Swyx Mobile - Commissioning to SwyxServer Step-by-Step Guide

As of: November 2020

Legal information

Swyx Solutions GmbH

Emil-Figge-Str. 86

D-44227 Dortmund

office@swyx.com

www.swyx.com

1 Swyx Mobile Client - Commissioning to SwyxServer

In this manual you will learn which steps are necessary to operate your Swyx Mobile Client or your Swyx Desktop Client on SwyxServer.

1.1 Sequence of setup

Requirements:

- SwyxServer and SwyxWare Administration are already installed
- You have purchased Swyx Mobile licenses

Execute the following steps in sequence:

1. Install Push Notification Service (see *Install Push Notification Service*, page 2)
2. Set up RemoteConnector (see *Set up RemoteConnector*, page 3)
3. Open and forward ports in the firewall (see *Open and forward ports in the firewall*, page 4)
4. Create and assign certificate for users (see *Create and assign certificate for users*, page 4)
5. Create and deliver welcome e-mail (see *Generate and deliver welcome email*, page 6)
6. Log on Swyx Mobile Client (see *Logging on Swyx Mobile Clients using the welcome email*, page 7)

1.2 Install Push Notification Service

The Push Notification Service enables server services to send notifications to client applications to alert them to specific events. The Push Notification Service is a SwyxServer service and acts as a link between SwyxServer and the corresponding services from Apple and Google. This technology eliminates the need for the client applications to constantly query the server for changes, making communication between server and client more efficient and eliminating unnecessary battery consumption.

For the Swyx Mobile for iOS Client, the Push Notification Service is required to use features available with iOS 10 (or later), such as CallKit integration. The support of the Push Notification Service as well as the above mentioned advantages are available in the Swyx Mobile Clients from version 2.0.0.

Swyx Mobile Clients with a version 1.x that do not support Push Notifications can still be operated up to a SwyxServer version 11. However, these clients do not include the CallKit integration mentioned above and will not be further developed. Users of these versions will be automatically referred to the new version when using them, if they are connected to an active Push Notification Service of SwyxServer. The previous configuration is automatically transferred to the current version.

A Swyx Mobile version 3.0.0 or higher requires a SwyxWare version 12.10 with the latest Push Notification Service.

The installation file "PushNotification.msi" can be found on the SwyxWare DVD in the directory "PushNotificationService".

Supported operating systems:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

To install the Push Notification Service

1 Start the installation file 'PushNotification.msi'.
✓ The installation wizard will open.

2 Click on "Next ".

3 Select the destination folder and click "Next".

4 Click on "Install" to start the installation.
✓ The service is installed.

5 Complete the installation by clicking on "Finish".

1.3 Set up RemoteConnector

For connections with the Swyx Mobile Clients SwyxWare from version 2015 R2 on uses an authentication service. This service enables connections to be established via SwyxRemoteConnector. Via SwyxRemoteConnector a user can log on to the SwyxServer outside the local (LAN) or virtual private network (VPN). The required client configuration will be reduced by one step: Within the client settings, users simply enter the public end point (as FQDN or IP Address) of the company network, to which the authentication service is connected.

When a connection is established, the client sends a request to the public endpoint and authenticates via HTTPS using the SwyxWare username and password. The required configuration data for the TLS tunnel (including the client certificate and the server address of the RemoteConnector) is transferred to the client computer (or smartphone), stored for future connections and later updated as required.

To set SwyxServer to connect to Swyx Mobile Clients you have to enter the FQDN or the public IP address(es) and port(es) where the SwyxRemoteConnector and the authentication service can be reached from the Internet.

You make these settings in the "Configure Remote Access" dialog in the SwyxWare Configuration Wizard, which you start after installing SwyxWare. If you have already run through the wizard, you must start it again to make the settings for the RemoteConnector later.

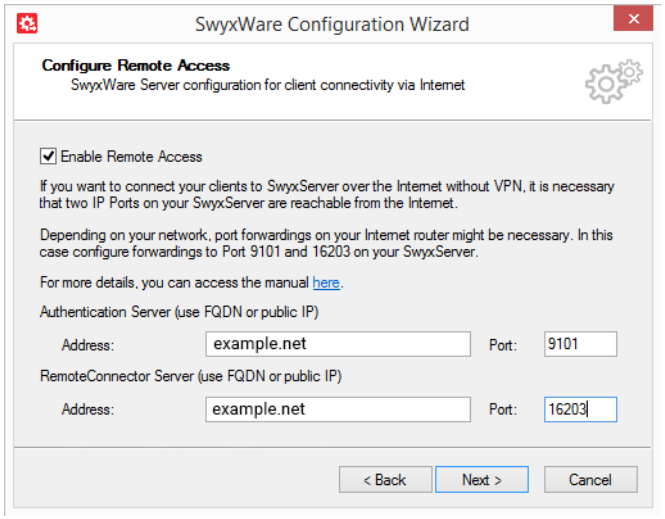
To configure remote access

1. Start the Configuration Wizard under "Start | Programs | SwyxWare | SwyxWare Configuration Wizard".
2. Navigate further to the step "Configure remote access".
3. Activate the checkbox "Enable remote access" to support direct internet connections with Swyx Mobile Clients.
4. Enter the public server address and port (default port: 9101) in the corresponding fields in the "Authentication Server (FQDN or public IP)" section, so that the Swyx Mobile Clients can reach you via InternetSwyxServer.

   The entered public address of the authentication service must also be configured in the settings of the Swyx Mobile Clients (Settings | External Server).

If you use a port other than the default port 9101, this port must be explicitly entered in the client settings.

5. In the RemoteConnector Server area, enter the public server address and the port of the SwyxRemoteConnector server in the corresponding fields. The default ports for the are SwyxRemoteConnector16203.
6. Click on "Next>".



7. RemoteConnector Properties:
   Select the mode for generating and managing certificates:
   - Automatic

     SwyxWare generates and manages certificates automatically.
     In the next step you let a master and a server certificate to be generated and set a password for the root certificate.
     Via the user interface of SwyxWare Administration you will later be able to generate the client certificates for the desired users.
     See *Use automatically generated certificate*, page 5

To generate the client certificates, you need the password with which you protected the root certificate. You should remember this one.

- Manually
  Only select this mode if you have your own certificates. The distribution of certificates is your task. SwyxWare stores no certificates but merely thumbprints.
  In the next step, you'll have to select the master certificate and the server certificate inferred from the master certificate in the corresponding dropdown list.
  Should you not yet have imported your certificates in the Windows certificate storage, you can do so via the "..." button.

If you change the mode for certificate generation and management at a later time, then all client certificates assigned to the users will become invalid.

8 Run the configuration wizard to the end.

1.4 Open and forward ports in the firewall

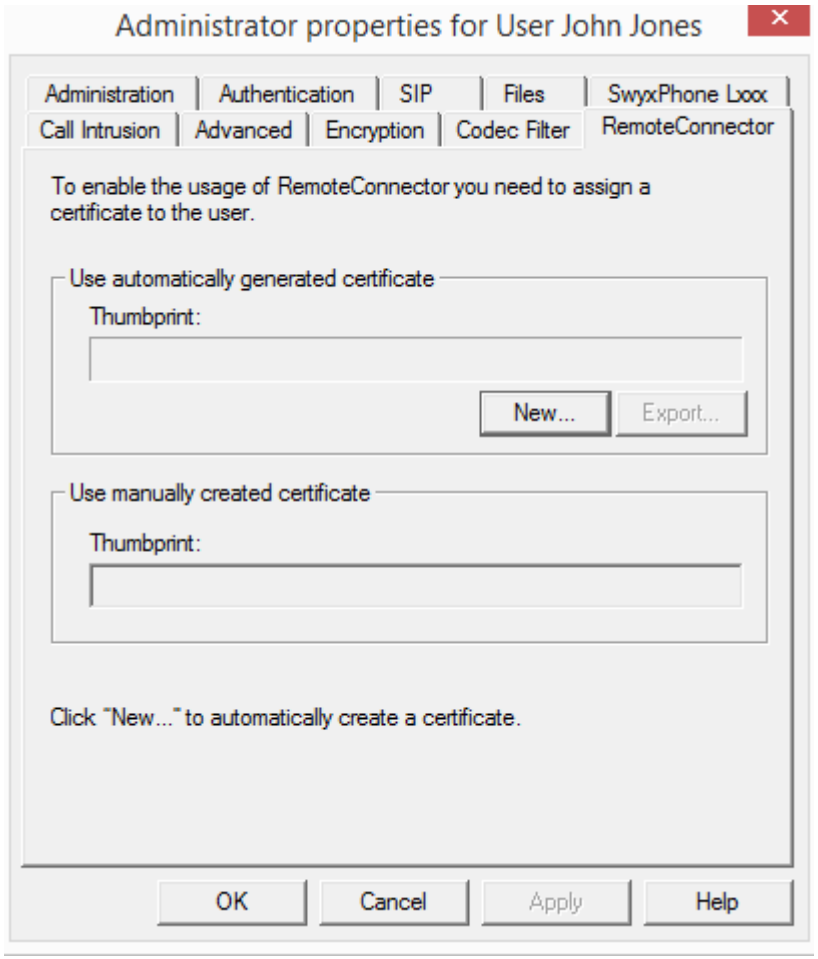
In order for the Authentication Service and RemoteConnector to be accessible from the Internet, you have to release the corresponding ports in the firewall and additionally configure port forwarding to your SwyxServer.

The following table illustrates an example configuration:

Port forwarding to...	Public IP address:TCP port	Target IP address:TCP port
Authentication Service	example.net:9101	192.168.0.4:9101
Authentication service a standby system	example.net:9102	192.168.0.5:9101
RemoteConnector Sever	example.net:16203	192.168.0.4:16203
RemoteConnector Server	example.net:16204	192.168.0.5:16203

1.5 Create and assign certificate for users

On this tab, you create the digital client certificate for the user or assign an existing one.



Only one of the two tab areas is active, depending on the mode selected for certificate management.

You have already selected the desired mode via the SwyxWare configuration wizard. See also *To configure remote access*, page 3.

In SwyxON the option "Use automatically generated certificate" is preconfigured and cannot be changed.

1.5.1 Use automatically generated certificate

In automatic mode, the root and server certificates are generated by SwyxWareand stored in the SwyxWaredatabase.

On the current tab, you can also have SwyxWare generate the client certificate and assign it to the user.

To generate the client certificate, maintain the password ready that you used to protect the root certificate during SwyxWare configuration.

In SwyxONdoes not require the password to generate the client certificate.

How to assign an automatically generated certificate to a user

1. Click with the mouse in the left window of the SwyxWare Administration on the directory "Users".
2. Right-click the user in the user list for whom you want to create a certificate.
3. In the context menu, select "Properties".
4. Click on "Administration".
5. Click the RemoteConnector tab
6. Click on the "New" button.
   ✓ A dialog window will appear with the entry field:
7. Enter the password and confirm with"OK."
   ✓ The RemoteConnector tab appears in the foreground.
8. Click on the "OK" button on the bottom of the tab.
   ✓ The dialog window "Administrator properties for users..." is closed.
   ✓ The certificate is generated.
9. Open the administrator properties and select the "RemoteConnector" tab.
   ✓ The certificate's digital thumbprint is entered in the "thumbprint" field.

In order to replace the certificate for the user, repeat steps **(5)** to **(9)**.

1.5.2 "Use manually generated certificate"

In manual mode, the root certificate, server certificate(s) and client certificates have to be generated by you and stored in the Windows certificate storage on the corresponding computers.

In the "RemoteConnector" tab, you have to enter the thumbprint of the client certificate that you generated for the user and imported to the Windows certificate storage on the user's computer.

How to enter the Client certificate's thumbprint

1. In the SwyxWare Administration open the "Administration Properties for Users..." and select the tab "RemoteConnector".
2. In the area "///Use manually generated certificate", enter the client certificate's thumbprint in the "thumbprint" field.
3. Confirm your entry with “OK”.
   The dialog window "Administrator properties for users..." is closed.
   The client certificate is assigned to the user.

1.6 Generate and deliver welcome email

You can send users logon credentials and configurations for your Swyx Mobile clients by means of a welcome email. You can define this data using a template.

On Swyx mobile clients, the configurations are automatically transferred by the user calling the corresponding URL in the welcome e-mail and thus being forwarded directly to his client.

Most of the configurations are linked to the template for the welcome emails via variables. When sending, the variables are then automatically replaced by the configurations. A list of all the variables is provided as a comment at the beginning of the template.

Some configurations for Swyx Mobile Clients are not defined in SwyxWare Administration, but are preset by values in the template for the welcome email or automatically defined by the installation, see *To edit the welcome email template*, page 6.

You have the following options for sending welcome e-mails:

- Use standard e-mail
  The standard e-mail contains the most important configurations that the user needs to log in and make calls.
- Customize e-mail

Edit the template from which the welcome emails are generated before you send the email. See also *To edit the welcome email template*, page 6.

To edit the welcome email template

1. Start the SwyxWare Administration and log on to the SwyxServer.
2. Right-click on the SwyxServer entry to open the context menu.
3. Select “Properties”.
4. Click on the Files tab.
5. Click on "Edit".
6. Select the file "WelcomeMailTemplate.html" from the list.
7. Click on the "Save as..." button and select a storage location.
8. Edit the template with any HTML editor, for example by changing the email texts, removing or adding configurations, or customizing the logo.
   To add configurations, use the available variables. A list of all the variables is provided as a comment at the beginning of the template.
   The default configurations for Swyx Mobile Clients can be changed directly in the URL:

Configuration	Available values	Description
connection-mode	default: "auto"	Connection mode default: available network is used automatically
	“Standard”	Internet
remoteconnector-mode	default: "auto"	RemoteConnector use default: is used automatically
	“always”	RemoteConnector is always used

Configuration	Available values	Description
connection-type	default setting: "business"	Connection type for data transmission preset: via VoIP
	“private”	via mobile network
	“request”	before each call, you are asked which connection type should be used

You must replace special characters with the corresponding hexadecimal code, e.g. comma='%2C', space='%20', colon='%3A' etc.

The configurations for server type and OEM variant are automatically determined by the installation.

9 Click the "Add..." button to save the edited file in the database.

You must not change the file name of the template, otherwise the file will not be recognized by the system.

You must select the Global section and the Templates category when adding the file.

10 Click on the "OK" button in the dialog window “Add file to the database”.

To send a welcome email

1 Start the SwyxWare Administration and log on to SwyxServer.
2 Right-click on the SwyxServer entry to open the context menu.
3 Select “Properties”.
4 Click on the Files tab.
5 If necessary, edit the template for welcome e-mails.
6 Click on the "Send welcome e-mail" button.
✓ The welcome email is sent to the email address you configured for the user during setup or editing.

You can also use the SwyxWare PowerShell module to send standard and individual welcome emails, for example to selected user groups. Please refer to the SwyxWare Administrator documentation for more information.

Settings which have already been determined before accessing the configuration URL in Swyx Mobile apps are overwritten with the settings in the URL. Settings that are not present in the URL are retained in Swyx Mobile apps.

Users of Swyx Mobile apps can skip the automatic configuration and thus keep the settings already defined in the app.

Swyx Mobile apps users can use the URLs you send multiple times, for example, to restore configurations.

1.7 Logging on Swyx Mobile Clients using the welcome email

The corresponding users receive the welcome e-mail with the preconfigured parameters.

The user should, if not already done, load the Swyx Mobile App from the App Store or Play Store. The link to the stores are also in the welcome email.

There is also a button "Configure your macOS or iOS client or Android client".

Behind the button is a URL with the following parameters:

Example:

```
swyx://import/?username=Ashton,Claire&&internalurl=DO-
EXAMPLE06.company.net&&externalurl=connect.company.net
:9102&&servertype=cpe&&oem=Company&&connectionmode=aut
o&&connectiontype=business&&remoteconnectormode=auto
```

Parameter	Content in the URL example	Description
User	"Ashton, Claire"	The name of the Swyx Mobile client user
Internal server	„DO-EXAMPLE06.company.net"	SwyxServer
External server	"connect.company.net:9102"	RemoteConnector-Server
Server variant	CPE (CUSTOMER PREMISES EQUIPMENT)	Server variant
OEM version	"Company"	Defines the OEM-Fixed variant
Connection mode	"Automatic"	Defines whether a connection is always established via the SwyxRemoteConnector or automatically if you are out of range of your company network
Connection type	"business&&remoteconnectormode=auto"	The connection type determines whether your calls are made via a VoIP or GSM connection by default or whether you want to decide spontaneously which connection type should be used before the call is established.

1.7.1 Register Swyx Mobile for iOS

The user has downloaded the Swyx Mobile App from the App Store. The link to the App Store is also included in the welcome email.

To configure Swyx Mobile for iOS using the link in the welcome email

1. In the welcome email, tap the "Configure your macOS or iOS client" button.
2. Enter user name and password to apply the settings and to log in at Swyx Mobile.
   ✓ Settings imported successfully.
3. Tap on "Continue".
   If a colored circle is shown around your profile picture, you are connected to SwyxServer and you can use Swyx Mobile for iOS.

Further information can be found in the Swyx Mobile for iOS online help.

1.7.2 Register Swyx Mobile for Android

The user has downloaded the Swyx Mobile App from the Play Store. The link to the store is also in the welcome email.

To configure Swyx Mobile for Android using the link in the welcome email

1. In the welcome email, tap the "Configure your Android client" button.
2. Enter your password in the Swyx Mobile Client under "Settings" and tap on "Logon".
   ✓ Settings imported successfully.

If a colored circle is shown around your profile picture, you are connected to SwyxServer and you can use Swyx Mobile for Android.

Further information can be found in the Swyx Mobile for Android online help.

1.8 Ideal Wifi Setup

If Coligo Mobile has to rely on a Wifi Network it is important that the network is optimised for the VoIP usage. Please use corresponding planning

and analysing tools and consider advices from the Wifi hardware manufactures for doing so. In general a Wifi network should comply with the following settings:

- Controller-based Wifi (hardware uses an intelligent Wifi controller)
- IEEE 802.11r Fast Roaming
- IEEE 802.11n or 802.11ac
- IEEE 802.11e (QoS) and WMM
- Use of two bands (2.4 GHz data, 5 GHz voice)
- Automatic Channel selection
- Automatic transmit power control
- Access Point Load Balancing

Only when an ideal Wifi Network is applied, a flawless call experience can be ensured.