Unify

Unify Phone-Administration

Dokumentation für Administratoren

A31003-F9910-M102-10-00A9

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.

Sachnummer: A31003-F9910-M102-10-00A9

atos.net

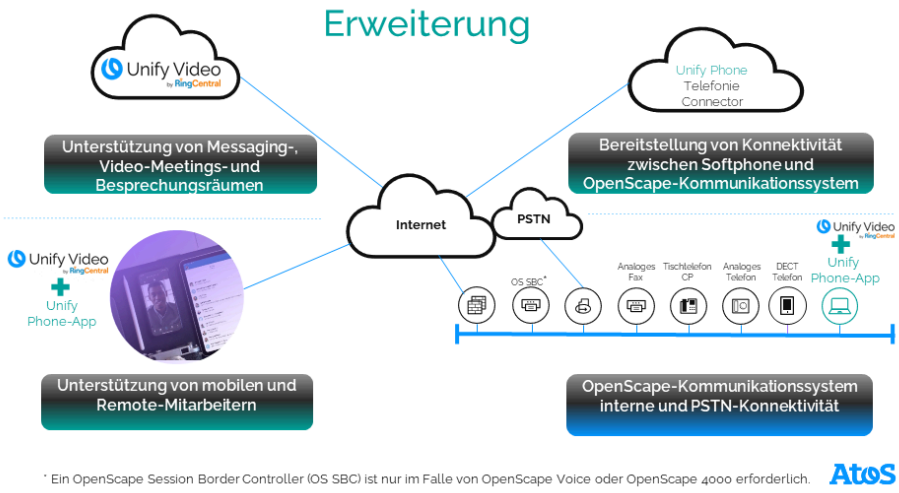
Inhalt

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 Telefonieanschluss für Unify Video. Es fungiert als Brücke zwischen einem OpenScape-Komunikationssystem und Unify Video und ermöglicht es den Benutzern, mit der Unify Phone-App Anrufe über ihre geschäftliche Telefonnummer zu tätigen und entgegenzunehmen.



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

> **Anmerkung:** Reine IPv6-Netze werden derzeit nicht unterstützt.

Voraussetzungen

Unify Phone 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

1.2 Übersicht über die Unify Phone-Verwaltung

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

- Unify Phone mit Unify Video zu verbinden
- den API-Schlüssel zu generieren, der für die Verbindung einer OpenScape-Telefonanlage mit Unify Phone erforderlich ist
- Status der Circuit Telephony Connectors zu überprüfen
- daten des Telefonieanschlusses exportieren
- hinzufügen oder Entfernen von benutzerdefinierten, selbstsignierten Zertifikaten für TLS-Verbindungen
- zertifikatsstatus und -details anzeigen
- benutzer in Ihrem Unify Phone-Tenant anzeigen, suchen und sortieren sowie neue Benutzer importieren.

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

2 Ersteinrichtung

Dieses Kapitel beschreibt die Ersteinrichtung von Unify Phone.

Die wichtigsten Schritte bei der Einrichtung sind die folgenden:

1) Registrieren für Unify Phone
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 Sie OpenScape Voice oder OpenScape 4000 als Kommunikationssystem nutzen, sollten Sie Ihren OpenScape SBC für die Verbindung mit Unify Phone konfigurieren.
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 des 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 zu Unify Phone- / Unify Video-Benutzern werden Änderungen an den Benutzerdetails im Unify Video-Administrationsportal nicht an Unify Phone bzw. 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

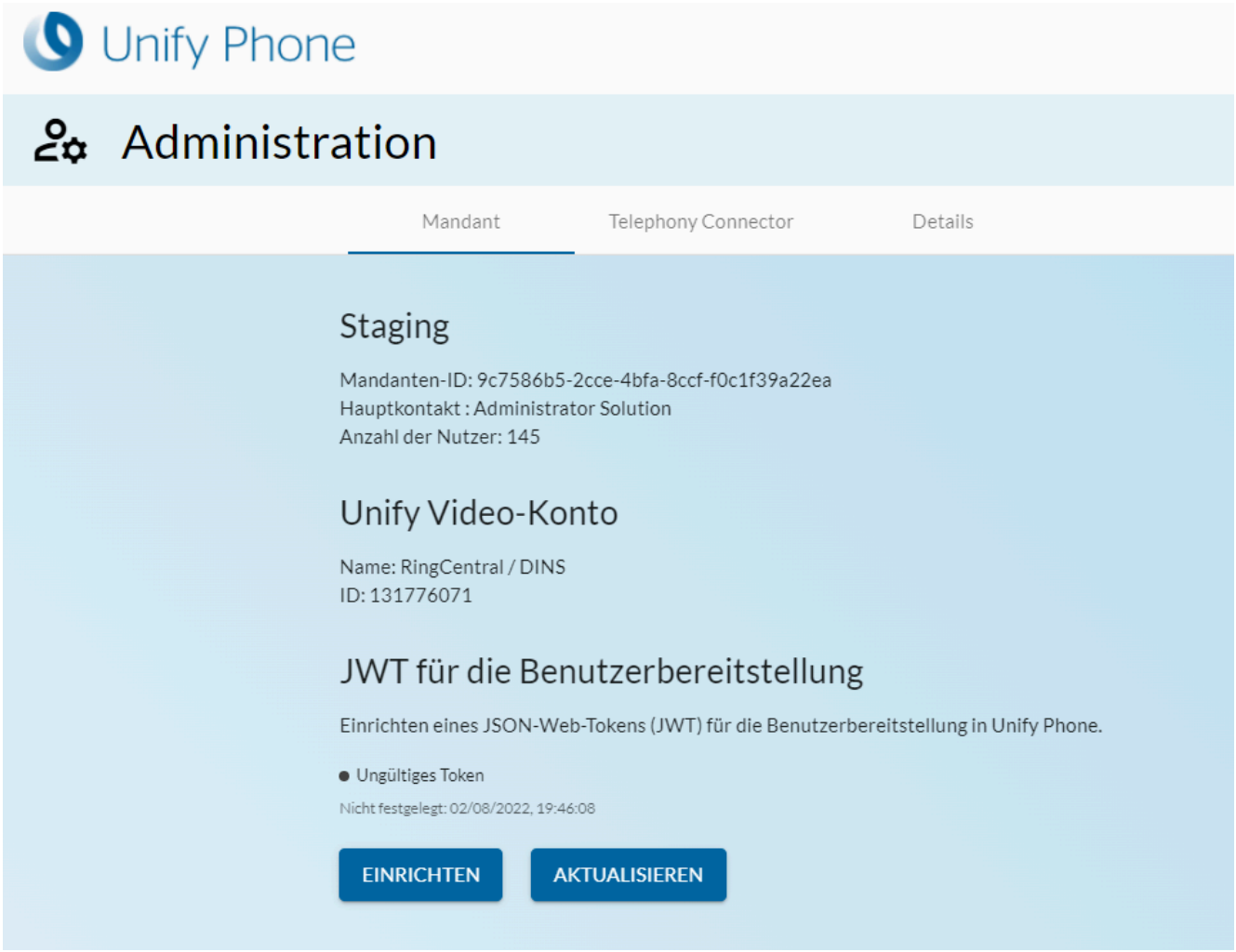
1) Öffnen Sie einen Webbrowser und geben Sie die Adresse (URL) der Unify Phone Administrations-App ein: https://phoneapp.unify.com/tenant/.
2) Wenn Sie aufgefordert werden, sich anzumelden, melden Sie sich mit Ihren Anmeldedaten für das Unify Video-Administrationskonto an.
3) Klicken Sie auf **Autorisieren**, um Unify Phone den erforderlichen Zugriff auf Unify Video zu ermöglichen.
4) 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**
5) Geben Sie einen **Mandantennamen** ein.
6) Bestätigen Sie Ihr Einverständnis mit den **Nutzungsbedingungen, den Datenschutzrichtlinien und den Richtlinien zur akzeptablen Nutzung**, indem Sie das Kontrollkästchen anklicken.
7) Bestätigen Sie, dass Sie mit der **Datenschutzvereinbarung** einverstanden sind, indem Sie das Kontrollkästchen anklicken.
8) Klicken Sie auf **Registrieren**.
   Es wird ein **API-Schlüssel** generiert, den Sie in Ihr OpenScape-Kommunikationssystem eingeben müssen.
9) Sie können auf **In die Zwischenablage kopieren** klicken, um den Schlüssel zu kopieren.
10) 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 **Telephony Connector** der Verwaltungs-App einsehen.

2.2 Einrichten eines JWTs für die Benutzerbereitstellung

Wenn ein Mandant zum ersten Mal erstellt wird, ist Unify Phone nicht mit Unify Video integriert. Sie müssen ein JSON-Web-Token (JWT) für die Benutzerbereitstellung in Unify Phone einrichten.



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 `Nicht gesetzt` 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 Portal zur JWT-Erstellung, 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) 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**.

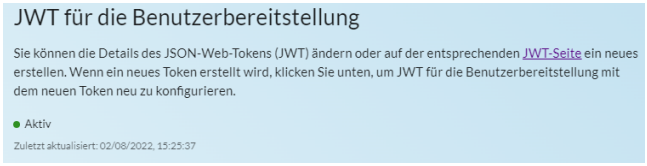
f) Klicken Sie auf , um das JWT in Ihre Zwischenablage zu kopieren.

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

8) Klicken Sie auf **Fertig**.

9) Warten Sie auf das Abschließen der JWT-Validierung.

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



2.3 Konfigurieren des Kommunikationssystems

Zum Konfigurieren Ihres OpenScape-Kommunikationssystems für die Verbindung mit Unify Phone ist Folgendes sicherzustellen:

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

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

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

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

Bei OpenScape Voice ist außerdem zwingend das Aktivieren der Option „Override Profile" (Profil überschreiben) in den Teilnehmereinstellungen des OND (One Number Service Device)

erforderlich. Die empfohlenen Rufdauer-Timer sind wie folgt eingestellt:

- Mobil (WLAN): 1 s
- Hauptgerät (ONS): 10 s
- Mobil (Mobilfunknetz): 15 s

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

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

  Detaillierte Informationen finden Sie im folgenden Dokument: *OpenScape Business V3, Administrator-Dokumentation* (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, Dokumentation für Administratoren*.
- OpenScape 4000 Assistant, im Falle von OpenScape 4000

  Detaillierte Informationen finden Sie in den folgenden Dokumenten:

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

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**).
3) 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, muss der OpenScape SBC-Administrator das RootCA-Zertifikat für den manuellen Import in Unify Phone mit dem Unify Phone-Supportteam teilen.

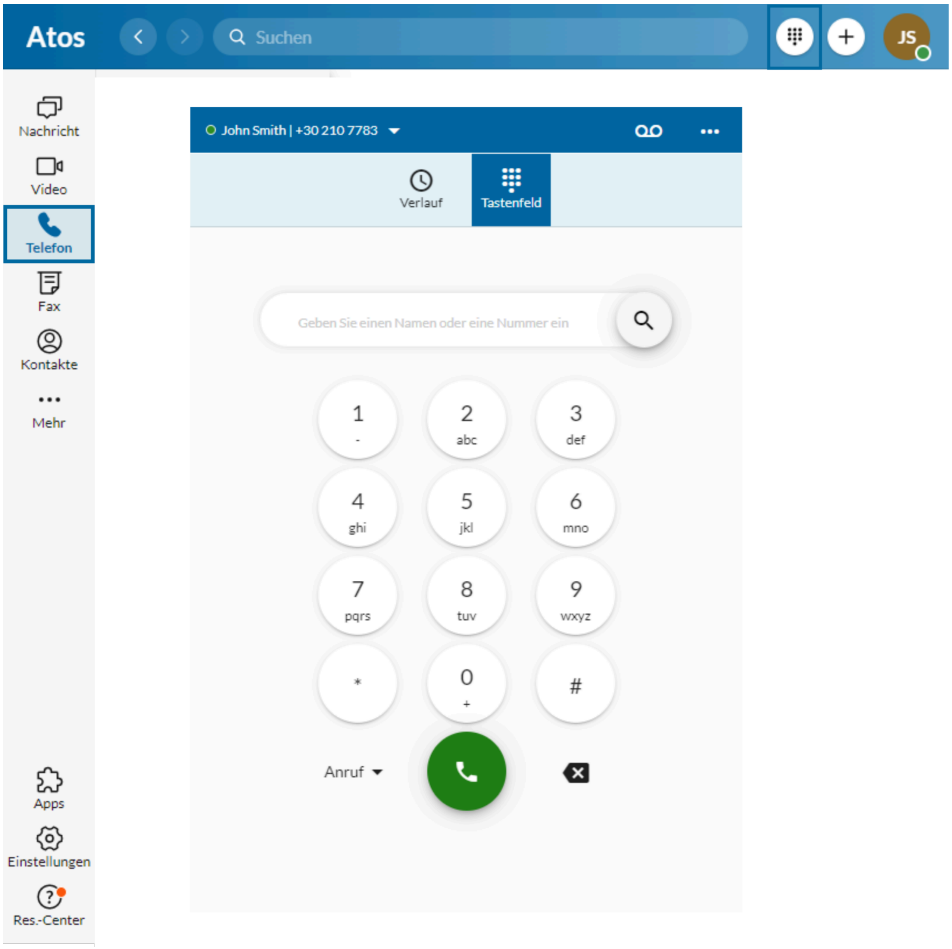
Es wird empfohlen, dass Ihr Unternehmen anstelle der Standardzertifikate eigene, selbstsignierte Zertifikate erstellt und verwendet.

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

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 An- und Abmeldung

3.1 Anmelden…

Sie können sich bei der Unify Phone-Verwaltungsanwendung mit den Anmeldedaten Ihres Unify Video-Verwaltungskontos anmelden.

Schritt für Schritt

1) Öffnen Sie einen Webbrowser und geben Sie die Adresse (URL) der Unify Phone-Mandantenverwaltung ein: https://phoneapp.unify.com/tenant/.
   Die App 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.

3.2 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.

4 Unify Phone JWT

Unify Phone ist über JWT für die Benutzerbereitstellung mit Unify Video integriert.

Um die Integration einzurichten, müssen Sie das JWT wie in Abschnitt Einrichten eines JWTs für die Benutzerbereitstellung auf Seite 7 beschrieben einrichten.

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

Anmerkung: Weitere Informationen über den JWT-Status finden Sie unter JWT-Status auf Seite 14.

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

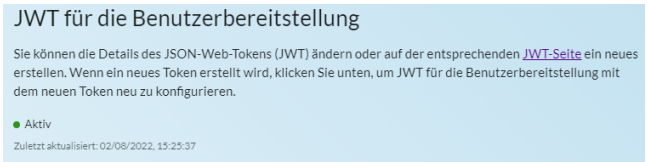
Anmerkung: Um ein neues Token zu erstellen, siehe Bearbeitung des JWT auf Seite 14.

4.1 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.



4.2 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

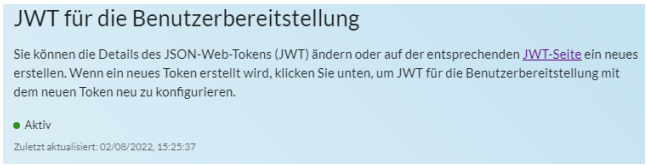
1) Öffnen Sie die Unify Phone Administrations-App.
2) Suchen Sie den Bereich **JWT für die Benutzerbereitstellung** . Sie sehen, dass der JWT-Status `Ungültiges Token` ist.
3) Klicken Sie auf **Bearbeiten**.
4) Suchen Sie die **Unify Phone Client-ID** und klicken Sie auf , um sie in Ihre Zwischenablage 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.



5 Telephony Connector

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

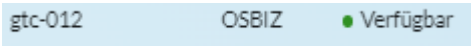
5.1 Anzeigen des Status des Telefonieanschlusses

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.

5.2 Exportieren von Telefonieanschlussdaten

Sie können Informationen über Ihre OpenScape Voice- oder OpenScape 4000-Telefonie-Connector(s) (SIP-Trunks) in eine JSON-Datei exportieren. Diese Datei kann mit dem 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 Video / 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 `OSV` oder `OS4K` wird im JSON-Format heruntergeladen.

Die JSON-Datei enthält die folgenden Felder:

- `ID`
- `Name`
- `Typ`
- `ip`
- `hafen`
- `Protokoll`

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

5.3 API-Schlüssel

5.3.1 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.

5.3.2 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.

5.4 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.

5.4.1 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.

5.4.2 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.

5.4.3 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.

5.4.4 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.

---

6 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.

6.1 Benutzer anzeigen

Sie können alle Benutzer in Ihrem Mandanten anzeigen.

Schritt für Schritt

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

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
Funktion	Die dem Benutzer zugewiesene Rolle
Amtsleitung	Der Telefonieanschluss (SIP-Trunk), dem der Benutzer zugewiesen ist
Telefonnummer	Die Telefonnummer des Benutzers

Die Gesamtzahl der Benutzer in Ihrem Mieter 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.

6.2 Benutzer importieren

Sie können Benutzer in Ihren Unify Phone-Tenant importieren, indem Sie eine JSON-Datei aus dem Unify Flip Tool exportieren.

Schritt für Schritt

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

2) Klicken Sie unter dem Bereich **Datenimport** auf **Importieren** .

3) Suchen Sie nach der vom Unify Flip Tool exportierten JSON-Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**.

4) Warten Sie auf das Abschließen der JWT-Validierung.

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 werden konnten.

6.3 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 Einhaltung der DSGVO

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

7.1 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.

8 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.

8.1 Stateful Firewall-Konfiguration und NAT für OpenScape Business

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

Die Firewall/NAT blockiert alle Pakete in eingehender Richtung, es sei denn, sie gehören zu einer bereits aufgebauten Sitzung, die zuvor in ausgehender Richtung aufgebaut wurde. Die Firewall/NAT sollte den Stateful-Modus sowohl für TCP als auch für UDP unterstützen. Im Gegensatz zum typischen Browserverkehr, der die Ziel-TCP-Ports 80 und 443 verwendet, verwenden WebRTC-Echtzeit- und Unify Phone-Sprachpakete UDP, während SIP-Signalisierung TLS über TCP verwendet. Die meisten modernen Firewalls unterstützen zustandsabhängige UDP-Datenströme. Pinholes und NAT-Bindungen müssen so lange eingerichtet und aufgefrischt werden, bis ein Timer aufgrund fehlender Pakete abläuft.

In Tabelle 2: Egress-Firewall-Regel-Tabelle auf Seite 26werden die Quellports im Bereich 1024-65536 der Geräte innerhalb des Unternehmensnetzwerks ausgelassen, da sie per Produktkonfiguration konfiguriert werden sollten. Die Ziel-IP und der Port sind in diesem Abschnitt aufgeführt. Die Firewall muss nicht alle diese Ports öffnen, sondern lässt nur Rückpakete 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 daher einfach auf der Grundlage der von innen nach außen aufgebauten ausgehenden Verbindung einschleusen. NAT-Bindungen bestehen nur für diese Verbindungen, so dass NAT keinen anderen Verkehr in der eingehenden Richtung zulässt.

Die Clients müssen in der Lage sein, sich über HTTPS mit Port 443 (HTTPS) der Unify Phone-URL zu verbinden. Solange das Unternehmensnetzwerk den Zugang zu allen Zielen im öffentlichen Internet zulässt, sollten die Benutzer in der Lage sein, die

Anmeldeseite von Unify Phone zu erreichen, genau wie jede andere sichere Internetanwendung (z. B. eine Bankanwendung). Wenn sich der Benutzer anmeldet, stellt der Client die WebSockets-Verbindung her.

Wenn das Netzwerk Ihres Unternehmens einen HTTP-Proxy verwendet, 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 hochrüstet. Der Proxy muss diesen Fluss unterstützen.

Verwendet der Proxy eine 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 es beim Medienpfad viel schwieriger, Firewalls, NATs und Proxies zu durchdringen. Das liegt daran, dass die Medien ephemere UDP-Ports (>1024) verwenden, die Medien Peer-to-Peer sind und Firewalls/NAT normalerweise eingehende Verbindungen verhindern.

Um diese Probleme zu lösen, verwendet Unify Phone Standardtechniken, die von der IETF empfohlen werden, 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-Regel-Tabelle

Beschreibu	Quelle IP	Quelle: Hafen	Ziel	Zielhafen	Kommentar
TURN für Kunden	Kunden-IP	Beliebig (1024-65.535)	34.159.228.55 turn.phoneapp.unify.com	3478 (TCP/ UDP)	Der SBC sollte in der Lage sein, eine Verbindung zum TURN-Server herzustellen.

Beschreibu	Quelle IP	Quelle: Hafen	Ziel	Zielhafen	Kommentar
HTTPS für Kunden	Kunden-IP	Beliebig (1024-65.535)	34.117.105.255 phoneapp.unify.com	443 (TCP)	Web-/Mobil-/Desktop-Clients müssen sich mit dem TURN-Server verbinden, daher sollte die Firewall die Verbindung zum TURN-Server erlauben. Wenn das Netzwerk Ihrer Organisation einen Proxy-Server verwendet, 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-Regel-Tabelle

Beschreibu	Ziel	Zielhafen	Quelle IP	Quelle: Hafen	Kommentar
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. Der Hostname ist phoneapp.unify.com
Unify Phone Connector SIP über TLS	35.246.178.13	65061	OpenScape Business Öffentliche IP	Beliebig (1024-65.535)	Erforderlich für SIP-Konnektivität über TLS mit Unify Phone. (Aufbau der Verbindung zulassen)
Medien RTP	GCP IP-Quellbereich für Europe-west3 (siehe: https://www.gstatic.com/ipranges/cloud.json)	Media RTP (UDP-Ports) an GCP-Knoten (Ziel): Ports 10000-49999	OpenScape Business Öffentliche IP	OpenScape Business Media-Anschlüsse	Medienpfad/RTP-Konfiguration zum Aufbau des Medienstroms.

Beschreibu	Ziel	Zielhafen	Quelle IP	Quelle: Hafen	Kommentar
DREHEN/ STUN	34.159.228.55	3478 (TCP/ UDP)	OpenScape Business Öffentliche IP	Beliebig (1024-65.535)	OpenScape Business sollte die Verbindung zum STUN/TURN-Server herstellen können.

Tabelle 3: Tabelle der Firewall-Regeln für den Zugang

Beschreibu	Quelle IP	Quelle: Hafen	Ziel	Zielhafen	Kommentar
OpenScape Business (SIP/ CSTA)	GCP IP-Quellbereich für die Region Europe-west3 (siehe: https://www.gstatic.com/ipranges/cloud.json)	Beliebig (1024-65.535) (TCP)	OpenScape Business Öffentliche IP	OpenScape Business Loadbalancer	Zurückgegebene SIP-Client-Verbindung, die OpenScape Business mit Unify Phone aufgebaut hat.
OpenScape Business Media RTP	GCP IP-Quellbereich für die Region Europe-west3 (siehe: https://www.gstatic.com/ipranges/cloud.json)	Media RTP (UDP-Ports) von GCP-Knoten: Ports 10000-49999	OpenScape Business Öffentliche IP	OpenScape Business Media-Anschlüsse	Medienpfad/RTP-Konfiguration zum Aufbau des Medienstroms.

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

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

Die Firewall/NAT sollte den Stateful-Modus sowohl für TCP als auch für UDP unterstützen. Im Gegensatz zum typischen Browserverkehr, der die Ziel-TCP-Ports 80 und 443 verwendet, verwenden WebRTC-Echtzeit- und Unify Phone-Sprachpakete UDP, während SIP-Signalisierung TLS über TCP verwendet. Die meisten modernen Firewalls unterstützen zustandsabhängige UDP-Datenströme. Pinholes und NAT-Bindungen müssen so lange eingerichtet und aufgefrischt werden, bis ein Timer aufgrund fehlender Pakete abläuft.

Die Clients müssen in der Lage sein, sich über HTTPS mit Port 443 (HTTPS) der Unify Phone-URL zu verbinden. Solange das Unternehmensnetzwerk den Zugang zu allen Zielen im öffentlichen Internet zulässt, sollten die Benutzer in der Lage sein, die Anmeldeseite von Unify Phone zu erreichen, genau wie jede andere sichere Internetanwendung (z. B. eine Bankanwendung). Wenn sich der Benutzer anmeldet, stellt der Client die WebSockets-Verbindung her.

Wenn das Netzwerk Ihres Unternehmens einen HTTP-Proxy verwendet, 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 hochrüstet. Der Proxy muss diesen Fluss unterstützen.

Verwendet der Proxy eine 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 es beim Medienpfad viel schwieriger, Firewalls, NATs und Proxies zu durchdringen. Das liegt daran, dass die Medien ephemere UDP-Ports (>1024) verwenden, die Medien Peer-to-Peer sind und Firewalls/NAT normalerweise eingehende Verbindungen verhindern.

Um diese Probleme zu lösen, verwendet Unify Phone Standardtechniken, die von der IETF empfohlen werden, 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-Regel-Tabelle

Beschreibu	Quelle IP	Quelle: Hafen	Ziel	Zielhafen	Kommentar
TURN für Kunden	Kunden-IP	Beliebig (1024-65.535)	34.159.228.55 turn.phoneapp.unify.com	3478 (TCP/ UDP)	Der SBC sollte in der Lage sein, eine Verbindung zum TURN-Server herzustellen.

Beschreibu	Quelle IP	Quelle: Hafen	Ziel	Zielhafen	Kommentar
HTTPS für Kunden	Kunden-IP	Beliebig (1024-65.535)	34.117.105.255 phoneapp.unify.com	443 (TCP)	Web-/Mobil-/Desktop-Clients müssen sich mit dem TURN-Server verbinden, daher sollte die Firewall die Verbindung zum TURN-Server erlauben. Wenn das Netzwerk Ihrer Organisation einen Proxy-Server verwendet, 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: Tabelle der Firewall-Regeln für den Zugang

Beschreibu	Quelle IP	Quelle: Hafen	Ziel	Zielhafen	Kommentar
SBC (SIP/CSTA)	GCP IP-Quellbereich für Europe-west3 (siehe: https://www.gstatic.com/ipranges/cloud.json)	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.

Beschreibu	Quelle IP	Quelle: Hafen	Ziel	Zielhafen	Kommentar
SBC Medien RTP	Trickle ICE direkter Medienpfad vom Kunden zum SBC. Jede IP. Im Falle eines Ausfalls wird das Unify Phone TURN verwendet: GCP IP-Quellbereich für Europe-west3 (siehe: https://www.gstatic.com/ipranges/cloud.json) Medienweg über UDP-Protokoll	Medien-RTP-UDP-Ports über DTLS Medienanschluss: Beliebig (1024-65.535)	SBC WAN IP	SBC-Medienanschluss UDP	Media Path/RTP-Konfiguration zum Aufbau des Medienstroms vom Client zum SBC.

Tabelle 6: Egress-Firewall-Regel-Tabelle

Beschreibu	Quelle IP	Quelle: Hafen	Ziel	Zielhafen	Kommentar
TURN	SBC WAN	Beliebig (1024-65.535)	(34.159.228.55) turn.phoneapp.unify.com	3478 (TCP/UDP)	Der SBC sollte in der Lage sein, eine Verbindung zum TURN-Server herzustellen.
Unify Phone Client REST API (HTTPS)	CMP	Beliebig (1024-65.535)	34.117.105.255	443	Die Unify Phone Client-Verbindung zur Bereitstellung der Unify Phone-Benutzer im OpenScape Voice/ OpenScape 4000 Kommunikationssystem.

9 Service und Support

Dokumentation für Administratoren

Sie können über die Unify Phone-Administrationsanwendung auf die Dokumentation für Administratoren zugreifen. Weitere Details finden Sie im Abschnitt Zugang zur Dokumentation für Administratoren auf Seite 31.

Online-Support ist auf der Unify Video-Website verfügbar

https://unify.com/unifyvideo

Dazu gehören:

- Wissensdatenbank - FAQs
- Anmeldung beim Support-Portal

9.1 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 Ellipsensymbol (...) oben rechts in der App.
2) Wählen Sie aus dem Dropdown-Menü **Hilfe** aus.
3) Klicken Sie auf **HTML öffnen** oder **PDF öffnen**, je nachdem, was Sie bevorzugen.

9.2 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.

9.3 Geschäftsbedingungen einsehen

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

Schritt für Schritt

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

10 Anhang

Dieser Abschnitt enthält zusätzliche Referenzinformationen.

10.1 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
```

10.2 Admin-Zustimmung für die Unify Phone-App erteilen

Damit Unify Phone-Benutzer eine Verbindung zum Microsoft Exchange Online-Konto ihres Unternehmens herstellen und ihre privaten Exchange-Kontakte für Anrufe verwenden können, muss ein Microsoft

Tenant-Administrator Ihres Unternehmens die Admin-Zustimmung für die Unify Phone-App in ihrem Mandanten erteilen.

Ein Microsoft Tenant-Administrator muss das Microsoft Azure-Portal öffnen und die folgenden Schritte ausführen, um der Unify Phone-App die Admin-Zustimmung zu erteilen:

Schritt für Schritt

1) Navigieren Sie auf der Registerkarte **Home** zu **Azure Active Directory > Unternehmensanwendungen**.
2) Geben Sie **Unify Phone** in das Suchfeld ein.

> **Anmerkung:** Die **Homepage-URL** von Unify Phone (https://phoneapp.unify.com/) wird in den Suchergebnissen angezeigt.

3) Klicken Sie auf **Unify Phone**.
4) Klicken Sie auf der Registerkarte **Sicherheit** auf **Berechtigungen**.
5) Klicken Sie auf **Admin-Zustimmung für "Unternehmen" erteilen**.

Unter **Admin-Zustimmung** können Sie die Liste der für die Unify Phone-App erteilten Berechtigungen sehen:

- Kontakte.Lesen
- Kontakte.Lesen.Freigegeben
- Benutzer.Lesen