Unify

Unify Phone V2-Administration

Dokumentation für Administratoren

A31003-F9920-M100-13-00A9

Atos

Senden Sie Ihr Feedback zur Verbesserung dieses Dokumentes an edoku@atos.net.

Als Reseller wenden sich für spezifische Presales-Fragen bitte an die entsprechende Presales-Organisation bei Unify oder Ihrem Distributor. Für spezifische technische Anfragen nutzen Sie die Support Knowledgebase, eröffnen - sofern entsprechender Software Support Vertrag vorliegt - ein Ticket über das Partner Portal oder kontaktieren Ihren Distributor.

Unser Qualitäts- und Umweltmanagementsystem ist entsprechend den Vorgaben der ISO9001 und ISO14001 implementiert und durch ein externes Zertifizierungsunternehmen zertifiziert.

Copyright © Unify Software and Solutions GmbH & Co. KG 10/11/2023
Alle Rechte vorbehalten.

Sachnummer: A31003-F9920-M100-13-00A9

Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, die je nach Anwendungsfall nicht immer in der beschriebenen Form zutreffen oder sich durch Weiterentwicklung der Produkte ändern können. Eine Verpflichtung, die jeweiligen Merkmale zu gewährleisten besteht nur, sofern diese ausdrücklich vertraglich zugesichert wurden.

Liefermöglichkeiten und technische Änderungen vorbehalten.

Unify, OpenScape, OpenStage und HiPath sind eingetragene Warenzeichen der Unify Software and Solutions GmbH & Co. KG. Alle anderen Marken-, Produkt- und Servicenamen sind Warenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Inhaber.

atos.net

Inhalt

1 Einführung..... 5
1.1 Unify Phone Übersicht..... 5
1.2 Übersicht über die Unify Phone-Administration..... 7

2 Ersteinrichtung von Unify Phone für Unify Video..... 9
2.1 Registrieren für Unify Phone..... 9
2.2 Einrichten eines JWT für die Benutzerbereitstellung..... 10
2.3 Kommunikationssystem konfigurieren..... 12
2.4 Konfigurieren des OpenScape SBC (für OpenScape Voice oder OpenScape 4000)..... 14
2.5 Aktivieren von Cross-Launch von Unify Video zu Unify Phone..... 15

3 Ersteinrichtung von Unify Phone for OpenScape..... 17
3.1 Einrichten des ersten Administratorkontos aus der Einladung..... 17
3.2 Für Unify Phone for OpenScape registrieren..... 18
3.3 Konfigurieren des Kommunikationssystems für die Verbindung mit Unify Phone..... 20
3.4 Benutzerbereitstellung..... 21
3.4.1 Benutzerbereitstellung auf Unify Phone for OpenScape Business..... 21
3.4.2 Benutzerbereitstellung auf Unify Phone for OpenScape Voice..... 23
3.4.3 Benutzerbereitstellung auf Unify Phone for OpenScape 4000..... 25
3.5 Konfigurieren des OpenScape SBC (für OpenScape Voice oder OpenScape 4000)..... 27

4 An- und Abmeldung..... 29
4.1 Anmelden..... 29
4.1.1 Anmeldung bei Unify Phone für Unify Video..... 29
4.1.2 Sich bei Unify Phone for OpenScape mit Ihren Unify Phone-Anmeldedaten anmelden..... 29
4.1.3 Anmeldung bei Unify Phone for OpenScape mit Single Sign On (SSO)..... 30
4.2 Abmeldung..... 30

5 Unify Phone JWT..... 31
5.1 JWT-Status..... 31
5.2 Bearbeitung des JWT..... 32

6 Telephony Connector..... 34
6.1 Anzeigen des Status des Telefonieanschlusses..... 34
6.2 Exportieren von Telefonieanschlussdaten..... 34
6.3 API-Schlüssel..... 35
6.3.1 API-Schlüssel anzeigen..... 35
6.3.2 API-Schlüssel neu generieren..... 35
6.4 Zertifikate..... 36
6.4.1 Hinzufügen eines Zertifikats..... 36
6.4.2 Anzeigen des Status eines Zertifikats..... 36
6.4.3 Details zu einem Zertifikat anzeigen..... 37
6.4.4 Zertifikat löschen..... 37

7 Benutzer..... 39
7.1 Benutzer anzeigen..... 39
7.2 Benutzer importieren..... 39
7.3 Suche nach einem Benutzer..... 40
7.4 Erneutes Versenden von Einladungen an Benutzer..... 41
7.5 Administratorfunktion zuweisen oder entfernen..... 41

8 Authentifizierung..... 43
8.1 SAML 2.0 SSO-Authentifizierungsmethode einrichten..... 43

8.1.1 Manuelle Eingabe von Metadaten für einen SAML 2.0 Identitätsanbieter.....44
8.1.2 Metadaten für einen SAML 2.0-Identitätsanbieter importieren.....45
8.2 Eine SAML 2.0-Authentifizierungsmethode bearbeiten..... 47
8.3 SAML 2.0-Attribute zuordnen..... 47
8.4 Eine Authentifizierungsmethode aktivieren oder deaktivieren.....48
8.5 Eine Authentifizierungsmethode testen.....49
8.6 Eine Authentifizierungsmethode aktivieren oder deaktivieren.....49
8.7 Eine Authentifizierungsmethode löschen..... 50

9 Integrationen..... 52
9.1 Unify Phone für Microsoft Teams..... 52
9.1.1 Unify Phone für Microsoft Teams herunterladen..... 52
9.1.2 Unify Phone für Microsoft Teams in das Microsoft Teams Admin Center hochladen.....53
9.1.3 Admin-Zustimmung für Unify Phone für Microsoft Teams erteilen..... 54

10 Einhaltung der DSGVO..... 55
10.1 Exportieren von Anrufdaten..... 55
10.2 Aufbewahrungsfrist für Anrufdaten einstellen..... 55

11 Mandantendetails..... 57
11.1 Mandantendetails ansehen..... 57
11.2 Mandantendetails bearbeiten.....57
11.3 Support-E-Mail-Adresse einrichten..... 57

12 Überlegungen zu Firewall und Proxy..... 58
12.1 Stateful Firewall-Konfiguration und NAT für OpenScape Business.....58
12.2 Stateful Firewall-Konfiguration und NAT für OpenScape Voice und OpenScape 4000..... 61

13 Service und Support.....64
13.1 Zugang zur Dokumentation für Administratoren..... 64
13.2 Anzeigen von Neuigkeiten.....64
13.3 Probleme melden.....64
13.4 Geschäftsbedingungen einsehen..... 65
13.5 Informationen über den Unify Phone-Status abrufen..... 65

14 Anhang.....66
14.1 Liste der vertrauenswürdigen Zertifizierungsstellen..... 66
14.2 GCP IP-Quellbereich für Europa-west3.....68
14.3 Admin-Zustimmung für Unify Phone für Microsoft Exchange Online erteilen..... 69
14.4 Konnektivitätsanforderungen für Microsoft Exchange lokal.....70

1 Einführung

Diese Anleitung beschreibt die Ersteinrichtung und Verwaltung von Unify Phone mit der Unify Phone-Administrations-App.

1.1 Unify Phone Übersicht

Unify Phone ist ein Cloud-basierter Telefonie-Connector, der mit den OpenScape-Kommunikationssystemen arbeitet:

- Atos Unify OpenScape Voice
- Atos Unify OpenScape 4000
- Atos Unify OpenScape Business

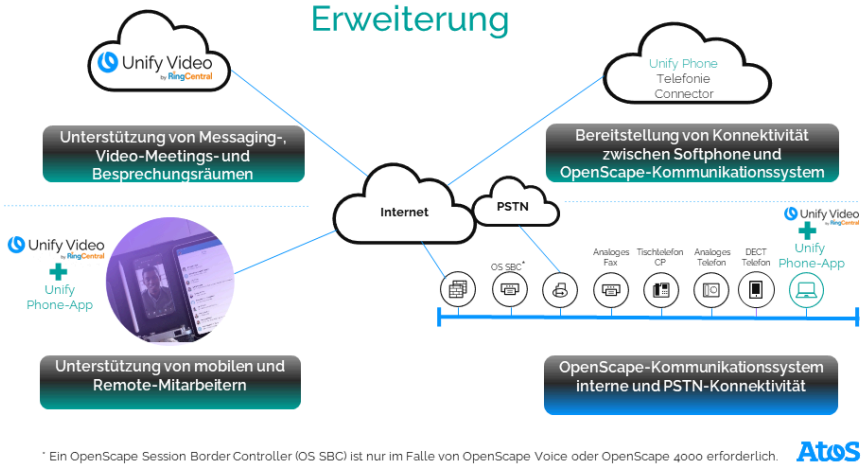
Damit können Sie über Ihre geschäftliche Telefonnummer mit der Unify Phone-App Anrufe tätigen und entgegennehmen.

Unify Phone-Varianten

Unify Phone gibt es in zwei verschiedenen Varianten:

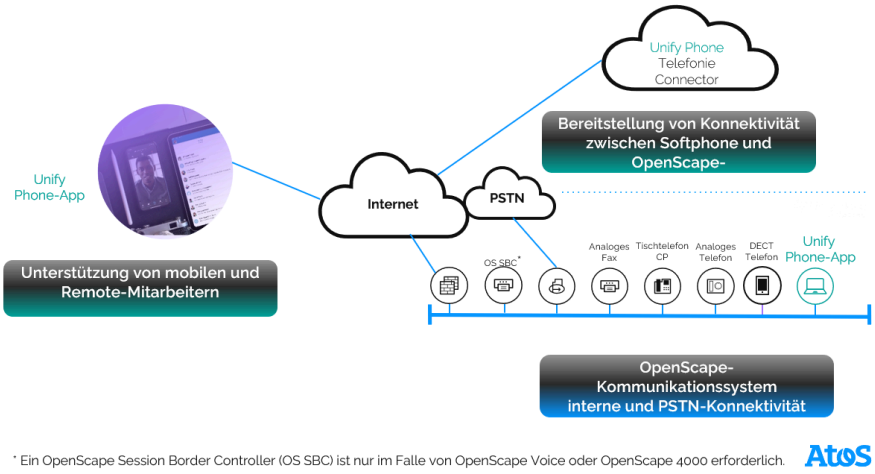
- **Unify Phone für Unify Video**

  Es wird in Verbindung mit Unify Video verwendet und ermöglicht es Unify Video-Benutzern, mit anderen über Telefonanrufe zu kommunizieren.



- **Unify Phone for OpenScape**

  Es wird als eigenständiger Telefonie-Client des OpenScape Kommunikationssystems verwendet.



Funktionen

Unify Phone unterstützt die folgenden Funktionen:

- Anruf tätigen
- Annehmen, Ablehnen oder Beenden eines Anrufs
- DTMF-Befehle während eines Anrufs senden
- Anruf halten und zurückholen
- Stummschalten/Stummschaltung aufheben
- Anruf übergeben
- Holen von Anrufen von anderen Unify Phone-Clients oder dem Tischtelefon (Pull-Funktion)
- Anruf verschieben auf Tischtelefon
- Push-Anruf an alternative Nummer[1]
- Einen zweiten Anruf tätigen oder annehmen
- Anrufe makeln (abwechseln)
- Zusammenführen von zwei Anrufen zu einer Konferenz
- Anrufweiterleitung
- Alternative Nummer (One Number Service)
- Anruf-Routing
- Voicemail
- Remoteanrufsteuerung von Tischtelefonen (Computer-Telefonie-Integration - CTI): Halten und Fortsetzen, Beenden von Anrufen, Makeln, Weiterleiten, Zusammenführen zu Konferenzen
- Cross-Launch von Unify Video (nur wenn Unify Phone in Verbindung mit Unify Video verwendet wird)

Anmerkung: Reine IPv6-Netze werden derzeit nicht unterstützt.

Voraussetzungen

Unify Phone für Unify Video ist in den folgenden Konfigurationen erhältlich:

- Unify Video-Lösung
  - Unify Video Pro+
- Kommunikationssystem
  - Atos Unify OpenScape Business V3 (mit einem Service Release 2 oder höher)
  - Atos Unify OpenScape Voice V10R2.14.0 (mit allen verfügbaren Hotfixes) oder höher
  - Atos Unify OpenScape 4000 V10R1 (mit allen verfügbaren Hotfixes) oder höher

Unify Phone for OpenScape ist in den folgenden Konfigurationen erhältlich:

- Kommunikationssystem
  - Atos Unify OpenScape Business V3 (mit einem Service Release 2 oder höher)
  - Atos Unify OpenScape Voice V10R2.14.0 (mit allen verfügbaren Hotfixes) oder höher
  - Atos Unify OpenScape 4000 V10R1.34 (mit allen verfügbaren Hotfixes) oder höher und die Berechtigungen für Assistant oder Manager

1.2 Übersicht über die Unify Phone-Administration

Die Administration von Unify Phone wird mit der Unify Phone-Administrations-App durchgeführt. Dies ist eine webbasierte Anwendung, die Ihnen auf einfache Weise Folgendes ermöglicht:

- Unify Phone mit Unify Video zu verbinden, wenn Sie Unify Phone in Verbindung mit Unify Video verwenden möchten
- den API-Schlüssel zu generieren, der für die Verbindung eines OpenScape-Kommunikationssystems mit Unify Phone erforderlich ist
- den Status des Telefonie-Connectors zu überprüfen
- Daten des Telefonie-Connectors zu exportieren
- benutzerdefinierte, selbstsignierte Zertifikate für TLS-Verbindungen hinzuzufügen oder zu entfernen
- Zertifikatsstatus und -details anzuzeigen
- Benutzer in Ihrem Unify Phone-Mandanten anzuzeigen, zu suchen und zu sortieren sowie neue Benutzer zu importieren
- eine erneute Einladung an OpenScape Business-Teilnehmer zu senden, um Ihrem Unify Phone-Mandanten beizutreten (nur für Unify Phone for OpenScape verfügbar)
- mehrere Authentifizierungsmethoden für das einmalige Anmelden (Single Sign On, SSO) einzurichten und eine davon als Standard-

[1] Verfügbar, wenn Unify Phone mit Atos Unify OpenScape Voice oder Atos Unify OpenScape 4000 arbeitet

Authentifizierungsmethode unter Verwendung der Unify Phone-Anmeldedaten festzulegen.

Diese Funktion ist nur für Unify Phone for OpenScape verfügbar.

- Informationen über den Status des Unify Phone abrufen.

2 Ersteinrichtung von Unify Phone für Unify Video

Dieses Kapitel beschreibt die Ersteinrichtung von Unify Phone für Unify Video.

Die wichtigsten Schritte bei der Einrichtung sind die folgenden:

1) Registrieren für Unify Phone für Unify Video
2) Einrichten eines JSON-Web-Tokens (JWT) für die Benutzerbereitstellung
3) Konfigurieren Sie Ihr Kommunikationssystem für die Verbindung mit Unify Phone und weisen Sie dann den Unify Phone-/Unify Video-Benutzern Telefonnummern und die erforderlichen Lizenzen zu.
4) Wenn Ihr Kommunikationssystem OpenScape Voice oder OpenScape 4000 ist, konfigurieren Sie Ihren OpenScape SBC für die Verbindung mit Unify Phone
5) Aktivieren Sie Cross-Launch von Unify Video zu Unify Phone.

Die Einrichtung von Unify Phone erfolgt über die folgenden Softwareanwendungen:

- Unify Phone Administrations-App, die in diesem Handbuch beschrieben wird
- Unify Video Verwaltungsportal
- Administrationsprogramm Ihres OpenScape-Kommunikationssystems, insbesondere:
  - OpenScape Business Assistant (WBM), im Falle von OpenScape Business
  - OpenScape Common Management Platform, im Falle von OpenScape Voice
  - OpenScape 4000 Assistant, im Falle von OpenScape 4000.
- Administrationsprogramm von OpenScape SBC (wird nur bei OpenScape Voice und OpenScape 4000 benötigt), d. h. OpenScape SBC Assistant.

Anmerkung: Nach der Zuweisung von Telefonnummern und den erforderlichen Lizenzen an Unify Phone- / Unify Video-Benutzer werden Änderungen an den Benutzerdetails im Unify Video-Administrationsportal nicht an Unify Phone oder das Kommunikationssystem weitergegeben und sollten daher in jedem Fall vermieden werden.

2.1 Registrieren für Unify Phone

Wenn Sie ein Administrator des Unify Video-Kontos Ihres Unternehmens sind, können Sie Ihr Unternehmen für Unify Phone registrieren.

Schritt für Schritt

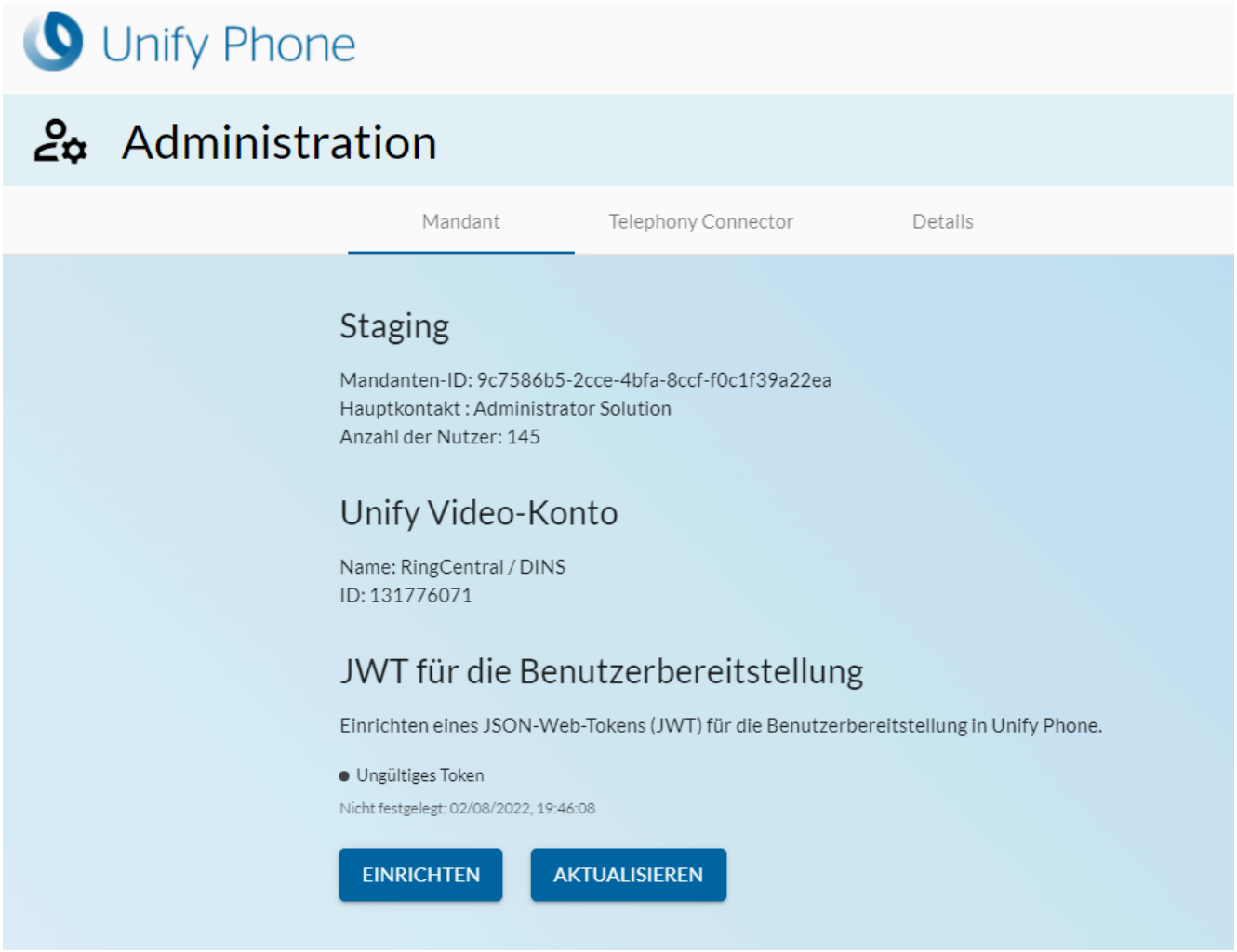
1) Öffnen Sie einen Webbrowser und geben Sie die Adresse (URL) der Unify Phone Administrations-App ein: https://phoneapp.unify.com/tenant/.
2) Wenn Sie aufgefordert werden, sich anzumelden, klicken Sie auf **Unify Office**.
3) Melden Sie sich mit den Anmeldedaten Ihres Unify Video-Administrationskontos an.
4) Klicken Sie auf **Autorisieren**, um Unify Phone den erforderlichen Zugriff auf Unify Video zu ermöglichen.
5) Geben Sie die Details des Hauptkontakts in Ihrem Unternehmen für den Unify Phone-Mandanten ein:
   a) **Vorname**
   b) **Nachname**
   c) **E-Mail**
   d) **Telefonnummer**
   e) **Land**
6) Geben Sie einen **Mandantennamen** ein.
7) Bestätigen Sie Ihr Einverständnis mit den **Nutzungsbedingungen, den Datenschutzrichtlinien und den Richtlinien zur akzeptablen Nutzung**, indem Sie das Kontrollkästchen anklicken.
8) Bestätigen Sie, dass Sie mit der **Datenschutzvereinbarung** einverstanden sind, indem Sie das Kontrollkästchen anklicken.
9) Klicken Sie auf **Registrieren**.
   Es wird ein **API-Schlüssel** generiert, den Sie in Ihr OpenScape-Kommunikationssystem eingeben müssen.
10) Sie können auf **In die Zwischenablage kopieren** klicken, um den Schlüssel zu kopieren.
11) Klicken Sie auf **Fertigstellen**.

Ein neuer Unify Phone-Mandant wird erstellt und Sie werden zur Hauptseite der Unify Phone-Verwaltungsanwendung weitergeleitet.

Sie können den API-Schlüssel jederzeit auf der Registerkarte **Telefonie-Connector** der Verwaltungs-App einsehen.

2.2 Einrichten eines JWT für die Benutzerbereitstellung

Wenn ein Mandant in Unify Phone für Unify Video zum ersten Mal erstellt wird, ist Unify Phone nicht mit Unify Video integriert. Einrichten eines JSON-Web-Tokens (JWT) für die Benutzerbereitstellung in Unify Phone.



Schritt für Schritt

1) Öffnen Sie die Unify Phone Administrations-App.
2) Suchen Sie den Bereich **JWT für Benutzerbereitstellung** .
   Sie sehen, dass der JWT-Status `Nicht eingestellt` ist.
3) Klicken Sie auf **Einrichten**.
4) Suchen Sie die **Unify Phone Client-ID** und klicken Sie auf , um sie in Ihre Zwischenablage zu kopieren.
5) Klicken Sie auf den Link JWT-Erstellungsportal, um das Portal zu öffnen, und melden Sie sich mit Ihren Anmeldedaten für das Unify Video-Administrationskonto an.

6) Erstellen Sie ein neues Token.

a) Fügen Sie eine Bezeichnung für das JWT in das Feld **Bezeichnung** ein.

b) Aktivieren Sie das Kontrollkästchen **Nur bestimmte Apps meiner Wahl** .

> **Anmerkung:** Dies ist eine Sicherheitsmaßnahme, um den Zugriff auf JWT für bestimmte Anwendungen zu beschränken.

c) Es erscheint ein neues Eingabefeld für die Kunden-ID. Fügen Sie die **Unify Phone-Client-ID** aus der Zwischenablage in dieses Feld ein und klicken Sie auf **App hinzufügen**.

d) Optional können Sie auf das Feld unter dem Bereich **Ablaufdatum (UTC)** klicken und ein Ablaufdatum für das JWT festlegen.

e) Klicken Sie auf **JWT erstellen**.

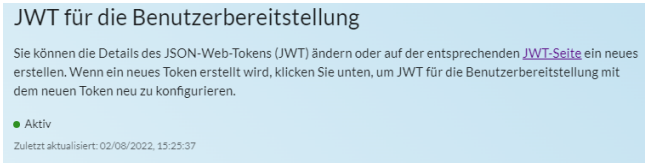
f) Klicken Sie auf , um das JWT in Ihre Zwischenablage zu kopieren.

7) Kehren Sie zur Unify Phone-Verwaltungsanwendung zurück und fügen Sie das JWT in das Feld **JWT-Token** ein.

8) Klicken Sie auf **Fertig**.

9) Warten Sie, bis die JWT-Validierung abgeschlossen ist.

Nach erfolgreicher Validierung ändert sich der JWT-Status in `Aktiv`.



Zugehörige Konzepte

Unify Phone JWT auf Seite 31

2.3 Kommunikationssystem konfigurieren

Um Ihr OpenScape-Kommunikationssystem für die Verbindung mit Unify Phone zu konfigurieren, stellen Sie Folgendes sicher:

1) Sie geben den API-Schlüssel Ihres Unify Phone-Mandanten an den Administrator Ihres Kommunikationssystems weiter.

Sie können den API-Schlüssel auf der Registerkarte **Telefonie Konnektor** der Unify Phone-Administrationsanwendung anzeigen.

2) Der Administrator Ihres Kommunikationssystems gibt den API-Schlüssel in das System ein.

3) Der Administrator Ihres Kommunikationssystems weist den Unify Phone-Benutzern Telefonnummern und die erforderlichen Lizenzen zu.

Bei OpenScape Voice ist es außerdem zwingend erforderlich, in den Teilnehmereinstellungen des OND (One Number Service Device) die Option „Profil überschreiben" zu aktivieren. Die empfohlenen Klingeldauer-Timer sind wie folgt:

- Mobil (WLAN): 1 Sek.
- Hauptgerät (ONS): 10 Sek.
- Mobil (Mobilfunk): 15 Sek.

Erlaubte Werte für Hauptgerät (ONS) und Mobilgerät (Mobilfunk) sind: 5, 10, 15, 20, 25.

Die ONS- und OND-Ressourcen eines Unify Phone-Benutzers müssen mit denselben Werten für die Felder **Realm** und **Passwort** der Digest-Authentifizierungsdaten konfiguriert werden.

Der Administrator des Kommunikationssystems kann die Schritte 2 und 3 insbesondere mit dem entsprechenden Administrationsprogramm durchführen:

- OpenScape Business Assistant (WBM), im Falle von OpenScape Business

  Detaillierte Informationen finden Sie im folgenden Dokument: *OpenScape Business V3, Administratordokumentation* (Abschnitt 23.10 Unify Phone).
- OpenScape Common Management Platform, im Falle von OpenScape Voice

  Detaillierte Informationen finden Sie im folgenden Dokument:

  – *OpenScape Common Management Platform V10, Administratordokumentation*.
  – *OpenScape Voice V10, Administratordokumentation*
- OpenScape 4000 Assistant, im Falle von OpenScape 4000

  Detaillierte Informationen finden Sie im folgenden Dokument:

  – *OpenScape 4000 V10, Band 4: IP-Lösungen, Servicedokumentation*
  – *OpenScape 4000 Assistant V10, Konfigurationsmanagement, Administratordokumentation*.

Anmerkung: Die Voicemail-Funktionalität wird nicht auf Unify Phone, sondern auf der Seite des OpenScape Kommunikationssystems konfiguriert. Die Konfiguration der Voicemail erfolgt bei OpenScape Business über den OpenScape Business Assistant (WBM) und bei OpenScape Voice oder OpenScape 4000 über OpenScape Xpressions.

2.4 Konfigurieren des OpenScape SBC (für OpenScape Voice oder OpenScape 4000)

Wenn Ihr Kommunikationssystem OpenScape Voice oder OpenScape 4000 ist, muss OpenScape SBC für die Verbindung mit Unify Phone konfiguriert werden. Dies ist erforderlich, um Anrufe vom Kommunikationssystem an Unify Phone weiterzuleiten.

Damit die Verbindung aufgebaut werden kann, muss der OpenScape SBC-Administrator auf dem OpenScape SBC Assistant (Version V10R2.4.0 oder höher) folgende Schritte durchführen:

1) **Aktivieren von Remote-Teilnehmern**, indem das entsprechende Kontrollkästchen unter **Leistungsmerkmale** aktiviert wird.
2) Zuweisung des Medienprofils **Unify_Phone_default** an den User Agent, der Unify Phone entspricht **(OpenScape Mobile Client - WebRTC NGTC**).

   Anmerkung: Achten Sie bei der Eingabe von `OpenScape Mobile Client - WebRTC NGTC` in das Feld **User Agent** darauf, dass Sie ein Minuszeichen (-) verwenden und nicht einen Halbgeviertstrich (–) oder Geviertstrich (—).

   ---

3) Aktivieren Sie die Option **NGTC WebRTC-Kompatibilität aktivieren**.
4) Stellen Sie sicher, dass das OpenScape SBC-Zertifikat von Unify Phone als vertrauenswürdig eingestuft wird.

   Standardmäßig vertraut Unify Phone nur Zertifikaten, die von bekannten Zertifizierungsstellen (CAs) signiert sind, sowie dem Standardzertifikat von OpenScape SBC (das im Lieferumfang der Appliance enthalten ist).

   Wenn das OpenScape SBC-Zertifikat von einer Zertifizierungsstelle signiert ist, die in der Liste der vertrauenswürdigen Zertifizierungsstellen aufgeführt ist, oder die Standardzertifizierungsstelle ist, sind keine weiteren Maßnahmen erforderlich.

   Wenn es sich bei dem Zertifikat um ein selbstsigniertes Zertifikat oder ein Zertifikat einer nicht vertrauenswürdigen Zertifizierungsstelle handelt, müssen Sie als Administrator des Mandanten das RootCA-Zertifikat zu Unify Phone hinzufügen, wie in Abschnitt Hinzufügen eines Zertifikats auf Seite 36 beschrieben.

   Es wird empfohlen, dass Ihr Unternehmen anstelle der Standardzertifikate eigene, selbstsignierte Zertifikate erstellt und verwendet.

Weitere Informationen zur Verwaltung und Konfiguration eines OpenScape SBC finden Sie in folgendem Dokument: *OpenScape SBC V10, Administratordokumentation*.

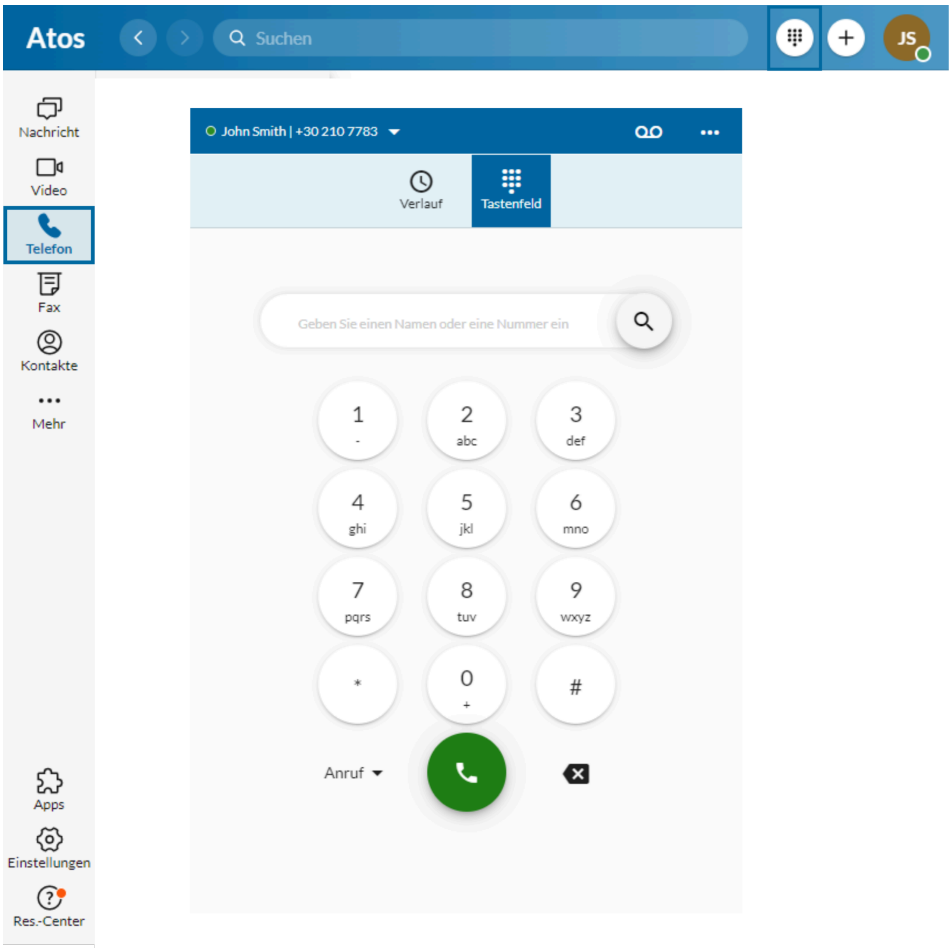
Zusätzlich zu den oben genannten Punkten müssen Sie die Digestauthentifizierung (DA) für Unify Phone-Remotebenutzer aktivieren. Weitere Informationen finden Sie im folgenden Dokument:

OpenScape SBC V10, Sicherheitscheckliste (Abschnitt 3.16 Unify Phone-Härtung).

2.5 Aktivieren von Cross-Launch von Unify Video zu Unify Phone

Damit Unify Video-Benutzer die Unify Phone-App direkt von Unify Video aus starten können, muss Cross-Launch für sie aktiviert sein.

Nach der Aktivierung können Unify Video-Benutzer das Wählscheiben-Symbol ⠿ oben rechts in ihrer Unify Video-App und das Telefon-Symbol in der linken Navigationsleiste sehen. Sie können auf eines dieser Symbole klicken, um Unify Phone zu öffnen und nach der Anmeldung zu beginnen, Anrufe zu tätigen und entgegenzunehmen.



Voraussetzungen

- Sie sind ein Administrator des Unify Video-Kontos Ihres Unternehmens.
- Die Benutzer haben die Unify Video Pro+ Lizenz.

Um Cross-Launch für Unify Phone/ Unify Video-Benutzer zu ermöglichen:

Schritt für Schritt

1) Melden Sie sich als Administrator am Unify Video-Administrationsportal an.
2) Klicken Sie auf die Registerkarte **Mehr**.
3) Klicken Sie im linken Navigationsbereich auf **Kontoeinstellungen** und wählen Sie dann **Cross-Launch**.
4) Suchen Sie den/die Benutzer, für den/die Sie Cross-Launch aktivieren möchten, und setzen Sie den Schieberegler für **Cross-Launch** auf Ein.

3 Ersteinrichtung von Unify Phone for OpenScape

Dieses Kapitel beschreibt die Ersteinrichtung von Unify Phone for OpenScape.

Die wichtigsten Schritte bei der Einrichtung sind die folgenden:

1) Erstes Administratorkonto auf Unify Phone for OpenScape aus der Einladung einrichten
2) Ihr Unternehmen für Unify Phone for OpenScape registrieren
3) Ihr OpenScape-Kommunikationssystem für die Verbindung mit Unify Phone konfigurieren
4) Benutzer bereitstellen
5) Wenn Ihr Kommunikationssystem OpenScape Voice oder OpenScape 4000 ist, konfigurieren Sie Ihren OpenScape SBC für die Verbindung mit Unify Phone

Die Einrichtung von Unify Phone for OpenScape erfolgt über die folgenden Softwareanwendungen:

- Unify Phone-Administrationsanwendung, die in diesem Handbuch beschrieben wird
- Administrationsprogramm Ihres OpenScape-Kommunikationssystems, insbesondere:
  - OpenScape Business Assistant (WBM), im Falle von OpenScape Business
  - OpenScape Common Management Platform, im Falle von OpenScape Voice
  - OpenScape 4000 Assistant, im Falle von OpenScape 4000.
- Administrationsprogramm von OpenScape SBC (wird nur bei OpenScape Voice und OpenScape 4000 benötigt), d. h. OpenScape SBC Assistant.

3.1 Einrichten des ersten Administratorkontos aus der Einladung

Der erste Schritt bei der Einrichtung von Unify Phone for OpenScape besteht darin, das erste Administratorkonto einzurichten. Dieses Konto wird erstellt, wenn eine Einladung von einem Unify Phone Operations-Mitarbeiter gesendet wird.

Voraussetzungen

Sie haben eine E-Mail-Einladung von noreply@unifyphone.app erhalten, um Ihr Administratorkonto einzurichten und Ihr Unternehmen für Unify Phone for OpenScape zu registrieren.

Folgen Sie den beschriebenen Schritten, um Ihr Konto einzurichten:

Schritt für Schritt

1) Öffnen Sie die E-Mail und klicken Sie auf **Konto einrichten**.

   Wenn der Link abgelaufen ist, wenden Sie sich bitte an den Unify Phone Support, um eine neue Einladung zu erhalten.
2) Wählen Sie **Hier klicken, um fortzufahren**.
3) Geben Sie auf dem Bildschirm Neues Passwort festlegen ein neues Passwort ein, und bestätigen Sie es dann erneut.

   Das Passwort muss mindestens 12 Zeichen lang sein, 1 Großbuchstaben, 1 Kleinbuchstaben, 1 Zahl und 1 Sonderzeichen enthalten und sich vom Benutzernamen unterscheiden.

   Wenn das Passwort nicht mit der Passwortrichtlinie übereinstimmt, erscheint eine Fehlermeldung.
4) Klicken Sie auf **Absenden**.

Ihr Konto als Administrator wurde eingerichtet.

Nächste Schritte

Klicken Sie auf **Zurück zur Anwendung** und Sie werden zur Anmeldeseite der Unify Phone Administrations-App weitergeleitet.

3.2 Für Unify Phone for OpenScape registrieren

Als Administrator können Sie Ihr Unternehmen für Unify Phone for OpenScape registrieren.

Schritt für Schritt

1) Wenn Sie sich noch nicht auf der Anmeldeseite der Unify Phone-Administrationsanwendung befinden, besuchen Sie https://phoneapp.unify.com/tenant/ und klicken Sie auf **Anmelden**.
2) Melden Sie sich mit Ihren Anmeldedaten für das Administrationskonto an:
   a) Geben Sie die E-Mail-Adresse ein, die mit Ihrem Konto verknüpft ist, und klicken Sie auf **Weiter**.
   b) Geben Sie das Passwort ein und klicken Sie auf **Anmelden**.
3) Geben Sie in das Feld **Name des Mandanten** den entsprechenden Namen ein.
4) Die E-Mail-Adresse des Mandantenerstellers wird im Feld **E-Mail des Administrators** angezeigt.

5) Geben Sie die Details des Hauptkontakts in Ihrem Unternehmen für den Unify Phone for OpenScape-Mandanten ein:

a) **Vorname**
b) **Nachname**
c) **E-Mail**
d) **Rufnummer**

Die Rufnummer muss im E.164-Format vorliegen.

Anmerkung: E.164-Nummern beginnen mit einem Pluszeichen (+) und enthalten 7 bis 15 Ziffern.

---

e) **Land**

6) Geben Sie optional unter **Zusätzlicher Administrator** dessen Details für den Unify Phone for OpenScape-Mandanten ein:

a) **Vorname**
b) **Nachname**
c) **E-Mail**

Wenn die E-Mail-Adresse eines zusätzlichen Administrators in das Feld **E-Mail** eingegeben wird, werden die Felder **Vorname** und **Nachname** obligatorisch.

Die E-Mail-Adresse darf nicht mit einem bestehenden Konto verknüpft sein.

Das zusätzliche Administratorkonto wird bei der Registrierung Ihres Unternehmens für Unify Phone for OpenScape erstellt.

7) Bestätigen Sie Ihr Einverständnis mit den **Allgemeinen Nutzungsbedingungen, der Datenschutzrichtlinie und der Vereinbarung über die angemessene Nutzung**, indem Sie das Kontrollkästchen anklicken.

8) Bestätigen Sie, dass Sie mit der **Datenschutzvereinbarung** einverstanden sind, indem Sie das Kontrollkästchen anklicken.

9) Klicken Sie auf **Registrieren**.

Ein neuer Unify Phone for OpenScape-Mandant wird erstellt und Sie werden zur Hauptseite der Unify Phone-Administrationsanwendung weitergeleitet.

Wenn Sie die Details eines zusätzlichen Administrators eingegeben haben, wird das Konto erstellt. Der zusätzliche Administrator erhält eine E-Mail-Einladung, um sein Konto einzurichten.

Es wird ein **API-Schlüssel** generiert, den Sie in Ihr OpenScape-Kommunikationssystem eingeben müssen.

Sie können den API-Schlüssel jederzeit auf der Registerkarte **Telefonie Konnektor** der Administrationsanwendung einsehen.

3.3 Konfigurieren des Kommunikationssystems für die Verbindung mit Unify Phone

Um Ihr OpenScape-Kommunikationssystem für die Verbindung mit Unify Phone zu konfigurieren, stellen Sie Folgendes sicher:

1) Sie geben den API-Schlüssel Ihres Unify Phone-Mandanten an den Administrator Ihres Kommunikationssystems weiter.

Sie können den API-Schlüssel auf der Registerkarte **Telefonie Konnektor** der Unify Phone-Administrationsanwendung anzeigen.

2) Der Administrator Ihres Kommunikationssystems gibt den API-Schlüssel in das System ein.

3) Bei OpenScape Voice oder OpenScape 4000 legt Ihr Administrator des Kommunikationssystems den SIP-Trunk an, der für die Verbindung verwendet werden soll.

Anmerkung: Im Falle von OpenScape Business werden die SIP-Trunks automatisch als Ergebnis von Schritt 2 auf Seite 20angelegt.

Der Administrator des Kommunikationssystems kann die Schritte 2 und 3 insbesondere mit dem entsprechenden Administrationsprogramm durchführen:

- OpenScape Business Assistant (WBM), im Falle von OpenScape Business

  Detaillierte Informationen finden Sie im folgenden Dokument: *OpenScape Business V3, Administratordokumentation* (Abschnitt 23.10 Unify Phone).
- OpenScape Common Management Platform, im Falle von OpenScape Voice

  Detaillierte Informationen finden Sie im folgenden Dokument: *OpenScape Common Management Platform V10, Administratordokumentation* (Abschnitt 4.2.17 Konfigurieren von Unify Phone Server und Abschnitt 10.1.1 Erstellen einer neuen SBC-Konfiguration für Unify Phone-Benutzer)
- OpenScape 4000 Assistant, im Falle von OpenScape 4000

  Detaillierte Informationen finden Sie im folgenden Dokument:

  – *OpenScape 4000 V10, Band 4: IP-Lösungen, Service-Dokumentation* (Abschnitt 17 Unify Phone Connectivity)
  – *OpenScape 4000 Assistant V10, Konfigurationsmanagement, Administratordokumentation*.

Anmerkung: Die Voicemail-Funktionalität wird nicht auf Unify Phone, sondern auf der Seite des OpenScape Kommunikationssystems konfiguriert. Die Konfiguration der Voicemail erfolgt bei OpenScape Business über den OpenScape Business Assistant (WBM) und bei OpenScape Voice oder OpenScape 4000 über OpenScape Xpressions.

3.4 Benutzerbereitstellung

3.4.1 Benutzerbereitstellung auf Unify Phone for OpenScape Business

Die Benutzerbereitstellung auf Unify Phone for OpenScape Business kann mit einer CSV-Datei (Comma-Separated Values) durchgeführt werden.
Die Voraussetzungen für die Benutzerbereitstellung auf Unify Phone for OpenScape Business sind die folgenden:

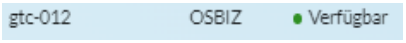
1) Einen Mandantenadministrator zum Erstellen von Benutzern auf dem Unify Phone-Mandanten
2) Einen OpenScape Business-Administrator, der den Unify Phone-Benutzern Telefonnummern und die erforderlichen Lizenzen zuweist.

Anmerkung: Die E-Mail-Adresse ist die eindeutige Kennung, die einen Benutzer mit einem einzelnen Unify Phone-Mandanten verknüpft und muss für alle Unify Phone-Mandanten eindeutig sein.

Benutzer auf Unify Phone anlegen

Gehen Sie als Mandantenadministrator wie folgt vor:

1) Öffnen Sie die Unify Phone Administrations-App: https://phoneapp.unify.com/tenant/.
2) Gehen Sie zur Registerkarte **Telephony Connector**.
3) Überprüfen Sie, ob der Status des für Ihren Mandanten konfigurierten OpenScape Business-Telefonie-Connectors (SIP-Trunk) auf `Verfügbar` steht.



4) Sie können Benutzerdetails in eine CSV-Datei (Comma-Separated Values) einfügen, wie unten beschrieben:

a) Erstellen Sie eine Excel-Datei mit den folgenden Spalten: `emailAddress`, `firstName`, `lastName`, `locale`.

Anmerkung: Bei den Einträgen in der Excel-Datei müssen Sie Groß- und Kleinschreibung verwenden.

---

b) Füllen Sie die Excel-Datei mit den Angaben zu den Benutzern aus, die Sie anlegen möchten.

Beispiel:

	A	B	C	D
1	emailAddress	firstName	lastName	locale
2	john.doe@example.com	John	Doe	en-US
3	jane.doe@example.com	Jane	Doe	en-US

Mögliche Gebietsschema-Werte sind:

- `en-US` (Standard)
- `de-DE`
- `fr-FR`
- `es-ES`
- `it-IT`
- `nl-NL`
- `ca-ES`

Wenn Sie kein Gebietsschema angeben, wird das Standardgebietsschema verwendet.

c) Gehen Sie in Excel auf **Datei** > **Speichern unter**. Ändern Sie den Dateityp in **CSV UTF-8 (Comma delimited) (*.csv)** und klicken Sie auf **Speichern**.

5) Navigieren Sie in der Unify Phone-Verwaltungsanwendung zur Registerkarte **Benutzer** .

6) Wählen Sie die OpenScape Business-Amtsleitung aus, den Sie bereitstellen möchten, und klicken Sie auf **CSV importieren**.

7) Suchen Sie nach der in Schritt 4 auf Seite 22 erstellten CSV-Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**.

8) Warten Sie, bis der Importvorgang abgeschlossen ist.

Nach erfolgreichem Abschluss wird die Anzahl der erstellten Benutzer angezeigt. Die neu angelegten Benutzer werden in der Benutzerliste angezeigt.

Wenn der Vorgang länger dauert als erwartet, wird die folgende Meldung angezeigt: `Die Bereitstellung von Benutzern dauert länger als erwartet und wird im Hintergrund fortgesetzt.`

Wenn der Importvorgang zwischendurch fehlschlägt, können Sie ihn jederzeit wiederholen. Der Importeur kann Duplikate erkennen und sie überspringen. Es werden nur Benutzer erstellt, die bei einem früheren Versuch nicht erfolgreich erstellt wurden.

Den Benutzern ist noch keine Telefonnummer zugewiesen.

Zuweisung von Telefonnummern und der erforderlichen Lizenzen an Unify Phone-Benutzer

Ihr OpenScape Business-Administrator muss die folgenden Schritte durchführen:

1) Öffnen Sie den OpenScape Business Assistant (WBM).

2) Zuweisen von Telefonnummern zu Unify Phone-Benutzern über **Einrichtung** > **Assistenten** > **Cloud-Dienste** > **Unify Phone Benutzer-Instanz** > **Bearbeiten** > **Hinzufügen**.

Auf diese Weise werden die Unify Phone-Benutzer dem Kommunikationssystem hinzugefügt.

Der OpenScape Business-Administrator kann so viele Unify Phone-Benutzer hinzufügen, wie er benötigt.

Wenn ein Benutzer hinzugefügt wird, erhält er eine E-Mail von noreply@unifyphone.app mit einem Link zum Einrichten seines Kontos.

3) Weisen Sie den Unify Phone-Benutzern die erforderlichen Lizenzen über **Lizenz-Management** > **Lokale Benutzerlizenzen** > **...** zu

Detaillierte Informationen finden Sie im folgenden Dokument: *OpenScape Business V3, Administrator-Dokumentation* (Abschnitt 23.10 Unify Phone).

3.4.2 Benutzerbereitstellung auf Unify Phone for OpenScape Voice

Die Bereitstellung von Benutzern auf Unify Phone for OpenScape Voice kann auf zwei Arten erfolgen:

- einer nach dem anderen oder
- in großen Mengen über eine JSON-Datei.

Anmerkung: Die E-Mail-Adresse ist die eindeutige Kennung, die einen Benutzer mit einem einzelnen Unify Phone-Mandanten verknüpft und muss für alle Unify Phone-Mandanten eindeutig sein.

Einzelne Benutzer einrichten

Die Bereitstellung der einzelnen Benutzer erfolgt in der OpenScape Common Management Platform durch einen OpenScape Voice-Administrator.

Ihr OpenScape Voice-Administrator muss die folgenden Schritte durchführen:

1) Öffnen Sie die OpenScape Common Management Platform.

2) Fügen Sie neue Telefonnummern für Unify Phone-Benutzer hinzu (falls erforderlich) über **Konfiguration** > **OpenScape Sprache** > **Business-Gruppe** > **Mitglieder** > **Teilnehmer** > **Hinzufügen**.

   Vergewissern Sie sich, dass die Option "Profil außer Kraft setzen" in den OND-Teilnehmereinstellungen (One Number Service Device) aktiviert ist. Die empfohlenen Klingeldauer-Timer sind wie folgt:

   - Mobil (WLAN): 1 Sek.
   - Hauptgerät (ONS): 10 Sek.
   - Mobil (Mobilfunk): 15 Sek.

   Erlaubte Werte für Hauptgerät (ONS) und Mobilgerät (Mobilfunk) sind: 5, 10, 15, 20, 25.

3) Fügen Sie neue Unify Phone-Benutzer hinzu und weisen Sie ihnen Telefonnummern zu über **Konfiguration** > **Benutzerverwaltung** > **Unify Phone** > **Benutzer** > **Hinzufügen**.

   Der OpenScape Voice-Administrator kann so viele Unify Phone-Benutzer hinzufügen, wie er benötigt.

   Wenn ein Benutzer hinzugefügt wird, erhält er eine E-Mail von noreply@unifyphone.app mit einem Link zum Einrichten seines Kontos.

Detaillierte Informationen finden Sie im folgenden Dokument: *OpenScape Common Management Platform V10, Administratordokumentation* (Abschnitt 10 OpenScape User Management Unify Phone und Abschnitt 11.3.9 Wie konfiguriere ich einen Unify Phone-Teilnehmer).

Massenweise Bereitstellung von Benutzern

Die Bereitstellung von Benutzern in großen Mengen erfolgt in der Unify Phone-Verwaltungsanwendung.

Als Mandantenadministrator müssen Sie Folgendes tun:

1) Öffnen Sie die Unify Phone Administrations-App.
2) Gehen Sie zur Registerkarte **Telephony Connector**.
3) Überprüfen Sie, ob der Status des für Ihren Mandanten konfigurierten OpenScape Voice-Telefonie-Connectors (SIP-Trunk) auf `Verfügbar` steht.

4) Klicken Sie unter dem Bereich **OpenScape Voice / OpenScape 4000** auf **Exportieren**.

   Eine Liste aller Trunks wird im JSON-Format heruntergeladen.

   Die Details Ihres OSV-Trunks sollten wie folgt aussehen:

```
[
  {
    "id": "<TRUNK_ID>",
    "name": "<TRUNK_NAME>",
    "type": "OSV_TRUNK_TYPE",
    "ip": "<SBC_PUBLIC_IP>",
    "port": "<SBC_TLS_PORT>",
    "protocol": "tls"
  }
]
```

5) Sorgen Sie für Folgendes:

   a) Die JSON-Datei wird innerhalb des Unify Flip User Migration Tools verwendet, um Ihrem Unternehmen die Migration von On-Premise- oder UCaaS-Ressourcen zu Unify Phone zu erleichtern.

   b) Als Ergebnis wird eine neue JSON-Datei aus dem Unify Flip Tool exportiert, die alle erforderlichen Daten enthält.

6) Navigieren Sie in der Unify Phone-Verwaltungsanwendung zur Registerkarte **Benutzer**.

7) Klicken Sie auf **JSON importieren**.

8) Suchen Sie nach der in Schritt 5 auf Seite 25 erstellten JSON-Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**.

9) Warten Sie, bis der Importvorgang abgeschlossen ist.

   Nach erfolgreichem Abschluss wird die Anzahl der erstellten Benutzer angezeigt. Die neu angelegten Benutzer werden in der Benutzerliste angezeigt.

   Wenn der Vorgang länger dauert als erwartet, wird die folgende Meldung angezeigt: `Die Bereitstellung von Benutzern dauert länger als erwartet und wird im Hintergrund fortgesetzt.`

   Wenn der Importvorgang zwischendurch fehlschlägt, können Sie ihn jederzeit wiederholen. Der Importeur kann Duplikate erkennen und sie überspringen. Es werden nur Benutzer erstellt, die bei einem früheren Versuch nicht erfolgreich erstellt wurden.

3.4.3 Benutzerbereitstellung auf Unify Phone for OpenScape 4000

Die Bereitstellung von Benutzern auf Unify Phone for OpenScape 4000 kann auf zwei Arten erfolgen:

- einer nach dem anderen oder
- in großen Mengen über eine JSON-Datei.

Anmerkung: Die E-Mail-Adresse ist die eindeutige Kennung, die einen Benutzer mit einem einzelnen Unify

Phone-Mandanten verknüpft und muss für alle Unify Phone-Mandanten eindeutig sein.

Einzelne Benutzer einrichten

Die Einrichtung der einzelnen Benutzer erfolgt im OpenScape 4000 Assistant durch einen OpenScape 4000-Administrator.

Ihr OpenScape 4000-Administrator muss die folgenden Schritte durchführen:

1) Öffnen des OpenScape 4000 Assistant.

2) Hinzufügen neuer Unify Phone-Benutzer über **Konfigurationsmanagement** > **Unify Phone** > **Benutzerdaten** > **Benutzer hinzufügen**.

Der OpenScape 4000-Administrator kann so viele Unify Phone-Benutzer hinzufügen, wie er benötigt.

3) Wenn die E-Mail-Adresse eines Unify Phone-Benutzers noch nicht auf OpenScape 4000 konfiguriert ist, konfigurieren Sie sie im **Konfigurationsmanagement**.

4) Konfigurieren Sie für jeden Unify Phone-Benutzer ein Zusatzgerät und weisen Sie ihm eine Unify Phone-Lizenz zu.

5) Aktualisieren Sie die Benutzerdaten auf dem Unify Phone-Mandanten wie unten beschrieben:

- Wenn Sie die Benutzerdaten für einen bestimmten neuen Benutzer aktualisieren möchten, navigieren Sie zu **Konfigurationsmanagement** > **Unify Phone** > **Benutzer** und klicken Sie neben diesem Benutzer auf **Aktualisieren**.
- Wenn Sie die Benutzerdaten für alle neuen Benutzer auf einmal aktualisieren möchten, navigieren Sie zu **Konfigurationsmanagement** > **Unify Phone** > **Benutzer** und klicken Sie auf **Alle aktualisieren**.

Wenn die Daten für neue Benutzer auf dem Unify Phone-Mandanten aktualisiert werden, wird ihnen eine E-Mail von noreply@unifyphone.app mit einem Link zur Einrichtung ihres Kontos gesendet.
Detaillierte Informationen finden Sie im folgenden Dokument: *OpenScape 4000 V10, Band 4: IP Solutions, Service-Dokumentation* (Abschnitt 17.3.2 Benutzerkonfiguration).

Massenweise Bereitstellung von Benutzern

Die Bereitstellung von Benutzern in großen Mengen erfolgt in der Unify Phone-Verwaltungsanwendung.

Als Mandantenadministrator müssen Sie Folgendes tun:

1) Öffnen Sie die Unify Phone Administrations-App.

2) Gehen Sie zur Registerkarte **Telephony Connector**.

3) Überprüfen Sie, ob der Status des für Ihren Mandanten konfigurierten OpenScape 4000-Telefonie-Connectors (SIP-Trunk) auf `Verfügbar` steht.

4) Klicken Sie unter dem Bereich **OpenScape Voice / OpenScape 4000** auf **Exportieren** .

   Eine Liste aller Trunks wird im JSON-Format heruntergeladen.

   Die Details Ihres OS4K-Trunks sollten wie folgt aussehen:

```
[
  {
    "id": "<TRUNK_ID>",
    "name": "<TRUNK_NAME>",
    "type": "OS4K_TRUNK_TYPE",
    "ip": "<SBC_PUBLIC_IP>",
    "port": "<SBC_TLS_PORT>",
    "protocol": "tls"
  }
]
```

5) Sorgen Sie für Folgendes:

   a) Die JSON-Datei wird innerhalb des Unify Flip User Migration Tools verwendet, um Ihrem Unternehmen die Migration von On-Premise- oder UCaaS-Ressourcen zu Unify Phone zu erleichtern.

   b) Als Ergebnis wird eine neue JSON-Datei aus dem Unify Flip Tool exportiert, die alle erforderlichen Daten enthält.

6) Navigieren Sie in der Unify Phone-Verwaltungsanwendung zur Registerkarte **Benutzer** .

7) Klicken Sie auf **JSON importieren**.

8) Suchen Sie nach der in Schritt 5 auf Seite 27 erstellten JSON-Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**.

9) Warten Sie, bis der Importvorgang abgeschlossen ist.

   Nach erfolgreichem Abschluss wird die Anzahl der erstellten Benutzer angezeigt. Die neu angelegten Benutzer werden in der Benutzerliste angezeigt.

   Wenn der Vorgang länger dauert als erwartet, wird die folgende Meldung angezeigt: `Die Bereitstellung von Benutzern dauert länger als erwartet und wird im Hintergrund fortgesetzt.`

   Wenn der Importvorgang zwischendurch fehlschlägt, können Sie ihn jederzeit wiederholen. Der Importeur kann Duplikate erkennen und sie überspringen. Es werden nur Benutzer erstellt, die bei einem früheren Versuch nicht erfolgreich erstellt wurden.

3.5 Konfigurieren des OpenScape SBC (für OpenScape Voice oder OpenScape 4000)

Wenn Ihr Kommunikationssystem OpenScape Voice oder OpenScape 4000 ist, muss OpenScape SBC für die Verbindung mit Unify Phone konfiguriert werden. Dies ist erforderlich, um Anrufe vom Kommunikationssystem an Unify Phone weiterzuleiten.

Damit die Verbindung aufgebaut werden kann, muss der OpenScape SBC-Administrator auf dem OpenScape SBC Assistant (Version V10R2.4.0 oder höher) folgende Schritte durchführen:

1) **Aktivieren von Remote-Teilnehmern**, indem das entsprechende Kontrollkästchen unter **Leistungsmerkmale** aktiviert wird.
2) Zuweisung des Medienprofils **Unify_Phone_default** an den User Agent, der Unify Phone entspricht **(OpenScape Mobile Client - WebRTC NGTC**).

Anmerkung: Achten Sie bei der Eingabe von `OpenScape Mobile Client - WebRTC NGTC` in das Feld **User Agent** darauf, dass Sie ein Minuszeichen (-) verwenden und nicht einen Halbgeviertstrich (–) oder Geviertstrich (—).

---

3) Aktivieren Sie die Option **NGTC WebRTC-Kompatibilität aktivieren**.
4) Stellen Sie sicher, dass das OpenScape SBC-Zertifikat von Unify Phone als vertrauenswürdig eingestuft wird.

   Standardmäßig vertraut Unify Phone nur Zertifikaten, die von bekannten Zertifizierungsstellen (CAs) signiert sind, sowie dem Standardzertifikat von OpenScape SBC (das im Lieferumfang der Appliance enthalten ist).

   Wenn das OpenScape SBC-Zertifikat von einer Zertifizierungsstelle signiert ist, die in der Liste der vertrauenswürdigen Zertifizierungsstellen aufgeführt ist, oder die Standardzertifizierungsstelle ist, sind keine weiteren Maßnahmen erforderlich.

   Wenn es sich bei dem Zertifikat um ein selbstsigniertes Zertifikat oder ein Zertifikat einer nicht vertrauenswürdigen Zertifizierungsstelle handelt, müssen Sie als Administrator des Mandanten das RootCA-Zertifikat zu Unify Phone hinzufügen, wie in Abschnitt Hinzufügen eines Zertifikats auf Seite 36 beschrieben.

   Es wird empfohlen, dass Ihr Unternehmen anstelle der Standardzertifikate eigene, selbstsignierte Zertifikate erstellt und verwendet.

Weitere Informationen zur Verwaltung und Konfiguration eines OpenScape SBC finden Sie in folgendem Dokument: *OpenScape SBC V10, Administratordokumentation*.

Zusätzlich zu den oben genannten Punkten müssen Sie die Digestauthentifizierung (DA) für Unify Phone-Remotebenutzer aktivieren. Weitere Informationen finden Sie im folgenden Dokument: *OpenScape SBC V10, Sicherheitscheckliste* (Abschnitt 3.16 Unify Phone-Härtung).

4 An- und Abmeldung

4.1 Anmelden…

In diesem Kapitel wird beschrieben, wie man sich anmeldet:

- Unify Phone for Unify Video
- Unify Phone for OpenScape, mit Ihren Unify Phone-Anmeldedaten
- Unify Phone for OpenScape mit einmaligem Anmelden (Single Sign On, SSO)

4.1.1 Anmeldung bei Unify Phone für Unify Video

Wenn Unify Phone in Verbindung mit Unify Video verwendet wird, können Sie sich mit den Anmeldedaten Ihres Unify Video-Administrationskontos bei der Administrationsanwendung anmelden.

Schritt für Schritt

1) Öffnen Sie einen Webbrowser und geben Sie die Adresse (URL) der Unify Phone-Mandantenadministration ein: https://phoneapp.unify.com/tenant/.
   Die Anwendung öffnet sich und fordert Sie auf, sich anzumelden.
2) Klicken Sie auf **Anmelden**.
3) Klicken Sie auf **Unify Office**.

   Anmerkung: Wenn Sie bereits ein Unify Phone-Benutzer mit Administratorrechten sind, können Sie alternativ die mit Ihrem Unify Video-Konto verbundene E-Mail-Adresse eingeben und auf **Weiter**klicken.

4) Geben Sie die E-Mail-Adresse oder Telefonnummer ein, die mit Ihrem Unify Video-Administrationskonto verbunden ist, und klicken Sie auf **Weiter**.
5) Geben Sie das Passwort ein und klicken Sie auf **Anmelden**.
6) Klicken Sie auf **Autorisieren**, damit Unify Phone und Unify Video auf Ihre Kontoinformationen zugreifen können.

4.1.2 Sich bei Unify Phone for OpenScape mit Ihren Unify Phone-Anmeldedaten anmelden

Wenn Unify Phone als eigenständiger Telefonie-Client verwendet wird, können Sie sich mit den Anmeldedaten Ihres Unify Phone-Kontos bei der Administrationsanwendung anmelden.

Schritt für Schritt

1) Öffnen Sie einen Webbrowser und geben Sie die Adresse (URL) der Unify Phone-Mandantenadministration ein: https://phoneapp.unify.com/tenant/.
   Die Anwendung öffnet sich und fordert Sie auf, sich anzumelden.
2) Klicken Sie auf **Anmelden**.
3) Geben Sie die E-Mail-Adresse ein, die mit Ihrem Konto verknüpft ist, und klicken Sie auf **Weiter**.
4) Geben Sie das Passwort ein und klicken Sie auf **Anmelden**.

4.1.3 Anmeldung bei Unify Phone for OpenScape mit Single Sign On (SSO)

Single Sign On Authentication (SSO) ermöglicht es Ihnen, sich mit einem einzigen Satz von Anmeldedaten bei mehreren Anwendungen anzumelden. Wenn eine SSO-Methode für Ihren Mandanten konfiguriert und aktiviert wurde, können Sie sich mit Ihrem Unternehmenskonto bei der Unify Phone-Administrationsanwendung anmelden.

Schritt für Schritt

1) Öffnen Sie einen Webbrowser und geben Sie die Adresse (URL) der Unify Phone-Administrationsanwendung ein: https://phoneapp.unify.com/tenant/.
2) Klicken Sie auf **Anmelden**.
3) Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **Weiter**.
4) Klicken Sie auf die Schaltfläche unter der Option **Anmelden mit**.
5) Sie werden zur Anmeldeseite des SSO-Anbieters weitergeleitet. Melden Sie sich mit den Anmeldedaten Ihres Unternehmenskontos an.
   Nach erfolgreicher Authentifizierung werden Sie zur Unify Phone-Administrationsanwendung zurückgeleitet.

4.2 Abmeldung

Sie können sich jederzeit abmelden:

Schritt für Schritt

1) Klicken Sie auf das Ellipsen-Symbol (...) oben rechts in der Unify Phone Administrations-App.
2) Wählen Sie **Abmelden** aus dem Dropdown-Menü aus.

5 Unify Phone JWT

JSON Web Token (JWT) ist ein offener Standard, der die sichere Übertragung von Informationen zwischen einem Client und einem Server ermöglicht.

Unify Phone kann über JWT für die Benutzerbereitstellung mit Unify Video integriert werden.

Um die Integration einzurichten, müssen Sie das JWT wie in Abschnitt Einrichten eines JWT für die Benutzerbereitstellung auf Seite 10 beschrieben einrichten.

Wenn das Token ungültig wird, abgelaufen ist oder demnächst abläuft, ändert sich der JWT-Status entsprechend.

Sie müssen ein neues Token im JWT-Erstellungsportal erstellen und dann das JWT für die Benutzerbereitstellung mit dem neuen Token neu konfigurieren.

Anmerkung: JWT für die Benutzerbereitstellung ist nur für Unify Phone für Unify Video verfügbar.

Zugehörige Konzepte

JWT-Status auf Seite 31

Zugehörige Informationen

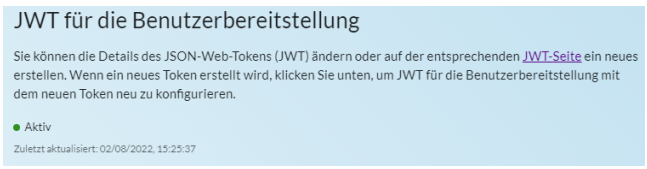
Einrichten eines JWT für die Benutzerbereitstellung auf Seite 10
Bearbeitung des JWT auf Seite 32

5.1 JWT-Status

Die verschiedenen Zustände eines JWT-Tokens werden in der folgenden Tabelle beschrieben:

Verbindungsstatus	Beschreibung
Nicht gesetzt	JWT ist nicht gesetzt. Unify Phone ist daher für Ihren Mandanten nicht funktionsfähig.
Aktiv	JWT ist aktiv. Unify Phone ist für Ihren Mandanten funktionsfähig.
Ungültiges Token	Das JWT ist ungültig geworden. Unify Phone ist daher für Ihren Mandanten nicht funktionsfähig.

Sie können den JWT-Status jederzeit auf der Registerkarte **Mandant** der Unify Phone-Administrations-App einsehen.



Zugehörige Konzepte
Unify Phone JWT auf Seite 31

5.2 Bearbeitung des JWT

Wenn der JWT-Status `Ungültiges Token` ist, was bedeutet, dass das Token ungültig geworden oder abgelaufen ist, müssen Sie ein neues Token erstellen und dann das JWT für die Benutzerbereitstellung mit diesem neu konfigurieren.

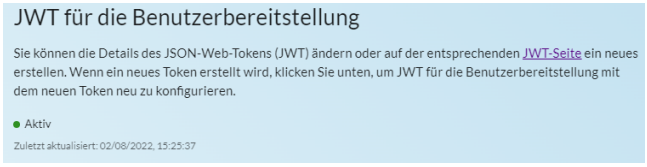
Schritt für Schritt

1) Öffnen Sie die Unify Phone Administrations-App.
2) Suchen Sie den Bereich **JWT für die Benutzerbereitstellung** . Sie sehen, dass der JWT-Status `Ungültiges Token` ist.
3) Klicken Sie auf **Bearbeiten**.
4) Suchen Sie die **Unify Phone Client-ID** und klicken Sie auf , um sie in Ihre Zwischenablage zu kopieren.
5) Klicken Sie auf den Link Portal zur JWT-Erstellung, um das Portal zu öffnen.
6) Gehen Sie zu **Anmeldedaten** und suchen Sie Ihr JWT.
   a) Klicken Sie auf , um das vorhandene Token zu löschen.
   b) Bestätigen Sie mit **Token löschen**.
7) Erstellen Sie ein neues Token.
   a) Geben Sie in das Feld **Bezeichnung** eine Bezeichnung für das JWT ein.
   b) Aktivieren Sie das Kontrollkästchen **Nur bestimmte Apps meiner Wahl** .

      Anmerkung: Dies ist eine Sicherheitsmaßnahme, um den Zugriff auf JWT auf bestimmte Apps zu beschränken.

   c) Es erscheint ein neues Eingabefeld für die Client-ID. Fügen Sie die **Unify Phone-Client-ID** aus der Zwischenablage in dieses Feld ein und klicken Sie auf **App hinzufügen**.
   d) Optional können Sie auch auf das Feld unter dem Bereich **Ablaufdatum (UTC)** klicken und ein Ablaufdatum für das JWT festlegen.
   e) Klicken Sie auf **JWT erstellen**.
   f) Klicken Sie auf , um das JWT in Ihre Zwischenablage zu kopieren.
8) Kehren Sie zur Unify Phone-Administration App zurück und fügen Sie das JWT in das Feld **JWT-Token** ein.
9) Klicken Sie auf **Fertig**.
10) Warten Sie auf das Abschließen der JWT-Validierung.

Nach erfolgreicher Validierung wird der JWT-Status auf `Aktiv` gesetzt.



Zugehörige Konzepte

Unify Phone JWT auf Seite 31

6 Telephony Connector

Der Telefonie-Connector ermöglicht es, Unify Phone-Benutzern eine öffentliche oder private Telefonnummer zuzuweisen, so dass sie von Unify Phone aus Anrufe tätigen und entgegennehmen können.

6.1 Anzeigen des Status des Telefonieanschlusses

Sie können den Status des für Ihren Mandanten konfigurierten Telefonie-Connectors einsehen.

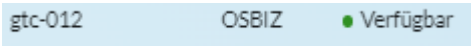
Schritt für Schritt

1) Gehen Sie zur Registerkarte **Telephony Connector**.

2) Unter dem Bereich **Telefoniestatus** können Sie Informationen zu den Telefonieanschlüssen anzeigen:

- Für `OpenScape Business` können Sie den Namen, den Typ und den Status der Leitung anzeigen.
- Für `OpenScape Voice / OpenScape 4000`können Sie den Leitungsnamen, den Typ, den Status, die IP-Adresse und den Port anzeigen.

Der Status einer Leitung sollte `Verfügbar` sein.



Sie können die Schaltfläche **Aktualisieren** verwenden, um die letzten Änderungen bei den Telefonieanschlüssen abzurufen.

6.2 Exportieren von Telefonieanschlussdaten

Sie können Informationen über Ihre Telefonie-Connectors (SIP-Trunks) in eine JSON-Datei exportieren.

Die Datei kann in den folgenden Fällen verwendet werden:

- Wenn Unify Phone als eigenständiger Telefonie-Client eines OpenScape Business-Kommunikationssystems verwendet wird, kann die Datei verwendet werden, um neue Benutzer auf Ihrem Mandanten anzulegen.
- Wenn Unify Phone so konfiguriert ist, dass es mit einem OpenScape Voice- oder OpenScape 4000-Kommunikationssystem zusammenarbeitet (entweder in Verbindung mit Unify Phone oder als eigenständiger Telefonie-Client), kann die Datei im Unify Flip User Migration Tool (in diesem Dokument als Unify Flip Tool bezeichnet) verwendet werden, um Ihrem Unternehmen die Migration von On-Premise- oder UCaaS-Ressourcen zu Unify Phone zu erleichtern.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Telephony Connector**.

2) Suchen Sie den Bereich **OpenScape Voice / OpenScape 4000** und blättern Sie an das Ende der Liste.
3) Klicken Sie auf **Exportieren**.

   Die Liste aller Unify Phone-Leitungen des Typs `OSBIZ`, `OSV` oder `OS4K` wird im JSON-Format heruntergeladen.

   Die JSON-Datei enthält die folgenden Felder:

   - `id`
   - `name`
   - `type`
   - `ip`
   - `port`
   - `protocol`

   Die Felder `ip`, `port` und `protocol` werden nur für OSV- und OS4K-Trunks verwendet.

6.3 API-Schlüssel

6.3.1 API-Schlüssel anzeigen

Sie können den API-Schlüssel Ihres Mandanten jederzeit anzeigen und kopieren.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Telephony Connector**.
2) Suchen Sie den Abschnitt **API-Schlüssel** .

   Der aktuelle API-Schlüssel wird angezeigt.
3) Klicken Sie auf **Auf Tastatur kopieren**, wenn Sie den Schlüssel in Ihr OpenScape-Kommunikationssystem eingeben möchten.

6.3.2 API-Schlüssel neu generieren

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Telephony Connector**.
2) Suchen Sie den Abschnitt API-Schlüssel.

   Der aktuelle API-Schlüssel wird angezeigt.
3) Klicken Sie auf **API-Schlüssel neu generieren**.
4) Wenn Sie dazu aufgefordert werden, die Generierung des neuen API-Schlüssels zu bestätigen, klicken Sie auf **Generieren**.

   Ein neuer Schlüssel wird erstellt. Der vorherige Schlüssel wird ungültig und bestehende Verbindungen von Ihrem/Ihren OpenScape-Kommunikationssytem(en) zu Unify Phone werden deaktiviert.

6.4 Zertifikate

Wenn Ihr Kommunikationssystem OpenScape Voice oder OpenScape 4000 ist, muss OpenScape SBC ein Zertifikat verwenden, das von Unify Phone als vertrauenswürdig eingestuft wird.

Standardmäßig vertraut Unify Phone nur Zertifikaten, die von bekannten Zertifizierungsstellen (CAs) signiert sind. Wenn es sich bei dem Zertifikat um ein selbstsigniertes Zertifikat oder ein Zertifikat von einer nicht vertrauenswürdigen Zertifizierungsstelle handelt, müssen Sie als Administrator des Mandanten dieses Zertifikat zu Unify Phone hinzufügen.

6.4.1 Hinzufügen eines Zertifikats

Sie können jederzeit ein benutzerdefiniertes, selbstsigniertes Zertifikat für TLS-Verbindungen in Ihrem Mandanten hinzufügen.

Standardzertifikate von OpenScape SBC können verwendet werden, ohne dass weitere Maßnahmen erforderlich sind.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Telephony Connector**.

2) Suchen Sie den Bereich **Zertifikate** .

a) Klicken Sie auf **Zertifikat hinzufügen** und wählen Sie das Zertifikat aus, das Sie von Ihrem Computer hinzufügen möchten.

oder

b) Ziehen Sie ein Zertifikat und legen Sie es im Bereich **Zertifikat hier ablegen** ab.

6.4.2 Anzeigen des Status eines Zertifikats

Sie können den Status der für Ihren Mandanten verfügbaren Zertifikate einsehen.

Der Status der Zertifikate wird in der folgenden Tabelle beschrieben:

Status des Zertifikats	Beschreibung
Gültig	Das Zertifikat ist gültig.
Ungültig	Das Zertifikat ist ungültig. Sie müssen ein neues Zertifikat in Ihrem Mandanten hinzufügen.

Status des Zertifikats	Beschreibung
Abgelaufen	Das Zertifikat ist abgelaufen. Sie müssen ein neues Zertifikat in Ihrem Mandanten hinzufügen.
Ablaufend	Das Zertifikat läuft in Kürze ab. Der Zertifikatsstatus ändert sich einen Monat vor dem Ablaufdatum in `Ablaufend` .
Überprüfung	Ihr Zertifikat wird gerade überprüft.
Fehler	Das Zertifikat konnte nicht zu Ihrem Mandanten hinzugefügt werden.

Sie können den Status Ihrer Zertifikate jederzeit in Ihrem Mandanten einsehen.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Telephony Connector**.
2) Unter dem Bereich **Zertifikate** können Sie den Status Ihrer Zertifikate in der Spalte **Status** einsehen.

6.4.3 Details zu einem Zertifikat anzeigen

Sie können die Details der für Ihren Mandanten verfügbaren Zertifikate einsehen.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Telephony Connector**.
2) Suchen Sie den Bereich **Zertifikate** .
3) Klicken Sie in der Spalte **Zertifikatname** auf das Zertifikat, zu dem Sie Details anzeigen möchten.

   Es wird ein Pop-up-Fenster angezeigt, in dem Sie die folgenden Zertifikatsdetails einsehen können: Betreff, Aussteller, Seriennummer, gültig von, gültig bis, öffentlicher Schlüssel, Signaturalgorithmus und Fingerabdruck.
4) Klicken Sie auf **Schließen**, um das Pop-up-Fenster mit den Zertifikatsdetails zu schließen.

6.4.4 Zertifikat löschen

Sie können ein Zertifikat aus Ihrem Mandanten löschen, wenn es nicht mehr benötigt wird.

Es wird empfohlen, vor dem Löschen eines gültigen oder ablaufenden Zertifikats zunächst ein neues Zertifikat hochzuladen, um eine Dienstunterbrechung zu vermeiden.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Telephony Connector**.
2) Suchen Sie den Bereich **Zertifikate** .
3) Suchen Sie das Zertifikat, das Sie löschen möchten, und klicken Sie auf **Löschen**.

   Es wird ein Pop-up-Fenster angezeigt, in dem Sie bestätigen müssen, dass Sie das Zertifikat löschen möchten.

Anmerkung: Das Löschen eines Zertifikats kann sich auf den Status der Leitungen auswirken.

---

7 Benutzer

Als Administrator können Sie Benutzer in Ihrem Mieter anzeigen, suchen und sortieren.

Sie können auch Benutzer und Benutzerdaten importieren, die mit dem Unify Flip User Migration Tool exportiert wurden.

7.1 Benutzer anzeigen

Sie können alle Benutzer in Ihrem Mandanten anzeigen.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Benutzer**.

Die Benutzer werden in einer Tabelle angezeigt, die nach ihrem Vornamen in aufsteigender Reihenfolge sortiert ist.

In der Tabelle werden die folgenden Informationen für jeden Benutzer angezeigt:

Feld	Beschreibung
Name	Vor- und Nachname des Benutzers
Rolle	Die dem Benutzer zugewiesene Rolle
Letzte Anmeldung	Die letzte Anmeldezeit des Benutzers
Trunk	Der Telefonieanschluss (SIP-Trunk), dem der Benutzer zugewiesen ist
Rufnummer	Die Telefonnummer des Benutzers

Die Gesamtzahl der Benutzer in Ihrem Mandanten wird ebenfalls angezeigt.

2) Wenn Sie möchten, dass die Liste der Benutzer anders sortiert wird:

- Klicken Sie auf die Kopfzeile **Telefonnummer**, um die Benutzer nach ihrer Telefonnummer zu sortieren (standardmäßig in aufsteigender Reihenfolge).
- Klicken Sie erneut auf die gleiche Spaltenüberschrift, um die Sortierreihenfolge zu ändern.

7.2 Benutzer importieren

Als Administrator können Sie Benutzer in Ihren Unify Phone-Mandanten importieren. Abhängig von Ihrem Kommunikationssystem können Sie eine CSV-Datei oder eine JSON-Datei für die Bereitstellung von Benutzern verwenden.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Benutzer**.

2) Benutzerdaten importieren.

a) Wenn Ihr Kommunikationssystem OpenScape Business ist:

- Wählen Sie die Leitung, die Sie bereitstellen möchten, aus dem Dropdown-Menü aus.
- Klicken Sie auf **CSV importieren**.
- Suchen Sie die CSV-Datei, wählen Sie sie aus und klicken Sie dann auf **Öffnen**.

b) Wenn Ihr Kommunikationssystem OpenScape Voice oder OpenScape 4000 ist:

- Klicken Sie auf **JSON importieren**.
- Suchen Sie die vom Unify Flip Tool exportierte JSON-Datei, wählen Sie sie aus und klicken Sie dann auf **Öffnen**.

3) Warten Sie, bis der Importvorgang abgeschlossen ist.

Nach erfolgreichem Abschluss wird die Anzahl der hinzugefügten Benutzer angezeigt. Die neu hinzugefügten Benutzer werden in der Benutzerliste angezeigt.

Wenn der Vorgang länger dauert als erwartet, wird die folgende Meldung angezeigt: `Die Bereitstellung von Benutzern dauert länger als erwartet und wird im Hintergrund fortgesetzt.`

Wenn der Importvorgang zwischendurch fehlschlägt, können Sie ihn jederzeit wiederholen. Der Importeur kann Duplikate erkennen und sie überspringen. Es werden nur Benutzer importiert, die bei einem früheren Versuch nicht erfolgreich importiert wurden.

7.3 Suche nach einem Benutzer

Sie können nach einem Benutzer anhand seines Namens oder seiner Telefonnummer suchen.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Teams**.

Es wird eine Liste mit allen Benutzern angezeigt.

2) Klicken Sie auf 🔍 oberhalb der Benutzerliste und geben Sie die gesuchten Informationen ein.

Die Suchergebnisse werden dynamisch angezeigt, während Sie tippen. Sie sind nach dem Vornamen des Benutzers in aufsteigender Reihenfolge sortiert.

Ihr Suchtext kann am Anfang, in der Mitte oder am Ende des Namens oder der Telefonnummer eines Nutzers gefunden werden.

3) So sortieren Sie die Suchergebnisse anders:

- Klicken Sie auf die Kopfzeile **Telefonnummer** , um die Benutzer nach ihrer Telefonnummer zu sortieren (standardmäßig in aufsteigender Reihenfolge).
- Klicken Sie erneut auf die gleiche Spaltenüberschrift, um die Sortierreihenfolge zu ändern.

4) Um Ihre Suchergebnisse zu löschen oder zur gesamten Benutzerliste zurückzukehren, löschen Sie den Suchbegriff.

7.4 Erneutes Versenden von Einladungen an Benutzer

Sie können einem OpenScape Business-Benutzer in Ihrem Mandanten, der sein Konto noch nicht aktiviert hat, erneut eine Einladung schicken.

Anmerkung: Diese Option ist nur für Unify Phone for OpenScape verfügbar.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Benutzer**.

Es wird eine Liste mit allen Benutzern angezeigt.

Für Benutzer, die ihr Konto noch nicht aktiviert haben, wird auf der Registerkarte **Einladungerneut senden** eine Schaltfläche **Erneut senden** angezeigt.

2) Suchen oder finden Sie den Benutzer, der Sie interessiert.

3) Klicken Sie auf **Erneut senden**, um eine neue Einladung zu versenden.

Wenn die Einladung erfolgreich gesendet wurde, wird die Meldung `Einladung gesendet` angezeigt.

7.5 Administratorfunktion zuweisen oder entfernen

Sie können einen Benutzer zum Administrator Ihres Mandanten machen und ihm Zugriff auf die Unify Phone-Administrationsanwendung geben. Sie können auch aktuellen Administratoren, die keinen Administratorzugriff mehr benötigen, die Administratorrechte entziehen.

Anmerkung: Diese Option ist nur für Unify Phone for OpenScape verfügbar.

Sie können die Administratorfunktion nicht aus Ihrem Konto entfernen.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Benutzer**.

Es wird eine Liste aller Benutzer angezeigt, deren Funktionen Sie in der Spalte **Funktion** sehen können.

2) So weisen Sie einem Benutzer die Administratorfunktion zu:

a) Suchen Sie den Benutzer in der Liste.

b) Klicken Sie auf **Benutzer** in der Spalte **Funktion** und wählen Sie **Administratorrechte hinzufügen**.

Die Benutzerfunktion ändert sich in **Administrator**.

Der Benutzer, dessen Funktion sich geändert hat, wird per E-Mail benachrichtigt und aufgefordert, sich bei der Unify Phone-Administrationsanwendung anzumelden und sein Passwort zu aktualisieren, um die Sicherheitsanforderungen für die Administratorfunktion zu erfüllen.

Wenn der Benutzer sein Unify Phone for OpenScape-Konto nicht vor der Funktionsänderung eingerichtet hat, wird anstelle einer E-Mail-Benachrichtigung eine E-Mail-Einladung an den Benutzer gesendet, damit er sein Administratorkonto einrichtet.

3) So entfernen Sie die Administratorfunktion eines Benutzers:

a) Suchen Sie den Benutzer in der Liste.

b) Klicken Sie in der Spalte **Funktion** auf **Administrator** und wählen Sie dann **Administratorrechte löschen**.

Die Benutzerfunktion ändert sich in **Benutzer**.

8 Authentifizierung

Unify Phone für Unify Video authentifiziert Benutzer anhand ihrer Unify Video-Kontoinformationen.

Unify Phone for OpenScape kann Benutzer auf eine der folgenden Arten authentifizieren:

- **Unify Phone-Anmeldedaten**: Das ist die Standard-Authentifizierungsmethode. Sie verwendet intern gespeicherte Anmeldedaten zur Authentifizierung von Benutzern.
- **Single Sign On-Authentifizierung**: Durch das einmalige Anmelden (SSO) können Benutzer sich mit ihren betrieblichen Anmeldedaten bei Unify Phone anmelden.

> **Anmerkung:** Derzeit wird nur die SAML 2.0 Single Sign On-Authentifizierungsmethode unterstützt.

Als Mandanten-Administrator können Sie mehrere Authentifizierungsmethoden für das einmalige Anmelden (Single Sign On, SSO) einrichten und eine davon als Standard-Authentifizierungsmethode unter Verwendung der Unify Phone-Anmeldedaten festlegen.

Um eine Authentifizierungsmethode zu verwenden, muss die Methode zunächst aktiviert und dann für Ihren Mandanten freigegeben werden. Durch die Aktivierung einer Authentifizierungsmethode wird diese zur Verwendung freigegeben. Durch die Aktivierung einer Authentifizierungsmethode wird diese in Betrieb genommen und die Benutzer können damit auf Unify Phone zugreifen.

Sie können eine SSO-Authentifizierungsmethode für Ihren Mandanten aktivieren oder deaktivieren. Die Standard-Authentifizierungsmethode kann nicht deaktiviert werden, da sie für Administratoren immer verfügbar sein muss, um sich bei der Administrationsanwendung anzumelden. Sie ist die Ausweichoption, wenn eine SSO-Methode fehlschlägt.

Sie können auch eine Authentifizierungsmethode aktivieren oder deaktivieren, aber es kann immer nur eine Authentifizierungsmethode für Ihren Mandanten aktiv sein.

Es wird dringend empfohlen, eine SSO-Methode zu testen, nachdem Sie die Methode hinzugefügt oder geändert haben und bevor Sie sie für alle Benutzer in Ihrem Mandanten aktivieren.

8.1 SAML 2.0 SSO-Authentifizierungsmethode einrichten

Sie können eine SAML 2.0 Single Sign On-Authentifizierungsmethode (SSO) für Ihr Unify Phone for OpenScape einrichten, indem Sie einen SAML 2.0 Identity Provider (IDP) konfigurieren.

Es gibt zwei Möglichkeiten, einen SAML 2.0 IDP zu konfigurieren:

- Sie können Metadaten für den IDP manuell eingeben.
- Sie können Metadaten für den IDP über eine vorkonfigurierte XML-Datei importieren.

8.1.1 Manuelle Eingabe von Metadaten für einen SAML 2.0 Identitätsanbieter

Wenn Sie eine SAML 2.0 SSO-Authentifizierungsmethode einrichten, können Sie Metadaten für den Identitätsanbieter manuell eingeben.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Authentifizierung**.
2) Suchen Sie den Bereich **Einmaliges Anmelden**.

   In diesem Bereich werden alle konfigurierten SSO-Authentifizierungsmethoden angezeigt.
3) Klicken Sie auf **SSO-Methode hinzufügen**.
4) Wählen Sie **Benutzerdefinierte SAML 2.0-Authentifizierung** und klicken Sie auf **Weiter**.

   Anmerkung: Derzeit wird nur die SAML 2.0 Single Sign On-Authentifizierungsmethode unterstützt.

   ---
5) Standardmäßig ist der Schieberegler **Aktiviert** auf AN (blau) eingestellt, was bedeutet, dass die Methode für die Aktivierung verfügbar ist. Wenn Sie diese Standardeinstellung ändern möchten, stellen Sie den Schieberegler auf AUS (grau).
6) Geben Sie die SAML-Einstellungen im Bereich **SAML-Konfiguration** manuell ein:
   a) Geben Sie in das Feld **Alias** eine eindeutige Kennung für Ihren Identitätsanbieter ein.
   b) Geben Sie in das Feld **Anzeigename** einen benutzerdefinierten Namen ein, der für Ihren Identitätsanbieter verwendet werden soll.
   c) Geben Sie in das Feld **Dienstanbieter Unternehmens-ID** die Unternehmens-ID ein, die Ihren SAML-Dienstanbieter eindeutig identifiziert.
   d) Geben Sie in das Feld **URL des Single Sign-On-Dienstes** die URL ein, die für das Senden von SAML-Authentifizierungsanforderungen verwendet werden soll.
   e) Wählen Sie aus dem Dropdown-Menü **Name IP Policy Format** das Format der Namenskennung aus.
   f) Wählen Sie aus dem Dropdown-Menü **Haupttyp** den Typ, der externe Benutzer identifiziert.
   g) Geben Sie in das Feld **Hauptattribut** einen benutzerdefinierten Namen ein, um externe Benutzer zu identifizieren.
   h) Stellen Sie den Schieberegler **HTTP-POST-Bindung Antwort** auf AN (blau) oder AUS (grau), um anzugeben, ob auf Anfragen mit HTTP-POST-Bindung geantwortet werden soll.
   i) Stellen Sie den Schieberegler **HTTP-POST-Bindung für AuthRequest** auf AN (blau) oder AUS (grau), um anzugeben, ob AuthRequest mit HTTP-POST-Bindung gesendet werden soll.
   j) Stellen Sie den Schieberegler **HTTP-POST-Bindung Abmeldung** auf AN (blau) oder AUS (grau), um anzugeben, ob

auf Anfragen mit HTTP-POST-Bindung geantwortet werden soll. Bei Deaktivierung wird die HTTP-REDIRECT-Bindung verwendet.

k) Stellen Sie den Schieberegler **AuthRequests sollen signiert werden** auf AN (blau) oder AUS (grau), um anzugeben, ob der Identitätsanbieter eine signierte AuthRequest erwartet.

l) Wählen Sie aus dem Dropdown-Menü **Signatur-Algorithmus** den zu verwendenden Signatur-Algorithmus aus.

Diese Option ist nur verfügbar, wenn der Schieberegler **AuthRequests sollen signiert werden** auf AN (blau) gestellt ist.

m) Wählen Sie aus dem Dropdown-Menü **Name des SAML-Einzelschlüssels** den Namen des zu verwendenden Signaturschlüssels aus.

Diese Option ist nur verfügbar, wenn der Schieberegler **AuthRequests sollen signiert werden** auf AN (blau) gestellt ist.

n) Stellen Sie den Schieberegler **Signatur validieren** auf AN (blau) oder AUS (grau), um die Signaturvalidierung für SAML-Antworten zu aktivieren/deaktivieren.

o) Geben Sie in das Feld **Zertifikat des Identitätsanbieters** das Zertifikat des Identitätsanbieters ein, das für die Signaturvalidierung von SAML-Antworten verwendet werden soll.

Diese Option ist nur verfügbar, wenn der Schieberegler **Signatur validieren** auf AN (blau) gestellt ist.

Die mit einem Sternchen (*) gekennzeichneten Einstellungen sind obligatorisch und können nicht weggelassen werden.

7) Klicken Sie auf **Hinzufügen**.

Wenn die Schaltfläche **Hinzufügen** nicht aktiviert ist, überprüfen Sie erneut, ob alle erforderlichen Felder ausgefüllt sind.

Die SAML 2.0-Authentifizierungsmethode wird zu Ihrem Mandanten hinzugefügt.

Nächste Schritte

- Die Methode muss erst freigegeben werden, bevor sie aktiviert werden kann.
- Es wird dringend empfohlen, die SAML 2.0 SSO-Authentifizierungsmethode zu testen, bevor Sie sie aktivieren.

8.1.2 Metadaten für einen SAML 2.0-Identitätsanbieter importieren

Wenn Sie eine SAML 2.0 SSO-Authentifizierungsmethode einrichten, können Sie Metadaten für den IDP über eine vorkonfigurierte XML-Datei importieren. Die Metadaten des Identitätsanbieters enthalten grundlegende Daten, die mit dem IDP verbunden sind.

Beim Importieren von Metadaten werden einige, aber nicht alle SAML 2.0 SSO-Konfigurationseinstellungen mit importierten Werten befüllt. Die restlichen Einstellungen müssen Sie noch manuell eingeben.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Authentifizierung**.
2) Suchen Sie den Bereich **Einmaliges Anmelden**.

   In diesem Bereich werden alle konfigurierten SSO-Authentifizierungsmethoden angezeigt.
3) Klicken Sie auf **SSO-Methode hinzufügen**.
4) Wählen Sie **Benutzerdefinierte SAML 2.0-Authentifizierung** und klicken Sie auf **Weiter**.

   Anmerkung:

   Derzeit wird nur die SAML 2.0 Single Sign On-Authentifizierungsmethode unterstützt.

   ---
5) Importieren Sie Metadaten für den IDP über eine vorkonfigurierte XML-Datei auf eine der folgenden Arten:

   - Klicken Sie auf **Wählen Sie**. Suchen Sie im Pop-up-Fenster nach der IDP-Datei, die Sie verwenden möchten, wählen Sie sie aus und klicken Sie auf **Öffnen**. Klicken Sie dann auf **Hochladen**.
   - Ziehen Sie die IDP-Datei in den Importbereich.

   Die folgenden SAML-Einstellungen können eingepflegt werden:

   - **URL des Single Sign-On-Dienstes**
   - **Name IP Policy Format**
   - **Haupttyp**
   - **HTTP-POST-Bindung Antwort**
   - **HTTP-POST-Bindung für AuthRequest**
   - **Zertifikat des Identitätsanbieters**

   Weitere Informationen zu den SAML 2.0 SSO-Einstellungen finden Sie unter Manuelle Eingabe von Metadaten für einen SAML 2.0 Identitätsanbieter auf Seite 44.
6) Standardmäßig ist der Schieberegler **Aktiviert** auf AN (blau) eingestellt, was bedeutet, dass die Methode für die Aktivierung verfügbar ist. Wenn Sie diese Standardeinstellung ändern möchten, stellen Sie den Schieberegler auf AUS (grau).
7) Geben Sie die SAML-Einstellungen, die nicht automatisch hinzugefügt wurden, manuell ein.

   Die mit einem Sternchen (*) gekennzeichneten Einstellungen sind obligatorisch und können nicht weggelassen werden.
8) Klicken Sie auf **Hinzufügen**.

   Wenn die Schaltfläche **Hinzufügen** nicht aktiviert ist, überprüfen Sie erneut, ob alle erforderlichen Felder ausgefüllt sind.

Die SAML 2.0-Authentifizierungsmethode wird zu Ihrem Mandanten hinzugefügt.

Nächste Schritte

- Die Methode muss erst freigegeben werden, bevor sie aktiviert werden kann.

- Es wird dringend empfohlen, die SAML 2.0 SSO-Authentifizierungsmethode zu testen, bevor Sie sie aktivieren.

8.2 Eine SAML 2.0-Authentifizierungsmethode bearbeiten

Sie können die Einstellungen einer SAML 2.0 Single Sign On-Authentifizierungsmethode (SSO) bearbeiten, die auf Ihrem Mandanten konfiguriert ist.

Sie können alle Einstellungen bis auf den Namen des Methodenalias bearbeiten.

Wenn die Methode, die Sie bearbeiten möchten, derzeit in Ihrem Mandanten aktiv ist, können Sie die Einstellung **Aktiviert** auch nicht aktualisieren.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Authentifizierung**.

2) Suchen Sie den Bereich **Einmaliges Anmelden**.

In diesem Bereich werden alle konfigurierten SSO-Authentifizierungsmethoden angezeigt.

3) Suchen Sie die SSO-Authentifizierungsmethode, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.

Sie werden auf die Seite **SSO-Methode bearbeiten** weitergeleitet.

4) Bearbeiten Sie die Einstellungen der SAML 2.0-Authentifizierungsmethode Ihren Anforderungen entsprechend.

5) Klicken Sie auf **Speichern**.

6) Klicken Sie auf **Zurück**, um die Seite **SSO-Methode bearbeiten** zu verlassen.

Nächste Schritte

Es wird dringend empfohlen, die aktualisierte SAML 2.0 SSO-Authentifizierungsmethode zu testen, bevor diese für alle Benutzer in Ihrem Mandanten aktiviert wird.

8.3 SAML 2.0-Attribute zuordnen

Nachdem Sie eine SAML 2.0 SSO-Authentifizierungsmethode eingerichtet haben, können Sie bestimmte Attribute, die von Ihrem Identitätsanbieter übergeben werden, wie z. B. E-Mail, benutzerdefinierten Attributen zuordnen, die in Unify Phone verwendet werden. Ihre Mappings haben Vorrang vor den Standardquellen.

Benutzerdefiniertes Attribut	Beschreibung
E-Mail	Das Mapping für das E-Mail-Attribut wird verwendet, um den Benutzer bei der Anmeldung zu validieren. Die Standardquelle für das Attribut E-Mail ist das Element NameID.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Authentifizierung**.
2) Suchen Sie den Bereich **Einmaliges Anmelden**.

   In diesem Bereich werden alle konfigurierten SSO-Authentifizierungsmethoden angezeigt.
3) Suchen Sie die SSO-Authentifizierungsmethode, mit der Sie arbeiten möchten, und klicken Sie auf **Bearbeiten**.

   Sie werden auf die Seite **SSO-Methode bearbeiten** weitergeleitet.
4) Suchen Sie den Abschnitt **Attribut-Mapping**.
5) Geben Sie in das Feld **E-Mail zugeordnet zu** den Namen des SAML-Feldes aus Ihrem IDP ein.
6) Klicken Sie auf **Attribut-Mapping speichern**.
7) Klicken Sie auf **Zurück**, um die Seite **SSO-Methode bearbeiten** zu verlassen.

8.4 Eine Authentifizierungsmethode aktivieren oder deaktivieren

Bevor Sie eine SSO-Authentifizierungsmethode für Ihren Mandanten aktivieren können, müssen Sie sie zunächst freigeben.

Sie können eine SSO-Authentifizierungsmethode auch deaktivieren, wenn sie derzeit in Ihrem Mandanten nicht aktiv ist und nicht mehr für die Aktivierung zur Verfügung stehen soll. Die Standard-Authentifizierungsmethode (Unify Phone-Anmeldedaten) kann nicht deaktiviert werden, da sie für Administratoren immer verfügbar sein muss, um sich bei der Administrationsanwendung anzumelden. Sie ist die Ausweichoption, wenn eine SSO-Methode fehlschlägt.

Sie können eine SSO-Methode aktivieren oder deaktivieren, wenn Sie sie zu Ihrem Mandanten hinzufügen oder danach.

Weitere Informationen zur Aktivierung einer SSO-Methode beim Hinzufügen zu Ihrem Mandanten finden Sie unter SAML 2.0 SSO-Authentifizierungsmethode einrichten auf Seite 43.

Um eine SSO-Methode zu aktivieren oder zu deaktivieren, nachdem sie zu Ihrem Mandanten hinzugefügt wurde, gehen Sie wie folgt vor:

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Authentifizierung**.

2) Suchen Sie die SSO-Authentifizierungsmethode, die Sie aktivieren oder deaktivieren möchten, und klicken Sie auf **Bearbeiten**. Sie werden auf die Seite **SSO-Methode bearbeiten** weitergeleitet.
3) Stellen Sie unter **SAML-Konfiguration** den Schieberegler **Aktiviert** auf:
   - AN (blau), um die SSO-Methode zu aktivieren

     oder
   - AUS (grau), um die SSO-Methode zu deaktivieren.
4) Klicken Sie auf **Speichern**.

8.5 Eine Authentifizierungsmethode testen

Nachdem Sie eine SSO-Authentifizierungsmethode hinzugefügt oder geändert haben und bevor Sie die Methode für alle Benutzer in Ihrem Mandanten aktivieren, können Sie sie testen. Dabei können Sie überprüfen, ob Sie Ihre SSO-Anmeldedaten verwenden können, um sich über den konfigurierten Identitätsanbieter bei Unify Phone anzumelden.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Authentifizierung**.
2) Suchen Sie die SSO-Authentifizierungsmethode, die Sie testen möchten.
3) Kopieren Sie die **Test-URL** und fügen Sie sie in ein Inkognito-Browserfenster ein.

   Sie sollten zur Anmeldeseite des Identitätsanbieters weitergeleitet werden.
4) Melden Sie sich mit Ihren SSO-Anmeldedaten an.

   Der Identitätsanbieter prüft Ihre Anmeldedaten und versucht, Sie zu authentifizieren.
5) Wenn die Authentifizierung erfolgreich ist, schließen Sie das Inkognito-Fenster und kehren Sie zur Unify Phone-Administrationsanwendung zurück, um weiterzuarbeiten.

   Sie können nun die SSO-Methode für Ihren Mandanten aktivieren.
6) Wenn die Authentifizierung nicht erfolgreich ist, wird eine Meldung angezeigt, die Sie über den Grund für das Scheitern der Authentifizierung informiert. Möglicherweise müssen Sie das Inkognito-Fenster schließen, zur Unify Phone-Administrationsanwendung zurückkehren, die Konfiguration der SSO-Methode erneut überprüfen und erneut einen Test durchführen.

8.6 Eine Authentifizierungsmethode aktivieren oder deaktivieren

Sie können eine Authentifizierungsmethode für Ihren Mandanten aktivieren oder deaktivieren. Wenn Sie eine

Authentifizierungsmethode aktivieren, können die Benutzer diese für den Zugriff auf Unify Phone verwenden. Die Deaktivierung einer Authentifizierungsmethode verhindert, dass Benutzer diese für den Zugriff auf Unify Phone verwenden können.

Administratoren können sich immer mit ihren Unify Phone-Anmeldedaten anmelden, auch wenn diese Methode derzeit nicht auf dem Mandanten aktiv ist.

Sie können nur freigegebene SSO-Methoden aktivieren. Weitere Informationen über die Aktivierung einer SSO-Methode finden Sie unter Eine Authentifizierungsmethode aktivieren oder deaktivieren auf Seite 48. Vor der Aktivierung einer SSO-Authentifizierungsmethode wird dringend empfohlen, ihre Konfiguration zu testen. Weitere Informationen über das Testen einer SSO-Methode finden Sie hier: Eine Authentifizierungsmethode testen auf Seite 49.

Sie können die Standard-Authentifizierungsmethode (Unify Phone-Anmeldedaten) jederzeit aktivieren, da sie immer freigegeben ist.

Für Ihren Mandanten kann jeweils nur eine Authentifizierungsmethode aktiv sein. Wenn Sie eine Authentifizierungsmethode aktivieren, werden alle anderen Methoden automatisch deaktiviert. Wenn Sie eine SSO-Authentifizierungsmethode deaktivieren, wird automatisch die Standard-Authentifizierungsmethode aktiviert.

Sie können eine Authentifizierungsmethode auch manuell aktivieren oder deaktivieren, wie unten beschrieben:

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Authentifizierung**.
   Der Status der Authentifizierungsmethode, die derzeit für Ihren Mandanten aktiv ist, lautet: `Aktiv`.
   Der Status jeder anderen Authentifizierungsmethode lautet: `Inaktiv`.
2) Suchen Sie die Authentifizierungsmethode, die Sie manuell aktivieren oder deaktivieren möchten, und klicken Sie auf **Aktivieren** oder **Deaktivieren**.

8.7 Eine Authentifizierungsmethode löschen

Sie können eine SSO-Authentifizierungsmethode löschen, die in Ihrem Mandanten nicht mehr benötigt wird. Die Standard-Authentifizierungsmethode (Unify Phone-Anmeldedaten) kann hingegen nicht gelöscht werden.

Voraussetzungen

Der Status der zu löschenden Authentifizierungsmethode lautet `Inaktiv`, d. h., die Methode wird derzeit nicht verwendet.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Authentifizierung**.

2) Suchen Sie die SSO-Authentifizierungsmethode, die Sie löschen möchten, und klicken Sie auf **Löschen**.

3) Klicken Sie zur Bestätigung auf **Ja**.

9 Integrationen

Integrationen ermöglichen es Ihnen, Unify Phone mit externen Anwendungen zu verbinden, sodass Ihre Benutzer nicht zwischen verschiedenen Anwendungen oder Plattformen wechseln müssen.

Derzeit unterstützt Unify Phone die Integration mit Microsoft Teams.

9.1 Unify Phone für Microsoft Teams

Unify Phone für Microsoft Teams ist eine Integration zwischen Unify Phone und Microsoft Teams. Mit dieser wird Microsoft Teams um Telefoniedienste erweitert, die von einem OpenScape-Kommunikationssystem (OpenScape Voice, OpenScape 4000 oder OpenScape Business) über den cloudbasierten Telefonie Konnektor Unify Phone bereitgestellt werden.

Anmerkung: Die Integration ist nur für Unify Phone for OpenScape verfügbar.

Um den Benutzern in Ihrem Mandanten die Verwendung von Unify Phone und Microsoft Teams zu ermöglichen, müssen Sie folgende Schritte durchführen:

- Das Unify Phone für Microsoft Teams-Plugin herunterladen.

  Weitere Informationen zum Herunterladen des Plugins finden Sie unter Unify Phone für Microsoft Teams herunterladen auf Seite 52.
- Das Plugin im Microsoft Teams Admin Center bereitstellen.

  Weitere Informationen zur Bereitstellung des Plugins finden Sie unter Unify Phone für Microsoft Teams in das Microsoft Teams Admin Center hochladen auf Seite 53.
- Admin-Zustimmung für die Anwesenheitssynchronisierung erteilen.

  Weitere Informationen zum Erteilen von Berechtigungen für die Anwesenheitssynchronisierung finden Sie unter Admin-Zustimmung für Unify Phone für Microsoft Teams erteilen auf Seite 54.

9.1.1 Unify Phone für Microsoft Teams herunterladen

Sie können die Unify Phone für Microsoft Teams-Integration von der Unify Phone-Administrations-App wie unten beschrieben herunterladen:

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Integrationen**.
2) Klicken Sie unter dem Abschnitt **Unify Phone für Microsoft Teams** auf **Herunterladen**.

Eine Zip-Datei mit den Integrationsdateien von Unify Phone für Microsoft Teams wird auf Ihren Computer heruntergeladen.

Nächste Schritte

Stellen Sie die Zip-Datei im Microsoft Teams Admin Center bereit, um die App für Ihre Benutzer über Microsoft Teams zugänglich zu machen.

9.1.2 Unify Phone für Microsoft Teams in das Microsoft Teams Admin Center hochladen

Sie können Unify Phone für Microsoft Teams für Benutzer in Ihrem Mandanten verfügbar machen, indem Sie die App in das Microsoft Teams Admin Center hochladen.

Voraussetzungen

- Sie haben Administrationsrechte für die Anwendung Microsoft Teams.
- Sie haben die Zip-Datei von Unify Phone für Microsoft Teams heruntergeladen.

Schritt für Schritt

1) Öffnen Sie Microsoft Teams Admin Center: https://admin.teams.microsoft.com/.
2) Klicken Sie im linken Navigationsbereich auf **Teams-Apps**.
3) Klicken Sie auf **Apps verwalten**.

   Die Ansicht Apps verwalten wird geöffnet, und Sie können eine Liste der Apps sehen, die für Benutzer in Ihrer Organisation verfügbar oder gesperrt sind.
4) Klicken Sie auf **+ Neue App hochladen** oben links in der Liste mit den Apps.
5) Klicken Sie im angezeigten Popup-Fenster auf **Hochladen**.
6) Suchen Sie die Zip-Datei, die Sie von der Unify Phone-Administrations-App heruntergeladen haben, und wählen Sie sie aus.

Nächste Schritte

Sobald die Unify Phone für Microsoft Teams-Integration hochgeladen ist, steht sie den Benutzern in Ihrem Mandanten zur Verfügung und kann zu ihrer Microsoft Teams-Anwendung hinzugefügt werden.

Für die Anwesenheitssynchronisierung zwischen Unify Phone und Microsoft Teams muss ein Microsoft-Mandantenadministrator die Admin-Zustimmung für Unify Phone für Microsoft Teams im entsprechenden Mandanten erteilen.

Wenn eine neue Version der App Unify Phone für Microsoft Teams in der Unify Phone-Administrations-App verfügbar wird, werden Sie auf praktische Weise benachrichtigt, damit Sie sie herunterladen und dann in das Microsoft Teams Admin Center hochladen können.

9.1.3 Admin-Zustimmung für Unify Phone für Microsoft Teams erteilen

Für die Anwesenheitssynchronisierung zwischen Unify Phone und Microsoft Teams muss ein Microsoft-Mandantenadministrator Ihrer Firma die Admin-Zustimmung für Unify Phone für Microsoft Teams im entsprechenden Mandanten erteilen.

Ein Microsoft-Mandantenadministrator muss die folgenden Schritte ausführen, um die Admin-Zustimmung für Unify Phone für Microsoft Teams zu erteilen:

Schritt für Schritt

1) Webbrowser öffnen und folgende Adresse (URL) eingeben:
https://login.microsoftonline.com/common/adminconsent?client_id=30836a97-580e-416b-bcbf-328520aedccf

2) Beim Microsoft-Konto anmelden.
Die Liste der Berechtigungen für die Anwesenheits- und Kontaktsynchronisierung zwischen Unify Phone und Microsoft Teams wird angezeigt.

Anmerkung:

Die folgenden Berechtigungen sind erforderlich:

- Contacts.Read
- Contacts.Read.Shared
- Directory.Read.All
- Presence.ReadWrite
- Presence.Read.All
- User.Read

---

3) Auf **Annehmen** klicken, um die Berechtigungen zu erteilen.

Nächste Schritte

Sobald die Berechtigungen erteilt sind, wird der Anwesenheitsstatus in Unify Phone für Microsoft Teams automatisch mit dem Anwesenheitsstatus in Unify Phone for OpenScape für alle Benutzer in Ihrem Mandanten synchronisiert. Darüber hinaus haben die Benutzer in Ihrem Mandanten Zugriff auf ihre Microsoft Exchange Online-Kontakte.

10 Einhaltung der DSGVO

In Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO) können Sie gespeicherte Anrufdaten für Benutzer in Ihrem Unify Phone-Mandanten exportieren.

Sie können auch festlegen, wie lange die Daten aufbewahrt werden sollen. Der Standardzeitraum für die Datenspeicherung beträgt 24 Monate.

10.1 Exportieren von Anrufdaten

Sie können die Anrufdaten für alle Benutzer Ihres Mandanten in den letzten 24 Monaten oder in einem ausgewählten Datumsbereich exportieren. Die Daten können anonymisiert werden.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Mandant**.
2) Legen Sie im Abschnitt **Datenexport für Anrufe** den Datumsbereich fest, für den die Daten in die Exportdatei aufgenommen werden sollen.
   - Geben Sie einen Datumsbereich ein.

     Die Datumswerte müssen im Format `MM/TT/JJJJ` vorliegen und durch einen Bindestrich (-) getrennt sein.

     Der Standard-Datumsbereich beträgt 24 Monate.
   - Klicken Sie auf , um einen Datumsbereich auszuwählen.

     Wählen Sie zuerst das Startdatum und dann das Enddatum für den Bereich.
3) Optional können Sie die Datenanonymisierung deaktivieren, indem Sie das Kontrollkästchen **Daten anonymisieren** anklicken.
4) Klicken Sie auf **Download**.

Eine Zip-Datei, die die CSV-Datei mit den Anrufdaten enthält, wird auf Ihren Computer heruntergeladen.

10.2 Aufbewahrungsfrist für Anrufdaten einstellen

Sie können die Datenaufbewahrungsfrist für die mit den Benutzern in Ihrem Mandanten verbundenen Anrufdaten festlegen. Die Datenaufbewahrungsfrist gibt an, wie lange die Daten aufbewahrt werden sollen.

Der Standardzeitraum für die Datenspeicherung beträgt 24 Monate. Sie können diese Standardeinstellung jederzeit ändern. Eine Änderung der Datenaufbewahrungsfrist hat zur Folge, dass Anrufdaten, die älter als die gewählte Frist sind, endgültig gelöscht werden, ohne dass die Möglichkeit besteht, sie wiederherzustellen.

Die Löschung wird in den nächsten 24 Stunden geplant und abgeschlossen, wenn Sie die nachstehenden Anweisungen befolgen:

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Mandant**.
2) Wählen Sie unter dem Abschnitt **Datenspeicherung** den Zeitraum für die Datenspeicherung aus.
3) Klicken Sie zur Bestätigung auf **OK**.

11 Mandantendetails

Als Administrator können Sie allgemeine Informationen über Ihren Unify Phone-Mandanten ansehen und bearbeiten, z. B. den Namen des Mandanten und den Hauptkontakt. Diese Informationen werden zunächst von einem Administrator bei der Erstellung eines Mandanten bereitgestellt.

Sie können auch eine Support-E-Mail-Adresse festlegen, an die sich die Benutzer Ihres Mandanten wenden können, wenn sie Unterstützung benötigen.

11.1 Mandantendetails ansehen

Sie können die Details zu Ihrem Mandanten auf den Registerkarten **Mandant** und **Details** der Administrationsanwendung einsehen.

Die Registerkarte **Mandant** zeigt die Mandanten-ID und den Mandantennamen, den Hauptkontakt sowie die Gesamtzahl der Benutzer in Ihrem Mandanten an.
Auf der Registerkarte **Details** werden der Name des Mandanten, der Hauptkontakt sowie eine Support-E-Mail-Adresse (falls vorhanden) angezeigt.

11.2 Mandantendetails bearbeiten

Sie können jederzeit allgemeine Informationen über Ihren Mandanten bearbeiten, z. B. den Namen des Mandanten und den Hauptkontakt.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Details**.
2) Klicken Sie auf **Bearbeiten**.
3) Bearbeiten Sie die Mandantendetails.
4) Klicken Sie auf **Speichern**.

11.3 Support-E-Mail-Adresse einrichten

Sie können eine E-Mail-Adresse einrichten, an die sich die Benutzer Ihres Mandanten wenden können, wenn sie Support benötigen. Wenn Benutzer oder Administratoren ein Problem melden, werden Support-Anfragen an diese E-Mail-Adresse weitergeleitet.

Schritt für Schritt

1) Gehen Sie zur Registerkarte **Details**.
2) Klicken Sie auf **Bearbeiten**.
3) Geben Sie die E-Mail-Adresse in das Feld **Support-E-Mail** ein.
4) Klicken Sie auf **Speichern**.

12 Überlegungen zu Firewall und Proxy

Unify Phone ist ein Cloud-basierter Software-as-a-Service. Das Netzwerk Ihres Unternehmens muss einige Konnektivitätsanforderungen erfüllen, damit Unify Phone ordnungsgemäß funktioniert. Diese Anforderungen werden im Folgenden näher erläutert.

Anmerkung: Reine IPv6-Netze werden derzeit nicht unterstützt.

12.1 Stateful Firewall-Konfiguration und NAT für OpenScape Business

Es wird davon ausgegangen, dass Ihr Unternehmen zum Schutz seiner privaten Netzwerke Stateful-Firewall/NAT-Geräte verwendet. Unify Phone-Verbindungen können solche Geräte mit Standardmethoden durchqueren, die dem Webbrowser-Datenverkehr ähneln. Insbesondere werden die Signalisierungs- und Medienverbindungen von Unify Phone stets in der abgehenden Richtung vom Unternehmensnetzwerk zur Cloud hergestellt. Die Firewall muss abgehende Verbindungen zu den in der folgenden Tabelle aufgeführten IP-Adressen zulassen.

Die Firewall/NAT blockiert alle Datenpakete in eingehender Richtung, es sei denn, sie gehören zu einer bereits aufgebauten Sitzung, die zuvor in abgehender Richtung aufgebaut wurde. Die Firewall/NAT muss den Stateful-Modus sowohl für TCP als auch für UDP unterstützen. Im Gegensatz zum typischen Browserdatenverkehr, der die TCP-Zielports 80 und 443 nutzt, verwenden WebRTC-Echtzeit- und Unify Phone-Sprachdatenpakete UDP, während SIP-Signalisierung TLS über TCP nutzt. Die meisten modernen Firewalls unterstützen zustandsabhängige UDP-Datenströme. Pinholes und NAT-Bindungen sind solange einzurichten und zu aktualisieren, bis ein Timer aufgrund fehlender Datenpakete abläuft.

In Tabelle 2: Egress-Firewall-Regeltabelle auf Seite 60 wurden die Quellports im Bereich 1024-65536 der Geräte innerhalb des Unternehmensnetzwerks weggelassen, da sie per Produktkonfiguration konfiguriert werden sollten. IP-Zieladresse und Port sind in diesem Abschnitt aufgeführt. Die Firewall muss nicht alle diese Ports öffnen, sondern lässt nur Rückdatenpakete auf der Verbindung zu, die von einem Gerät zu Unify Phone hergestellt wurde.

Für SIP-Signalisierung und Medien sollte die Stateful-Firewall/NAT den Datenverkehr also einfach auf Grundlage der von innen nach außen aufgebauten abgehenden Verbindung einschleusen. NAT-Bindungen bestehen nur für diese Verbindungen, sodass NAT keinen anderen Datenverkehr in eingehender Richtung zulässt.

Die Clients müssen sich über HTTPS mit Port 443 (HTTPS) der Unify Phone-URL verbinden können. Solange das Unternehmensnetzwerk den Zugang zu allen Zielen im öffentlichen Internet zulässt, müssten

Benutzer in der Lage sein, die Anmeldeseite von Unify Phone zu erreichen, genau wie das bei anderen sicheren Internetanwendungen (z. B. Bankanwendungen) üblich ist. Wenn sich der Benutzer anmeldet, stellt der Client die WebSockets-Verbindung her.

Nutzt das Netzwerk Ihres Unternehmens einen HTTP-Proxy, erkennt der Browser die Proxy-Einstellung automatisch. Nach der Anmeldung bei Unify Phone fordert der Browser die Einrichtung des WebSockets an, indem er zunächst die HTTPS-Verbindung einrichtet und sie dann auf WebSockets secure aufrüstet. Der Proxy muss diesen Fluss unterstützen.

Nutzt der Proxy Authentifizierung, gibt der Browser als Antwort auf die Abfrage die Anmeldedaten des Benutzers an.

Wenn der Proxy spezielle Whitelists verwendet, muss die Unify Phone-URL zur Whitelist hinzugefügt werden.

Im Gegensatz zum Signalisierungspfad ist das Passieren von Firewalls, NATs und Proxys beim Medienpfad viel schwieriger. Das liegt daran, dass die Medien ephemere UDP-Ports (>1024) nutzen, die Medien Peer-to-Peer sind und Firewalls/NAT normalerweise eingehende Verbindungen verhindern.

Zum Lösen dieser Probleme nutzt Unify Phone von der IETF empfohlene Standardverfahren wie STUN (Session Traversal Utilities for NAT), TURN (Traversal Using Relays around NAT) und ICE (Interactive Connectivity Establishment).

Da jedoch nicht alle Produkte die oben genannte Technologie unterstützen oder die Firewall Ihres Unternehmens **möglicherweise nicht zustandsorientiert ist**, müssen Sie möglicherweise die Konfiguration in der folgenden Tabelle anwenden.

Tabelle 1: Client Egress-Firewall-Regeltabelle

Beschreibun	Quell-IP	Quellport	IP-Zieladresse	Zielport	Anmerkung
TURN für Clients	Kunden-IP	Beliebig (1024-65.535)	34.159.228.55 turn.phoneapp.unify.com	3478 (TCP/ UDP)	Web-/Mobil-/ Desktop-Clients müssen sich mit dem TURN-Server verbinden, daher sollte die Firewall die Verbindung zum TURN-Server erlauben.
HTTPS für Clients	Kunden-IP	Beliebig (1024-65.535)	34.117.105.255 phoneapp.unify.com	443 (TCP)	Wenn das Netzwerk Ihrer Organisation einen Proxy-Server nutzt, stellt der Browser die Verbindung über den Proxy her.

Die folgende Tabelle enthält die erforderlichen Firewall-Regeln in der **Infrastruktur Ihres Unternehmens**, damit Unify Phone mit OpenScape Business zusammenarbeiten kann.

Tabelle 2: Egress-Firewall-Regeltabelle

Beschreibun	IP-Zieladresse	Zielport	Quell-IP	Quellport	Anmerkung
Unify Phone Client REST API (HTTPS)	34.117.105.255	443	OpenScape Business Öffentliche IP	Beliebig (1024-65.535)	Unify Phone-Client-Verbindung zur Bereitstellung von Unify Phone-Benutzern in OpenScape Business. Hostname: phoneapp.unify.com
Unify Phone Connector SIP über TLS	35.246.178.13	65.061	OpenScape Business Öffentliche IP	Beliebig (1024-65.535)	Erforderlich für SIP-Konnektivität über TLS mit Unify Phone. (Hergestellte Verbindung zulassen)
Medien-RTP	GCP IP-Quellbereich für Europa-west3	Medien-RTP (UDP-Ports) an GCP-Knoten (Ziel): Ports 10000-49999	OpenScape Business Öffentliche IP	OpenScape Business Medienanschlüsse	Medienpfad/RTP-Konfiguration zum Aufbau des Medienstroms.
TURN/STUN	34.159.228.55	3478 (TCP/UDP)	OpenScape Business Öffentliche IP	Beliebig (1024-65.535)	OpenScape Business muss eine Verbindung zum STUN/TURN-Server herstellen können.

Tabelle 3: Ingress-Firewall-Regeltabelle

Beschreibun	Quell-IP	Quellport	IP-Zieladresse	Zielport	Anmerkung
OpenScape Business (SIP/CSTA)	GCP IP-Quellbereich für Europa-west3	Beliebig (1024-65.535) (TCP)	OpenScape Business Öffentliche IP	OpenScape Business Ports	Zurückgegebene SIP-Client-Verbindung, die OpenScape Business mit Unify Phone hergestellt hat.

Beschreibun	Quell-IP	Quellport	IP-Zieladresse	Zielport	Anmerkung
OpenScape Business Medien-RTP	GCP IP-Quellbereich für Europa-west3	Medien-RTP (UDP-Ports) von GCP-Knoten: Ports 10000-49999	OpenScape Business Öffentliche IP	OpenScape Business Medienanschlüsse	Medienpfad/RTP-Konfiguration zum Aufbau des Medienstroms.

12.2 Stateful Firewall-Konfiguration und NAT für OpenScape Voice und OpenScape 4000

Es wird davon ausgegangen, dass Ihr Unternehmen zum Schutz seiner privaten Netzwerke Stateful-Firewall/NAT-Geräte verwendet. Unify Phone-Verbindungen können solche Geräte mit Standardmethoden durchqueren, die dem Webbrowser-Datenverkehr ähneln. Insbesondere werden die Signalisierungs- und Medienverbindungen von Unify Phone stets in der eingehenden Richtung von der Cloud zum Unternehmensnetzwerk hergestellt. Die Firewall muss eingehende Verbindungen von den in der folgenden Tabelle aufgeführten IP-Adressen zulassen.

Die Firewall/NAT muss den Stateful-Modus sowohl für TCP als auch für UDP unterstützen. Im Gegensatz zum typischen Browserdatenverkehr, der die TCP-Zielports 80 und 443 nutzt, verwenden WebRTC-Echtzeit- und Unify Phone-Sprachdatenpakete UDP, während SIP-Signalisierung TLS über TCP nutzt. Die meisten modernen Firewalls unterstützen zustandsabhängige UDP-Datenströme. Pinholes und NAT-Bindungen sind solange einzurichten und zu aktualisieren, bis ein Timer aufgrund fehlender Datenpakete abläuft.

Die Clients müssen sich über HTTPS mit Port 443 (HTTPS) der Unify Phone-URL verbinden können. Solange das Unternehmensnetzwerk den Zugang zu allen Zielen im öffentlichen Internet zulässt, müssten Benutzer in der Lage sein, die Anmeldeseite von Unify Phone zu erreichen, genau wie das bei anderen sicheren Internetanwendungen (z. B. Bankanwendungen) üblich ist. Wenn sich der Benutzer anmeldet, stellt der Client die WebSockets-Verbindung her.

Nutzt das Netzwerk Ihres Unternehmens einen HTTP-Proxy, erkennt der Browser die Proxy-Einstellung automatisch. Nach der Anmeldung bei Unify Phone fordert der Browser die Einrichtung des WebSockets an, indem er zunächst die HTTPS-Verbindung einrichtet und sie dann auf WebSockets secure aufrüstet. Der Proxy muss diesen Fluss unterstützen.

Nutzt der Proxy Authentifizierung, gibt der Browser als Antwort auf die Abfrage die Anmeldedaten des Benutzers an.

Wenn der Proxy spezielle Whitelists verwendet, muss die Unify Phone-URL zur Whitelist hinzugefügt werden.

Im Gegensatz zum Signalisierungspfad ist das Passieren von Firewalls, NATs und Proxys beim Medienpfad viel schwieriger. Das liegt daran, dass die Medien ephemere UDP-Ports (>1024) nutzen,

die Medien Peer-to-Peer sind und Firewalls/NAT normalerweise eingehende Verbindungen verhindern.

Zum Lösen dieser Probleme nutzt Unify Phone von der IETF empfohlene Standardverfahren wie STUN (Session Traversal Utilities for NAT), TURN (Traversal Using Relays around NAT) und ICE (Interactive Connectivity Establishment).

Da jedoch nicht alle Produkte die oben genannte Technologie unterstützen oder die Firewall Ihres Unternehmens möglicherweise nicht zustandsorientiert ist, müssen Sie möglicherweise die Konfiguration in der folgenden Tabelle anwenden.

Tabelle 4: Client Egress-Firewall-Regeltabelle

Beschreibun	Quell-IP	Quellport	IP-Zieladresse	Zielport	Anmerkung
STUN für Clients	Kunden-IP	Beliebig (1024-65.535)	34.159.228.55 turn.phoneapp.unify.com	3478 (TCP/UDP)	Clients müssen eine Verbindung zum STUN-Server herstellen können.
TURN für Clients	Kunden-IP	Beliebig (1024-65.535)	34.159.228.55 turn.phoneapp.unify.com	3478 (TCP/UDP) 443 (TCP)	Clients müssen eine Verbindung zum TURN-Server herstellen können.
HTTPS für Clients	Kunden-IP	Beliebig (1024-65.535)	34.117.105.255 phoneapp.unify.com	443 (TCP)	Wenn das Netzwerk Ihrer Organisation einen Proxy-Server nutzt, stellt der Browser die Verbindung über den Proxy her.

Die folgende Tabelle enthält die erforderlichen Firewall-Regeln in der **Infrastruktur Ihres Unternehmens**, damit Unify Phone mit OpenScape Voice oder OpenScape 4000 zusammenarbeiten kann.

Tabelle 5: Ingress-Firewall-Regeltabelle

Beschreibun	Quell-IP	Quellport	IP-Zieladresse	Zielport	Anmerkung
SBC (SIP/CSTA)	GCP IP-Quellbereich für Europa-west3	Beliebig (1024-65.535) Protokoll TCP	SBC WAN IP	SBC SIP WAN-Anschluss	Der Unify Phone SIP-Client öffnet eine Verbindung zum SBC der Organisation und stellt die SIP-über-TLS-Kommunikation mit Unify Phone her.

Beschreibun	Quell-IP	Quellport	IP-Zieladresse	Zielport	Anmerkung
SBC-Medien-RTP	Trickle ICE direkter Medienpfad von Clients zum SBC. Jede IP. Im Falle eines Ausfalls wird Unify Phone TURN verwendet: GCP IP-Quellbereich für Europa-west3 Medienpfad über UDP-Protokoll	Medien-RTP-UDP-Ports über DTLS Medienanschluss: Beliebig (1024-65.535)	SBC WAN IP	SBC-Medienanschluss UDP	Medienpfad/RTP-Konfiguration zum Aufbau des Medienstroms vom Client zum SBC. Optional. Nicht erforderlich, wenn die Firewall Ihrer Firma die SBC-Pinhole-Funktion unterstützt. Die SBC-Pinhole-Funktion sorgt dafür, dass die benötigten UDP-Ports auf Anfrage geöffnet werden.

Tabelle 6: Egress-Firewall-Regeltabelle

Beschreibun	Quell-IP	Quellport	IP-Zieladresse	Zielport	Anmerkung
TURN/STUN-Anfragen für Medienpfad	SBC WAN Medienanschlussbereich (UDP)	SBC-Medienanschlussbereich (UDP)	GCP IP-Quellbereich für Europa-west3	Beliebig (1024-65.535)	SBC muss eine Verbindung zum TURN-Server für den Medienpfad herstellen können. Optional. Wird nur benötigt, wenn die Firewall Ihrer Firma keine ausgehenden Verbindungen zulässt.
Unify Phone Client REST API (HTTPS)	CMP	Beliebig (1024-65.535)	34.117.105.255	443	Die Unify Phone-Client-Verbindung zur Bereitstellung von Unify Phone-Benutzern im OpenScape Voice / OpenScape 4000-Kommunikationssystem.

13 Service und Support

Dokumentation für Administratoren

Sie können über die Unify Phone-Administrationsanwendung auf die Dokumentation für Administratoren zugreifen. Weitere Informationen finden Sie im Abschnitt Zugang zur Dokumentation für Administratoren auf Seite 64.

Online-Support ist auf der Unify Video-Website verfügbar

https://unify.com/unifyvideo

Dazu gehören:

- Wissensdatenbank - FAQs
- Anmeldung beim Support-Portal

Siehe Abschnitt Probleme melden auf Seite 64, wenn ein Problem auftritt oder Sie uns Ihre Meinung mitteilen möchten.

13.1 Zugang zur Dokumentation für Administratoren

Sie können über die Unify Phone-Administrationsanwendung auf die Dokumentation für Administratoren zugreifen.

Die Dokumentation ist in den folgenden Formaten verfügbar: PDF und HTML.

Schritt für Schritt

1) Klicken Sie auf das Ellipsen-Symbol (...) oben rechts in der Anwendung.
2) Wählen Sie **Hilfe** aus dem Dropdown-Menü aus.
3) Klicken Sie auf **HTML öffnen** oder **PDF öffnen**, je nachdem, was Sie bevorzugen.

13.2 Anzeigen von Neuigkeiten

Sie können sich über die wichtigsten Funktionen und Änderungen in Unify Phone in der Unify Phone-App informieren.

Schritt für Schritt

1) Klicken Sie auf das Ellipsensymbol (...) oben rechts in der App.
2) Wählen Sie aus dem Dropdown-Menü die Option **Neuigkeiten** .
3) Wenn es unter „Neuigkeiten" mehr als einen Eintrag gibt, klicken Sie auf **Weiter** bzw. **Zurück** , um durch die Liste zu blättern.

13.3 Probleme melden

Wenn Sie ein Problem mit der Unify Phone-Administrationsanwendung haben, können Sie es direkt in der Anwendung melden.

Schritt für Schritt

1) Klicken Sie auf das Ellipsen-Symbol (...) oben rechts in der Anwendung.
2) Wählen Sie **Problem melden** aus dem Dropdown-Menü aus. Ihr Standard-E-Mail-Programm öffnet sich mit einer vorausgefüllten Nachricht.
3) Geben Sie eine kurze Beschreibung des Problems in der Betreffzeile und eine detaillierte Beschreibung des Problems im Text der E-Mail an.

   Bitte beschreiben Sie das Problem genau und fügen Sie alle Meldungen hinzu, die angezeigt werden und anderen bei der Lösung des Problems helfen können.
4) Hängen Sie die Protokolldateien von Ihrer Unify Phone-Administrationsanwendung an (deren Name mit "wcans" beginnt).

   Ihre Protokolldateien wurden im Standard-Download-Ordner Ihres Computers gespeichert.
5) Klicken Sie auf **Senden**.

Die E-Mail wird an die für Ihren Mandanten konfigurierte Support-E-Mail-Adresse gesendet.

13.4 Geschäftsbedingungen einsehen

Sie können die Allgemeinen Geschäftsbedingungen jederzeit in der Unify Phone-Administrations-App einsehen.

Schritt für Schritt

1) Klicken Sie auf das Ellipsen-Symbol (...) oben rechts in der Anwendung.
2) Wählen Sie **Info** aus dem Dropdown-Menü aus.

13.5 Informationen über den Unify Phone-Status abrufen

Sie können jederzeit von der Unify Phone-Administrations-App aus auf Informationen über den Unify Phone-Status zugreifen.

Prozedur

- Klicken Sie oben rechts in der App auf .
  Sie werden zu einem Artikel der Unify Office-Wissensdatenbank weitergeleitet, der den Status des Unify Phone Connectors, das Datum des nächsten geplanten Updates, die Versionshinweise und andere wichtige Informationen beschreibt.

14 Anhang

Dieser Abschnitt enthält zusätzliche Referenzinformationen.

14.1 Liste der vertrauenswürdigen Zertifizierungsstellen

Sie können diese Liste der vertrauenswürdigen Zertifizierungsstellen verwenden, um eine sichere Verbindung zwischen Ihrer lokalen Umgebung und Unify Phone herzustellen.

```
e-commerce monitoring GmbH, GLOBALTRUST 2020
GlobalSign nv-sa, GlobalSign Root E46
GlobalSign nv-sa, GlobalSign Root R46
GlobalSign nv-sa, Root CA, GlobalSign Root CA
QuoVadis Limited, QuoVadis Root CA 1 G3
QuoVadis Limited, QuoVadis Root CA 2
QuoVadis Limited, QuoVadis Root CA 2 G3
QuoVadis Limited, QuoVadis Root CA 3
QuoVadis Limited, QuoVadis Root CA 3 G3
SwissSign AG, SwissSign Gold CA - G2
SwissSign AG, SwissSign Silver CA - G2
WISeKey, OISTE Foundation Endorsed, OISTE WISeKey Global Root GB CA
WISeKey, OISTE Foundation Endorsed, OISTE WISeKey Global Root GC CA
China Financial Certification Authority, CFCA EV ROOT
GUANG DONG CERTIFICATE AUTHORITY CO.,LTD., GDCA TrustAUTH R5 ROOT
iTrusChina Co.,Ltd., vTrus ECC Root CA
iTrusChina Co.,Ltd., vTrus Root CA
UniTrust, UCA Extended Validation Root
UniTrust, UCA Global G2 Root
D-Trust GmbH, D-TRUST Root Class 3 CA 2 2009
D-Trust GmbH, D-TRUST Root Class 3 CA 2 EV 2009
T-Systems Enterprise Services GmbHi, T-Systems Trust Center, T-TeleSec GlobalRoot
 Class 2
T-Systems Enterprise Services GmbH, T-Systems Trust Center, T-TeleSec GlobalRoot
 Class 3
Autoridad de Certificacion Firmaprofesional CIF A62634068
Agencia Catalana de Certificacio (NIF Q-0801176-I) Serveis Publics de Certificacio
 Vegeu https://www.catcert.net/verarrel (c)03 Jerarquia Entitats de Certificacio
 Catalanes EC-ACC
FNMT-RCM, AC RAIZ FNMT-RCM
FNMT-RCM, Ceres, VATES-Q2826004J, AC RAIZ FNMT-RCM SERVIDORES SEGUROS
IZENPE S.A., Izenpe.com
Dhimyotis, Certigna
Dhimyotis, 0002 48146308100036, Certigna Root CA
Comodo CA Limited, AAA Certificate Services
COMODO CA Limited, COMODO Certification Authority
COMODO CA Limited, COMODO ECC Certification Authority
COMODO CA Limited, COMODO RSA Certification Authority
Hellenic Academic and Research Institutions Cert. Authority, Hellenic Academic and
 Research Institutions ECC RootCA 2015
Hellenic Academic and Research Institutions Cert. Authority, Hellenic Academic and
 Research Institutions RootCA 2015
Hellenic Academic and Research Institutions CA, HARICA TLS ECC Root CA 2021
```

```
Hellenic Academic and Research Institutions CA, HARICA TLS RSA Root CA 2021
Hellenic Academic and Research Institutions Cert. Authority, Hellenic Academic and
 Research Institutions RootCA 2011
Hongkong Post, Hongkong Post Root CA 1
Hongkong Post, Hongkong Post Root CA 3
Microsec Ltd.,  Microsec e-Szigno Root CA 2009
Microsec Ltd.,  VATHU-23584497, e-Szigno Root CA 2017
NetLock Kft.,  Tan\C3\BAs\C3\ADtv\C3\A1nykiad\C3\B3k (Certification Services),
 NetLock Arany (Class Gold) F\C5\91tan\C3\BAs\C3\ADtv\C3\A1ny
CyberTrust, Baltimore CyberTrust Root
emSign PKI, eMudhra Technologies Limited, emSign ECC Root CA - G3
emSign PKI, eMudhra Technologies Limited, emSign Root CA - G1
Actalis S.p.A./03358520967, Actalis Authentication Root CA
Japan Certification Services Inc., SecureSign RootCA11
SECOM Trust.net, Security Communication RootCA1
SECOM Trust Systems CO.,LTD., Security Communication RootCA2
NAVER BUSINESS PLATFORM Corp.,  NAVER Global Root Certification Authority
ACCVRAIZ1, PKIACCV, ACCV
Atos TrustedRoot 2011, Atos
Staat der Nederlanden, Staat der Nederlanden EV Root CA
Buypass AS-983163327, Buypass Class 2 Root CA
Buypass AS-983163327, Buypass Class 3 Root CA
TrustCor Systems S. de R.L.,  TrustCor Certificate Authority, TrustCor ECA-1
TrustCor Systems S. de R.L.,  TrustCor Certificate Authority, TrustCor RootCert
 CA-1
TrustCor Systems S. de R.L.,  TrustCor Certificate Authority, TrustCor RootCert
 CA-2
Asseco Data Systems S.A.,  Certum Certification Authority, Certum EC-384 CA
Asseco Data Systems S.A.,  Certum Certification Authority, Certum Trusted Root CA
Krajowa Izba Rozliczeniowa S.A.,  SZAFIR ROOT CA2
Unizeto Technologies S.A.,  Certum Certification Authority, Certum Trusted Network
 CA
Unizeto Technologies S.A.,  Certum Certification Authority, Certum Trusted Network
 CA 2
certSIGN, certSIGN ROOT CA
CERTSIGN SA, certSIGN ROOT CA G2
Disig a.s.,  CA Disig Root R2
Agence Nationale de Certification Electronique, TunTrust Root CA
E-Tu\C4\9Fra EBG Bili\C5\9Fim Teknolojileri ve Hizmetleri A.\C5\9E.,  E-Tugra
 Sertifikasyon Merkezi, E-Tugra Certification Authority
Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK, Kamu Sertifikasyon
 Merkezi - Kamu SM, TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1
Chunghwa Telecom Co. Ltd., HiPKI Root CA - G1
Chunghwa Telecom Co. Ltd., ePKI Root Certification Authority
TAIWAN-CA, Root CA, TWCA Global Root CA
TAIWAN-CA, Root CA, TWCA Root Certification Authority
AffirmTrust, AffirmTrust Commercial
AffirmTrust, AffirmTrust Networking
AffirmTrust, AffirmTrust Premium
AffirmTrust, AffirmTrust Premium ECC
Amazon, Amazon Root CA 1
Amazon, Amazon Root CA 2
Amazon, Amazon Root CA 3
Amazon, Amazon Root CA 4
DigiCert Inc, www.digicert.com, DigiCert Assured ID Root CA
DigiCert Inc, www.digicert.com, DigiCert Assured ID Root G2
```

```
DigiCert Inc, www.digicert.com, DigiCert Assured ID Root G3
DigiCert Inc, www.digicert.com, DigiCert Global Root CA
DigiCert Inc, www.digicert.com, DigiCert Global Root G2
DigiCert Inc, www.digicert.com, DigiCert Global Root G3
DigiCert Inc, www.digicert.com, DigiCert High Assurance EV Root CA
DigiCert Inc, www.digicert.com, DigiCert Trusted Root G4
Entrust Inc., Entrust Root Certification Authority - G2
Entrust Inc., Entrust Root Certification Authority - EC1
Entrust Inc., Entrust Root Certification Authority - G4
Entrust Inc., Entrust Root Certification Authority
Google Trust Services LLC, GTS Root R1
Google Trust Services LLC, GTS Root R2
Google Trust Services LLC, GTS Root R3
Google Trust Services LLC, GTS Root R4
IdenTrust, IdenTrust Commercial Root CA 1
IdenTrust, IdenTrust Public Sector Root CA 1
Internet Security Research Group, ISRG Root X1
Internet Security Research Group, ISRG Root X2
Microsoft Corporation, Microsoft ECC Root Certificate Authority 2017
Microsoft Corporation, Microsoft RSA Root Certificate Authority 2017
Network Solutions L.L.C.,  Network Solutions Certificate Authority
SecureTrust Corporation, Secure Global CA
SecureTrust Corporation, SecureTrust CA
Starfield Technologies Inc., Starfield Class 2 Certification Authority
The Go Daddy Group Inc., Go Daddy Class 2 Certification Authority
emSign PKI, eMudhra Inc, emSign ECC Root CA - C3
emSign PKI, eMudhra Inc, emSign Root CA - C1
www.xrampsecurity.com, XRamp Security Services Inc, XRamp Global Certification
 Authority
GoDaddy.com Inc., Go Daddy Root Certificate Authority - G2
Starfield Technologies Inc., Starfield Root Certificate Authority - G2
Starfield Technologies Inc., Starfield Services Root Certificate Authority - G2
Trustwave Holdings Inc., Trustwave Global Certification Authority
Trustwave Holdings Inc., Trustwave Global ECC P256 Certification Authority
Trustwave Holdings Inc., Trustwave Global ECC P384 Certification Authority
The USERTRUST Network, USERTrust ECC Certification Authority
The USERTRUST Network, USERTrust RSA Certification Authority
SSL Corporation, SSL.com EV Root Certification Authority ECC
SSL Corporation, SSL.com EV Root Certification Authority RSA R2
SSL Corporation, SSL.com Root Certification Authority ECC
SSL Corporation, SSL.com Root Certification Authority RSA
Entrust.net, Entrust.net Certification Authority (2048)
TeliaSonera, TeliaSonera Root CA v1
GlobalSign, GlobalSign ECC Root CA - R4
GlobalSign, GlobalSign ECC Root CA - R5
GlobalSign, GlobalSign Root CA - R3
GlobalSign, GlobalSign Root CA - R6
ANF Autoridad de Certificacion, ANF CA Raiz, ANF Secure Server Root CA
```

14.2 GCP IP-Quellbereich für Europa-west3

Im Folgenden sind die IP-Quellbereiche von Google Cloud Platform (GCP) für Europe-west3 aufgeführt. Die vollständige Liste der IP-

Bereiche, die Google den Benutzern im Internet zur Verfügung stellt, finden Sie hier:
https://www.gstatic.com/ipranges/cloud.json

```
ipv4: 34.0.224.0/24
ipv4: 34.0.226.0/24
ipv4: 34.40.0.0/17
ipv4: 34.89.128.0/17
ipv4: 34.104.112.0/23
ipv4: 34.107.0.0/17
ipv4: 34.118.244.0/22
ipv4: 34.124.48.0/23
ipv4: 34.141.0.0/17
ipv4: 34.157.48.0/20
ipv4: 34.157.176.0/20
ipv4: 34.159.0.0/16
ipv4: 35.198.64.0/18
ipv4: 35.198.128.0/18
ipv4: 35.207.64.0/18
ipv4: 35.207.128.0/18
ipv4: 35.220.18.0/23
ipv4: 35.234.64.0/18
ipv4: 35.235.32.0/20
ipv4: 35.242.18.0/23
ipv4: 35.242.192.0/18
ipv4: 35.246.128.0/17
ipv6: 2600:1900:40d0::/44
```

14.3 Admin-Zustimmung für Unify Phone für Microsoft Exchange Online erteilen

Damit sich Unify Phone-Benutzer mit dem Microsoft Exchange Online-Konto ihres Unternehmens verbinden und ihre privaten und globalen Exchange-Kontakte für Telefonate nutzen können, muss ein Microsoft-Mandantenadministrator aus Ihrem Unternehmen die Admin-Zustimmung für die Unify Phone-Anwendung in seinem Mandanten erteilen.

Schritt für Schritt

1) Webbrowser öffnen und folgende Adresse (URL) eingeben:
https://login.microsoftonline.com/common/adminconsent?client_id=f557fa47-b81d-4a3e-963c-4e3e57ee5d80

2) Beim Microsoft-Konto anmelden.

Die Liste der Berechtigungen für Microsoft Exchange Online-Kontakte wird angezeigt.

Anmerkung:

Die folgenden Berechtigungen sind erforderlich:

- Contacts.Read.Shared
- Contacts.Read
- Directory.Read.All
- User.Read

---

3) Auf **Annehmen** klicken, um die Berechtigungen zu erteilen.

Nächste Schritte

Sobald die Berechtigungen erteilt sind, können die Benutzer in Ihrem Mandanten ihre Exchange-Kontakte für Anrufe verwenden.

14.4 Konnektivitätsanforderungen für Microsoft Exchange lokal

Damit Unify Phone-Benutzer eine Verbindung zum lokalen Microsoft Exchange-Konto ihres Unternehmens herstellen und ihre Exchange-Kontakte für Telefonanrufe verwenden können, müssen die folgenden Anforderungen erfüllt sein:

- Der Exchange-Server muss über ein gültiges Zertifikat verfügen.
- Die EWS-URL muss von den Clients aus zugänglich sein.

  Dies kann erfolgen, wenn die Clients auf eine der folgenden Arten verbunden sind:

  – VPN-Verbindung: Clients (lokal, Web oder mobil) sind mit einem privaten Netz verbunden.
  – Internetverbindung: Die Clients sind mit dem Internet verbunden und der Exchange-Server befindet sich in einem lokalen Netzwerk.

    In diesem Fall wird der lokale Microsoft Exchange-Datenfluss über einen Edge-Transport-Server geleitet. Der Server muss in einer DMZ platziert werden, um die öffentliche URL dem Internet zugänglich zu machen.