



Swyx Mobile - Inbetriebnahme an SwyxServer Schritt für Schritt-Anleitung

Stand: November 2020

Rechtliche Hinweise

© 2020 Swyx Solutions GmbH. Alle Rechte vorbehalten.

Marken: Swyx, SwyxIt! und SwyxON sind eingetragene Marken der Swyx Solutions GmbH.

Alle anderen Marken, Produktnamen, Unternehmensnamen, Handelsmarken und Servicemarken sind Eigentum der entsprechenden Rechtsinhaber.

Die Inhalte dieser Dokumentation sind urheberrechtlich geschützt. Die Veröffentlichung im World Wide Web oder in sonstigen Diensten des Internets bedeutet noch keine Einverständniserklärung für eine anderweitige Nutzung durch Dritte. Jede vom deutschen Urheberrecht nicht zugelassene Verwertung bedarf der vorherigen schriftlichen Zustimmung der Swyx Solutions GmbH.

Die Informationen in dieser Dokumentation wurden sorgfältig auf ihre Korrektheit überprüft, können aufgrund ständiger Aktualisierung und Änderungen jedoch Fehler enthalten.

Swyx Solutions GmbH übernimmt keine Verantwortung für Druck- und Schreibfehler.

Trotz sorgfältiger inhaltlicher Kontrolle übernimmt Swyx Solutions GmbH keine Haftung für die Inhalte externer Links und macht sich diese nicht zu eigen. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich.

Swyx Solutions GmbH

Emil-Figge-Str. 86

D-44227 Dortmund

office@swyx.com

www.swyx.com

Swyx Mobile Client - Inbetriebnahme an SwyxServer	2
1.1 Reihenfolge der Einrichtung	2
1.2 Push Notification Service installieren	2
1.3 RemoteConnector einrichten	3
1.4 Ports in der Firewall öffnen und weiterleiten.....	4
1.5 Zertifikat für Benutzer erstellen und zuweisen.....	4
1.5.1 Automatisch erzeugtes Zertifikat verwenden	5
1.5.2 Manuell erzeugtes Zertifikat verwenden	6
1.6 Willkommens-E-Mail generieren und zustellen	6
1.7 Swyx Mobile Clients mit Hilfe der Willkommens-E-Mail anmelden	8
1.7.1 Swyx Mobile for iOS anmelden	8
1.7.2 Swyx Mobile for Android anmelden	9
1.8 Ideale WLAN-Konfiguration	9

1 Swyx Mobile Client - Inbetriebnahme an SwyxServer

In dieser Anleitung erfahren Sie, welche Schritte notwendig sind, um Ihren Swyx Mobile Client oder Ihren Swyx Desktop Client an SwyxServer betreiben zu können.

1.1 Reihenfolge der Einrichtung

Voraussetzungen:

- SwyxServer und SwyxWare Administration sind bereits installiert
- Sie haben Swyx Mobile-Lizenzen erworben

Führen Sie folgende Schritte der Reihe nach aus:

1. Push Notification Service installieren (siehe *Push Notification Service installieren*, Seite 2)
2. RemoteConnector einrichten (siehe *RemoteConnector einrichten*, Seite 3)
3. Ports in der Firewall öffnen und weiterleiten (siehe *Ports in der Firewall öffnen und weiterleiten*, Seite 4)
4. Zertifikat für Benutzer erstellen und zuweisen (siehe *Zertifikat für Benutzer erstellen und zuweisen*, Seite 4)
5. Willkommens-E-Mail erstellen und zustellen (siehe *Willkommens-E-Mail generieren und zustellen*, Seite 6)
6. Swyx Mobile Clients anmelden (siehe *Swyx Mobile Clients mit Hilfe der Willkommens-E-Mail anmelden*, Seite 8)

1.2 Push Notification Service installieren

Über den Push Notification Service haben Serverdienste die Möglichkeit, Benachrichtigungen an Client-Anwendungen zu senden, um diese auf bestimmte Ereignisse aufmerksam zu machen. Der Push Notification Service ist ein SwyxServer-Dienst und fungiert als ein Bindeglied zwischen SwyxServer und der entsprechenden Dienste von Apple und Google. Durch diese Technologie entfällt die ständige Änderungsabfrage der Client-Anwendungen beim Server wodurch die Kommunikation zwischen

Server und Client effizienter wird und ein unnötiger Akkuverbrauch entfällt.

Beim Swyx Mobile for iOS Client wird der Push Notification Service benötigt, um Funktionen zu nutzen, die mit iOS 10 (oder folgende) verfügbar sind, wie z. B. die CallKit Integration. Die Unterstützung des Push Notification Services sowie die oben genannten Vorteile sind in den Swyx Mobile Clients ab Version 2.0.0 verfügbar.

Swyx Mobile Clients mit einer Version 1.x, die keine Push-Benachrichtigungen unterstützen, können weiterhin bis zu einer SwyxServer Version 11 betrieben werden. Diese Clients beinhalten allerdings nicht die oben genannte CallKit-Integration und werden nicht weiterentwickelt. Benutzer dieser Versionen werden bei Anwendung automatisch auf die neue Version verwiesen, sofern sie mit einem aktiven Push Notification Service von SwyxServer verbunden sind. Die bisherige Konfiguration wird automatisch auf die aktuelle Version übertragen.



Eine Swyx Mobile Version 3.0.0 oder höher setzt eine SwyxWare Version 12.10 mit der aktuellsten Push Notification Service Version voraus.

Die Installationsdatei „PushNotification.msi“ finden Sie auf der SwyxWare-DVD im Verzeichnis „PushNotificationService“.

Unterstützte Betriebssysteme:

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

So installieren Sie den Push-Benachrichtigungsdienst

- 1 Starten Sie die Installationsdatei ‚PushNotification.msi‘.
✓ Der Installationsassistent öffnet sich.
- 2 Klicken Sie auf „Weiter“.
- 3 Wählen Sie den Zielordner aus und klicken Sie auf „Weiter“.
- 4 Klicken Sie auf „Installieren“, um die Installation zu starten.
✓ Der Dienst wird installiert.
- 5 Schließen Sie die Installation durch Klick auf „Fertig stellen“ ab.

1.3 RemoteConnector einrichten

Für Verbindungen mit den Swyx Mobile Clients verwendet SwyxWare ab Version 2015 R2 einen Authentifizierungsdienst. Dieser Dienst ermöglicht es, Verbindungen über SwyxRemoteConnector aufzubauen. Über SwyxRemoteConnector kann sich ein Benutzer außerhalb des lokalen (LAN) oder virtuellen privaten Netzwerks (VPN) am SwyxServer anmelden. Die benötigte Client-Konfiguration wird auf einen Schritt reduziert: Der Benutzer braucht lediglich den öffentlichen Endpunkt (als FQDN oder IP-Adresse) des Firmennetzwerks über welchen der Authentifizierungsdienst erreichbar ist, in die Client-Einstellungen einzutragen.

Bei Verbindungsaufbau schickt der Client eine Anfrage zu dem öffentlichen Endpunkt und authentifiziert sich über HTTPS mit dem SwyxWare-Benutzernamen und Kennwort. Die benötigten Konfigurationsdaten für den TLS-Tunnel (u. a. das Client-Zertifikat und die Server-Adresse des RemoteConnectors) werden auf den Client-Rechner (bzw. Smartphone) übertragen, für die zukünftigen Verbindungen gespeichert und später nach Bedarf aktualisiert.

Um SwyxServer für die Verbindung mit Swyx Mobile Clients einzustellen, müssen Sie den FQDN oder die öffentliche IP-Adresse(n) und Port eintragen, über die der SwyxRemoteConnector und der Authentifizierungsdienst aus dem Internet erreichbar sind.

Diese Einstellungen nehmen Sie im Dialog „Remotenzugriff konfigurieren“ im SwyxWare Konfigurationsassistenten vor, den Sie nach der Installation von SwyxWare starten. Haben Sie den Assistenten bereits durchlaufen, müssen Sie ihn erneut starten, um die Einstellungen zum RemoteConnector nachträglich vorzunehmen.

So konfigurieren Sie den Remotenzugriff

- 1 Starten Sie den Konfigurationsassistenten unter „Start | Programme | SwyxWare | SwyxWare Konfigurationsassistent“.
- 2 Navigieren Sie weiter bis zum Schritt „Remotenzugriff konfigurieren“.
- 3 Aktivieren Sie das Kontrollfeld „Remotenzugriff aktivieren“, um direkte Internet-Verbindungen mit Swyx Mobile Clients zu unterstützen.
- 4 Geben Sie im Bereich „Authentifizierungsserver (FQDN oder öffentliche IP)“ in die entsprechenden Felder die öffentliche Server-

Adresse und den Port (Standardport: 9101) ein, damit die Swyx Mobile Clients via Internet SwyxServer erreichen können.

Die eingetragene öffentliche Adresse des Authentifizierungsdienstes muss ebenfalls in den Einstellungen der Swyx Mobile Clients (Einstellungen | Externer Server) konfiguriert werden.



Wenn Sie einen anderen als den Standardport 9101 verwenden, muss dieser Port in den Client-Einstellungen explizit eingegeben werden.

- 5 Geben Sie im Bereich „RemoteConnector Server“ in die entsprechenden Felder die öffentliche Server-Adresse und den Port des SwyxRemoteConnector Servers ein. Die Standardports für den SwyxRemoteConnector sind 16203.
- 6 Klicken Sie auf „Weiter>“.

The screenshot shows the 'SwyxWare-Konfigurationsassistent' window with the 'Remotenzugriff konfigurieren' step. The 'Remotenzugriff aktivieren' checkbox is checked. Below it, there are two sections for server configuration. The first section is for the 'Authentifizierungsserver (FQDN oder Öffentliche IP)' with 'Adresse' set to 'server.net' and 'Port' set to '9101'. The second section is for the 'RemoteConnector Server (FQDN oder Öffentliche IP)' with 'Adresse' set to 'server.net' and 'Port' set to '16203'. At the bottom, there are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

- 7 RemoteConnector Eigenschaften:
Wählen Sie den Modus für Erzeugung und Verwaltung von Zertifikaten:
 - Automatisch
Erzeugung und Verwaltung von Zertifikaten wird von SwyxWare durchgeführt.
Im Weiteren werden Sie aufgefordert Stamm- und Serverzertifikat

erzeugen zu lassen und das Kennwort für das Stammzertifikat zu vergeben.

Über die Benutzeroberfläche der SwyxWare Administration werden Sie dann später die Client-Zertifikate für die gewünschten Benutzer erzeugen können.

Siehe *Automatisch erzeugtes Zertifikat verwenden*, Seite 5



Für die Erzeugung der Client-Zertifikate, benötigen Sie das Kennwort, mit dem Sie das Stammzertifikat geschützt haben. Dieses sollten Sie sich gut merken.

- **Manuell**
Wählen Sie diesen Modus nur, wenn Sie über eigene Zertifikate verfügen. Sie sind für die Verteilung der Zertifikate selbst verantwortlich. SwyxWare speichert in diesem Modus keine Zertifikate, sondern nur Fingerabdrücke (Thumbprints).
Im nächsten Schritt müssen Sie das Stammzertifikat und vom Stammzertifikat abgeleitetes Serverzertifikat in der entsprechenden Dropdown-Liste auswählen.
Sollten Sie Ihre Zertifikate noch nicht in den Windows-Zertifikatspeicher importiert haben, können Sie dies über die Schaltfläche „...“ tun.



Wenn Sie den Modus für Zertifikate-Erzeugung und -Verwaltung später ändern, werden alle den Benutzern zugewiesenen Client-Zertifikate ungültig.

8 Führen Sie den Konfigurationsassistenten bis zum Ende durch.

1.4 Ports in der Firewall öffnen und weiterleiten

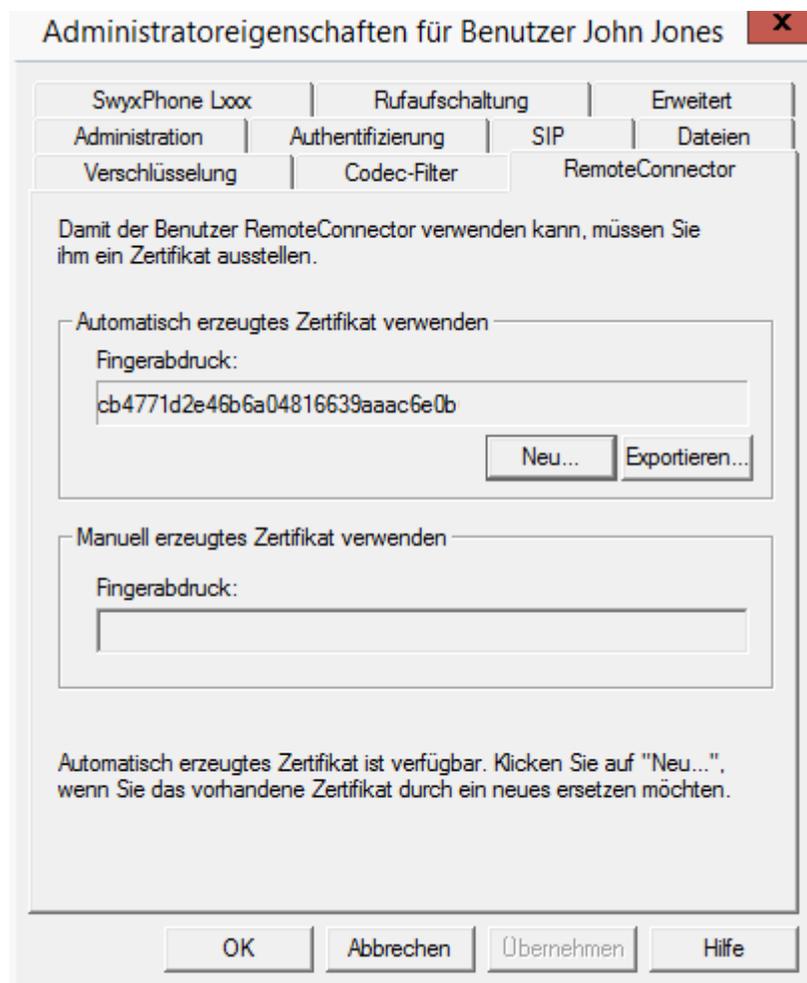
Damit Authentifizierungsdienst und RemoteConnector aus dem Internet erreichbar sind, müssen Sie die entsprechenden Ports in der Firewall freigeben und zusätzlich eine Portweiterleitung zu Ihrem SwyxServer konfigurieren.

In der folgenden Tabelle wird eine Beispielkonfiguration dargestellt:

Portweiterleitung zu...	Öffentliche IP-Adresse:TCP-Port	Ziel-IP-Adresse:TCP-Port
Authentifizierungsdienst	example.net:9101	192.168.0.4:9101
Authentifizierungsdienst auf 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 Zertifikat für Benutzer erstellen und zuweisen

Auf dieser Registerkarte erzeugen Sie für den Benutzer das digitale Client-Zertifikat oder weisen ein existierendes zu.



Nur einer der zwei Bereiche der Registerkarte ist aktiv, je nachdem welcher Modus für die Verwaltung von Zertifikaten gewählt wurde.

Den gewünschten Modus haben Sie bereits über den SwyxWare-Konfigurationsassistenten gewählt. Siehe *So konfigurieren Sie den Remotezugriff*, Seite 3.



In SwyxON ist die Option „Automatisch erzeugtes Zertifikat verwenden“ vorkonfiguriert und kann nicht verändert werden.

1.5.1 Automatisch erzeugtes Zertifikat verwenden

Im automatischen Modus werden das Stamm- und das Serverzertifikat von SwyxWare erzeugt und in der SwyxWare-Datenbank abgelegt.

Das Client-Zertifikat lassen Sie auf der aktuellen Registerkarte auch von SwyxWare erzeugen und dem Benutzer zuweisen.



Für die Erzeugung des Client-Zertifikats halten Sie das Kennwort bereit, mit dem Sie das Stammzertifikat während der SwyxWare-Konfiguration geschützt haben.



In SwyxON ist das Kennwort für die Erzeugung des Client-Zertifikats nicht erforderlich.

So weisen Sie dem Benutzer ein automatisch erzeugtes Zertifikat zu

- 1 Klicken Sie mit der Maus im linken Fenster der SwyxWare Administration auf das Verzeichnis „Benutzer“.
- 2 Klicken Sie mit der rechten Maustaste auf den Benutzer in der Benutzerliste, für den Sie ein Zertifikat erstellen möchten.
- 3 Wählen Sie im Kontextmenü „Eigenschaften“.
- 4 Klicken Sie auf „Administration“.
- 5 Klicken Sie auf die Registerkarte „RemoteConnector“.
- 6 Klicken Sie auf die Schaltfläche „Neu“.
 - ✓ Es erscheint das Dialogfenster mit dem Eingabefeld: „Kennwort des Stammzertifikats“.
- 7 Geben Sie das Kennwort ein und bestätigen mit „OK“.
 - ✓ Die Registerkarte „RemoteConnector“ erscheint im Vordergrund.
- 8 Klicken Sie auf die Schaltfläche „OK“ unten auf der Registerkarte.
 - ✓ Das Dialogfenster „Administratoreigenschaften für Benutzer...“ wird geschlossen.
 - ✓ Das Zertifikat wird erzeugt.
- 9 Öffnen Sie die Administratoreigenschaften und wählen Sie die Registerkarte „RemoteConnector“.
 - ✓ Im Feld „Fingerabdruck“ ist der digitale Fingerabdruck des Zertifikats eingetragen.

Um das Zertifikat für den Benutzer zu ersetzen, wiederholen Sie die Schritte (5) bis (9).

1.5.2 Manuell erzeugtes Zertifikat verwenden

Im manuellen Modus müssen das Stammzertifikat, Serverzertifikat(e) und Clientzertifikate von Ihnen erzeugt und im Windows-Zertifikatspeicher auf den entsprechenden Rechnern abgelegt werden.

Auf der Registerkarte „RemoteConnector“ müssen Sie den Fingerabdruck des Client-Zertifikats eintragen, das Sie für den Benutzer erzeugt und auf seinem Rechner in den Windows-Zertifikatspeicher importiert haben.

So tragen Sie den Fingerabdruck des Client-Zertifikats ein

- 1 Öffnen Sie in der SwyxWare Administration die „Administrationseigenschaften für Benutzer...“ und wählen Sie die Registerkarte „RemoteConnector“.
- 2 Im Bereich „Manuell erzeugtes Zertifikat verwenden“ tragen Sie den Fingerabdruck des Client-Zertifikats ins Feld „Fingerabdruck“ ein.
- 3 Bestätigen Sie Ihre Angabe mit „OK“.
Das Dialogfenster „Administratoreigenschaften für Benutzer...“ wird geschlossen. Das Client-Zertifikat ist dem Benutzer zugewiesen.

1.6 Willkommens-E-Mail generieren und zustellen

Sie können Benutzern mit Hilfe einer Willkommens-E-Mail Anmeldedaten und Konfigurationen für Ihre Swyx Mobile Clients zukommen lassen. Diese Daten können Sie über eine Vorlage festlegen.

Auf Swyx Mobile Clients werden die Konfigurationen automatisch übertragen, indem der Benutzer die entsprechende URL in der Willkommens-E-Mail aufruft und dadurch direkt zu seinem Client weitergeleitet wird.

Der Großteil der Konfigurationen ist über Variablen mit der Vorlage für die Willkommens-E-Mails verknüpft. Beim Senden werden die Variablen dann automatisch durch die Konfigurationen ersetzt. Eine Liste aller Variablen finden Sie als Kommentar am Anfang der Vorlage.

Einige Konfigurationen für Swyx Mobile Clients werden nicht in der SwyxWare Administration festgelegt, sondern sind durch Werte in der Vorlage für die Willkommens-E-Mail voreingestellt oder automatisch durch die Installation festgelegt, siehe *So bearbeiten Sie die Vorlage für Willkommens-E-Mails*, Seite 6.

Zum Senden von Willkommens-E-Mails haben Sie folgende Möglichkeiten:

- Standard-E-Mail verwenden
Die Standard-E-Mail enthält die wichtigsten Konfigurationen, die der Benutzer zum Anmelden und Telefonieren benötigt.
- E-Mail individuell anpassen

Bearbeiten Sie die Vorlage, aus der die Willkommens-E-Mails generiert werden, bevor Sie die E-Mail senden. Siehe *So bearbeiten Sie die Vorlage für Willkommens-E-Mails*, Seite 6.

So bearbeiten Sie die Vorlage für Willkommens-E-Mails

- 1 Starten Sie die SwyxWare Administration und melden Sie sich an dem SwyxServer an.
- 2 Klicken Sie mit der rechten Maustaste auf den SwyxServer-Eintrag, um das Kontextmenü zu öffnen.
- 3 Wählen Sie „Eigenschaften“.
- 4 Klicken Sie auf die Registerkarte „Dateien“.
- 5 Klicken Sie auf „Bearbeiten...“.
- 6 Wählen Sie aus der Liste die Datei „WelcomeMailTemplate.html“.
- 7 Klicken Sie auf die Schaltfläche „Speichern unter...“ und wählen Sie einen Speicherort.
- 8 Bearbeiten Sie die Vorlage mit einem beliebigen HTML-Editor, indem Sie z. B. die E-Mail-Texte ändern, Konfigurationen entfernen oder hinzufügen oder das Logo anpassen.
Um Konfigurationen hinzuzufügen, verwenden Sie die verfügbaren Variablen. Eine Liste aller Variablen finden Sie als Kommentar am Anfang der Vorlage.
Die voreingestellten Konfigurationen für Swyx Mobile Clients ändern Sie ggf. direkt in der URL:

Konfiguration	Verfügbare Werte	Erläuterung
connection-mode	voreingestellt: „auto“	Verbindungsmodus voreingestellt: verfügbares Netz wird automatisch verwendet
	„standard“	Internet
remoteconnector-mode	voreingestellt: „auto“	RemoteConnector verwenden voreingestellt: wird automatisch verwendet
	„always“	RemoteConnector wird immer verwendet
connection-type	voreingestellt: „business“	Verbindungsart für die Datenübertragung voreingestellt: via VoIP
	„private“	via Mobilfunknetz
	„request“	vor jedem Anruf wird gefragt, welche Verbindungsart verwendet werden soll



Sie müssen Sonderzeichen durch den entsprechenden Hexadezimal-Code ersetzen, z. B. Komma='%2C', Leerzeichen='%20', Doppelpunkt='%3A' etc.



Die Konfigurationen für Servertyp und OEM-Variante werden automatisch durch die Installation festgelegt.

- 9 Klicken Sie auf die Schaltfläche „Hinzufügen...“, um die bearbeitete Datei in der Datenbank zu speichern.



Sie dürfen den Dateinamen der Vorlage nicht ändern, da die Datei sonst nicht vom System erkannt wird.



Sie müssen beim Hinzufügen der Datei den Bereich „Global“ und die Kategorie „Templates“ wählen.

- 10 Klicken Sie im Dialogfenster „Datei zur Datenbank hinzufügen“ auf die Schaltfläche „OK“.

So senden Sie eine Willkommens-E-Mail

- 1 Starten Sie die SwyxWare Administration und melden Sie sich an SwyxServer an.
- 2 Klicken Sie mit der rechten Maustaste auf den SwyxServer-Eintrag, um das Kontextmenü zu öffnen.
- 3 Wählen Sie „Eigenschaften“.
- 4 Klicken Sie auf die Registerkarte „Dateien“.
- 5 Bearbeiten Sie ggf. die Vorlage für Willkommens-E-Mails.
- 6 Klicken Sie auf die Schaltfläche „Willkommens-E-Mail senden“.
 - ✓ Die Willkommens-E-Mail wird an die E-Mail-Adresse gesendet, die Sie für den Benutzer beim Einrichten oder Bearbeiten konfiguriert haben.

Sie können auch via SwyxWare PowerShell Modul Standard- und individuelle Willkommens-E-Mails, z. B. an ausgewählte Benutzergruppen senden. Informationen dazu finden Sie in der SwyxWare Administrator Dokumentation.



Einstellungen, die bereits vor dem Aufruf der Konfigurations-URL in Swyx Mobile Apps festgelegt wurden, werden mit den Einstellungen in der URL überschrieben. Einstellungen, die nicht in der URL vorhanden sind, werden in Swyx Mobile Apps beibehalten.



Benutzer von Swyx Mobile Apps können die automatische Konfiguration überspringen und damit die bereits in der App festgelegten Einstellungen beibehalten.



Benutzer von Swyx Mobile Apps können die von Ihnen gesendeten URLs mehrmals verwenden, z. B. um Konfigurationen wiederherzustellen.

1.7 Swyx Mobile Clients mit Hilfe der Willkommens-E-Mail anmelden

Die entsprechenden Benutzer erhalten die Willkommens-E-Mail mit den vorkonfigurierten Parametern.

Der Benutzer sollte, sofern noch nicht geschehen, die Swyx Mobile App aus dem App Store bzw. Play Store laden. Der Link zu den Stores befinden sich ebenfalls in der Willkommens-E-Mail.

Außerdem befindet sich dort eine Schaltfläche „Konfigurieren Sie Ihren macOS oder iOS-Client bzw. Android Client“.

Hinter der Schaltfläche verbirgt sich eine URL mit folgenden Parametern:

Beispiel:

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

Parameter	Inhalt im URL-Beispiel	Erläuterung
Benutzername	„Ashton, Claire“	Der Name des Swyx Mobile Client-Benutzers
Interner Server	„DO-EXAMPLE06.company.net“	SwyxServer
Externer Server	„connect.company.net:9102“	RemoteConnector-Server
Server-Variante	„CPE“	Legt die Server-Variante fest
OEM-Variante	„Company“	Legt die OEM-Variante fest

Parameter	Inhalt im URL-Beispiel	Erläuterung
Verbindungsmodus	„Automatisch“	Legt fest, ob immer eine Verbindung über den SwyxRemoteConnector hergestellt wird oder automatisch, sofern Sie sich außer Reichweite Ihres Firmennetzwerkes befinden
Verbindungsart	„business&&remoteconnectormode=auto“	Über die Verbindungsart wird festgelegt, ob Ihre Gespräche standardmäßig über eine VoIP- oder GSM-Verbindung geführt werden oder ob Sie vor Aufbau des Gesprächs spontan entscheiden möchten, welche Verbindungsart genutzt werden soll.

1.7.1 Swyx Mobile for iOS anmelden

Der Benutzer hat die Swyx Mobile App aus dem App Store geladen. Der Link zum App Store befindet sich ebenfalls in der Willkommens-E-Mail.

So konfigurieren Sie Swyx Mobile for iOS mit Hilfe des Links in der Willkommens-E-Mail

- 1 Tippen Sie in der Willkommens-E-Mail auf die Schaltfläche „Konfigurieren Sie Ihren macOS oder iOS-Client“.
- 2 Geben Sie zur Übernahme der Daten sowie zur Anmeldung an Swyx Mobile Ihr Kennwort ein und tippen Sie auf „Speichern“.
 - ✓ Die Einstellungen wurden erfolgreich importiert.
- 3 Tippen Sie auf „Fortfahren“.

Erscheint Ihr Profilbild mit einem farbigen Kreis, sind Sie mit SwyxServer verbunden und können Swyx Mobile for iOS nutzen.

Weitere Informationen finden Sie in der Swyx Mobile for iOS Online-Hilfe.

1.7.2 Swyx Mobile for Android anmelden

Der Benutzer hat die Swyx Mobile App aus dem Play Store geladen. Der Link zum Store befindet sich ebenfalls in der Willkommens-E-Mail.

So konfigurieren Sie Swyx Mobile for Android mit Hilfe des Links in der Willkommens-E-Mail

- 1 Tippen Sie in der Willkommens-E-Mail auf die Schaltfläche „Konfigurieren Sie Ihren Android Client“.
- 2 Geben Sie im Swyx Mobile Client unter „Einstellungen“ Ihr Kennwort ein und tippen Sie auf „Anmelden“.
✓ Die Einstellungen wurden erfolgreich importiert.

Erscheint Ihr Profilbild mit einem farbigen Kreis, sind Sie mit SwyxServer verbunden und können Swyx Mobile for Android nutzen.

Weitere Informationen finden Sie in der Swyx Mobile for Android Online-Hilfe.

1.8 Ideale WLAN-Konfiguration

Wenn Swyx Mobile auf ein WLAN-Netzwerk angewiesen ist, ist es wichtig, dass das Netzwerk für die VoIP-Nutzung optimiert ist. Bitte verwenden Sie entsprechende Planungs- und Analysewerkzeuge und berücksichtigen Sie dabei die Ratschläge der WLAN-Hardwarehersteller. Im Allgemeinen sollte ein Wifi-Netzwerk den folgenden Einstellungen entsprechen:

- Controller-basiertes WLAN (Hardware verwendet einen intelligenten WLAN-Controller)
- IEEE 802.11r Fast Roaming
- IEEE 802.11n oder 802.11ac
- IEEE 802.11e (QoS) und WMM
- Nutzung von zwei Bändern (2,4 GHz Data, 5 GHz Voice)
- Automatic Channel selection
- Automatic transmit power control
- Access Point Load Balancing



Nur wenn ein ideales WLAN-Netzwerk angewendet wird, kann ein einwandfreies Anruferlebnis gewährleistet werden.