Phone.

5 Click on **Copy**.

6 Click on **Save all**.
✓ The function key assignment is copied and saved.

12.1.7 DELETING DESK PHONES

You can delete logged on and logged off certified SIP devices.

To delete a logged off Desk Phone

1 In the menu, select **Devices | Desk Phones**.
Click on **Unassigned certified phones**.

2 In the line of the appropriate Desk Phone, click on 🗑.

3 Click on **Yes** to confirm the process.
✓ The Desk Phone is deleted and can no longer be used.

To delete a logged off Desk Phone

1 In the menu, select **Devices | Desk Phones**.

2 In the line of the appropriate Desk Phone, click on 🗑.

3 Click on **Delete Desk Phone**.
✓ The Desk Phone is deleted and can no longer be used.

12.2 CONNECT DESK PHONES TO UC TENANTS VIA THE INTERNET

Certified SIP phones can be used outside the company network with UC Tenants (SwyxON). For example, desk phones can be used in a branch office that is not connected via the SwyxON VPN or by a user working at home.

The SwyxWare functionality of the desk phones is not affected.

This functionality is guaranteed by the free "Swyx RemoteConnector for Yealink" option.

The Swyx RemoteConnector for Yealink supports the Swyx-certified Yealink T31G phones, the T5 series and the CP9x5 conference phones.
If the technical requirements are met, older devices from the T4S and CP9x0 series can also be connected. The requirements are design-related and apply to all devices produced before January 1, 2019.
The Enreach Helpcenter article describes how to identify suitable phones: service.swyx.net/hc/articles/12113156639644

Up to 20 devices are supported in RemoteConnector mode on one UC Tenant.

Requirements:

1 The SwyxON service provider must install the Solution AddOn "Swyx RemoteConnector for Yealink" for your UC Tenant, see help.enreach.com/swyxon/1.00/Partner/Swyx/en-US/#context/help/solution_addOn_$
Once the add-on has been successfully installed, the following input fields will appear on your UC Tenant under **General Settings | System | Provisioning**:

Field name and input value	Explanation
Swyx RemoteConnector for Yealink endpoint e.g.: rcfg01.host.name:2201	The public endpoint via which desk phones that are activated for RemoteConnector can reach SwyxWare. In addition to the public endpoint, the desk phones must also be able to reach Swyx RPS (https://phone.swyx.com) and Yealink RPS (https://dm.yealink.com) via port 443.
Swyx RemoteConnector for Yealink setup status Available	The RemoteConnector for Yealink is installed and active.

2. Corresponding desk phone objects must be created in the system, see section **12.1.3 Creating Desk Phones**, page 124.

3. Corresponding desktop phones must be enabled for connection via the Internet, see **12.2.1 Activate desk phones for RemoteConnector**, page 130.

12.2.1 ACTIVATE DESK PHONES FOR REMOTECONNECTOR

You can activate existing desk phone objects for the RemoteConnector for Yealink, e.g. for devices that have already been installed for SwyxON VPN, or create new desk phone objects for devices that are not yet in use.

You can deactivate the desk phone again and use it in the local company network, see **How to switch a desk phone to SwyxON VPN**, page 131.

To activate a desk phone for the RemoteConnector

You have created a desk phone object for the device that is to be used in RemoteConnector mode or there is a desk phone that currently active in the company network.

1 In the menu, select **Devices | Desk Phones**.
   ✓ The list of all desk phones appears.
   ✓ If the Solution AddOn "RemoteConnector for Yealink" is installed, the **RemoteConnector column** appears in the list of desk phones:

RemoteConnector status	Explanation
Activated	The desk phone has been activated for the RemoteConnector and can now be used outside your network.
Deactivated	The desk phone is not activated for the RemoteConnector and can be assigned to a user in the local office.
Not supported	The desk phone does not support the RemoteConnector function.
Initializing	The desk phone is currently being activated for RemoteConnector.
Failed	The attempt to activate the desk phone for RemoteConnector has failed.

2 In the line of a deactivated desk phone (status **Deactivated**), click on .
   ✓ The RemoteConnector status changes to **Initializing** and then to **Activated**.
   ✓ The corresponding device can connect to SwyxWare via the Internet, see the next section.

To connect an activated desk phone via RemoteConnector

You have activated the desk phone for the RemoteConnector for Yealink.

1 Connect the device to the power supply and the network.
or
1 Press and hold the OK button to perform a restart.
   ✓ The desk phone restarts and is made available for SwyxWare. The required data is downloaded. In the meantime, the desk phone restarts again. The "V" symbol then appears in the status bar at the top of the screen.
   ✓ A secure connection to SwyxWare has been established.

How to switch a desk phone to SwyxON VPN

The desk phone has been activated for RemoteConnector for Yealink and should now be used again via the SwyxON VPN.

1 In the menu, select **Devices | Desk Phones**.
   ✓ The list of all desk phones appears.
2 In the line of an activated desk phone (status **Activated**), click on .
3 Confirm with **Yes**.
   ✓ RemoteConnector status changes to **Deactivated**.
   ✓ The corresponding device can no longer be connected to SwyxWare via RemoteConnector for Yealink.

It may be necessary to perform a factory reset on the device before this desk phone can be connected to SwyxWare via the SwyxON VPN.

12.3 DECT PHONES

You can connect SwyxPhones of the DECT 800 series in your local network with SwyxServer/NetPhone.

There are two different variants for the provision and activation of DECT 800 systems:

Provisioning in Swyx Control Center via DCF for DECT

(Available as of SwyxWare/NetPhone 13.00)

This variant is described in this chapter. It is simpler, takes less time and additionally offers the following DCF for DECT functionality:

- Access to the Global Phonebook
- Easy switching of the CTI+ mode
- Call pick-up
- Synchronization with SwyxWare user account:
  - Call Journal
  - Speed dial keys

If you use or want to use your DECT system in combination with "Unite", you must configure the DECT system conventionally and do without the DCF-based functions.

The following functions are currently not available within the DCF deployment, but can subsequently be configured manually via the base station's administration web interface:
- Provisioning of IP DECT gateways,
- Set up more than one Synch Region,
- Connection of base stations from other subnets, see **12.3.1.6 Configure subnet base stations (optional)**, page 137

See **12.3.1 DCF DECT system put into operation**, page 132.

Conventional configuration (without DCF) of all individual DECT components

You must choose this variant if you absolutely want to use the following functions:

- Mirror function support
- A hybrid scenario with extensions or "Unite" functionality enabled.

The detailed documentation for the conventional configuration can be found at:
help.enreach.com/docs/manuals/english/SwyxDECT800.pdf

12.3.1 DCF DECT SYSTEM PUT INTO OPERATION

To connect a DCF DECT system to SwyxServer, observe the following sequence of configuration steps:

1 *Prepare hardware*

In Swyx Control Center you have to create the following objects:

2. *Create DECT system*
3. *Create DECT base station(s)*
4. *Creating DECT handsets*

Finally, you need to configure the master base station:

5. *Activating DECT system*

12.3.1.1 PREPARE HARDWARE

- All DECT base stations must be connected to your LAN and switched on.
- The DECT base station you want to provide as master base station must have Ascom AG firmware 11.4.4 or higher.

If you are already operating a conventionally configured DECT system in your network which should remain, you must also update its base stations to firmware 11.4.4 or higher.
When deploying the new system, the already configured base stations remain assigned to the existing DECT system and are not automatically provisioned for the new system.

If your DECT base stations are still operating with an older firmware version, you must update them manually.
On the master base station, you must also manually update the bootloader. See the section "Updating SwyxDECT 800" in help.enreach.com/docs/manuals/english/SwyxDECT800.pdf

- A factory reset must be performed on the base station that you want to configure as master, see **12.3.3 Perform factory reset**, page 141.
- The **Ascom AG** Firmware 11.4.4 or higher for DECT base stations and DECT handsets must be available in your SwyxWare system, released for the corresponding end devices and distributed, see **4.15 Distributing software to clients or devices**, page 30.

If the handset was already in use, you must perform a factory reset via the administration menu for successful provisioning. See **To unlock the administration menu**, page 142.
Dial on the handset:
Menu | Calls | Admin Menu | Factory reset

12.3.1.2 CREATE DECT SYSTEM

You need to create a DECT system object in Swyx Control Center.

Have the SARI ready that you purchased from your service provider. The SARI (Secondary Access Right Identity) is a unique system ID. It is used to identify a DECT system and protect it from unauthorized access.

To create a DECT system

1. Select **Terminals | DECT**.
2. Select the Tab DECT systems.
3. Click on **Create DECT system**.

Designation	Explanation
Name	Enter a unique name for the new DECT system.
SARI	Enter the SARI.

4. Click on **Create**.
   ✓ The DECT system is created and appears in the list **DECT systems**.
5. Follow the steps at *Create DECT base station(s)*.

12.3.1.3 CREATE DECT BASE STATION(S)

At least one DECT system must already have been created.

For each DECT base station you want to use, you need to create a base station object.

Have the MAC address ready. The MAC address of the DECT base station can be found on the packaging or in the last line of the white label on the bottom of the case:

To create base stations manually

1. Select **Terminals | DECT**.
2. Select the Tab **DECT base stations**.
3. Click on **Create DECT base station**.

In the name of the base station, you can refer to the location of the terminal to facilitate maintenance work.

Label	Explanation
Name	Enter a unique name for the new DECT base station.
MAC-adress	Enter the MAC address of the base station. *e.g. a1:c2:e3:f4:11:12*
DECT system	Select an existing DECT system to which the base station is to be assigned.

4 Click on **Create**.
✓ The DECT base station is created and appears in the list **DECT base stations**.

5 If necessary, repeat steps 3 and 4 to create additional base stations.

To import a list of base stations

As an alternative to creating Base Station objects manually, you can import a .CSV file.

Separated by semicolons, enter the MAC addresses, the names of the base stations and optionally the names of the DECT systems to be assigned. The Entries must be placed one below the other.
e.g.
a1:c2:e3:f4:11:15;BaseStation01;DECT_System01
a1:c2:e3:f5:12:12;BaseStation02
a1:c2:e3:f6:15:14;BaseStation03;DECT_System01

- The MAC addresses can be found on the bottom of the respective housing, see **12.3.1.3 Create DECT base station(s)**, page 133
- You can define the unique names of the base stations individually.
- The names of the DECT systems can be found in the list under **Terminals | DECT | DECT Systems**.

If you have not entered the DECT systems in the .CSV file, you can still perform the corresponding assignment manually after uploading the file, see step 6 below.

The .CSV file must not contain more than 100 entries.

1 Select **Terminals | DECT**.

2 Select the Tab **DECT base stations**.

3 Click on **Import DECT base stations**.
✓ The **Import DECT base stations** configuration wizard appears.

4 Click on **Select file** and d select the prepared .CSV file from your file system.

Click the cross icon to remove the file from the selection.

5 Click on **Upload**.

6 If necessary, select existing DECT systems to which the base stations are to be assigned.

7 Click on **Import base stations**.

8 Check if all entries have been imported.
In case of failed imports, you can adjust the erroneous lines in the .CSV file or manually create the corresponding base stations one by one in Swyx Control Center.

9 Click on **Finish**.
✓ The base stations have been registered in the system according to the import result and appear in the list **DECT base stations**.

10 Follow the steps at *Creating DECT handsets*.

12.3.1.4 CREATING DECT HANDSETS

As of SwyxWare V13.30, a certified SIP end device (desk phone or DECT) can only be assigned to a user with a system telephone license.

At least one DECT system and one base station must already have been created.

You can also assign the handset to a user at a later time, see **12.3.2.3 Edit DECT handsets**, page 139.
Unassigned handsets cannot be used.

Make sure that the SIP credentials are entered for the desired users:
User | <Username> | SIP

Have the IPEI number of the DECT handset ready. The IPEI number can be found on the handset packaging.
To display the IPEI number on the handset, dial *#06#

To create DECT handsets manually

1 Select **Terminals | DECT**.
2 Select the tab **Assigned handsets** or **Unassigned handsets**.
3 Click on **Create DECT handset**.

Label	Explanation
DECT handset user	If necessary, select the user for whom the terminal device is to be automatically logged on, or keep **Not assigned**.
IPEI	Enter the IPEI number of the handset. *e. g. 00012 0000137 9*
DECT system	Select a DECT system to which the handset is to be assigned.

4 Click on **Save**.
✓ The new handset appears in the list **Assigned handsets** or **Unassigned handsets**.
5 Repeat steps 3 and 4 to create more handset objects.

To import a list of DECT handsetsets

As an alternative to creating handset objects manually, you can import a .CSV file containing the IPEI numbers:

Enter the following data separated by semicolons:
- The IPEI number of the handset,
the user name to which the handset is to be assigned, if applicable (optional),
- the name of the DECT system to which the handset is to be assigned, if applicable (optional).
- The entries must be one below the other.
e.g.
00012 0000135 9
00012 0000136 9;user_1
00012 0000136 9;user_1
00012 0000138 9;user_2;DECT_System01

The .CSV file may contain a maximum of 100 entries.

1 Select **Terminals | DECT**.
2 Select the tab **Assigned handsets** or **Unassigned handsets**.
3 Click on **Import DECT handsets**.
✓ The configuration wizard appears **Import DECT handsets**.
4 Click on **Select file** and select the prepared .CSV file from your file system.

Click the cross icon to remove the file from the selection.

5 Click on **Upload**.
6 If necessary, select the users to which the handsets are to be assigned.

7 Check if all entries have been imported.
In case of failed imports, you can adjust the erroneous lines in the .CSV file or manually create the corresponding handsets one by one in Swyx Control Center.

8 Click on **Finish**.
✓ The handsets have been registered in the system according to the import result and appear in the list **Assigned handsets** or **Unassigned handsets**.

You can now *Activating DECT system*.

12.3.1.5 ACTIVATING DECT SYSTEM

To activate the new DECT system and put all assigned DECT devices into operation, you must configure a base station.

You only need to configure the base station that you want to use as the master. The other base stations assigned to the DECT system are automatically detected.

A factory reset must be performed on the base station that you want to configure as master, see **12.3.3 Perform factory reset**, page 141.

The master base station receives the AirSync role.
Therefore, place the base station centrally and within range of all other base stations in the DECT system.

Requirements:

- All DECT base stations are connected to your LAN and switched on. The master base station has firmware 11.4.4 or higher with a factory reset, see **12.3.1.1 Prepare hardware**, page 132.
- DECT system objects (also base stations and handsets) have been created, see **12.3.1.2 Create DECT system**, page 133
- Have the following data ready:
  - **MAC address** of the base station,
  - **Activation key**,
  - **Provisioning-URL**.
  You can find this data in Swyx Control Center at **Devices | DECT | DECT Base Stations | Edit DECT Base Station** ( ). You have to activate the checkbox **Show configuration info** check box.
  Click to copy the corresponding data to the clipboard.

To open the administration web interface within the local network, you can also use the following line in the browser instead of the IP address of the base station: https://<Base station model>-<last three bytes of the MAC address>.

e.g. http://ipbs3-28-07-bb

The corresponding data can be found on the white label on the bottom of the base station.

If you cannot open the configuration wizard, perform a factory reset, see **12.3.3 Perform factory reset**, page 141

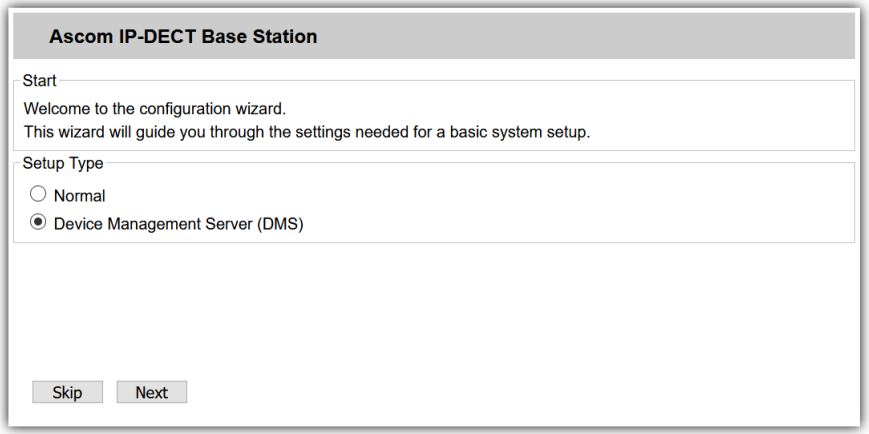
To configure the master base station

1 Enter 'https://<IP address of the master base station>' in the address line of your browser to open the administration web interface of the device.
✓ The login dialog appears.

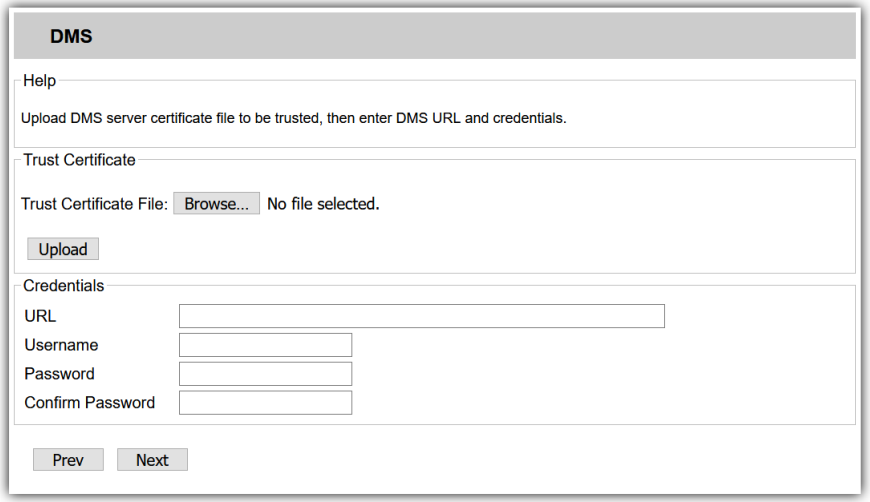
2 Enter the default name "admin" and the default password "changeme".

3 Click on **Login** and subsequently auf **OK**.
✓ The Ascom configuration wizard appears.

4 Select as **Setup Type** the **Device Management Server (DMS)**:



5 Click on **Next**.



6 Upload a TLS root certificate if necessary.
This step is only necessary if you have enabled TLS configuration via SCST, see https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/SCST.

7 Enter under **URL** enter the provisioning URL.

8 Enter under **Username** enter the MAC address of the base station with ":" or without separator.

e.g. a1:c2:e3:f4:11:12

9 Enter the password under **Password** and **Confirm Password** enter the activation key.

10 Click on **Next**.

11 Check your information.

12 Click on **Finish**.
✓ The base station is restarted. The LED on the base station first flashes red, then blue. At the end of the successful activation (can take up to two minutes), the LED will turn solid blue.

It can take up to five minutes before other base stations are activated. The base stations operating in a subnet must configure them manually, see **12.3.1.6 Configure subnet base stations (optional)**, page 137.

12.3.1.6 CONFIGURE SUBNET BASE STATIONS (OPTIONAL)

If a base station is operated in a subnet, this base station must be added to the DECT system manually.

To configure subnet base stations

The base station object was created in Swyx Control Center, see **12.3.1.3 Create DECT base station(s)**, page 133

1 In the address line of your browser, enter 'https://<IP address of the subnet base station>' to open the administration web interface of the device.
✓ The login dialog appears.

2 Enter the default name "admin" and the default password "changeme".

3 Click on **Login** and subsequently auf **OK**.
✓ The Ascom configuration wizard appears.

4 Go through the configuration wizard by clicking on **Next** until you reach the page **Radio**.

5 On the page **Radio** page, enter the following settings:

Label	Explanation
Name	Enter "DECT".

Label	Explanation
Password	Under Password, enter the activation key. (The activation key can be found in Swyx Control Center under **Devices | DECT | DECT Base Stations | Edit DECT Base Station**).
PARI Master IP Address	Enter the IP address of the master base station.

If the configuration wizard is not displayed, you can find these settings on the administration interface under **DECT | Radio**.

6 Click on **OK**.

7 Restart the base station.

12.3.1.7 CHECK COMMISSIONING

You can check whether the new DECT system and the assigned terminals have been activated. After a successful provisioning, new data must appear in the lines of the corresponding DECT objects:

You may need to refresh the page in Swyx Control Center to see the changes.

1 Select **Terminals | DECT**.

2 Select the Tab DECT systems.
   ✓ In the line of the corresponding DECT system, in the column **Type** appears **D800**.

3 Select the Tab **DECT base stations**.
   ✓ In the rows of the created base stations the correct values appear in the columns **Device type** and **Firmware version**.
   ✓ In the line of the master base station the column **Master** is marked with a check mark.

4 Select the Tab **Assigned handsets**.
   ✓ In the rows of the created handsets the correct values appear in the columns **Terminal type** and **Firmware version**.
   ✓ The DECT handsets are assigned to all desired users.

The DECT system is activated and connected to SwyxServer. Users can make calls with their DECT handsets.

Make sure that the new firmware is fully downloaded before using the handsets.

Downloading firmware on DECT 800 handsets can take 10 to 30 minutes depending on the model.
You can check the status of the firmware on the handset via the administration menu: (See **To unlock the administration menu**, page 142).

Menu | Calls | Admin Menu | Centr. Management
- **No FDL** (No firmware download) - No firmware is downloaded.
- **NN%** - Firmware is being downloaded, NN% of the operation is finished.

12.3.2 EDITING THE DECT SYSTEMS

You can:

- Change names and SARI of DECT systems, delete DECT systems, see **12.3.2.1 Edit DECT systems**, page 138
- Assign DECT base station(s) to another DECT system, change master base station, delete DECT base station(s), see **12.3.2.2 Edit DECT base station**, page 139
- Assign DECT handsets to another DECT system or another user and delete DECT handsets, see **12.3.2.3 Edit DECT handsets**, page 139
- Assign function keys as name keys, copy key assignment from another DECT handset, see **12.3.2.4 Assigning function keys on the DECT handset**, page 140

12.3.2.1 EDIT DECT SYSTEMS

You are logged in to Swyx Control Center as administrator.

1 Select **Terminals | DECT**.
2 Select the Tab DECT systems.
✓ The list of DECT systems appears.
3 Click on in the row of the corresponding DECT system to edit the DECT system, see the table at **12.3.2.1 Edit DECT systems**, page 138.
4 Click on Save.
✓ The changes appear in the line of the DECT system.

To delete DECT systems

If you delete a DECT system, the assigned base stations are marked as unassigned and cannot be used.

1 Select **Terminals | DECT**.
2 Select the Tab DECT systems.
✓ The list of DECT systems appears.
3 Click on in the line of the corresponding DECT system to delete a DECT system or select the corresponding lines and click on **Delete multiple DECT systems**.
4 Confirm the operation.
✓ The selected DECT systems are deleted.

12.3.2.2 EDIT DECT BASE STATION

You can assign DECT base stations to another DECT system or one or change the name.

1 Select **Terminals | DECT**.
2 Select the tab **DECT base station**.
✓ The list of DECT base stations appears.
3 In the row of the corresponding DECT base station, click to edit the base station:

Designation	Explanation
Name	Enter a unique name for the DECT base station.
DECT system	Select an existing DECT system to which the base station is to be assigned.
Firmware version	The installed firmware version
Device type	The device model (manufacturer)
Master	Clear the check box if you do not want to use the base station as a master base station. You must then set another base station as the "master".
Show configuration info	Select the check box to display the provisioning key and provisioning URL.
MAC-adress	The data necessary for the activation of the DECT system, see **12.3.1 DCF DECT system put into operation**, page 132 Click to copy the corresponding data to the clipboard.
Provisioning key	
Provisioning URL	

4 If applicable, click **Save**.

To delete DECT base stations

1 Select **Terminals | DECT**.
2 Select the tab **DECT base station**.
✓ The list of DECT base stations appears.
3 Click on in the line the corresponding DECT base station to delete one base station or select the corresponding lines and click on **Delete multiple DECT base stations**.
4 Confirm the operation.
✓ The selected DECT base stations are deleted.

12.3.2.3 EDIT DECT HANDSETS

You can assign DECT handsets to another DECT system or another user.

If you have assigned handsets to other users after the SwyxWare/NetPhone database has been backed up and restore SwyxWare/NetPhone from this database, automatic logon will not work for the newly assigned handsets.
Reset the SIP credentials under **General Settings | System | Provisioning** reset.
See **4.6 Configuring the provisioning of SIP phones**, page 20

To reassign DECT handsets

1 Select **Terminals | DECT**.
2 Select the tab **Assigned handsets** or **Unassigned handsets**.
3 In the row of the corresponding DECT handset, click to reassign the handset.
✓ The configuration wizard appears **Reassign DECT handset**.
4 Select the desired destinations from the list **New user** or **New DECT system**.
5 If necessary, activate **Notify user**.
6 Confirm with **OK**.

To delete DECT handsets

1 Select **Terminals | DECT**.
2 Select the tab **Assigned handsets** or **Unassigned handsets**.
3 Click on in the line of the corresponding DECT system to delete a DECT system or select the corresponding lines and click on **Delete multiple DECT systems**.
4 Confirm the operation.
✓ The selected DECT handsets are deleted.

12.3.2.4 ASSIGNING FUNCTION KEYS ON THE DECT HANDSET

You can edit the following settings:

- Assigning name keys to contacts
- Copying function key assignment from another DECT handset

Do not assign the function keys directly on the device. Otherwise, configuration errors may occur.
The configuration may only be done via Swyx Control Center.

The user settings for a DECT handset can only be edited if the handset is assigned to a user.

To assign function keys as name keys

1 Select **Terminals | DECT**.
2 Select the Tab **Assigned handsets**.
3 In the line of the corresponding Handset, click on .
✓ The configuration wizard appears **Edit DECT handset for user...**.

Designation	Explanation
Button no.	Number of the assignable key according to the adopted numbering.
Labelling	Designation that appears in the key list.
Function	If you select **Speed dial**, the appropriate input fields **Index** and **Number** as well as the **Edit option are** activated, see **To assign a Speed Dial**, page 140.

4 Click on **Save all**.
✓ The changes are saved and updated on the DECT handset.

To assign a Speed Dial

1 Select **Terminals | DECT**.
2 Select the Tab **Assigned handsets**.
3 In the line of the corresponding Handset, click on .
✓ The configuration wizard appears **Edit DECT handset for user...**.
4 Select the **Speed dial** option from the dropdown list.

5 Select the number for the intended speed dial under **Index**.

The "Index" number is used to assign the name key in the user account and does not determine the order of the name keys on the handset.

6 Click on ✎ in the line of the speed dial selected.

The settings for the dialing options and the user image are only relevant for SwyxIt! and SwyxPhone Lxxx, respectively.

Designation	Explanation
Labelling	Enter the display name for the corresponding name key.
Number/URI	Enter the phone number which will be dialed via the name key. The corresponding label is entered automatically.
---	Or: Use the button to select a user from the phone book.
Dialing options	If necessary, activate the corresponding options: **Immediate Dial** Pressing the name key starts the call. **Deleting the display before dialing** The display is cleared before dialing. **Intercom Connection** Pressing the name key starts a direct address.
User's picture	Choose whether to display a user image and upload a file from your file system if necessary. **Automatic** The User picture is ´transmitted by SwyxServer.

To copy the assignment of name keys from another handset

1 Select **Terminals | DECT**.

2 Select the Tab **Assigned handsets**.

3 In the line of the corresponding Handset, click on ✎.
✓ The configuration wizard appears **Edit DECT handset for user...**.

4 Click on **Copy settings from another DECT handset**.

5 Activate the checkbox in the row of the desired handset.

6 Click on **Copy**.

7 Click on **Save all**.
✓ The assignment of the function keys is copied and saved.

12.3.3 PERFORM FACTORY RESET

You can perform a factory reset to clear any errors.

A factory reset sets all configuration parameters to default values. The reset button is located on the back of the base station:

To perform a factory reset

Base station is connected to the power supply or PoE.

1 Press and hold the reset button with a pointed object for several seconds.
✓ After approx. 3 seconds, the LED starts flashing blue at short intervals.

2 Press and hold the reset button for another 5 seconds until the LED flashes blue at longer intervals, then release it.
✓ The configuration parameters are reset.

3 When the LED is solid yellow, disconnect the base station from the power supply and turn it back on after a few seconds.
✓ The base station is restarted.

12.3.4 ACTIVATE ADMINISTRATION MENU ON A DECT 800 HANDSET

In the handset administration menu, you can perform a factory reset of the handset, check the current firmware version, or track the status of the firmware download.

To unlock the administration menu

1 Select on the handset **Menu | Calls | Call time**.

2 Enter the following symbol string using the navigation key and the asterisk symbol: ">*<<*<"
✓ You can now open the administration menu via **Menu | Calls | Admin Menu**

12.3.5 ERROR MESSAGES FROM DECT HANDSETS

The following error messages may appear on the handset screen:

Error message	Meaning	Solution
Call list synchronization is not available	Synchronization with the SwyxWare user's call journal cannot be performed. Probably the connection with the base station is interrupted.	Move closer to the base station. As soon as the synchronization starts, the colored loading circle appears with the message "Synchronizing call list"
Could not sync call list	The synchronization with the call journal is interrupted.	Go back within range of the base station. When synchronization is running again, the colored loading circle appears with the message "Synchronizing call list".

12.4 SWYXPHONES

You can connect the SwyxPhones in your local network via SwyxPhoneManager service to SwyxServer. SwyxPhoneManager is a component of SwyxServer and can also be used as a remote service. Additionally, you can use more than one PhoneManager.

In order for the SwyxPhones to be able to log on to SwyxServer via PhoneManager, you must distribute the IP address of the corresponding SwyxPhoneManagers to the SwyxPhones. You can set the IP address range for searching SwyxPhones and the PhoneManager address in Swyx Control Center. When you start the search process, all phones that are within the specified IP address range will be connected to the corresponding PhoneManager.

The PhoneManager IP address remains stored in the SwyxPhones. Accordingly, you only need to start the search process if you want to commission new SwyxPhones in the network.

To connect SwyxPhones to SwyxServer

1 In the menu, select **Desk Phones**.
✓ A list appears with all Desk Phones.

2 Click on SwyxPhones.
✓ A list appears with all IP address ranges.

3 Click on **Create IP address range**.
✓ The **Create IP address range** configuration wizard appears.

Designation	Explanation
From	Enter the first IP address range to be searched for SwyxPhones.
To	Enter the last IP address range to be searched for SwyxPhones.
PhoneManager	Enter the IP address of the PhoneManager to which the found SwyxPhones are to be connected.
Search period [1-72 hours]	Define how long you want the search to take.
Start	Start the search process.
Stop	Stop the search process.

4 Click on **Save**.

You can create another IP address range with the IP address of the corresponding PhoneManager to add more PhoneManagers.

5 In the line of the appropriate IP address range, click on to edit an IP address range.

6 In the line of the appropriate IP address range, click on to delete an IP address range or on **Delete multiple IP address ranges** to delete more than one IP address range.

12.4.1 EDITSWYXPHONES

You can edit the SwyxPhone settings.

With the PIN that you define for SwyxPhones, the user can also log in to certified SIP devices.

To edit the settings for a SwyxPhone

1 In the menu, select **User**.

2 In the line of the appropriate User, click on .

3 Click on on the right next to the User name.

4 Click on the sub-menu item **Desk Phones** that additionally appears.

5 Click on SwyxPhone.

Designation	Explanation
SwyxPhone	Activate the checkbox to permit the use of SwyxPhones for the User.
User-PIN on Desk Phone	Enter a PIN or have a PIN created so that the User can log in to SwyxServer with any SwyxPhone and use his or her own number and key configuration. The name must be unique within SwyxServer.
Create PIN	Click on the button to create a new client certificate for the User. The User's current PIN becomes invalid.
MAC-address	Enter the Desk Phone's MAC address, if applicable, so that a SwyxPhone can be assigned to the appropriate User during an automatic logon. If you do not enter any information here, SwyxServer will note the MAC address of the SwyxPhone when the User logs in for the first time. If a User wants to log in with another SwyxPhone, you must delete the input field for the MAC address in order to enable taking over of the new telephone's MAC address.
Automatic logon	Activate the checkbox to permit STUN support. In this case, the User is permanently logged in to this SwyxPhone after rebooting the SwyxPhone.

Designation	Explanation
Speech Codec	Select how the language data will be compressed during transfer. **Prefer voice quality. If possible, use HD audio.** 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. Only compress audio data if necessary.** Voice data is only compressed if necessary. An attempt is made in this case to use Codecs in the order G.711a/G.711µ/G.729. Codec G.722 is never used. **Prefer low bandwidth To spare bandwidth, the voice data is compressed.** 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. Codec G.722 is never used. **Use lowest bandwidth. Always compress audio data.** In order to use the lowest bandwidth, the voice data is always compressed. The Codec G.729 is used. See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/small_office_$.

6 Click on **Save**.

13 EDITING PHONEBOOKS

The following Users can be displayed in the Global Phonebook:

- Users at the same SwyxServer
- Users connected to SwyxServer via SwyxLink trunk

For Users to appear in the Global Phonebook, the "Show in Phonebook" option must be activated in the user settings, see step **Activate the checkbox if you want the numbers to appear in the Global Phonebook.**, page 87.

Each User also has a Personal Phonebook. The Personal Phonebook can be edited by the appropriate User and the system administrator.

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.

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 setting options on menu pages and in configuration wizards depend on your administration profile and your SwyxWare solution.

Creating phonebook entries
Editing phonebook entries
Exporting phone books
Importing phonebook entries

13.1 CREATING PHONEBOOK ENTRIES

To create an entry in the Global Phonebook

1. In the menu, select **Global Phonebook**.
   ✓ A list appears with all entries in the Global Phonebook.
2. Click on **Create phonebook entry**.
   ✓ The **Create phone book entry** configuration wizard appears.

Label	Explanation
Name	Enter a name.
Description	Enter a description, if applicable.
Number	Enter a phone number or URI.
Displaying in the Phonebook	Activate the checkbox if you want the number to be displayed in the Global Phonebook.
	Click on the button to delete the phone book entry.
	Click on the button to download the phone book entry.

3. Click on **OK** to save the entry.
   ✓ The phonebook entry is created or updated and appears in the list of all Global Phonebook entries.

To create an entry in the Personal Phonebook

1. In the menu, select **User**.
   ✓ For administrators, a list appears with all Users.
2. As administrator, click on > in the line of the appropriate user.
3. Click on the submenu item **Personal Phonebook**.
4. Click on **Create phonebook entry**.
   ✓ A list appears with all entries in the Personal Phonebook of the appropriate User.

5 Click on **Create phonebook entry**.

6 The **Create phone book entry** configuration wizard appears.

Label	Explanation
Name	Enter the name.
Number	Enter a phone number or URI.
Private	Activate the check box if you only want to signal the phone number of the entry and not the name to other Users who receive call signaling. ✓ = Private ⊘ = Non private
🗑	Click on the button to delete the phone book entry.
✎	Click on the button to download the phone book entry.

To delete several entries at the same time, activate the checkbox in the line of the appropirate entry, click on **Delete multiple phonebook entries** and confirm with **Yes**.

13.2 EDITING PHONEBOOK ENTRIES

The name must be unambiguous within SwyxServer.

To edit an entry in the Global Phonebook

1 In the menu, select **Global Phonebook**.
✓ A list appears with all entries in the Global Phonebook.

2 In the line of the appropriate entry, click on ✎, to edit the entry.
See also step **Enter a name.**, page 145

3 In the line of the appropriate entry, click on 🗑, to delete the entry.

To edit an entry in the Personal Phonebook

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the submenu item **Personal Phonebook**.

4 In the line of the appropriate entry, click on ✎.
See also step **Enter the name.**, page 146

5 In the line of the appropriate entry, click on 🗑, to delete the entry.

13.3 EXPORTING PHONE BOOKS

You can export the phonebooks for editing or as a safety copy in .CSV format.

To export the Global Phonebook

1 In the menu, select **Global Phonebook**.
✓ A list appears with all entries in the Global Phonebook.

2 Click on **Export Phonebook**.
✓ The **Export Phonebook** configuration wizard appears.

Label	Explanation
Include descriptions	Activate the checkbox if you want optional descriptions of the entries to appear (optional).
The first row has column names	Activate the checkbox if you want the column headers for the appropriate entries to appear in the first line.

3 Click on **OK**.
✓ The Global Phonebook is saved under the name "SwyxWarePhonebook.csv" in the directory set in your browser for downloads, e.g. "C:\Users\<Userrname>\Downloads.

To export the Personal Phonebook

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the submenu item **Personal Phonebook**.

4 Click on **Export Phonebook**.
✓ The **Export Phonebook** configuration wizard appears.

Label	Explanation
The first row has column names	Activate the checkbox if you want the column headers for the appropriate entries to appear in the first line.

13.4 IMPORTING PHONEBOOK ENTRIES

You can import Phonebooks in CSV format. The imported CSV file should have the following format:

First name 1; Surname 1; Phone number 1

First name 2; Surname 2; Phone number 2

or

First name 1; Surname 1; Phone number 1

First name 2; Surname 2; Phone number 2

To import entries into the Global Phonebook

1 In the menu, select **Global Phonebook**.
✓ A list appears with all entries in the Global Phonebook.

2 Click on **Import Phonebook**.
✓ The **Import Phonebook** configuration wizard appears.

3 Click on **Select file**.

4 Select the CSV file and click on **Next**.

5 Activate **Automatically add the additional marking to the name entered** as applicable if you wish to distinguish Users optically from other SwyxServers in the Phonebook.

6 Click on **Next**.

7 Select the update mode:

Mode	Explanation
Update the existing entry	If an entry exists under the same name, the fields **Telephone number** and **Description** are overwritten with the contents of the import file.
Rename a new entry	If an entry exists under the same name, the entry of the import file is added under a different name. *Example* *'Franz Mustermann' is added as 'Franz Mustermann (2)'.*
Skipp a new entry	If an entry exists under the same name, the entry of the import file is not taken into account.
Delete existing Phonebook before import	The Phonebook is replaced in-full with the import file contents.

8 Click on **Import**.
✓ The Global Phonebook is imported in accordance with the mode selected.
✓ The list of all entries in the Global Phonebook is updated.

To import entries into the Global Phonebook

1 In the menu, select **User**.
✓ For administrators, a list appears with all Users.

2 As administrator, click on > in the line of the appropriate user.

3 Click on the submenu item **Personal Phonebook**.
See section **To import entries into the Global Phonebook**, page 147

14 DATA STORAGE

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

Data Storage Location

As of SwyxWare V13.27, the data processing of some files managed by the system has been changed.

- Trunk recordings,
- Voice messages and
- Fax files

of all **UC Tenants (**SwyxON**)** are stored in the **Enreach S3 object storage**. The administrator of a UC tenant does not need to make any settings for the storage location.

The system administrator of an **On Premises** SwyxWare on the other hand, can choose from three different storage destinations:

Storage Destination	SwyxON	On Premises
S3 object storage	Yes, mandatory (data platform managed by Enreach) The retention period is controlled in accordance with the GDPR.	Yes, optional The customer can set up an S3 bucket with a third-party provider and connect it to SwyxWare.
Internal Database (SQL database configured in SwyxWare)	No	Yes, default
File System (any directory in the client's file system)	No	Yes, optional The customer defines a directory in his own file system. Files are managed via SwyxWare. This option reduces the amount of memory required in the database.

When saving to the internal database, note that there is a storage limit depending on the type of SQL database configured.

Please observe the appropriate applicable legal regulations. Please observe this in particular if you change the settings for the memory limit and/or the storage location.

The internal SQL database is used as a fall-back if the configured S3 object store is no longer available.
To avoid data loss, make sure that the configured storage location is accessible at all times and has sufficient capacity.

Changing the configuration can start a copy process of the existing files in the background.

To set the storage destination

1 Select **Data & Storage | General | Target storage**.

Label	Explanation
Storage destination (only selectable in On Premises)	Select the desired storage destination **S3 object storage** (S3 service from a third-party provider) **Internal database** (SQL database configured in SwyxWare) **File system** (any directory in the client's file system)
File count	This overview shows where and how many trunk recordings, conversation (call) recordings, voice messages and fax files are currently stored. Changing a storage location can start a copy process of the existing files in the background.

2 Click on **Save**.

If you have selected **S3 object storage** or **File system**, you must enter further configuration data, see **14.1 Storage location configuration**, page 149

14.1 STORAGE LOCATION CONFIGURATION

If you have selected **S3 object storage** or **File system**, you must enter further configuration data, see

- for the S3 service provider or
- for the desired directory.

To enter the S3 provider information

1 Select **Data & Storage | General | S3 Configuration**.

Label	Explanation
Service URL	Enter the address of the access point to the provider's S3 service. *e.g. https://s3-eu.central-1.example.com*
Bucket name	The designation of the configured bucket. *e.g. examplecorp-prod-data-bucket-9824-7619*
Connection status	Status of the S3 service **Connected** Connected to the S3 object storage **Failed** Connection failed **Bucket missing** The corresponding S3 bucket could not be found **None** No connection to an S3 object store has been configured
Access key	Enter the access data that you have received from the service provider.
Private key	
Test connection	Click the button to check the status of the connection.

2 Click on **Save**.

To configure a directory in the file system

1 Select **Data & Storage | General | File system configuration**.

Once the configured directory is used to store the data, you can no longer change the path.

Label	Explanation
Path	Enter the path to the directory in your file system. *e.g. C:\ProgramData\Swyx\IpPbxServer\Data\FileData* or *\example.net\branch\Storage\FileData*
Use credentials	If the files are stored in a network directory, specify a user account and password that allows access to this directory.
User name	
Password	
Domain	If necessary, enter the domain name of the network.
Connection status	Connection to SQL database **Connected** Connected to the database **Not connected** Connection failed
Test connection	Click the button to check the status of the connection.

2 Click on **Save**.

14.2 TRUNK RECORDING

Conversations via Trunks can be recorded.

When saving and processing personal data, observe the appropriate 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 (TKG).
Recording without the express consent of all participants in the conversation is considered unauthorized and will be prosecuted under Section 201 (1) of the German Criminal Code (StGB).

If you have not enabled the options under **Retention and Quotas**, you may need to manually delete the files in the database to comply with applicable privacy regulations, see **4.12 Edit files**, page 26.

Permanent Recording

If the Option Pack SwyxMonitor is installed, all calls on a trunk can be permanently recorded.

The desired trunk groups, must be activated for recording, see step **(10)** in **To specify settings for trunk recordings**, page 152.

Calls over SwyxLink trunks can only be recorded if they are locally administered on this server. Calls via an SIP gateway trunk (SwyxConnect) can not be recorded.

Internal calls, i.e. calls between two users logged in to the same SwyxServer, are not recorded.

No audio signal announces this permanent recording.

Recording initiated by the user (Conversation recordings)

If additionally the option package SwyxRecord is licensed and installed, users can record any conversations or parts of conversations.

A user can record a conversation:

- If the **Allow all users to start and stop recording** option is enabled. (This affects all users who log in to SwyxServer) See also step **(5)**.
- If the **Call recording** function is activated in the user's function profile, see **9.17.3 Activating conversation recordings**, page 104

Recording is independent of the terminal device used. The user must enter the **DTMF sequence to start recording**, you have set, during the call to start a recording. If he then enters the **DTMF sequence to end the recording** during the call, the recording is ended. A beep will sound to announce the recording, and a second beep will sound to signal the end of the recording.

File name of a recording

The recordings are saved as OPUS file or WAV file. For UC Tenants on the SwyxON Portal only the OPUS format is available.

The name of a file is composed as follows:

Section	Explanation
1) <Direction of the conversation>#	**OUT#** outgoing call **IN#** incoming call
2) <Phone number of the recorder>#	The called internal number (IN) or the number from which this call was started (OUT)
3) <Name of the interlocutor># (optional)	The name can only be given if the number has been assigned a name.
4) <Phone number of the call partner>#	Will be displayed if one exists. Please note that the public line access will also be saved.
5) <Date of call>#	Date in the format <yyyymmdd>
6) <Time of the call>	Start time of the call using the format <hhmmss>

Example:

Out#123#Schulz, Eva#0012345678#20200217#155844.wav

means that an outgoing call from the number "123" to Eva Schulz with the number "0012345678" was recorded on February 17, 2020 at 15:58:44.

Storage of the trunk recordings

While recording a trunk recording, the data is stored in a temporary file on the hard disk of the SwyxServer or the virtual machine. The data is then forwarded to the configured storage destination.

If there is no connection to the SQL data base or the capacity of the location is not sufficient for new data, the data will remain in the temporary file.

The space for temporary data is limited and is also used for other system processes. Data overflow can affect the functionality of the UC Tenant.
To avoid data loss, make sure that the configured storage location is accessible at all times and has sufficient capacity.

UC tenants (SwyxON) store trunk recordings in the Enreach S3 object storage. Per UC tenant, 5 GB is available by default as storage for trunk recordings.

For local SwyxWare installations (On Premises) a customer defined location for all data can be chosen, see **Data Storage Location**, page 148

A SwyxWare system administrator has the option to download the trunk recordings from the database, e.g. to archive desired recordings in a different location. See **4.17.1 Downloading trunk recordings**, page 34 and **4.12 Edit files**, page 26.

You can configure the behaviour when saving trunk recordings even more specifically.

Depending on your situation (new installation or upgrade), use one of the following options:

Option	Effect on new installation	Effect with update
Configured destination (Default setting for new installation)	Store trunk recordings in the configured location	The data is then forwarded to the configured storage location.
Working directory only (Default setting for Updating)	Store trunk recordings only in the file directory configured by the customer	Continue to use file directory for trunk recordings. Files cannot be managed via SwyxWare (e.g. retention and quotas).
Both	-	Leave existing trunk recordings in the file directory. Store new recordings in the configured location. The trunk recordings can be managed via SwyxWare. However, a copy remains in the file directory for recordings. There, the data protection measures (GDPR) must be taken manually.

To specify settings for trunk recordings

1 Select **Data & Storage | Trunk Recordings**.
✓ The general settings for storage of trunk recordings appear.

Label	Explanation

Working directory for recordings (On Premises only)	If you want to place trunk recordings in a desired location in the file system, enter a path to the directory. A dummy [trunkname] can be used for relating the recordings to the different trunks.
	Example:
	`\\fileserver\recordings\[trunkname]`
	The default setting uses the path:
	`%APPDATA%\Swyx\Recording\[trunkname]`
	All recordings are then saved locally among the application data of the user account under which SwyxServer is running.
	To make the recordings accessible to various users, we recommend creating a share for which SwyxServer has write authorization. Access to the trunk recordings can be controlled via the corresponding read rights of the individual users.

Codec to be used for all Recordings (On Premises only)	Select the codec to be used for the recordings. The following codecs are available: (OPUS is preset for UC Tenants and cannot be changed) **Open standard RFC 6716 (.opus)** Dynamically adjustable bit rate. Best audio quality / storage space ratio. **Microsoft Wave Audio G.711 (.wav)** Mono, compressed 64kBit/s **Microsoft Wave Audio GSM (.wav)** Mono, compressed 13kBit/s **Microsoft Wave Audio PCM (.wav)** not compressed

Label	Explanation
Recorded call parties	Select which side of a conversation to record. These Setting applies both to permanent recording and for recording initiated by the user with DTMF digits. **Both** The complete conversation is recorded. **Local** Only the conversations of the user logged on to this SwyxServer are recorded. **Remote** Only the conversations of the interlocutor are recorded.
Storage (On Premises only)	For a local (On Premises) SwyxWare installation, you can specify where the recorded trunk recordings are subsequently stored, see the section **Storage of the trunk recordings**, page 151 **Configured destination** Default setting for a new installation and for all UC tenants on SwyxON **Working directory only** Default setting for an update of SwyxWare **Both** Default setting for an update of SwyxWare with activated trunk recordings

2 Click on **Save**.

3 Select **Retention & Quotas**.

If you have not enabled the options under **Retention and Quotas**, you may need to manually delete the files in the database to comply with applicable privacy regulations, see **4.12 Edit files**, page 26.
Trunk recordings in the file directory are not managed by SwyxWare.

Label	Explanation
Activate retention settings	Select the check box if you want to limit the storage time for trunk recordings.
Retention (in days)	Number of days trunk recordings may be stored in the database before they are automatically deleted. (Default setting 30)
Activating quota settings	Select the check box if you want to limit the storage space for trunk recordings.
Quota (in MB)	Set the storage quota to be reserved specifically for trunk recordings. (default setting 5000)

4 Click on **Save**.

5 Select **User initiated recordings**.

Label	Explanation
Allow all users to start and stop recording	Activate the checkbox if all users logged on to this SwyxServer are allowed to record calls, see **Recording initiated by the user (Conversation recordings)**, page 151
DTMF sequence to start recording	Enter a DTMF key sequence to be used by users to start recordings.
DTMF sequence to stop recording	Enter a DTMF key sequence to be used by users to stop recordings.

6 Click on **Save**.

7 Select **Permanent recordings**.

Label	Explanation
Enable permanent Trunk Recording	Activate the checkbox if calls are to be permanently recorded. Select an option: **Record all trunk calls** All calls are recorded. **Record all trunk calls from or to the following internal numbers** You can enter several internal numbers (separated by semicolons) or internal number ranges In the field, for which the calls should be recorded (both incoming and outgoing). You cannot use wildcards here! Only a maximum of 255 characters (including the semicolon) are accepted.

8 Click on **Save**.

9 Select **Trunk groups**.

10 Mark the desired trunk groups with ✓ to enable permanent recording on the corresponding trunks.

11 Click on **Save**.

14.3 VOICE MESSAGES

Callers can leave voice messages for users and user groups.

The Voice Box function (SwyxVoicemail) is only available if it is activated in a user's function profile.

If the caller enters the DTMF digit '0' during the Voice Box announcement, the Voice Box will be interrupted and the caller will be connected to an operator. See also https://help.enreach.com/cpe/13.30/Administration/Swyx/en-US/#context/help/auto_attendant_$.

You can define the storage location for voice messages under **Data & Storage | General | Target storage** , see **14.1 Storage location configuration**, page 149

You can set a default Voice Box greeting that will be used server-wide for all users created in the future. Additionally, you can select the codec for voice messages.

Codec used for Recordings

Voice messages are sent as OPUS file or WAV file. For UC Tenants on SwyxON Portal only the OPUS format is available.

The compression to be used can be set for all users, or individually for each user.

Open standard RFC 6716 (.opus)	Dynamically adjustable bit rate. Best audio quality / storage space ratio (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	Default WAV file, not compressed

To set the storage options for voice messages

1 Select **Data & Storage | Voice Messages**.

Label	Explanation
Codec used for Recordings	Select the desired audio format, see the table above.

2 Click on **Save**.

3 Select **Retention & Quotas**.

Label	Explanation
Memory per User	Enter how much memory should be available to each user for received voice messages. (default 20 MB)
Memory per Group	Enter how much storage space each user group should have available for received voice messages. (default 20 MB)
Activate retention settings	Select the check box to limit the storage time for voice messages.
Retention (in days)	Enter how long received voice messages should be stored. After this period, the files are deleted.

4 Click on **Save**.

5 Select **Announcement**.

Label	Explanation
Default Voice Box announcement	All announcement files stored in the database appear in the dropdown list, see also https ://help.enreach.com/cpe/latest.version/Administration/Swyx/en-US/#context/help/tab_files_$. The files have the audio format "16 kHz 16 Bit PCM mono".
	Click the button to search for files in a wav format on the network. After selecting a wav file, it is converted to the configured format and stored in the database. The Windows functions used in this conversion process may degrade the audio quality. In this case, use a professional conversion program instead of Windows conversion to create WAV files in the above format. You can record announcements via SwyxIt!, for example (**Settings | Announcement Wizard** menu, see also https ://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/#context/help/recording_wizard_$).
	Click on the button to delete the selected announcement. You can only delete files you have created yourself.
	Click on the button to test play the currently selected greeting.
	Click the button to adjust the volume for test playback.
	Click on the button to download the currently selected file.

6 Click on **Save**.

14.4 CALL DETAIL RECORDS (CDR)

SwyxWare allows you to record information concerning connected calls, so-called "Call Detail Records", in a text file.

See also **14 Call Detail Records (CDR)**, page 140

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

To set the settings for the CDRs

Call Detail Records can only be exported or deleted if "Internal database" has been selected as the storage location. Please observe the appropriate applicable legal regulations. Please observe this in particular if you select the database as the memory Location.

1 Select **Data & Storage | Call Detail Records | Configuration**.
✓ The general settings for saving of call detail records appear.

Label	Explanation
Activate CDR	Recording is preset as deactivated. Select the check box if you want to record call details (CDR) in the form of a text file.
Anonymization	Specify the format in which external phone numbers are stored in the file: **Store complete 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'. In the field **Number of digits** how many digits (from the end) are to be replaced. **Hide complete number** 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.
Storage Destination (On Premises only)	Select the storage location for CDR. **Store to file** Enter 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 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. **External database (not for SwyxON)** Call Detail Records are stored in an external database. Enter the database connection string. Via **Test Connection** you can check the connection to the database. According to data protection regulations, the deletion of CDR in this database should be executed manually. See also https://service.swyx.net/hc/en-gb/articles/360000013819-Write-Call-Details-Records-into-a-database (you may need to be logged in to view the content). **Internal database** Call Detail Records are stored in the SwyxWare database. Under **Delete after (days)** you define after how many days CDR are deleted automatically.

2 Click on **Save**.

3 Select **Retention & Quotas**.

Label	Explanation
Delete after (days)	When the specified number of days is exceeded, a new file with the same name and an attached counter is created and filled. The existing files are only deleted if you select time restriction.

4 Click on **Save**.

5 Select **Export**.

Label	Explanation
<Year, month>	Select the month for which you want to export and download the call detail records.
Export	Click the button to save the corresponding file. The text file is stored under the name „calldetail-records<yyyy>.<mm>.txt" in the downloads directory of your browser., e.g. "C:\Users\<Username>\Downloads".

6 Click on **Save**.

7 Select **Delete**.

Label	Explanation
<Year, month>	Select the month for which you want to delete Call Detail Records.
Delete	Click on the button to delete the call detail records of the selected period.

14.4.1 FILE FORMAT

The recorded ASCII text file contains one CDR per line. Each CDR, in turn, contains attributes separated by commas and enclosed in quotation marks. The first line contains a header line with column names enclosed in quotation marks separated by commas.

Each row contains the following attributes in the specified order:

Attribute	Explanation
CallID	**Identification for a call** Each call (each CDR) contains a unique number. This ID is communicated to SwyxIt! as well, so it can be used via Client SDK, and can also be queried in the call routing script. Format: String
Origination-Number	**Caller number** For internal calls this is only the internal extension number, for external calls this is the number that is signaled in the network. If the call goes through a Trunk, the complete number in canonical format is entered here (+492314777222). 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 with which the call was started, User name or name from the global SwyxWare phonebook. Format: String
CalledNum-ber	**Called number** Number originally dialed by the caller Format: String
CalledName	**Name of the person called** Name of the subscriber called, User name or name from the SwyxWare global phonebook Format: String
Destination-Number	**Destination Number** Number of the subscriber who picked up the call This is the same as CalledNumber for calls which have not been picked up. Format: String
Destination-Name	**Destination Name** Name of the subscriber called, User name or 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 received the client's call Format: dd.mm.yyyy

Attribute	Explanation
StartTime	**Start time** Time at which SwyxServer received the client's call Format: hh:mm:ss
ScriptConnectDate	**Script start date** Date on which the call was picked up via script (for incoming calls only) Format: dd.mm.yyyy
ScriptConnectTime	**Script start time** Time at which the call was picked up via script (for incoming calls only) Format: hh:mm:ss
DeliveredDate	**Delivery date** Date on which the call was delivered, e.g. by a ConnectTo in the script (for incoming calls only) Format: dd.mm.yyyy
DeliveredTime	**Delivery time** Time at which the call was 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 was picked up Format: dd.mm.yyyy
ConnectTime	**Connection time** Time at which the call was transferred 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 was terminated Format: hh:mm:ss

Attribute	Explanation
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
Costs	**Cost of a call** 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 units, the calculated value of the costs included here as configured in the SwyxWare Administration. If AOC = '0', no charging information was delivered. '00' = no costs Format: String
State	**State of the call** • Initialized: This is the 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
PublicAccessPrefix	**Public Line Access** Dialed public access number (for outgoing external calls only; optional) Format: String

Attribute	Explanation
LCRProvider	**LCR code** This field remains empty. Format: String
ProjectNum-ber	**Project codes** Code for a project (optional) Format: String
AOC	**Charges information (Advice of Charge)** ''1''= Advice of charge information was taken from the network '0' = The advice of charge information could not be taken from the network. Format: String
Origination-Device	**Origin (Trunk)** Origin of the call (name of the Trunk) Format: String
Destination-Device	**Destination (Trunk)** Destination of the call (name of the Trunk) Format: String
Transferred-ByNumber	**Number of the transferor** Number of the subscriber who transferred the call Format: String
Transferred-ByName	**Name of the transferor** Name of the subscriber who transferred the call Format: String
Transferred-CallID1	**ID of the first call** CallID of the first CDR from which this CDR stems (for call transfers only) Format: String
Transferred-CallID2	**ID of the second call** CallID of the second CDR from which this CDR stems (for call transfers only) Format: String

Attribute	Explanation
Transferred-ToCallID	**ID of the transferred call** CallID of the new CDR resulting from a call transfer Format: String
Transfer-Date	**Date of transfer** Date on which the call was transferred Format: dd.mm.yyyy
Transfer-Time	**Time of transfer** Time at which the call was 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: 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: 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 end of call • CallDeflected: Call was manually diverted to another number or a voicemail without picking up • 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: Call was transferred (call was recorded further under the newly assigned TransferredToCallID) Format: String

14.4.2 EXAMPLES FOR CDR

The following examples are given to help you better understand CDR. These are CDR 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.

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

CDR for an External Call

User A (number +492314777123) forwards an external call to John Jones (number +49231456789). 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).

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	"+4916012345678"
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	""

Attribute	Content
DestinationDevice	"SwyxGate1"
DisconnectReason	CallDisconnected

CDR for a Transferred Call

User C (number +492314777101) calls User A (number +4916012345678) and puts this call on "Hold". User C then calls User B (+49521087654321) 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 CDR, 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	"+4916012345678"
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 A)

Attribute	Content
CallID	7
OriginationNumber	"+44204777101"
OriginationName	"User C"
CalledNumber	"+49521087654321"
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"

Attribute	Content
DisconnectReason	CallTransferred

CDR 3 (Transferred Call; A Speaks to B)

Attribute	Content
CallID	8
OriginationNumber	"+4916012345678"
OriginationName	"User A"
CalledNumber	"+49521087654321"
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

15 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 (**8.7.1 Defining call number substitutions for a trunk group**, page 81).

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 (**8.7 Forwarding and number substitution**, page 79). The call permission for a user or a trunk group defines whether a call has the right to be made via this trunk group (**8.2 Edit trunk groups**, page 67).

Number Types
Number concept
Mapping of numbers
Examples of number mappings
Placeholder
Further examples of number replacement

15.1 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.

15.1.1 INTERNAL NUMBERS

The numbers 110 and 112 are reserved for emergency calls in Germany. As of SwyxWare V13.30, these numbers are always interpreted as emergency calls, even if they are assigned to an internal user.

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.

This approach will be briefly illuminated in the following 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.

15.1.2 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 (**15.3Mapping of numbers**, page 167). 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.

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.

15.1.3 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.

15.2 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 **7 Creating and editing Locations**, page 62.

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.com** **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.

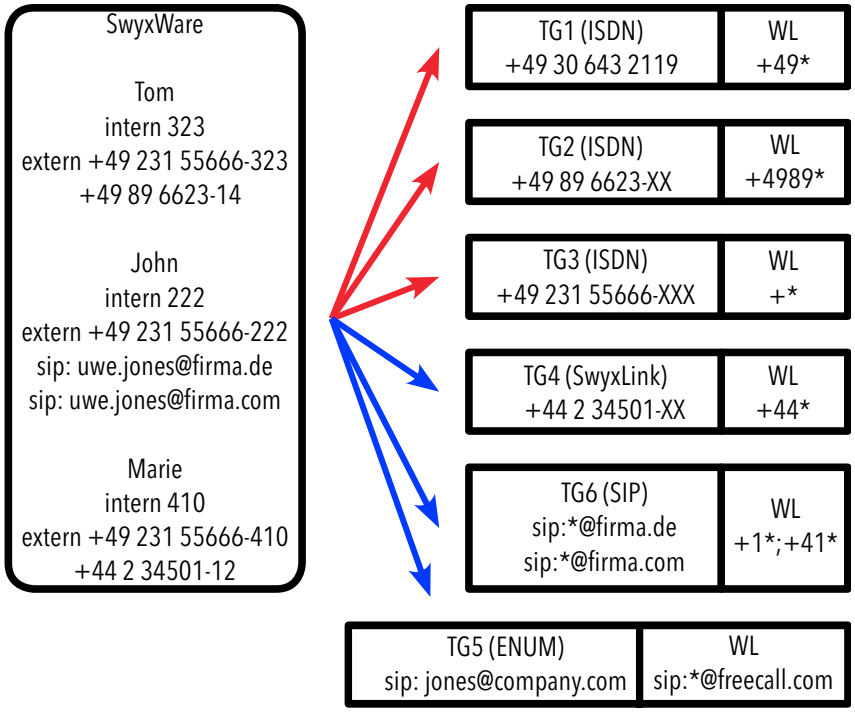


Fig. 15-1: Configuration example for a number plan, trunk groups (TG) and routing (WL)

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 **8.7 Forwarding and number substitution**, page 79.

15.3 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 (**9.3 Creating Users**, page 86 or for groups).

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 **15.1.2External numbers**, page 165).

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.

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.

15.4 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.

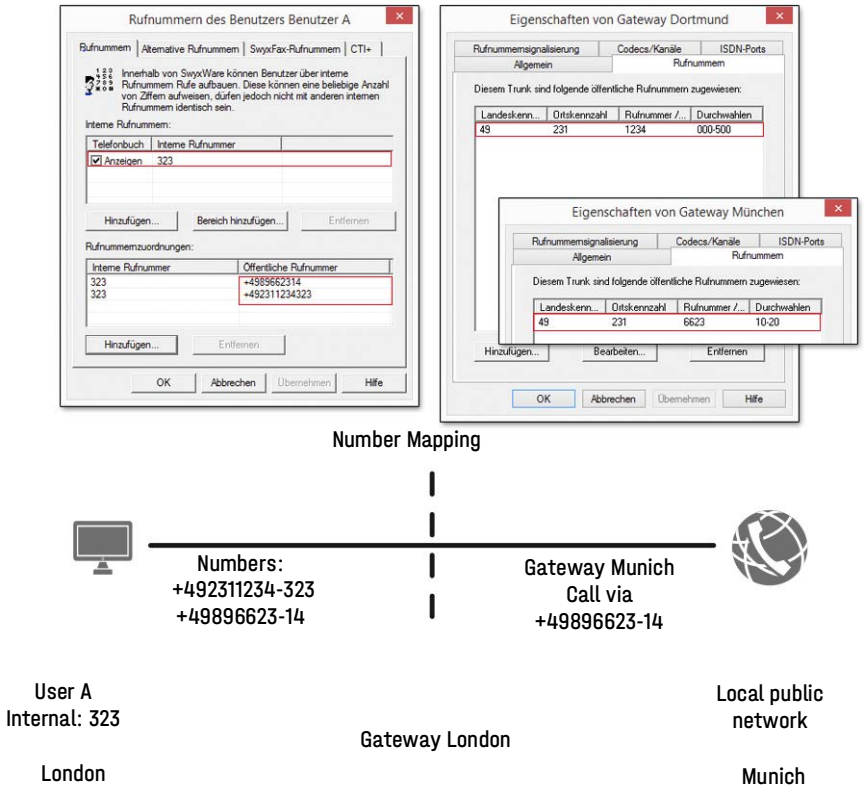
User A

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 Manches-

ter 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 call number in Munich (49 89 6623-14) is signaled to the caller.

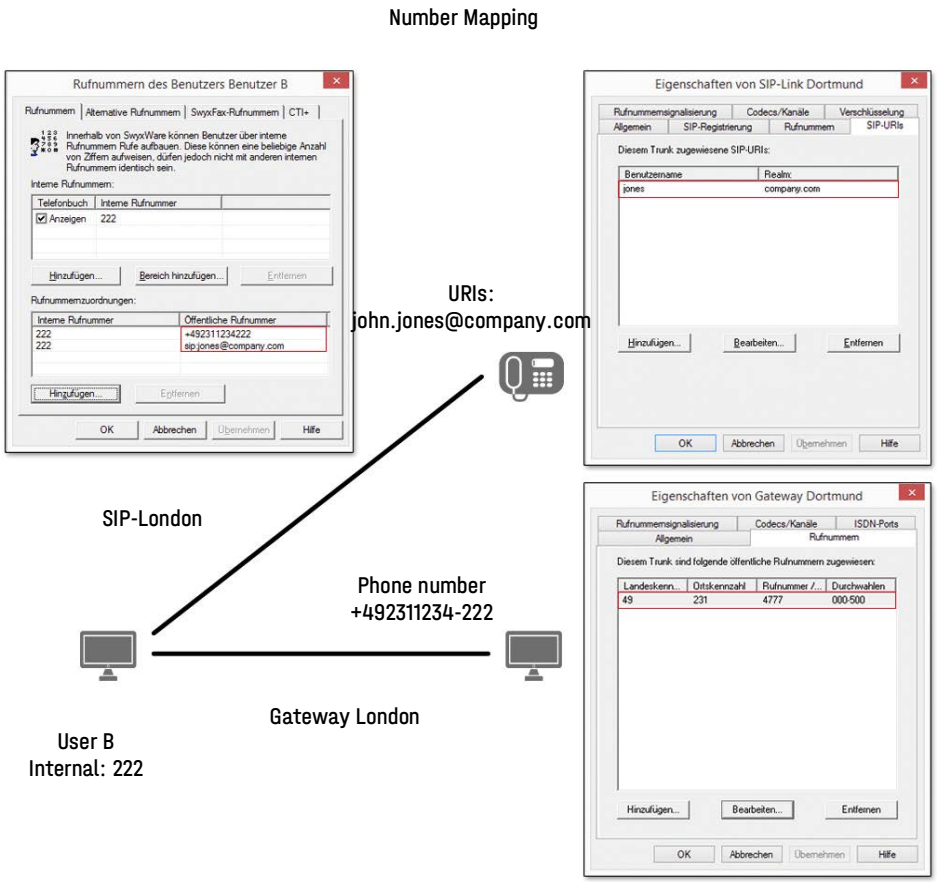
Other internal callers dialing from anywhere in the company can contact him at any time via his internal number (323).



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).

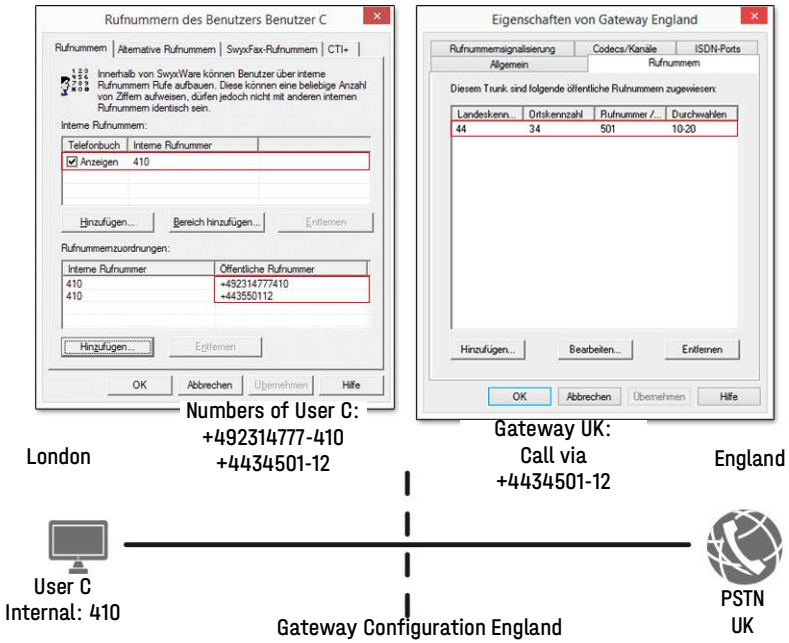


User C

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.

Number Assignment



15.5 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.

15.5.1 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
*	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 171.

Placeholder	Type of number	Explanation
+	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

15.5.2 SPECIAL PLACEHOLDERS

In connection with the call authorizations, and the call number substitution, see **8.7 Forwarding and number substitution**, page 79, further special placeholders are available. 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.

15.5.2.1 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.
[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 these placeholders is then taken from the configuration of the trunk group or user.

15.5.2.2 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.

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.
[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.

Original	Replacement	Explanation
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 +448002830151234567.

15.6 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

15.6.1 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 telephone number externally in the case of 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.

Format	Explanation
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
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 call numbers are expected in canonical format. **Example:** +<Country code><Area code><Number> +442314777555

Format	Explanation
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

Format	Explanation
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 Swyx if there is a missing special telephone code, so that we can consider this code in future versions.

15.6.2 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 (**8.1 Create trunk groups**, page 65).

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.