Release Notes

Swyx 14

Product Version: 14.25

Status: "General Availability"

1. Overview

1.1. Software Versions

Component	Version
Server	14.25.8537.0
Swyx Control Center	14.25.5793.0
Administration	14.25.8537.0
SwyxIt	14.25.8537.0

These release notes cover changes compared to v14.21 If you are updating from an older major version less than v14, please refer to the v14 release notes first

1.2. Version history

Version	Release date	Release Notes
Swyx 14.00	16. Mai 2024	Release Notes 14.00
Swyx 14.01	17. Juni 2024	Release Notes 14.01
Swyx 14.10	14. October 2024	Release Notes 14.10
Swyx 14.11	23. October 2024	Release Notes 14.11
Swyx 14.20	16. June 2025	Release Notes 14.20
Swyx 14.21	26. June 2025	Release Notes 14.21

2. Changes

SWYX 14.25	**3**

2.1. Swyx 14.25

2.1.1.   New features

Deliver call to mobile

Starting with Swyx 14.25 it is now possible to deliver an incoming call to the user's mobile number in addition to the regular internal destinations (logged in clients and devices). This functionality is configurable in Swyx Extended Call Routing [ConnectTo Block] which now offers two new configuration options:

- Deliver to user's mobile number
- Wait for DTMF confirmation

User's mobile number for additional call delivery can be configured in Swyx Control Center.

Mobile number configuration can be performed by system administrators or the user himself.

Once "Also deliver to user's mobile number" option is enabled, the call will not only be delivered to the destination defined in the ConnectTo Block, but also to the mobile number of the user, if configured.

Same option is also available for group call routing scripts. Once enabled, an incoming call will be delivered to the configured mobile numbers of all the group members in addition to the configured internal numbers.

This works for sequential and random delivery hunt groups only. Behavior for parallel delivery hunt groups is not defined, especially in combination with the "DTMF Confirmation" functionality.

A call delivered with a GSE - ConnectTo Block can optionally wait for a DTMF confirmation tone sent by the called party before the call is considered "Connected".

The DTMF character sequence is configurable, as well as an optional announcement to be played to the called party.

Microsoft 365 Mail Mode

With Swyx 14.25, Microsoft 365 (Exchange Online) email support is introduced. This functionality enables the system to send Emails via your Microsoft 365 service without the need to enable SMTP and switch off Microsoft 365 secure defaults.

This enhancement uses the existing Swyx Entra ID federated services configuration to authenticate and send emails using Microsoft 365 (Exchange Online).

If you already used Entra ID federated Services in Swyx, refer to the SwyxWare manual for necessary changes to the existing Entra ID App registration. For sending emails the app registration needs to have the Mail.Send permission for Swyx to send emails via this Entra ID application.

All email operations occur within Microsoft's trusted cloud infrastructure, adhering to enterprise-grade compliance and security standards.

Calendar-based call routing for Microsoft 365

With the new Microsoft 365 integration introduced in 14.20, Swyx uses Graph API to get user's appointments for the automatic away presence state detection. This feature now also uses that information to implement the calendar-based call routing so that it is fully available for Microsoft 365 as well, starting with Swyx 14.25

Some notes:

Microsoft Exchange (EWS) based functionality remains without changes, but will only be used by the SwyxServer if the new Microsooft 365 implementation is not available.

The special service settings (in Swyx Control Center > General Settings > Special Service Settings > IpPbxSrv): "CalendarAccessM365", "CalendarAccessEWS", and "CalendarAccessWorkingElsewhereIsOoo" keys had been introduced for the Beta-Phase in Swyx 14.20 are re no longer needed and have been removed in Swyx 14.25.

Enhanced Firmware distribution for Unify devices

Swyx 14.25 unified the firmware distribution process and configuration. Starting with this version, firmware downloads and distribution for Unify devices are handled in the same way as DCF Devices and SwyxIt! Clients, i.e. via Swyx Control Center and Firmware Information Service (FIS).

The goal of this enhancement is to deliver a consistent and unified firmware management experience across all device types integrated with Swyx solution. This improvement simplifies administration, reduces configuration errors, and removes the dependency on legacy distribution methods.

Before updating to Swyx 14.25, it should be ensured that all connected SwyxPhones are running the latest firmware version. Older firmware versions do not support firmware downloads via https and can therefore only be updated manually after updating to Swyx 14.25.

Enhanced Administrator-Password security for DCF Devices

In alignment with the EU Radio Equipment Directive (RED) and the latest European cybersecurity requirements, Swyx 14.25 enforces updated password complexity standards for all managed devices.

This update introduces a unified, regulation-compliant password generation mechanism that automatically applies to new and existing devices. The change ensures enhanced device security and compliance with evolving EU regulations affecting connected equipment. Our revised password management approach standardizes these requirements across all devices — ensuring compliance and reducing administrative overhead.

Devices that have already been commissioned will be automatically reprovisioned to apply the new compliant password format. No manual action is required for this transition.

Support for Yealink WiFi-phones AX8-series

With this release, Enreach extends the Swyx device integration portfolio by adding support for the Yealink AX83H – a next-generation cordless handset now fully integrated as a DCF device.

This integration brings the well-known Swyx–Yealink experience from desktop devices to the Yealink handset format, providing users with a familiar and feature-rich communication environment while ensuring seamless management and provisioning through the DCF framework.

Some desktop-oriented functions are not applicable or practical for the Yealink AX83H handset form factor and are therefore not supported in this integration:

 - Logging on/off users directly at the device

 - Displaying Swyx Presence Contacts (not supported in handset hardware)

Swyx Control Center: List of active devices

Administrators are used to being able to see a list of all currently logged in devices with information about firmware/versions and user the device belongs to. Until Swyx 14.25 Swyx Control Center offered this information only as an accumulated list of versions on the Telemetry page. With Swyx 14.25 we've added a page to display all currently active devices and allow filtering for certain values, like name, owner, version and MAC/IP addresses. Some information will be added in a detailed view, like information about the user's OS.

The list is automatically refreshed every 30 seconds.

Swyx Control Center: Quick access menu

The Quick Access Menu provides a fast and accessible way for users to navigate between pages without using the mouse. It is designed to improve productivity, especially for power users and administrators who frequently move between different sections of the Control Center.

- The menu can be opened from any page by pressing the keyboard shortcut Alt + Q (Option + Q for Mac users).
- Once opened, users can type or scroll through a combo box containing a list of available pages.

The content of the Quick Access Menu dynamically adapts to:

- User role: The list of available pages depends on the role of the logged-in user.
  - Example: A System Administrator will see different entries than a User Administrator.
- Current context: The available entries also depend on the current selection or context within the Control Center.
  - Example: If no User or Trunk is selected, related pages will not appear in the menu.

2.1.2. Technical Improvements / Changes

SwyxIt! HTTP Proxy Detection

When using a remote connector tunnel connection to access Swyx-Server, SwyxIt! 14.25 can establish that connection via an HTTP proxy configured in Windows. Per default SwyxIt! only uses a proxy when the remote connector port to connect to is 443 which is rarely the case and never when connecting to a SwyxON tenant.

This detection is already present in previous SwyxIt! versions but did not work properly when auto-detection or proxy script had been configured.

To enable proxy detection and usage regardless of the destination RC tunnel port, set the following registry key

Path	HKLM\Software\Swyx\Client Line Manager\CurrentVersion\Options
Name	AlwaysUseProxyForRC
Type	REG_DWORD
Value	1 = always try Windows http proxy when configured
Default	0 = only use Windows http proxy for HTTP Rest API requests and RC tunnel connections to port 443

The initial HTTPS REST API connection SwyxIt! makes for authentication and retrieving tunnel configuration always detects and uses an HTTP proxy if configured in Windows.

Detection

SwyxIt! retrieves proxy configuration from Windows and uses the following precedence

- Proxy auto-detection
- Proxy script (PAC)
- Static proxy configured for the Windows user
- Static proxy configured for the Windows system

The first three options can be set via Windows Settings - Network & Internet - Proxy, the fourth one using the "`netsh winhttp set proxy`" command. When any of the 4 options returns a valid proxy configuration, that configuration is used. Option 1 and 2 can have four results (proxy, no proxy, detection failed, not configured). Only in the "detection failed" and "not configured" cases the detection proceeds with the next option.

Connection

SwyxIt! first tries to get a proxy configuration from Windows for destination `<public-server-address>:<public-server-port>` using the above-described order. If that detection returns a proxy, SwyxIt! uses that to authenticate and to get the RC tunnel parameters. SwyxIt! always uses http to connect to the proxy, but https to connect to the Server API via that proxy. If authentication succeeds, proxy detection runs again for the destination `<rc-tunnel-address>:<rc-runnel-port>`. If that detection returns a proxy, SwyxIt! uses it to establish the TLS RC tunnel connection to SwyxWare.

Proxy requirements

The proxy you use must support HTTP/HTTPS and not intercept TLS connections. It must be able to forward the Swyx authentication REST API and tunnel ports. On-premises these are 9101 and 16203 per default. For SwyxON both ports are custom defined per-tenant.

We tested SwyxIt!s proxy support with Squid (https://www.squid-cache.org/).

Troubleshooting

SwyxIt!s proxy detection is logged in the clmgr trace when trace module RestAPI is set to level 6. The RC tunnel part of the proxy detection is logged with trace module Tunnel and TunnelMgr set to 6

Updated Provider Profiles

Following Provider Profile changes are introduced in Swyx 14.25:

Profile	Changes
NFON SIP Trunk Flexx	Added Attributes • TransportType="UDP" • IgnoreSIPDiversionHeader="true"
NewVoice Mobicall alarm server	New
iWay (CH)	• attribute proxy changed from 'sip3.phone.iway.ch' to 'sip01.iway.ch' • attribute reRegistrationTimeout changed from '600' to '300'
isp voip (CH)	New
RussMedia (AT)	New
Swyx Trunk (DE) / Swyx Trunk TLS (DE)	Name Changed to Enreach Trunk (DE) / Enreach Trunk TLS (DE)

Improved SwyxPhone Whitelist Download

To keep the SwyxPhone Whitelist up-to-date, Swyx downloads the current whitelist file using a scheduled task running once per night.

With this improvement, the file will not be fully downloaded every time, but only when changes have been detected. The scheduled task still runs every night when enabled but first uses an HTTP HEAD request and checks some response headers (ETag and LastModified) to detect if the already downloaded whitelist file is still up-to-date and download the updated file if not.

Swyx Control Center Improvements

Improved keyboard navigation

With Swyx 14.25, we improved the keyboard navigation in Swyx Control Center in order to simplify the administration and improve the workflows. In Swyx 14.25 the well-known navigation behavior in wizards by pressing "Enter" key ware unified and improved. As long as no validation errors appear, administrator is able to go to the next wizard page directly.

Improved activation process

With Swyx 14.25 Swyx Control Center offers an activation wizard under Licenses and Features page instead of a simple Input. It will improve the activation workflow and increase the visibility of the single activation steps.

Improved trunk group deletion confirmation

Removing a configured Trunk Group from the system might have a huge impact on the telephony in general. Due to the fact that related configuration, such as assigned trunks, routed number etc., is not directly visible on the Trunk Group page, it might be difficult to keep an overview. To make sure the Administrator is informed about all the related configuration items, that would also be deleted, Swyx Control Center will display it in the "Delete Trunk Group" confirmation dialog.

Inter-location information display

Following information is added:

- Limit Inter-Location calls flag is added to the locations overview grid.
- Max. number of allowed simultaneous calls added to the location details view.

Error message on deletion of locations is now improved and contains a clear reason description (Assigned to a user / Assigned to a Trunk Group)

Fixed Issues (reported by customers)

ID	Support Ticket ID	Title
223843	342401, 345999	Modern S!: On terminal server cluster the app is only installed upon very first login
225914, 225856, 226185	364344	EntraID: SDC login via EntraID is possible although the feature profile does not include Federated Authentication EntraID: SwyxWare SDC - Federated Login not possible - "User not licensed" EntraID: SwyxWare Classic - Federated Login not possible - "User not licensed"
225838	365076	One-way mediastreaming on parallel calls
225111	349036, 358428, 358409, 358307, 355141	IpPbxSrv: Call dropped by '500 internal server error' if CR CR forwards call to external number (->media brigde activated) and 'Tones Available' event is processed
225697	349036, 358428, 358409, 358307, 355141	IpPbxSrv: No media from CR after call was forwarded to external number (->media brigde activated) with timeout
207916	247245, 320307	ONPA: Yealink kann an deaktivierten Usern angemeldet werden
225882	365542	AscomDCF: SetStatus calls fail and firmware version info in SCC is not up to date
226389	351053	PhoneMgr: DLS property is not stimulus-service-menu-key is provisioned to phones not supporting it
225860		IpPbxSrv: After RI to group voice box all group members get 'missed call' pcle
225734	363207	SwyxON - SCC nach Update auf 14.21 Benutzer Passwort wird nicht mehr übernommen - Copy
226559	368360	Memory leak in IpPbxSrv with more than 62 active or hanging auto-delete threads
225311, 225312	360213	ConfigurationPlanner: OutboundProxy is not considered Users are not added to Everyone Group
225856	364344	EntraID: SwyxWare SDC - Federated Login not possible - "User not licensed"
226553, 226561	371106, 371105, 371103, 372966	SCST timeout for PutDNSChallenge too short SCST scheduled task for LE cert check and IP check runs always at the same time

226662	366846	IpPbxSrv: No media after ConnectTo with external number and 'proceed with destination script ' enabled
226660	372573	MgmtApi does not use same mechanism for QRCode URL in method for SCC as for welcome mail

ConfigDataStore Client API Changes

Mail Server Configuration

The new Email sending feature and improvements in the way the SMTP password is stored in the Swyx database needed some changes to the CDS client API.

Mail sending parameters can no longer be retrieved or set via the **[GlobalConfigEntry]** object. All Mail/SMTP related properties either return **[null]** or an empty string. Setting these properties has no effect.

There are two new methods on the **[AdminFacade]** object:

[GetMailServerConfiguration]

[PutMailServerConfiguration]

to get and set the mail server configuration. It supports the same parameters you can set in SCC.

The SMTP password cannot be retrieved. Neither via the old, nor via the new API. **[GetMailServerConfiguration]** only returns if a password has been set or not. A new password can be set via the **[PutMailServerConfiguration]**

Remote Connector Configuration

The remote connector configuration which can be set via **[GetGlobalConfigEnum.SaveRemoteConnectorConfig()]** ignores all parameters and values regarding manual certificate mode, because we removed that functionality.

Unattended Setup Changes

The SwyxServer unattended setup definition file (unattended.xml) has changed to support the Microsoft 365 Mail Sending Mode and SwyxPhone firmware update changes. If you deploy SwyxServer unattended do not use an unattended.xml from an older Swyx version. Use the version shipped with 14.25 and apply the changes from your old xml to the new one.

2.1.3.   Discontinuations

SwyxIt! Analytics removed

With the new SwyxIt! client (SwyxIt! 14.00) we introduced a new modern way to gather user feedback. That makes the opt-in SwyxIt! Analytics, introduced in previous versions, obsolete. With Swyx 14.25 we entirely removed the SwyxIt! Analytics from the client.

Removed Remote Connector manual certificate handling

Swyx previously offered both automatic and manual modes for adding and maintaining Remote Connector Tunnel Root, Server, and Client TLS certificates. Most Swyx installations utilized the automatic mode, while Swyx Mobile never supported the manual mode. Starting with version 14.25, only the automatic mode is available.

This enables Swyx to automatically renew expired certificates and create client certificates for new users.

- When updating Swyx to 14.25 from a version with automatically created certificates: Existing RC certificates will continue to be used until they expire.
- When updating Swyx to 14.25 from a version with automatically created certificates, but with customer managed certificate security: The remote connector configuration will be changed to the new automatic mode. All RC certificates will be replaced with new ones.
- When updating Swyx to 14.25 from a version with manual configured RC Certificates: The remote connector configuration will be changed to the new automatic mode. All RC certificates will be replaced with new ones.

SwyxIt! Video Removed

Native Swyx Video functionality integrated in server and SwyxIt! Client (Classic) was already deprecated in SwyxWare Release v13.26 and is now completely removed.

The SwyxIt! MSI had "Video" as a feature you could select, e.g. for unattended setups. Specifying that feature explicitly, e.g. via
`[msiexe.exe /I SwyxIt!EnglishUK64.msi ADDLOCAL=…,VIDEO,… ]`

will fail the setup with an error.

Firmware distribution for SwyxPhones via FTP

The firmware distribution via FTP for SwyxPhones has been abolished. Instead, SwyxPhones now get their firmware updates via https. If you keep using the default firmware versions, then nothing changes for you. If you have configured some specific firmware versions to be distributed locally, then you need to offer the corresponding firmware files from https-URLs instead and configure those in Swyx Control Center under *[General Settings → Versions → SwyxPhones]*.

2.1.4.   Issues / Limitations / Challenges

Microsoft 365 Mail Support

Using this Feature require configuration of Federated Authentication with Microsoft Entra ID. Additionally, special permission need to be granted to the Swyx Application (Mail.Send) in order for Swyx to be able to use E-Mail functionality.

For GDPR compliance reasons, it is recommended to disable Sent mailbox or limit the access to it. This helps minimize the storage of personal data and reduces the risk of unauthorized access.

Sending E-Mails with ECR

Starting with 14.25 SwyxServer will always use the sender address configured in Swyx Control Center for sending emails. If you have ECR scripts sending emails with a custom sender address, that address is retained in the script but will not be accepted and email sending may **<u>fail</u>**.

Because GSE in 14.25 no longer allows to set the sender address in the *[SendEmail]* block remove and re-add the *[SendEmail]* block in your ECR scripts to remove the custom sender address from the script.

2.1.5. Introduced beta features

None in this version.

3. System requirements
3.1. Hardware recommendations

Table below shows recommended hardware specification depending on the system-size. We reommend to monitor your system utilization and adapt theVM size accordingly.

Size (User)	< 75	75 to 200	200 to 1000	1000 to 1500
CPU	2 Cores	4 Cores	4 to 6 Cores	6 to 10 Cores
RAM	6 GB	6 to 8 GB	8 to 12 GB	12 to 16 GB
Storage	128 GB	128 GB	128 to 512 GB	
Network	100 Mbit		1 to 10 Gbit	

For Installations larger than 250 users or high call-ratio (call-volume), please contact our Swyx Presales team (presales@swyx.com) for detailed recommendations on your specific setup.

Detailed and up-to-date system hardware requirements, as well as additional information on Sizing Options are published in our knowledge base: https://service.swyx.net/hc/en-gb/articles/13772878531996

3.2. Software

Please ensure that ongoing windows updates are completed before starting to install or update Swyx components.

After the installation of the server components, the Config Wizard starts and must run to the end. Do not terminate the Config Wizard during the process is running.

The table below shows the Operating System and software requirements for the corresponding Swyx components (Current version only).

Component	Operating system	Software Components
Swyx Server	Windows Server 2019, LTSC Windows Server 2022, LTSC Windows Server 2025, LTSC	Microsoft 365 Office 2024 SQL Server 2019 SQL Server 2022 .NET Framework 4.8
SwyxIt! (TS)	Windows Server 2019, LTSC Windows Server 2022, LTSC	.NET Framework 4.8
SwyxIt! Swyx Ware Administration (MMC)	Windows 11 Windows Server 2019 Windows Server 2022 Windows Server 2025	.NET Framework 4.8
Swyx Connector for MS Teams	Windows 11	Microsoft 365

Detailed and up-to-date software requirements are published in our knowledge base: https://service.swyx.net/hc/en-gb/articles/13916515322908

4. Installation/Update

Instructions for installation and updates can be found in the Swyx documentation: https://help.enreach.com/cpe/14.25/Administration/Swyx/en-US/index.html - page/help/chap_installation.08.01.html

5. Specific behavior and environments

Use of Jabra devices with SwyxIt!

If you want to use devices of Jabra together with SwyxIt!, please mind the following hints:

- Accepting a secondary incoming call using Jabra device buttons may terminate an existing primary call
- Toggling between two concurrent calls or putting an existing call on hold using Jabra device buttons may not be possible
- The ringing behaviour of Jabra devices is not only determined by settings in SwyxIt! but is also impacted by settings in Jabra Direct

SwyxIlt! with Microsoft Outlook

In the context of removing an issue with security warnings that appear when Outlook is used together with SwyxIt! (Swyx bug 185649) a new Windows Registry Key has been introduced that rules if the previous Outlook warning appears. In the registry key path "**Computer \ HKEY_CURRENT_USER \ Software \ [XXX] \ OutlookAddIn \ SecurityManager\"** (with [XXX] being Swyx or T-Com), the registry value is named "DisableOutlookSecurityWarnings", the type is a DWORD and the values are: '0' to have the security warnings enabled (default behaviour); '1' to have them disabled. Even if the Registry Key was set to '1', the warning messages still appear, though, when creating, editing or deleting an Outlook contact. If the new Registry Key was not already created by SwyxIt!, the user can do so at the aforementioned path with the specified type and desired value.

Use of generic USB- or Bluetooth-Headsets

- Any generic headset must be configured manually in SwyxIt! (in Audio Modes/Headset and Audio Modes/Ringtones)
- Volume sliders and microphone mute/unmute buttons are working but are not in sync with SwyxIt!/Headset. E.g. If the headset has an own button to mute/unmute the mic, the mic will be muted/unmuted when the button is pressed, but it won't be displayed in the SwyxIt! client (and vice versa)
- Air Pods cannot be controlled via Air Pods gestures
- Air Pods appear twice in the SwyxIt! Audio device list: "Air Pods Hands-Free AG Audio" and " Air Pods Stereo". In order to get them working, user MUST configure the following:
  - As Headset configure: Air Pods Hands-Free AG Audio.
  - For Ringtones both will work, but to make it easier it is recommended to select "Air Pods Hands-Free AG Audio"

Use of SwyxIt! in RDS/Terminal-Server environments

When multiple users use their SwyxIt! on the same RDS/Terminal-Server environment, the Remote Connector tunnel is started by the first SwyxIt!. All subsequently started SwyxIt! instances use the same Remote Connector tunnel instance. In case the first-started SwyxIt! is stopped, the commonly used Remote Connector tunnel is decommissioned, and all other SwyxIt! instances lose their connection to the server until a new Remote Connector tunnel is established by a restart of one of the remaining SwyxIt! instances.

LDAPS support for the Yealink global phonebook

All necessary certificates for the LDAPS support of the Yealink global phonebook are autogenerated during the installation. If the SwyxWare Server domain association is changed after installation, those certificates have to be regenerated. In order to do that the certificates under ADAM_SwyxGlobalPhonebook\Trusted RootCertificate Authorities and ADAM_SwyxGlobalPhonebook\Personal, issued for your server has to be deleted. After the deletion of the root and sever certificates for the SwyxGlobalPhonebook rerun the configuration wizard. This will generate new certificates for the LDAPS support.

If you used *Swyx Connectivity Setup Tool* to provision a TLS server certificate to SwyxWare re-run that tool to re-provision the certificate after a server name update.

Changes to call notes creation

With the Call Journal extension displaying the call duration, the Call journal entries are now created after a call is finished. Users which utilized the Call Journal entry to create an e-mail for call notes can now use the context menu of an active line to create this e-mail. For this, users can find a new entry labelled E-Mail, which launches the same functionality as the similar button in the Call Journal header.

MS Teams Presence Sync Service Enablement

With SwyxWare 13 the MS Teams User Presence Sync Service is always installed. Its functionality can be enabled or disabled in Swyx Control Center. If you do not have this service installed before you update to SwyxWare 13 it will not be installed during the update.

In that case, if you intend to use it, run the setup again after the update, choose *Modify* and select the *MS Teams User Presence* and enable it in Swyx Control Center.

Licensing for MS Teams Connector

For the Swyx Connector for MS Teams to work it must, that each user has an assigned MS Teams Connector License. Otherwise, the MS Teams Connector application in MS Teams won't load. In case the MS Teams Connector doesn't load any more after an update from Versions 13.00 or 13.05 please check the proper Connector license assignment.

6. Supported portfolio products, add-ons and devices

Type	Product	Preferred Version
LDAP Directory	ESTOS Metadirectory Standard	v5.0.7.10657 or v6.0.0.12135 or v6.2.4.14520
LDAP Directory	C4B XPhone Connect	v7.0.74 or v8.x
Call analysis	Swyx Analytics by Aurenz	v14.x Earlier versions are not supported
	Swyx Analytics for MS Teams	v14.1.0.3 or newer
Microsoft Office Add-In	Microsoft Office 32-bit	Office 2019-2021
	Microsoft Office 64-bit	Office 2019-2022
Lotus Notes	Info	The Swyx Connector for Notes Integration is compatible with IBM Notes/Domino 9, 10 and HCL Notes/Domino 11. Out of support starting with Swyx 14
Call Queue	Visual Groups	1.16 or newer

Type	Product	Preferred Version
SwyxPhone	SwyxPhone L62 100 MBPS	HFA V1 R8.2.0
	SwyxPhone L62	HFA V1 R8.2.0
	SwyxPhone L64	HFA V1 R8.2.0
	SwyxPhone L66	HFA V1 R8.2.0
	SwyxPhone L71	HFA V2 R0.18.1
	SwyxPhone L72	HFA V2 R0.18.1
	SwyxPhone L74	HFA V2 R0.18.1
	SwyxPhone L77	HFA V2 R0.18.1
	SwyxPhone L615	HFA V3 R0.42.1
	SwyxPhone L620	HFA V3 R0.42.1
	SwyxPhone L640	HFA V3 R0.42.1
	SwyxPhone L660	HFA V3 R0.42.1
	Swyx Handset P280	V 1.88
	Swyx Handset P300	Most actual firmware
Yealink	Phone T31G	124.86.133.6
	Phone T41S	66.85.133.12
	Phone T42S	66.85.133.12
	Phone T46S	66.85.133.12
	Phone T48S	66.85.133.12
	Phone T53	96.87.133.2
	Phone T53W	96.87.133.2
	Phone T54W	96.87.133.2
	Phone T57W	96.87.133.2
	Expansion Module EXP40	11.16.0.0
	Expansion Module EXP50	1.0.1.8
	WiFi Handset AX83H	180.87.133.2
	WiFi Handset AX86R	180.87.133.2
	Conference Phone CP920	78.85.133.5
	Conference Phone CP925	148.86.133.4

Information on preferred firmware of TAP certified products can be found here:
https://www.swyx.com/products/third-party-products.html

For portfolio audio products, please always use the latest recommended firmware by the vendor, unless otherwise announced in our help centre: service.swyx.net

Type	Product	Preferred Version
DECT	SwyxDECT 500	FW Pack v.5.30.B09 includes the latest FW versions for supported base stations, handsets and repeater
	Enreach DECT 600	FW Pack 7.70.B0200 (v1) includes the latest FW versions for supported base stations, handsets and repeater
	SwyxDECT 800 (Ascom)	FW Pack v.13.1.2 (v2) includes the latest FW versions for base stations, IP-gateways, and handsets
Gateways	AudioCodes: MGW Cloud S (M500-2B-2S-NLV)	7.24A.356.069 or higher
	SwyxConnect 8xxx	
	AudioCodes: MGW Cloud M (M800-4S-4O-4B-4L –NLV)	Firmware 6.80A.308.003 or higher
	AudioCodes: MGW Cloud L (M1KB-MSBG1 ,M1k-VM-1SPAN,M1k-VM-4BRI,M1K-VM-4FXS-NLV)	F6.80A.365.002 or higher
	Lancom 17xx, R8XX	Firmware 10.42.0.280 RU1 or higher
	Bintec: Digitalisierungsbox	11.01.03.103 or newer
Media Packs	AudioCodes	6.60A.369.002

We recommend customers use the "Preferred Version" for the given products. The preferred software versions offer tested and confirmed level of functionality. However, the devices might also operate with older or newer software version with the caveat that recently added interoperability or advanced features may not be possible when using these versions. In cases, if a defect is found when using other versions, it may be necessary to update to the supported version.

7. Known issues

ID	Support Ticket ID	Title
225803		Yealink-Wifi: It's not possible to pick up a call when external party has number suppression activated
226141		SCC: Telemetry - "Seconds since last call" only shows time since last internal call
226612	372258	After the function user logoff from all devices the PresenceSync device/publication will be removed too.
225857	366073, 364936, 362734, 363992, 361199, 361218, 361060, 362774, 368164, 373307, 373710	Swyx user loose the "Use server default" login device type setting
225978		Federated contacts with numbers from the pbx will be synced and used for name resolution
224616	364570	SCFM365: Personal outlook contacts is displayed for non contacts after call transfer

8. Everything else

Beta feedback

Please use beta@enreach.de as a feedback channel for introduced beta-feature

Documentation

Please refer to
https://www.enreach.de/en/products/support/documentation.html#jump-SwyxWare
for detailed documentation of the product.

Please use our knowledge base under https://service.swyx.net/

Service & Support

The support for Enreach product line 'Swyx' is handled through the regular Swyx Support process: https://swyx.zendesk.com/