
EdgeMarc 2900 POE Interop with Swyx PBX - Use Case 1



Table of Contents

- [Interoperable Vendors](#)
- [Copyright](#)
- [Document Overview](#)
- [Scope](#)
- [Non-Goals](#)
- [Audience](#)
- [Pre-Requisites](#)
- [Product and Device Details](#)
- [Network Topology Diagram](#)
 - [Use Case 1 Deployment Topology](#)
 - [Interoperability Test Lab Topology \(or Call Flow Diagram\)](#)
- [Section-A: EdgeMarc Configuration](#)
 - [Connectivity](#)
 - [Configuring EdgeMarc A](#)
 - [Configuring EdgeMarc B](#)
- [Section-B: SwyxWare, SwyxIt and HFA Phone Configuration](#)
 - [Configuring SwyxPBX](#)
 - [Adding a User](#)
 - [Configuring a SIP Trunk](#)
 - [Configuring the SwyxIt Client](#)
 - [Configuring the HFA Phone](#)
- [Supplementary Services and Features Coverage](#)
- [Caveats](#)
- [Support](#)
- [References](#)
- [Conclusion](#)

Interoperable Vendors



Copyright

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved. The compilation (meaning the collection, arrangement and assembly) of all content on this site is protected by U.S. and international copyright laws and treaty provisions and may not be used, copied, reproduced, modified, published, uploaded, posted, transmitted or distributed in any way, without prior written consent of Ribbon Communications Inc.

The trademarks, logos, service marks, trade names, and trade dress ("look and feel") on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

Document Overview

This document outlines the configuration best practices for Vodafone involving EdgeMarc 2900 when deployed with SwyxPBX. This document also provides the configuration snapshot of the interoperability performed between Ribbon's EdgeMarc 2900 and SwyxPBX, SwyxIt and Swyx Phone. SwyxPBX is a fully “**Hosted PBX Service**” with cloud telephony. In cases when you no longer have a PBX in your company, you obtain all functions and features of a PBX as a service from the cloud.

Scope

This document provides configuration best practices for deploying Ribbon's EdgeMarc 2900 with SwyxPBX and associated users. Note that these are configuration best practices and each customer may have unique needs and networks. Ribbon recommends that customers work with network design and deployment engineers to establish the network design which best meets their requirements.

Non-Goals

It is not the goal of this document to provide detailed configurations that will meet the requirements of every customer. Use this document as a starting point and build the SBC configurations in consultation with network design and deployment engineers.

Audience

This technical document is intended for telecommunications engineers with the purpose of configuring both the Ribbon EdgeMarc 2900 and the SwyxPBX and associated users.

Steps will require navigating the third-party product as well as the Ribbon product using graphical user interface (GUI) or command line interface (CLI). An understanding of the basic concepts of TCP/UDP/TLS, IP/Routing, and SIP/RTP/SRTP is needed to complete the configuration and any necessary troubleshooting.

Pre-Requisites

The following aspects are required before proceeding with Ribbon EM 2900 POE and SwyxWare 12.10:

- SwyxWare 12.10 is installed in a Windows Server Platform and connected to the network.
- A 190 trial license is available and obtained from Swyx.
- Remote Desktop access to a Windows host is available for remote access and configuration.
- A valid 6 months trial License is running on the Server.
- HFA firmware is loaded and installed on a Unify CP205 Phone Unit.

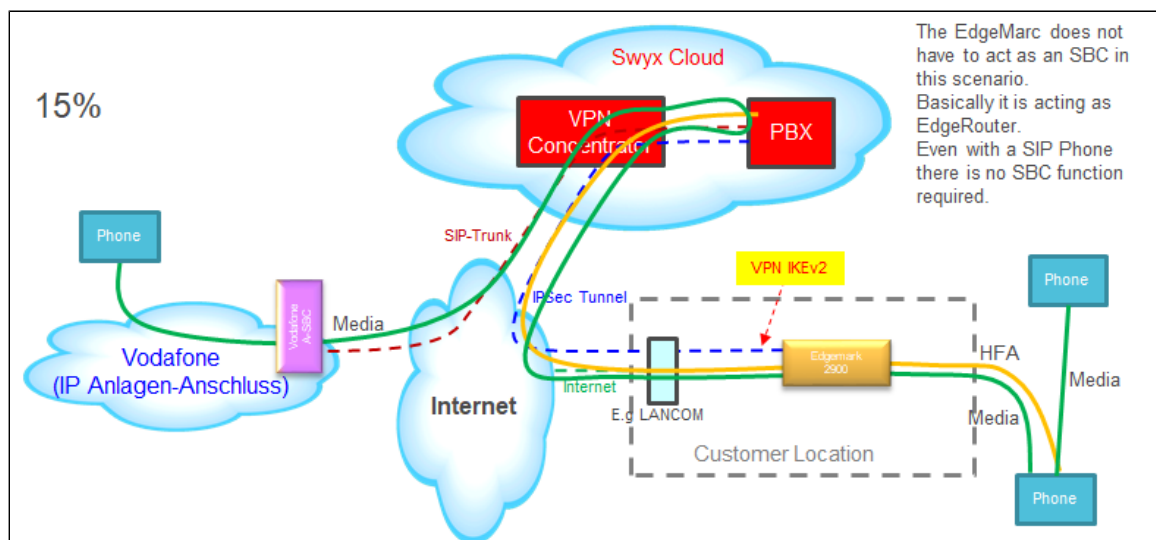
Product and Device Details

	Equipment/Product	Software Version
Ribbon Communications	EdgeMarc 2900 POE	Version 15.8.3
Third-Party Products	SwyxWare	V12.10.16296.0
	SwyxIt	V12.10.16296
	Windows Server	2019
	Unify CP205	V1 R3.9.0 HFA 190516

Network Topology Diagram

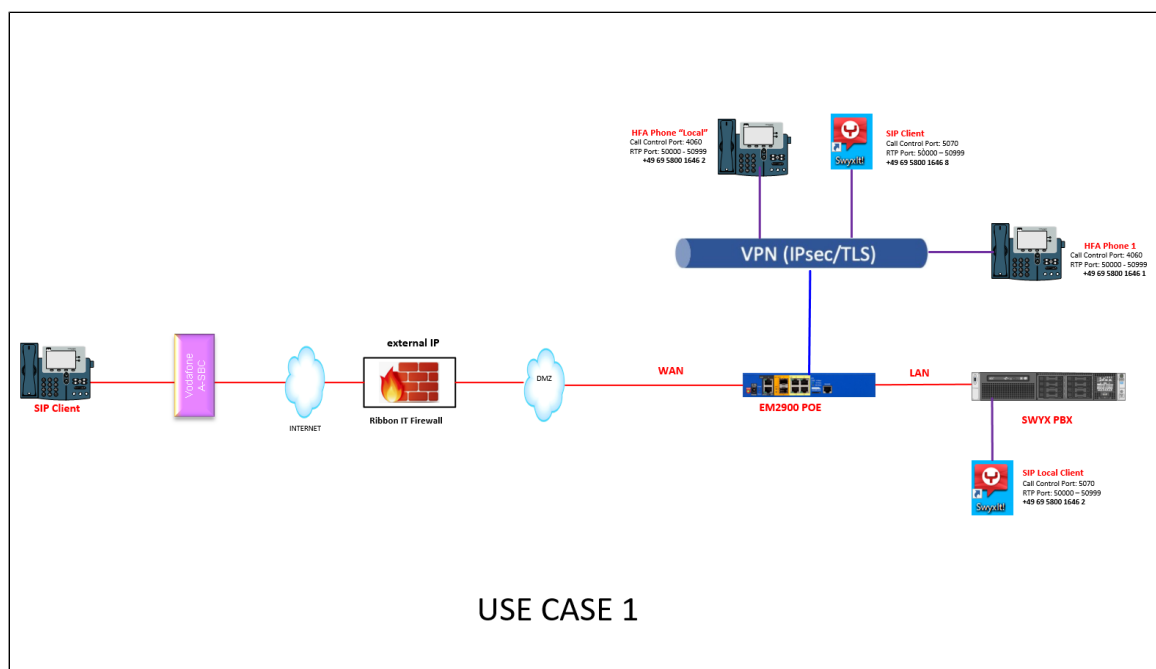
Use Case 1 Deployment Topology

The deployment topology diagram is depicted below.



Interoperability Test Lab Topology (or Call Flow Diagram)

IOT high-level architecture covering call flows and overall topology is depicted below.

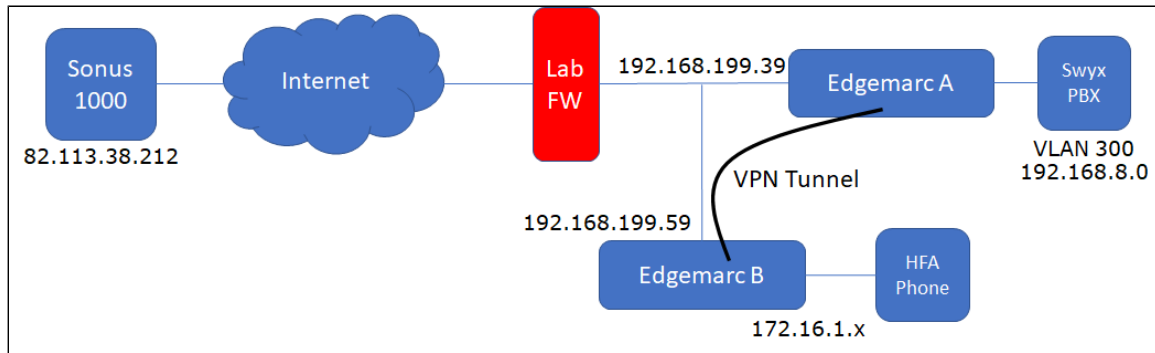


Section-A: EdgeMarc Configuration

Connectivity

Two EdgeMarcs were employed in the lab in order to achieve the desired topology:

- EdgeMarc A terminates a VPN tunnel and has its SIP ALG function enabled to support connectivity to the SIP Service Provider.
- EdgeMarc B is serving the role of a remote office with phones only. EdgeMarc B has a VPN tunnel configured, but no SIP functionality.



Configuring EdgeMarc A

In this use case, EdgeMarc A serves as a VPN termination device in addition to supporting SIP. An IPSec tunnel was configured:

1. Enable the VPN module on the main VPN page, then click Add a new tunnel.

VPN
[Help](#)

Configuration Menu

- + [Admin](#)
- + [Network](#)
- + [Users](#)
- + [Security](#)
 - [SD-WAN](#)
- + [VoIP](#)
- [VPN](#)
 - [VPN Subnets](#)
 - + [PPTP Server](#)
 - [GRE](#)

Global Settings:
 Enable the VPN module: ☒
[Refresh Status](#)
Current time:
Mon Aug 2 15:19:14 2021

VPN Tunnels		
Select: All None		Delete
	Tunnel Name	Status
<input type="checkbox"/>	ToPBX	Tunnel established i

[Add a new tunnel](#)

2. Configure the following:
 - The Protected Local Network - voice VLAN of the EdgeMarc.
 - The Remote VPN Gateway - WAN IP of EdgeMarc B

- The Protected Remote network - voice VLAN of EdgeMarc B.

[Help](#)

VPN Tunnel Settings

[Refresh Status](#)
[Back to VPN overview](#)

Status:	Tunnel established
Name:	<input type="text" value="ToPBX"/>
Enabled:	<input checked="" type="checkbox"/>
Shared Secret:	<input type="text" value="....."/>
Local VPN Gateway:	<input type="text" value="WAN_IP"/>
Protected Local Network:	<input type="text" value="192.168.8.0/24"/>
Remote VPN Gateway:	<input type="text" value="192.168.199.59"/>
Protected Remote Network:	<input type="text" value="172.16.1.0/24"/>
DH Group:	<input type="text" value="DH Group 2 - 1024 bits"/>
Phase 1:	<input type="text" value="3DES"/> - <input type="text" value="MD5"/>
Phase 2:	<input type="text" value="AES128"/> - <input type="text" value="MD5"/>
Phase 1 Lifetime:	<input type="text" value="28800"/> seconds
Phase 2 Lifetime:	<input type="text" value="86400"/> seconds
Perfect Forward Secrecy:	<input checked="" type="checkbox"/>
Early Start:	<input checked="" type="checkbox"/>
Keepalive Ping (Optional)	
Source IP address:	<input type="text"/>
Destination IP address:	<input type="text"/>

- Since EdgeMarc A is responsible for communication to the SAP provider, its ALG must be configured starting with the main VoIP page:
 - The ALG VLAN is set to the voice VLAN of the EdgeMarc.
 - Route all signaling through B2BUA is configured to provide for any needed SIP header manipulation.

VoIP

[help](#)

VoIP ALG allows the system to recognize and register network devices.

Enable ALG Multi-VLAN support: ☐

Since VLAN support is enabled, you must select a VLAN for the ALG to support. The ALG can only support one VLAN.

ALG LAN using VLAN ID

Enable LLDP: ☒

LLDP Broadcast Interval (sec):

IPv4 only.

TFTP Server IP address:

In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports. The addresses will be alias addresses that have been configured on the ports. In general, the user should leave this feature disabled.

Use ALG Alias IP Addresses: ☐

ALG LAN Interface IP Address: 192.168.8.1

ALG LAN Interface IPv6 Address:

ALG WAN Interface IP Address: 192.168.199.39

ALG WAN Interface IPv6 Address:

Public NAT WAN IP address:

Private NAT LAN IP address:

Do strict RTP source check: ☐

Enable Client List lockdown: ☐

Allow Shared Usernames: ☐

Strip G.729 from calls: ☐

B2BUA Options:

Route all SIP signalling through B2BUA: ☒

4. On the SIP Settings page The SIP server is configured under List of SIP Servers to facilitate the use of the EdgeMarc Survivable Gateway function. The IP address configured is that of the Sonus 1000 acting as the Service Provider SBC in this lab. Other settings on the page are left at their default values.

SIP Settings [Help](#)

SIP protocol settings.

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Transport: UDP

Use Custom Domain: ☐

SIP Server Domain:

List of SIP Servers				
Select: All None				Delete
	Lookup Status	Priority	SIP Server Address/FQDN	Port
<input type="checkbox"/>		0	82.113.38.212	5060

Add a new SIP Server

IP Address/FQDN:

Port:

[Add](#) [Reset](#)

Enable Multi-homed Outbound Proxy Mode: ☐

Enable Transparent Proxy Mode: ☐

Limit Outbound to listed SIP Servers: ☒

Limit Inbound to listed SIP Servers: ☒

Include UPDATE In Allow: ☒

PRACK Support: ☒

GEOLOCATION Support: ☐

Call Audit Support: ☒

Enable Sub Domain Pass Through support: ☐

5. Finally, configure the SIP endpoint for the Swyx PBX and dial rules under the SIP B2BUA settings beginning with the Trunking Devices section:

Note The Swyx PBX requires the use of a non-standard SIP port, in this case 65002.

B2BUA Trunking Configuration [Help](#)

This page supports only IPv4 addressing.

In order for changes to this page to be applied, you must click the "Submit" or "Apply Later" button at the bottom of the page

Trunking Devices

Name	Address	Port	Group	Username	Registration Status	Transport
SwyxPBX	192.168.8.39	65002				UDP

[New Entry](#)

Name: Model: Generic PBX

☒ Address(IP/FQDN): Use DNS SRV: ☐

Port: Transport: UDP

Source FQDN:

☐ Username: Password:

Authenticate Registration: ☐

6. The B2BUA Actions are configured next:

- The ToPBX action sends calls to the previously configured Trunking Device SwyxPBX.

- The ToSIP action handles calls destined for the SIP Provider. Although no header manipulation was used in the lab, it may be configured here as needed. Refer to EdgeMarc documentation for syntax and capabilities.

Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
✖	ToPBX	✓				
✖	ToSIP	✓				

New Entry

Name:

Send To: ☒ Trunking Device:

☐ Client:

☐ URI:

☐ Response:

Prioritize: ☐

Serial Hunting:

E.164 Conversion rule: Conversion mode:

Refer to Re-INVITE: ☐

Header Manipulations:

	Header	Value
Header:	<input type="text" value="Request-URI"/> <input type="button" value="v"/>	<input type="button" value="Add"/>
Value:	<input type="text"/>	

7. Lastly, configure any required dial rules:

- The first rule is created to send calls to the soft client registered with the Provider SBC for testing.
- The second rule routes any inbound calls to the Swyx PBX.

Match

	Direction	Mode	Def	Called		Calling		Source	Action
				Match	Pattern	Match	Pattern		
✖	Outbound	BothModes		matches	jojo			SwyxPBX	ToSIP
✖	Inbound	BothModes		matches	.			Any	ToPBX

New Entry

Direction:

Mode:

☐ default

☒ Pattern:

Called Party:

Calling Party:


Source:

Action:

Configuring EdgeMarc B

EdgeMarc B serves as the remote site in this use case. As such, EdgeMarc B has a simple configuration consisting only of a standard networking configuration and an IPSec VPN tunnel.

1. Enable the VPN module, then Add a new tunnel.

**VPN**[Help](#)

Configuration Menu

- + [Admin](#)
- + [Network](#)
- + [Users](#)
- + [Security](#)
- [SD-WAN](#)
- + [VoIP](#)
- [VPN](#)
 - [VPN Subnets](#)
 - + [PPTP Server](#)
- + [Switch](#)

Global Settings:
Enable the VPN module: ☒
[Refresh Status](#)
Current time: Mon Aug 2 17:17:23 2021

VPN Tunnels		
Select: All None		Delete
	Tunnel Name	Status
<input type="checkbox"/>	ToPhone	Tunnel established i

[Add a new tunnel](#)

2. Configure the following:

- Protected Network - Voice VLAN of EdgeMarc B
- Remote VPN Gateway - WAN IP of EdgeMarc A
- Protected Remote Network - Voice VLAN of EdgeMarc A

VPN Tunnel Settings[Help](#)

[Refresh Status](#)[Back to VPN overview](#)

Status:	Tunnel established i
Name:	<input type="text" value="ToPhone"/>
Enabled:	<input checked="" type="checkbox"/>
Shared Secret:	<input type="text" value="....."/>
Local VPN Gateway:	<input type="text" value="WAN_IP"/>
Protected Local Network:	<input type="text" value="172.16.1.0/24"/>
Remote VPN Gateway:	<input type="text" value="192.168.199.39"/>
Protected Remote Network:	<input type="text" value="192.168.8.0/24"/>
DH Group:	<input type="text" value="DH Group 2 - 1024 bits"/>
Phase 1:	<input type="text" value="3DES"/> - <input type="text" value="MD5"/>
Phase 2:	<input type="text" value="AES128"/> - <input type="text" value="MD5"/>
Phase 1 Lifetime:	<input type="text" value="28800"/> seconds
Phase 2 Lifetime:	<input type="text" value="86400"/> seconds
Perfect Forward Secrecy:	<input checked="" type="checkbox"/>
Early Start:	<input checked="" type="checkbox"/>
Keepalive Ping (Optional)	
Source IP address:	<input type="text"/>
Destination IP address:	<input type="text"/>

Section-B: SwyxWare, SwyxIt and HFA Phone Configuration

Configuring SwyxPBX

1. Right Click on Location > Add Location.

Add new Location

Location Name

Enter the name and description of the new Location.

A Location defines a site and its specific parameters. In a multi site SwyxWare installation, the definition of several locations is required. SwyxWare Users and Trunk Groups are being assigned to Locations.

Name:

VO TEST

Description:

SwyxPBX at VO Lab

☐ Set this Location as the default Location.

All new users will be assigned to this Location unless explicitly changed.

< Back

Next >

Cancel

A Location defines a site and its specific parameters. In a multi site SwyxWare installation, the definition of several locations is required. SwyxWare Users and Trunk Groups are being assigned to Locations.

Name:

VO TEST

Description:

SwyxPBX at VO Lab

☐ Set this Location as the default Location.

All new users will be assigned to this Location unless explicitly changed.

< Back

Next >

Cancel

2. Add codes and prefixes then click Next.

Add new Location

Location specific codes and prefixes

Specify the codes and prefixes which are related to this Location.

The prompted parameters determine how the destination number of a call, originated by a SwyxWare User or a Trunk, is interpreted by the system. This is in particular needed to identify calls that remain in the same area or county.

A typical German Location in Berlin would have a Country Code set to '49', Area Code to '30', International Prefix to '00' and Long Distance Prefix to '0'.

Own Country Code:

1

Own Area Code:

214

Prefix for International Calls:

11

Prefix for Long Distance Calls:

0

< Back

Next >

Cancel

3. Add access to Dial out and click Next.

Add new Location

Private Branch Exchange related properties

Specify the PBX settings which are related to this Location.

The Public Line Access prefix defines which number has to be dialed to obtain access to the public network.

It is possible to define multiple Public Access Prefixes, separated by a semicolon.

The Internal Number for undeliverable calls defines where incoming calls will be transferred when the called public number is not assigned to a SwyxWare User or Group.

Public Line Access Prefixes:

9

Route undeliverable calls to Internal Number:

...

< Back

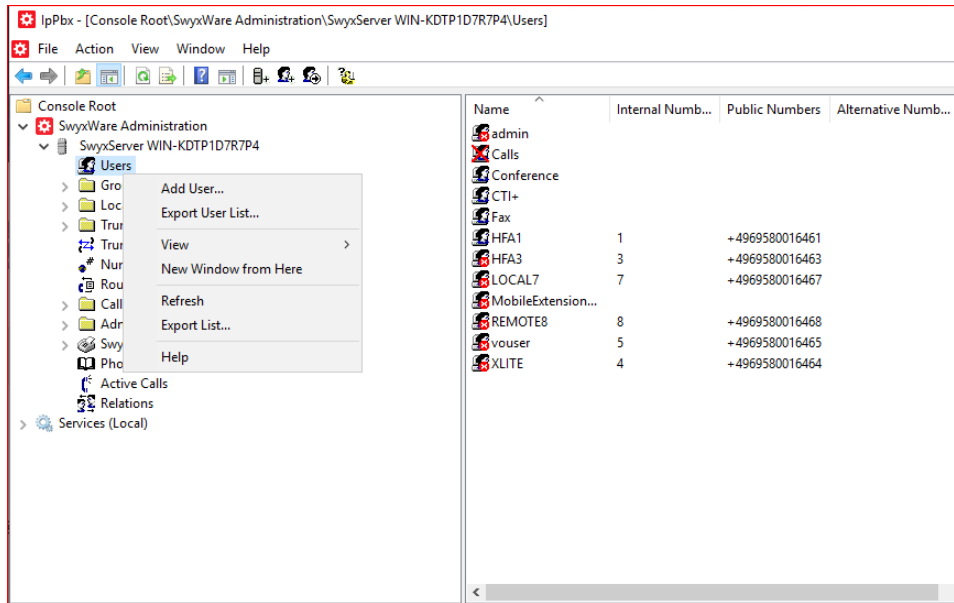
Next >

Cancel

Adding a User

Confidential and Proprietary. Copyright © 2020-2023 Ribbon Communications Operating Company, Inc. © 2020-2023 ECI Telecom Ltd.

1. Click on Server > right click on User > click Add User.



2. Add Name and Description then Click Next.

The 'Add new User' dialog box is shown. It has a title bar with a close button. Below the title bar, it says 'Name and type of the new User' and 'Enter name and type of the new User.' with a gear icon. A message states: 'An unambiguous name for the new User is required. The description is optional.' There are two input fields: 'Name:' with the text 'New User' and 'Description:' with the text 'New User'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

3. Select the Location and click Next.

Add new User

Location of the new User

Please select a Location for the new User.

A Location within SwyxWare defines all location specific settings like the time zone, the required public access code, the country and area codes.

Please select one of the listed Locations which will be assigned to this User.

Location:

Ribbon USTX

Description

< Back

Next >

Cancel


4. Select a new internal number and click Verify to check if available. Click OK and then click Next.

Add new User

×

Internal Number of the new User

Enter the Internal Number,
under which the new User will be reachable.



To define a Internal Number for this User, enter the chosen number and click "Verify" for checking if it is already in use. By entering a number and clicking "Next unused" the system will suggest the next free number after the given.

Uncheck "Show in Phonebook" if you e.g. want to use the Internal Number for call routing purposes only.

New Internal Number:

Verify

Next unused

☒ Show in Phonebook


< Back

Next >

Cancel

Verify Internal Number

×



Internal Number '2' is valid and can be assigned to this User.

OK

5. The Internal Number selected will be mapped to a public number, then click Next.

Add new User

Internal Number mapping

Specify the Public Number to which the User's Internal Number will be mapped.

To permit calling this User directly from the public network, you have to associate the Internal Number to a Public Number.

To do so, choose one of the suggested Public Numbers from the drop-down list, or enter a Public Number (canonical format) or SIP URI manually.

Use the "Select..." button to obtain an overview of Public Numbers available in the entire system.

Internal Number:

2

Associated Public Number:

+4969580016462

Select...

< Back

Next >

Cancel

6. Select the Terminals by checking the boxes and then click Next.

Add new User

Terminals

Choose which terminals are used.

A User can make phone calls using different terminals. Check the terminals to be used by the new User. The required settings will be configured in the following dialogs.

☒ SwyxIt! and SwyxFax Client

☒ SIP devices

☒ SwyxPhone Lxxx

☐ Simple User account for call routing. No logins allowed.

< Back

Next >


Cancel

7. Create a Password for the user login then click Next.

Add new User

SwyxIt! and SwyxFax Client Login Settings

Define how the new user can login with SwyxIt! and SwyxFax Client.



Specify a Windows account, e.g. when SwyxServer and SwyxIt! or the SwyxFax Client are in the same Windows domain or define a User name and password the clients have to use for login.

☐ Windows Account

Windows User Account:

☒ User Name and Password

User Login: @

Password:

Repeat Password:


☐ User must change password at next logon

8. Create a SIP user ID and password and then click Next.

Add new User

SIP parameters

Configure the SIP parameters.



To logon via SIP it's necessary to specify a unique User ID for each User.
In case authentication is enabled you must enter a username and a password, too.

User ID:

Authentication Mode: ▼

User Name:

Password:


Repeat Password:

Confidential and Proprietary. Copyright © 2020-2023 Ribbon Communications Operating Company, Inc. © 2020-2023 ECI Telecom Ltd.

9. Create a Swyx Phone Pin and then click Next.

Add new User

PIN for SwyxPhone Lxxx
Enter the PIN.



For using SwyxPhone Lxxx a PIN is required. Click on 'Create PIN' for assigning a new, unique PIN to the User.

Please inform the User about the created PIN.

You can change the PIN later on the User's 'Administration' property page.

SwyxPhone Lxxx PIN:

Create PIN

< Back


Next >

Cancel

10. Select a Calling Right and then click Next.

Add new User

Calling Rights
Choose Calling Right.



Calling Rights represent individual call permissions or restrictions which can be assigned to a User.

Please select one of the listed Calling Rights to define the call permissions of the User.

Calling Right:

No call restrictions

▼

Description

Default profile allowing calls to all destinations.

< Back

Next >

Cancel

11. Select a Feature Profile and click Next.

The screenshot shows a dialog box titled "Add new User" with a close button (X) in the top right corner. Below the title bar, the section is titled "Feature Profiles" with a subtitle "Choose Feature Profile." and a gear icon. The main content area contains the following text: "Feature Profile defines which features a User is allowed to use." and "Please select one of the listed Feature Profiles to define the available features for the User." Below this text is a label "Feature Profile:" followed by a dropdown menu showing "Standard". Underneath the dropdown is a text box labeled "Description" containing the text "Provides the complete feature set offered by the server." At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

12. Assign properties to the new user and click Finish.

The screenshot shows a dialog box titled "Add new User" with a close button (X) in the top right corner. Below the title bar, the section is titled "Assign properties to the new User" with a subtitle "Choose an existing User for transferring his properties to the new User." and a gear icon. The main content area contains the following text: "You can transfer some properties of an existing User to the new User." and "These properties are mainly SwyxIt! related settings for Skins and ringing sounds. Relationships and group memberships of the existing user are also copied." Below this text is a paragraph: "In case you would like to use this function, select 'Create new User account and apply properties of an existing User' and choose the user to transfer properties from." Below this paragraph are three radio button options: "Create new User account only", "Create new User account and install sample files for Call Routing" (which is selected), and "Create new User account and apply properties of an existing User:". Below the radio buttons is a dropdown menu showing "admin" with a user icon. At the bottom of the dialog are three buttons: "< Back", "Finish", and "Cancel".

Configuring a SIP Trunk

1. Right click on Trunk Group and select Add Trunk Group. The Add Trunk Group Wizard pops up then click Next.

Console Root

SwyxWare Administration

SwyxServer WIN-KDTP1D7R7P4

Users

Groups

Everyone

Sales

Support

VOTEST

Locations

Ribbon USTX

Trunk Groups

Trunks

Number Map

Routing Table

Calling Right

Administrative

SwyxFax

Phonebook

Active Calls

Relations

Services (Local)

Add Trunk Group...

View

New Window from Here

Refresh

Export List...

Help

Name	Description	Type
SBC1KTG	SBC1K Ribbon Lab Prague	SIP

Add new Trunk Group

×



Welcome to the Add Trunk Group Wizard

This wizard will guide you through the process of adding a new Trunk Group.

 Trunk Groups consist of one or more Trunks sharing most of the Trunk properties.

From a users point of view, there is no need to differentiate between individual Trunks of a Trunk Group: One more Trunk within the same Trunk Group is nothing more than a capacity enhancement with all Trunks offering the same properties for use.

< Back

Next >

Cancel

2. Add the Trunk Group Name and Description and click Next.

Add new Trunk Group

Trunk Group Name and Description

Specify Trunk Group name and description.

Enter a unique Trunk Group name, i.e. not used otherwise as Trunk name, User name, Group name or Phonebook entry.

Enter the optional description that will later on help you identifying this Trunk Group.

Trunk Group Name:

Description:

< Back

Next >

Cancel

3. Select the Trunk Group Type and click Next.

Add new Trunk Group

Trunk Group Type

Specify the type of the Trunk Group and select the appropriate profile.

Select the Type of Trunk Group to be added from the first list and choose the applicable profile from the second list. If you are uncertain, which profile is applicable for your installation, consult the SwyxWare Administration documentation.

If you want to add a Trunk Group for a non-listed SIP service provider, select the Profile "Custom". This will allow entering all required parameters in subsequent steps.

Trunk Group Type:

Profile:

< Back

Next >

Cancel

4. Add SIP settings and click Next.

Add new Trunk Group

SIP settings

Please specify whether SIP registration is enabled for this Trunk Group.

The subsequently prompted information must have been supplied by your SIP service provider.

If your service provider requires a SIP registration (usual case), enable the checkmark and enter the registrar's name or IP address.

The SIP account specific information must be entered when you add a Trunk to the Trunk Group you are currently creating.

☐ Enable SIP registration

Registrar:

:

Re-registration Interval:

120

seconds

< Back

Next >

Cancel

5. Add the SIP Proxy but leave the SIP port blank (auto-resolves) and click Next.

Add new Trunk Group

SIP Settings

Specify SIP settings for this Trunk Group.

The SIP Proxy is the service provider's interface for call control. Therefore its name or IP address must have been provided.

The SIP realm is part of the SIP addressing mechanism, i.e. it is used for SIP URI composition. The parameter "DTMF Mode" determines how a user's keypad input is passed to the provider.

Outbound Proxy:

:

Proxy:

192.168.6.1

:

Realm:

DTMF Mode:

RFC 2833 Event

< Back

Next >

Cancel

Confidential and Proprietary. Copyright © 2020-2023 Ribbon Communications Operating Company, Inc. © 2020-2023 ECI Telecom Ltd.

6. If a STUN server is supported, check the box and add the IP for the STUN server and click Next.

Add new Trunk Group

STUN Server Settings

Specify STUN Server Settings.

A STUN server can be used to traverse non-symmetric NAT firewalls, in order to access another SIP proxy. The STUN server must be located in the public Internet.

Please enter the name or IP address of the STUN server and the STUN service port (usually 3478). A publicly available STUN server is e.g. "stunserver.org".

☐ Enable STUN support

STUN Server:

Port:

3478

< Back

Next >

Cancel

7. Select the Transport Protocol and click Next.

Add new Trunk Group

Encryption Settings

Please specify the SIP Transport Protocol and the Voice Encryption Mode for this Trunk Group.

Some SIP providers require a specific transport protocol. If you choose "Automatic", the transport protocol will be determined via DNS resolution.

Voice Encryption can only be configured, if "TLS" is selected as transport protocol.

Transport Protocol:

UDP

Encryption Mode:

No encryption

< Back

Next >

Cancel

Confidential and Proprietary. Copyright © 2020-2023 Ribbon Communications Operating Company, Inc. © 2020-2023 ECI Telecom Ltd.

8. Select the Routing Definition and click Next.

Add new Trunk Group

Definition of Routing

Specify for what calls this Trunk Group is supposed to be used.

Depending on your choice, initial Routing Records will be created.
Public Numbers should be added in canonical format (e.g. "+4930123456"), ""*"" can be used as a wildcard.

Use Trunks of this Trunk Group...

☐ for all external calls

☐ for all external calls to the following Called Party Number or SIP URI only:

☒ for all external calls and all unassigned Internal Numbers

☐ for Internal Numbers:

☐ Do not create initial Routing Records.

< Back

Next >

Cancel

9. Select the Location Profile and click Next.

Add new Trunk Group

Location Profile

Select the applicable Location Profile for this Trunk Group.

A Location within SwyxWare defines all location specific settings like the time zone, the required public access code, the country and area codes.

Please select one of the listed Locations which will be assigned to this Trunk Group.

Location:

Description

< Back

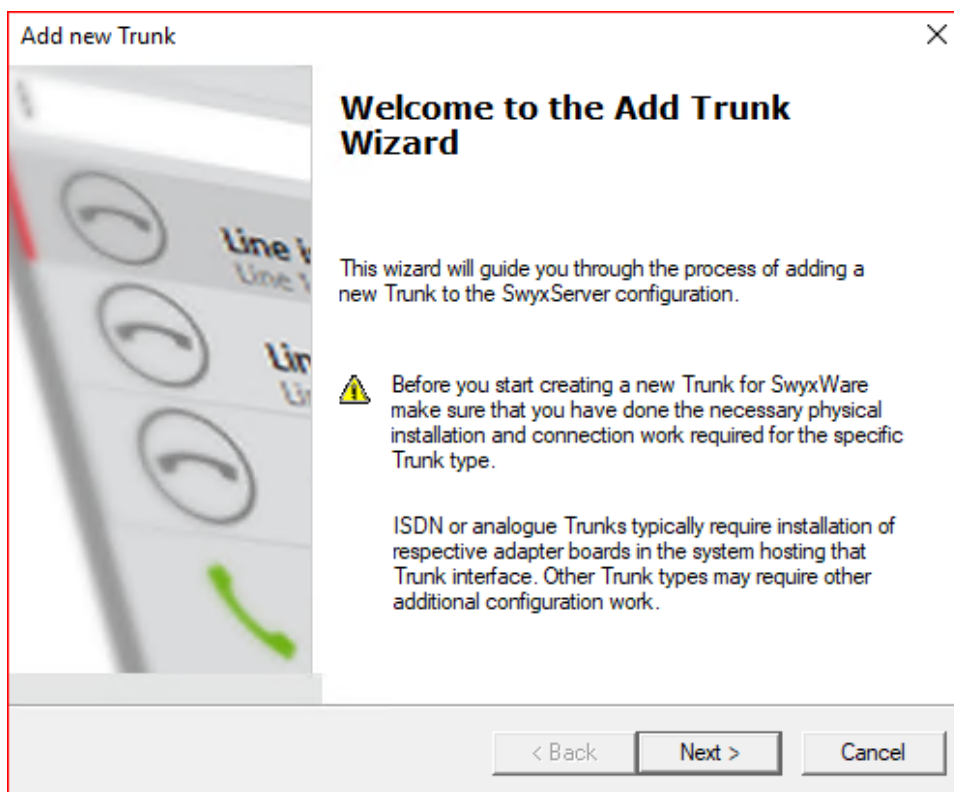
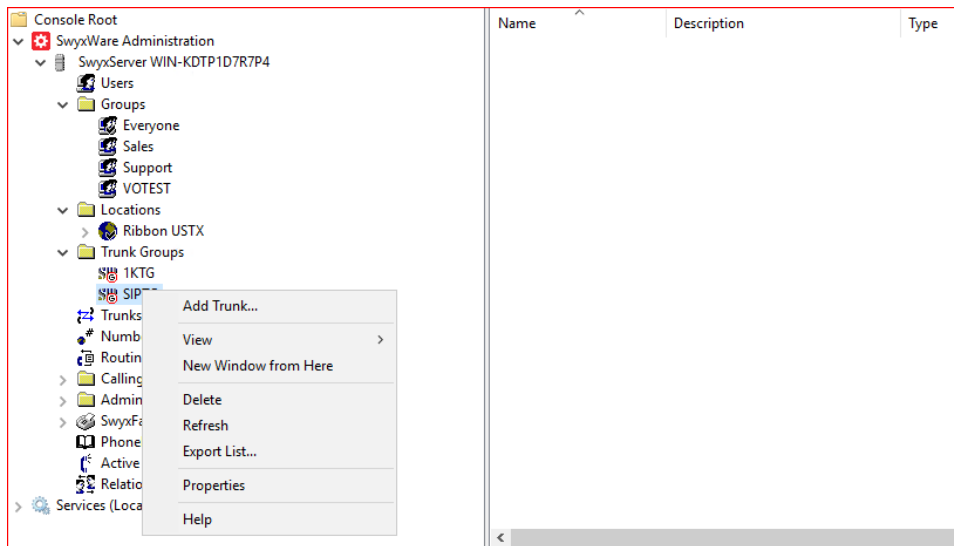
Next >

Cancel

10. Click Finish.



11. Right click on the newly created Trunk Group and click Add Trunk. The Add Trunk Wizard pops up, then click Next.



12. Add a Trunk Name and Description.

Add new Trunk

Trunk Name

Choose an unique name for the new Trunk.

Enter a unique Trunk name, i.e. not used otherwise as Trunk Group name, User name, Group name or Phonebook entry.

Enter the optional description that will later on help you identifying this Trunk.

Trunk Name:

NewSIPTrunk

Description:

New SIP Trunk

< Back

Next >

Cancel

13. Add the SIP trunk Provider and User Data then click Next.

Add new Trunk

SIP Trunk Provider / User Data

Specify your account data.

Enter the user identification data as provided by your SIP service provider. The user ID will be used to compose your SIP address while user name and password will be used for authentication.

SIP Provider:

SIP (Customized)

User ID:

User Name:

Password:

Repeat Password:

< Back

Next >

Cancel

Confidential and Proprietary. Copyright © 2020-2023 Ribbon Communications Operating Company, Inc. © 2020-2023 ECI Telecom Ltd.

14. Select the Subscriber Number using the SIP Trunk and click Next.

Add new Trunk

Subscriber Numbers

Specify Subscriber Numbers.

Enter the subscriber number part of the Public Numbers that are terminated by this Trunk.

If your set of subscriber numbers is incoherent enter only the first subscriber number and add the other subscriber numbers later via the Trunk's properties.

If this Trunk does not add any Public Numbers to the system, leave all fields empty and click 'Next'.

Note: Country Code and Area Code have been pre-determined by the Trunk Group's location.

Country Code	Area Code	First Subscriber Number	Last Subscriber Number
49	68	580016461	580016469

< Back

Next >

Cancel

15. Add a SIP URI (wild card "*" for any) and then click Next.

Add new Trunk

SIP URI

Specify SIP URI.

If this Trunk is supposed to handle non-numeric SIP URIs (e.g. assigned by your SIP service provider) you can enter one of these bellow and add other URIs later via the Trunk's properties.

SIP URIs have the following format:

sip:<name1> @ <name2>

with <name1> reflecting the user's name and <name2> the realm.

For convenient input "*" can be used as wildcard so that *@company.com would address all users in the realm "company.com". The realm field shown below is pre-filled with the configured realm in the SIP properties but may be overwritten case by case.

URI: sip: * @ *

< Back

Next >

Cancel

16. Select the Codecs supported by the SIP trunk and click Next.

Add new Trunk

Codecs

Select the codecs to be used for data transmission.

The selected codec preference and filter defines the type of compression for calls using this Trunk. Therefore the selected codec has an impact on the used bandwidth and the quality of the call.

Codecs Preference and Filter

Prefer Quality

☐ G.722 (approx. 84 kBit/s per call)

☒ G.711a (approx. 84 kBit/s per call)

☒ G.711μ (approx. 84 kBit/s per call)

☒ G.729 (approx. 24 kBit/s per call)

☐ Fax over IP (T.38, approx. 20 kBit/s per call)

< Back

Next >

Cancel

17. Select the Number of simultaneous calls possible in the SIP trunk and click Next.

Add new Trunk

Number of Channels

Select number of Channels to be used by this Trunk.

The number of concurrent calls via a specific Trunk is usually limited by the Trunk's physics, the available bandwidth or by a provider limitation.

Furthermore the number of simultaneous calls can artificially be limited to reserve (e.g. ISDN) channels or bandwidth for other applications.

Usually ISDN BRI interfaces would allow to make up to 2 simultaneous calls, while ISDN PRI interfaces allow up to 30 calls.

Number of simultaneous calls on this Trunk:

< Back

Next >

Cancel

18. Choose PSX server or Computer Name and click Finish.

Add new Trunk

Computer Name

Define the computer name where the Trunk is hosted.

The Trunk may be hosted on another computer than the SwyxServer. In this case, the computer name must be provided here, otherwise keep the proposed default.

Please enter the computer name as it is given in the Windows Server's system properties.

Computer Name:

WIN-KDTP1D7R7P4

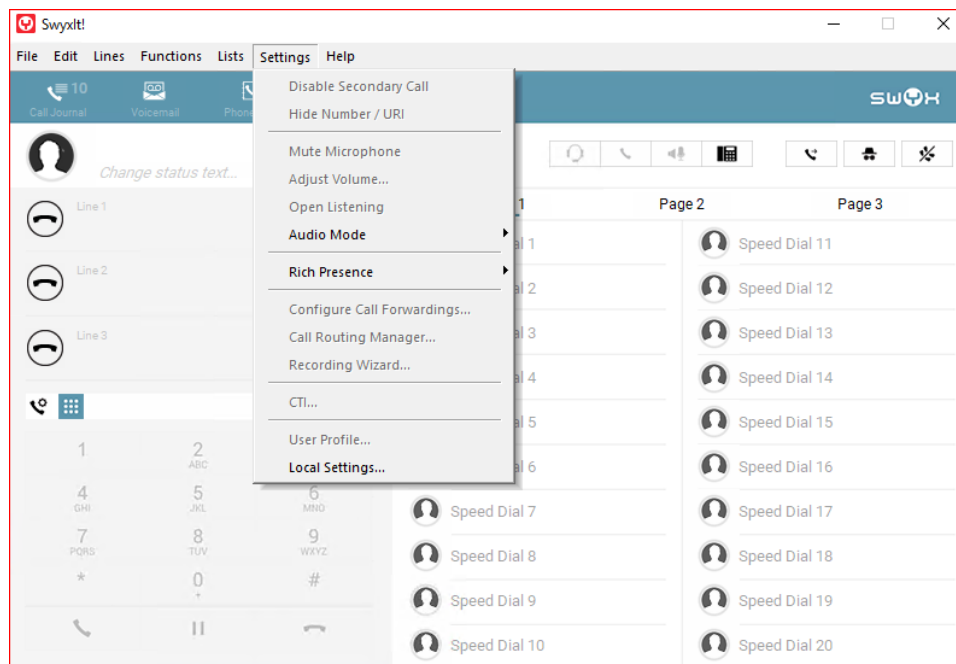
< Back

Finish

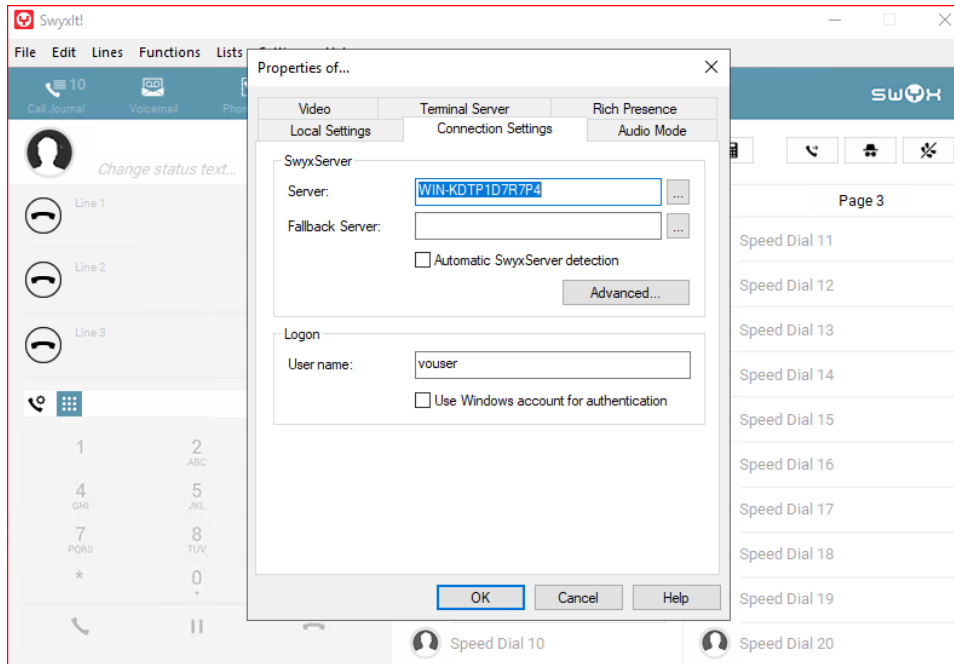
Cancel

Configuring the SwyxIt Client

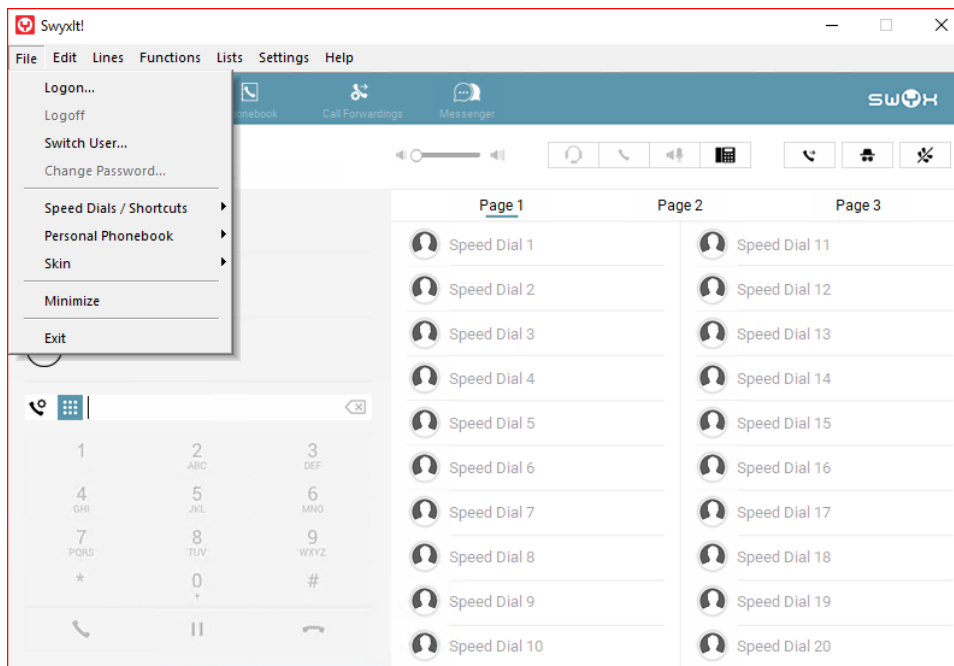
1. Click On Settings and select Local Settings.



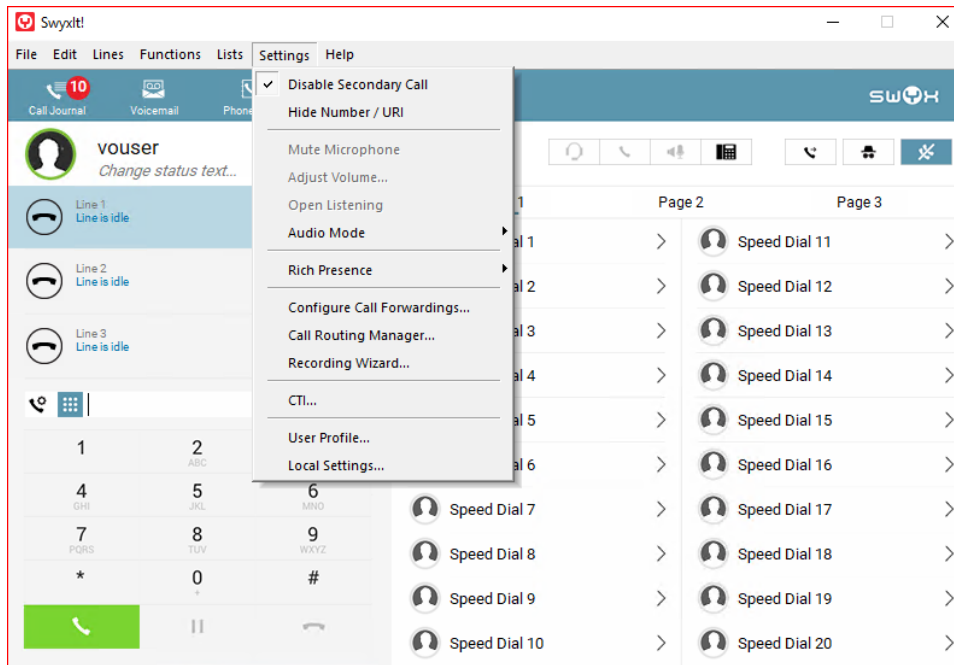
2. Click the Connections Settings Tab and add the Server name or IP address and the User Name, then click OK.



3. From the File Menu select Logon.



- Once Logged in more choices are available in the Settings Menu. Some configuration capability is also available from the User Properties on the PBX server.

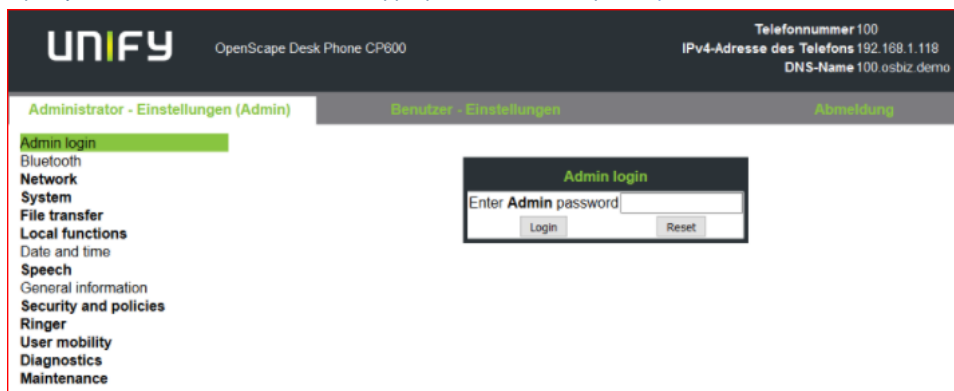


Configuring the HFA Phone

The Unify CP 205 comes out of the box as a SIP Phone. You must upgrade the firmware before configuring the HFA Phone. Upgrade the firmware using FTP/HTTPS Access Data.

By default, the phone has DHCP enabled. Look on the EdgeMarc 2900 for the IP leased to the CP205 unit.

- Open your web browser and enter the appropriate URL. Example: <https://192.168.1.15>.



Note: the default password is 123456.

2. From the Administration via Web-Based Management (WBM), select File transfer > Phone application.

Click Browse to find the corresponding L62.iso file to upload to the Unify CP205 Phones. Then, click Submit.

Phone application

Upgrade using file

Choose the image file you wish to use to upgrade the phone

Closing or navigating away from this page will cancel the file upload

Upgrade using FTP/HTTPS

Use defaults ☐

Download method

FTP

FTP Server address

FTP Server port

21

FTP account

FTP username

FTP password

••••••

FTP path

HTTPS base URL

Filename

After submit

do nothing

3. Once the firmware has been upgraded, login to Web-Based Management to configure the network settings by selecting Network > General IP configuration, then click Submit.
Choose between DHCP or Static IP assignment.

General IP configuration

Protocol mode	IPv4	▼
LLDP-MED enabled	<input checked="" type="checkbox"/>	
DHCP enabled	<input checked="" type="checkbox"/>	
VLAN discovery	LLDP-MED	▼
VLAN ID	1	
DNS domain		
Primary DNS	172.16.1.1	
Secondary DNS		
Ip TTL	64	▼
<input type="button" value="Submit"/>		<input type="button" value="Reset"/>

General IP configuration

Protocol mode	IPv4	▼
LLDP-MED enabled	<input type="checkbox"/>	
DHCP enabled	<input type="checkbox"/>	
VLAN discovery	Manual	▼
VLAN ID	1	
DNS domain		
Primary DNS	172.16.1.1	
Secondary DNS		
Ip TTL	64	▼
<input type="button" value="Submit"/>		<input type="button" value="Reset"/>

4. Select [Network > IPv4 configuration](#), then click [Submit](#). Add IP address, Subnet Mask, and Default Route.

Note: If DHCP is enabled the values will be fetched automatically.

IPv4 configuration

LLDP-MED enabled	<input type="checkbox"/>
DHCP enabled	<input type="checkbox"/>
DHCP lease reuse	<input checked="" type="checkbox"/>
IP address	<input type="text" value="172.16.1.100"/>
Subnet mask	<input type="text" value="255.255.255.0"/>
Default route	<input type="text" value="172.16.1.1"/>
Route 1 IP address	<input type="text"/>
Route 1 gateway	<input type="text"/>
Route 1 mask	<input type="text"/>
Route 2 IP address	<input type="text"/>
Route 2 gateway	<input type="text"/>
Route 2 mask	<input type="text"/>

5. Add Gateway information by selecting [System > Gateway](#), then click [Submit](#).

Gateway

System type	<input type="text" value="HiPath 3000 V7.0"/>
IP address	<input type="text" value="192.168.8.39"/>
Gateway ID	<input type="text"/>
Subscriber number	<input type="text" value="1"/>
Password	<input type="password" value="•••••"/>

6. Choose Codecs by selecting Speech > Codec preferences, then click Submit.

Codec preferences

Silence suppression ☐

Packet size Automatic ▼

G.711 ranking ▼ ✖

G.729 ranking ▲ ▼ ✖

G.722 ranking ▲ ✖

Submit Reset

7. Go to the Phone and login to SwyxPBX using the user created in section [Adding a User](#).



Supplementary Services and Features Coverage

The following checklist identifies the set of supplementary services/features covered through the configuration defined in this Interop document.

Sr. No.	Supplementary Services/Features	Coverage
1	Registration over UDP/TCP/TLS	✓
2	Basic Call Setup & Termination	✓
3	Ringling & Local Ringback Tone	✓
4	Remote Ringback Tone Handling	✓
5	Cancel Call & Call Rejection	✓

6	Call Forwarding Busy	✓
7	Call Forward No Answer	✓
8	Call Transfer (Attended)	✓
9	Call Transfer (Blind/ Unattended)	✓
10	Call Conference	✓

Legend

Supported	✓
Not Supported	✗

Caveats

The following items should be noted in relation to this Interop document. These are either limitations, untested elements, or useful information pertaining to the Interoperability.

- Fax calls and other tests were not performed due to unavailability of required devices at the Ribbon Lab.

Support

For any support related queries about this guide, please contact your local Ribbon representative, or use the details below:

- Sales and Support: 1-833-742-2661
- Other Queries: 1-877-412-8867
- Website: <https://ribboncommunications.com/about-us>

References

For detailed information about Ribbon products & solutions, please visit:

<https://ribboncommunications.com/products>

Conclusion

This Interoperability document describes a successful configuration and interop involving EdgeMarc 2900 and SwyxWare PBX.

All features and capabilities tested are detailed within this document. Any limitations, notes or observations are also recorded to provide the reader with an accurate understanding of what has been covered, and what has not.

Configuration guidance is provided to enable the reader to replicate the same base setup - there may be additional configuration changes required to suit the exact deployment environment.

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved.