A MITEL
PRODUCT
GUIDE

Unify OpenScape Contact Center V11 R1

Web Manager V11 R1

Web Manager Administrationshandbuch

Administrationshandbuch
09/2024

A31003-S22B1-M100-02-00A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Inhalt

1 Informationen zu diesem Handbuch

Dieses Handbuch bietet eine Übersicht über die OpenScape Contact Center Manager-Anwendung und führt den Benutzer durch die verschiedenen regelmäßig auszuführenden Administrationsaufgaben.

1.1 An wen richtet sich dieses Handbuch?

Dieses Handbuch richtet sich an Contact-Center-Administratoren, die für die Konfiguration und Wartung zuständig sind, und an Supervisors und Manager, die die OpenScape Contact Center-Produktivitätstools verwenden.

1.2 Formatierungskonventionen

In diesem Handbuch werden folgende Formatierungskonventionen verwendet:

Fettdruck
In dieser Formatierung erscheinen OpenScape Contact Center Komponenten, Fenster- und Dialogfeldtitel sowie Elementnamen.

Kursiv
In dieser Formatierung erscheinen Verweise auf verwandte Dokumentationen.

Nichtproportionale Schrift
In dieser Schrift erscheint Text, den Sie eingeben müssen oder der vom Computer in einer Meldung angezeigt wird.

HINWEIS: Hinweise heben Informationen hervor, die nützlich, aber nicht wesentlich sind, zum Beispiel Tipps oder alternative Methoden zum Durchführen einer Aufgabe.

WICHTIG: Wichtige Hinweise machen auf Aktionen aufmerksam, die den Betrieb der Anwendung beeinträchtigen oder zum Verlust von Daten führen können.

1.3 Feedback zur Dokumentation

Wenn Sie Probleme im Zusammenhang mit diesem Dokument mitteilen möchten, wenden Sie sich bitte an das Kundendienst-Center.

Bitte halten Sie bei Ihrem Anruf folgende Angaben bereit. Dadurch können wir das Dokument, mit dem Sie Schwierigkeiten haben, schneller identifizieren.

- **Titel:** Web Manager Administrationshandbuch
- **Sachnummer:** A31003-S22B1-M100-02-00A9

2 Web Manager

2.1 Erste Schritte

Web Manager ist eine Anwendung, die die Konfiguration von Funktionen in OpenScape Contact Center über einen Webbrowser ermöglicht.

2.2 Zugangsdetails

Web Manager ist eine browserbasierte Anwendung, die mit dem Paket OpenScape Contact Center-Anwendungsserver installiert wird.

Für den Zugang zu Web Manager benötigen Sie das Benutzeranmeldeprofil Haupt-Administrator.

Mit dem Web Manager können Sie Folgendes konfigurieren:

- Einmaliges Anmelden mit dem SAML2-Protokoll für Agenten-Portal-Web
- Einmaliges Anmelden mit Circuit für Agenten-Portal-Web
- Virtuelle Agenten zur Aktivierung der Chatbot-Funktionalität
- REST SDK
- Telefonie

Um auf den Web Manager zuzugreifen, öffnen Sie einen Browser und geben Sie die folgende URL ein:
https://<OSCC_ApplicationServer_hostname_or_ip>/webmanager

3 Einmaliges Anmelden mit SAML2-Protokoll

Die Security Assertion Markup Language (kurz SAML) ist ein XML-basiertes Open-Standard-Datenformat zum Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen einem Identitätsanbieter und einem Dienstanbieter.

Da die meisten Organisationen bereits die Identität der in ihrer Active-Directory-Domäne oder in ihrem Intranet angemeldeten Benutzer kennen, können diese Informationen zum einmaligen Anmelden (Single Sign On, SSO) von Benutzern bei OpenScape Contact Center-Anwendungen verwendet werden. OpenScape Contact Center unterstützt SAML in der Version 2.0 (SAML2).

NOTE: SSO über SAML2 wird nur für die webbasierte Anwendung Agenten-Portal-Web unterstützt. Diese SSO-Konfigurationen gelten nicht für andere Anwendungen wie Agenten-Portal-Java, Client Desktop oder Manager Desktop, weil sie die in Manager Desktop konfigurierten Anmeldemethoden verwenden. Web Manager unterstützt nur die OSCC-Anmeldemethode.

Die SAML-Spezifikation definiert die folgenden Rollen:

- **Benutzer**: Diese Rolle ist dem Webbrowser zugewiesen, der die URL zum Ausführen der Anwendung auf dem Anwendungsserver verwendet.
- **Dienstanbieter (SP)**: Diese Rolle ist dem Anwendungsserver zugewiesen, der die Anwendung ausführt.

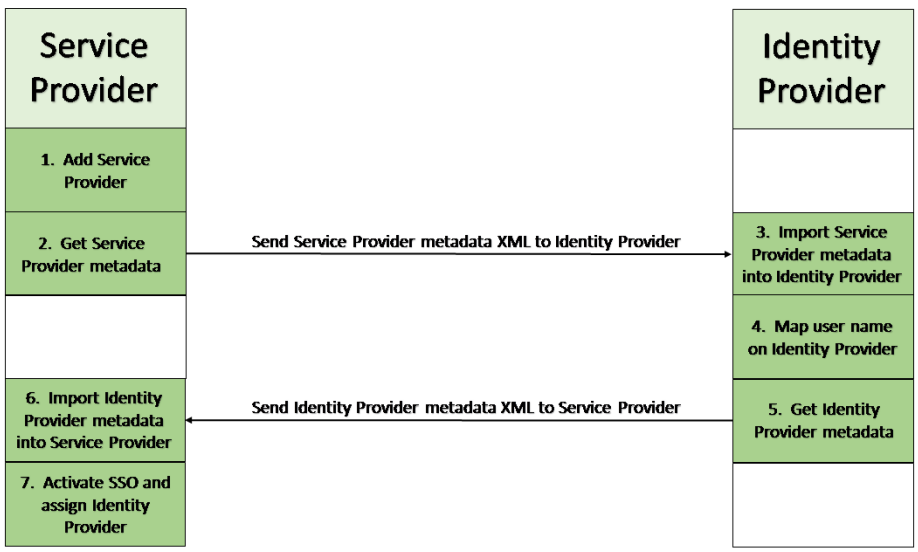
- **Identitätsanbieter (IdP)**: Diese Rolle ist einer Systementität (Authentifizierungsbefugnis) zugewiesen, die die Benutzerauthentifizierung besorgt.

NOTE: Es können viele verschiedene IdPs wie zum Beispiel ADFS oder Gluu verwendet werden. Hier verwenden wir Active Directory Federation Services (ADFS) als Beispiel, um zu beschreiben, welche Informationen erforderlich sind, um SSO in der OpenScape Contact Center-Lösung zu konfigurieren. Wenn andere IdPs verwendet werden, müssen aus diesen IdPs die gleichen Informationen extrahiert werden.

NOTE: ADFS ist eine von Microsoft angebotene SSO-Lösung. Als Komponente der Windows Server-Betriebssysteme bietet es Benutzern authentifizierten Zugriff auf Anwendungen durch Active Directory (AD).

NOTE: Der IdP-Dienst ist eine Anwendung von Drittanbietern, die nicht von Unify geliefert oder unterstützt wird. Deswegen können sich die in diesem Dokument beschriebenen Beispiele für AFDS ändern.

SSO wird in der Web Manager-Anwendung durch die Konfiguration des Dienstanbieters auf der OSCC-Seite und durch die Konfiguration des Identitätsanbieters auf der anderen Seite eingerichtet. Die folgende Abbildung zeigt die Reihenfolge der Konfigurationsschritte:



1. Dienstanbieter hinzufügen

    1. Melden Sie sich bei der Web Manager-Anwendung als Master Administrator-Benutzer mit dem entsprechenden Kennwort an. Wählen Sie zuerst **Anmeldekonfiguration** und dann **Dienstanbieter**.
    2. Klicken Sie auf **Dienstanbieter**:

        - **Host-URL**: Die URL des Agenten-Portal-Web-Service. Zum Beispiel:

        `https://<ApplicationServer_hostname_or_ip>/agentportal`

        Dieser Wert muss mit der URL übereinstimmen, die in der XML-Konfigurationsdatei des Agenten-Portals konfiguriert wurde. Um diesen Wert zu finden, gehen Sie zum Computer, auf dem der Anwendungsserver ausgeführt wird, öffnen Sie die folgende Datei aus dem Installationsverzeichnis und kopieren Sie den Inhalt des Elements „service-provider-host-url“: `.\ApplicationServer\ApacheWebServer\conf\webagent.xml`

        - **Zertifikat**: Ein optionaler Wert für den Dienstanbieter. Damit können Sie ein Zertifikat einfügen, das die Nachrichten an den IdP verschlüsselt.
        - **Öffentlicher Schlüssel**: Ein optionaler Wert für den im Zertifikat verwendeten Schlüssel zur Validierung der Zertifizierung mit dem Dienstanbieter. Dieser Wert muss dem Dienstanbieter und dem IdP bekannt sein.

NOTE: Für OpenScape Contact Center kann der Dienstanbieter das Agenten-Portal-Web selbst sein. Sie können mehr als einen Dienstanbieter im System konfigurieren.

---

2. Metadaten des Dienstanbieters abrufen

Rufen Sie die Metadaten des Dienstanbieters ab, während sie noch bei der Web Manager-Anwendung angemeldet sind, und importieren Sie sie in den Identitätsanbieter-Dienst

1. Bewegen Sie den Mauszeiger über den hinzugefügten Dienstanbieter und klicken Sie auf **Metadaten abrufen**
2. Klicken Sie auf **In die Zwischenablage kopieren**, speichern Sie den Inhalt in einer Textdatei auf Ihrem Computer ab und benennen Sie die Dateierweiterung auf „xml“ um. Wählen Sie den Dateinamen so, dass deutlich wird, dass die Metadaten des Dienstanbieters darin enthalten sind, zum Beispiel: `OSCC_<customer>_metadata.xml`

3. Metadaten des Dienstanbieters in den Identitätsanbieter importieren

   Sie müssen den Dienstanbieter dem Identitätsanbieter als vertrauende Seite hinzufügen, indem Sie seine Metadaten importieren. Übertragen Sie die in Schritt 2) erstellte XML-Datei an einen Ort, der für den Identitätsanbieter zugänglich ist und greifen Sie auf den Identitätsanbieter zu.

   Das folgende Beispiel zeigt, wie die Metadaten des Dienstanbieters in das Microsoft Active Directory Federation Service (ADFS) importiert werden:

   1. Navigieren Sie in der ADFS-Verwaltungskonsole zum Ordner:
      Vertrauensstellung > Vertrauensstellungen der vertrauenden Seite
   2. Klicken Sie auf **Vertrauensstellung der vertrauenden Seite hinzufügen**
   3. Der Bildschirm **Assistent zum Hinzufügen von Vertrauensstellungen der vertrauenden Seite** wird angezeigt. Klicken Sie auf **Starten**
   4. Wählen Sie **Daten über die vertrauende Seite aus einer Datei importieren** und wählen Sie die in Schritt 2) erstellte XML-Datei aus. Verwenden Sie **Durchsuchen**, um die Datei zu suchen.
   5. Klicken Sie auf **Weiter**
   6. Geben Sie einen beliebigen Namen im Feld **Anzeigename** ein
   7. Klicken Sie auf **Weiter**
   8. Wählen Sie **Allen Benutzern den Zugriff auf diese vertrauende Seite erlauben**
   9. Klicken Sie auf **Weiter**
   10. Klicken Sie auf **Schließen**

4. Ordnen Sie den Benutzernamen auf dem Identitätsanbieter zu

Fügen Sie eine Anspruchsregel für die in Schritt 3) erstellte Vertrauensstellung der vertrauenden Seite hinzu.

Anspruchsregeln werden verwenden, um einen eingehenden Anspruchstyp einem ausgehenden Anspruchstyp zuzuordnen. In der Anspruchsregel geben Sie an, welches Feld in der Benutzerdatenbank des Identitätsanbieters mit dem OSCC-Benutzernamen übereinstimmt.

1. Wählen Sie in der ADFS-Verwaltungskonsole die erstellten Vertrauensstellungen der vertrauenden Seite und klicken Sie auf **Anspruchsausstellungsrichtlinie bearbeiten.**
2. Klicken Sie auf **Regel hinzufügen**, um den Anspruchsregelassistenten zu öffnen.
3. Wählen Sie im Fenster **Regelvorlage auswählen** aus dem Dropdownmenü **LDAP-Attribute als Ansprüche senden**.

   NOTE: Im folgenden Beispiel wird der OSCC-Benutzername mithilfe von LDAP authentifiziert.

4. Klicken Sie auf **Weiter**
5. **Zuordnung von LDAP-Attributen zu Typen ausgehender Ansprüche** (Active Directory) für die Authentifizierung durch SAML

   NOTE: In diesem Beispiel wird der Windows-Kontoname für die Zuordnung des OSCC-Benutzernamens verwendet, der auf dem LDAP-Server (Active Directory) konfiguriert ist. Für ADFS ist zusätzlich die Zuordnung der Namenskennung erforderlich.

6. Klicken Sie auf **Fertigstellen**

5. Metadaten des Identitätsanbieters abrufen

   Importieren Sie nach der Konfiguration des Identitätsanbieters seine Metadaten in den Dienstanbieter.

   Wie im Endpunktverzeichnis der ADFS-Verwaltungskonsole ersichtlich, kann auf die Metadaten wie folgt zugegriffen werden:

   `https://<ADFSServerName>/FederationMetadata/2007-06/FederationMetadata.xml`

6. Importieren Sie die Identitätsanbieter-Metadaten in den Dienstanbieter

   1. Melden Sie sich bei der Web Manager-Anwendung mit den Master Administrator-Benutzeranmeldeinformationen an. Wählen Sie zuerst **Anmeldekonfiguration** und dann **Identitätsanbieter**.

      Sie können einen Identitätsanbieter entweder manuell über **Identitätsanbieter hinzufügen** oder automatisch über **Von Metadaten importieren** hinzufügen. Es wird empfohlen, einen

Identitätsanbieter durch Importieren hinzuzufügen. Übertragen Sie die in Schritt 5 erstellte XML-Datei an einen Ort, der für den Dienstanbieter zugänglich ist.

Wenn Sie einen Identitätsanbieter manuell hinzufügen möchten, klicken Sie auf **Identitätsanbieter hinzufügen**.

NOTE: Alle Konfigurationen können aus der IdP-Metadatendatei abgerufen werden.

- **Entitätskennung**: Kennung der IdP-Entität (muss eine URL sein). In den Metadaten finden Sie diese URL, indem Sie im Tag **EntityDescriptor** nach dem Attribut **entityID** suchen.
- **SSO-URL**: SSO-Endpunktinformationen des IdP. Dies ist das URL-Ziel des IdP, an das der SP die Authentifizierungsanforderungsnachricht sendet. In den Metadaten finden Sie diese URL innerhalb des Tags **IDPSSODescriptor**, indem Sie nach dem Attribut **Location** im Tag **SingleSignOnService** suchen.

NOTE: Verwenden Sie den Wert **Location** aus der Zeile mit dem Wert "**...HTTP-POST**" im Attribut **Binding**.

- **Benutzernamensübereinstimmung**: Das ist der vom IdP zurückgegebene Parameter, der mit dem konfigurierten OSCC-Benutzer verglichen wird.

In den Metadaten, zum Beispiel in ADFS, wurde der **Windows-Kontoname** als **Typ des ausgehenden Anspruchs** ausgewählt (siehe Schritt 4 - **Benutzernamen auf dem Identitätsanbieter zuordnen - Regel hinzufügen**). Wenn Sie in der Metadatendatei nach dem Wert **Windows-Kontoname** suchen, ist der Wert für die **Benutzernamensübereinstimmung** unter dem Attribut **Name** zu finden. In diesem Beispiel lautet es:

```
http://schemas.microsoft.com/ws/2008/06/identity/
claims/windowsaccountname
```

In der Regel muss der Wert des Parameters **Benutzernamensübereinstimmung** mit dem für die Zuordnung von SAML-LDAP-Attributen im IdP konfigurierten Typ des ausgehenden Anspruchs übereinstimmen, siehe Schritt 4) **Zuordnung von LDAP-Attributen zu Typen des**

ausgehenden Anspruchs. Es ist der Wert des LDAP-Parameters, der von AFDS zur Identifizierung (Übereinstimmung) des OSCC-Benutzers verwendet wird.

NOTE: Andere IdPs haben möglicherweise eine andere Benutzernamensübereinstimmung.

- **Dienst-URL für einmaliges Abmelden**: Die URL-Adresse des IdP, an die der SP die Einzelabmeldungsanforderung sendet. In den Metadaten finden Sie diese URL innerhalb des Tags **IDPSSODescriptor**, indem Sie nach dem Attribut **Location** im Tag **SingleLogoutService** suchen.

NOTE: Verwenden Sie den Wert **Location** aus der Zeile mit dem Wert "**...HTTP-POST**" im Attribut **Binding**.

- **Antwort-URL des Einzelabmeldungsdienstes**: Die URL-Adresse des IdP, an die der SP die Einzelabmeldungsantwort sendet. Dieser Wert ist optional und wird in der Regel leer gelassen. Wenn Sie ihn leer lassen, wird die gleiche URL wie die **Dienst-URL für einmaliges Abmelden** als Endpunktinformation für die Einzelabmeldungsanforderung des IdP verwendet. Einige IdPs verwenden eine verschiedene URL für das Senden einer Abmeldungsanforderung und -antwort. Verwenden Sie diese Eigenschaft zum Einstellen einer separaten Antwort-URL.
- **x509-Zertifikat**: Das öffentliche x509-Zertifikat des IdP. In den Metadaten finden Sie diesen Zertifikatswert indem Sie im Tag **X509Certificate**, innerhalb des Tags **IDPSSODescriptor** und innerhalb des Tags **KeyDescriptor** nach dem Attribut **use="signing"** suchen.

NOTE: Achten Sie bei der manuellen Eingabe eines Zertifikats darauf, dass nur die Hash-Zeile enthalten ist und entfernen Sie eventuelle Kommentare oder zusätzliche Zeilen davor oder dahinter.

- **Zertifikatsfingerabdruck**: Anstatt des gesamten x509-Zertifikats können Sie einen Fingerabdruck verwenden. Liegt ein Fingerabdruck vor, ist der Fingerabdruckalgorithmus erforderlich, um dem OSCC mitzuteilen, welcher Algorithmus verwendet wurde. Mögliche Werte sind: SHA1, SHA256, SHA384, SHA512.

Wenn Sie einen Identitätsanbieter durch das Importieren von Metadaten hinzufügen möchten, klicken Sie auf **Von Metadaten importieren**, was die empfohlene Vorgangsweise für die Konfiguration des IdP ist.

- **Benutzernamensübereinstimmung**: Das ist der vom IdP zurückgegebene Parameter, der für den Vergleich mit dem konfigurierten OSCC-Benutzer verwendet wird.

In den Metadaten, zum Beispiel in ADFS, wurde der **Windows-Kontoname** als **Typ des ausgehenden Anspruchs** ausgewählt (siehe Schritt 4 - **Benutzernamen auf dem Identitätsanbieter zuordnen - Regel hinzufügen**). Wenn Sie in der Metadatendatei nach dem Wert **Windows-Kontoname** suchen, ist der Wert für die **Benutzernamensübereinstimmung** unter dem Attribut **Name** zu finden. In diesem Beispiel lautet es:

```
http://schemas.microsoft.com/ws/2008/06/identity/
claims/windowsaccountname
```

In der Regel muss der Wert des Parameters **Benutzernamensübereinstimmung** mit dem für die Zuordnung von SAML-LDAP-Attributen im IdP konfigurierten Typ des ausgehenden Anspruchs übereinstimmen, siehe Schritt 4) **Zuordnung von LDAP-Attributen zu Typen des ausgehenden Anspruchs**. Es ist der Wert des LDAP-Parameters, der von AFDS zur Identifizierung (Übereinstimmung) des OSCC-Benutzers verwendet wird.

NOTE: Andere IdPs haben möglicherweise eine andere Benutzernamensübereinstimmung.

Nach dem Ausfüllen von **Benutzernamensübereinstimmung** wählen Sie**Metadaten hochladen**, klicken Sie auf **Datei wählen** und wählen Sie die Metadatendatei. Klicken Sie auf **Hinzufügen**.

Eine andere Möglichkeit zum Auswählen von Typmetadaten besteht darin, im Feld **Metadateninhalt** Metadaten zu bearbeiten bzw. diese zu kopieren oder einzufügen. Klicken Sie auf **Hinzufügen**

7. Aktivieren Sie SSO und weisen Sie den Identitätsanbieter zu

1. Nach dem Importieren der Metadaten des Identitätsanbieters in den Dienstanbieter, klicken Sie auf die Registerkarte **Mandant**, während Sie noch bei der Web Manager-Anwendung angemeldet sind.
2. Die Registerkarte **Mandant** zeigt eine Liste der Mandanten. Bewegen Sie den Mauszeiger über den Mandanten und klicken Sie auf **Bearbeiten**.
3. Aktivieren oder deaktivieren Sie im Fenster **Mandanten konfigurieren** die Funktionen **Einmaliges Anmelden** und **Einmaliges Abmelden**:
   - **Einmaliges Anmelden**: Erlaubt die SAML2-Integration
   - **Identitätsanbieter**: Wählen Sie den zuvor in Schritt 6 auf der Registerkarte „Identitätsanbieter" konfigurierten Identitätsanbieter
   - **Einmaliges Abmelden (SLO)**: Wenn diese Funktion aktiviert ist und Sie sich vom Agenten-Portal-Web abmelden, führt das System eine Abmeldung vom Identitätsanbieter-Server durch. Wenn diese Funktion aktiviert ist, wird der Benutzer von allen anderen Anwendungen abgemeldet, die den gleichen IdP verwenden.

NOTE: Wenn Sie OpenScape Contact Center für Einzelmandantenfähigkeit konfigurieren, ist SSO über SAML2 eine systemweite Funktionalität. Wenn Sie OpenScape Contact Center für Mehrmandantenfähigkeit konfigurieren, kann SSO über SAML2 pro Mandant aktiviert werden. Für diejenigen Mandanten, wo SSO über SAML2 nicht aktiviert ist, gelten die in Manager Desktop konfigurierten Anmeldemethoden.

Starten Sie nach dem Abschluss der Konfiguration des einmaligen Anmeldens den Webbrowser, melden Sie sich im Agenten-Portal-Web an und geben Sie Folgendes ein:

```
https://<ApplicationServer_hostname_or_ip>/agentportal
```

Für die erste Authentifizierung in dieser Browsersitzung werden Sie zum Identitätsanbieter weitergeleitet.

1. Geben Sie <user>@<domain> oder <domain>\<user> ein, wobei
   - <domain> der Kundendomänenname ist und

- <user>der in Active Directory konfigurierte Benutzer (Kontoname) ist

  NOTE: <user> muss auch als Benutzer in OpenScape Contact Center konfiguriert sein

- Geben Sie das Active Directory-Kennwort ein.

Für weitere Authentifizierungen (Anmeldungen) in der gleichen Browsersitzung wird SSO durchgeführt und es müssen weder Kontodaten noch Kennwort eingegeben werden.

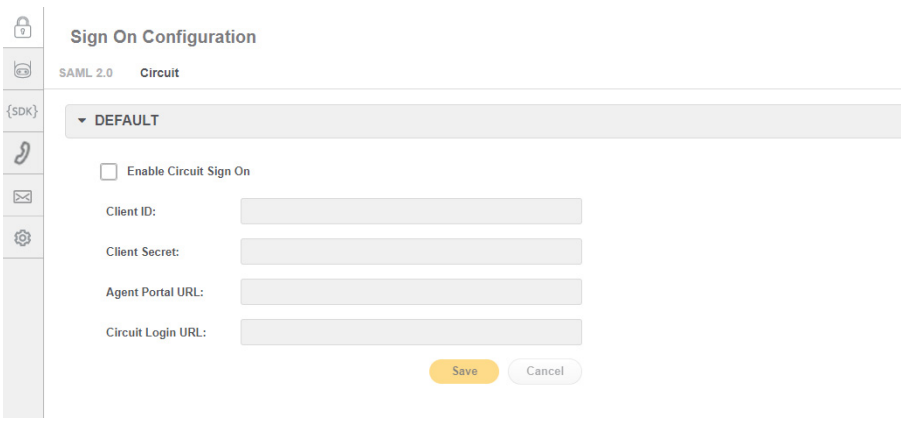
4 Einmaliges Anmelden in Circuit konfigurieren

Im Anschluss an die Konfiguration der benutzerdefinierten Anwendung in Circuit (siehe *OpenScape Contact Center Enterprise V10 Integrationshandbuch für Kommunikationsplattformen*) müssen die Client-ID und der geheime Schlüssel des Client mit OpenScape Contact Center synchronisiert werden.

Öffnen Sie die OSCC Web Manager-Anwendung und melden Sie sich mit einem Manager-Konto für Mandanten an. Klicken Sie unter „Anmeldekonfiguration" auf die Registerkarte „Circuit" und auf die OSCC-Mandanten, die Zugriff auf die Circuit-Integrationsfunktion haben.

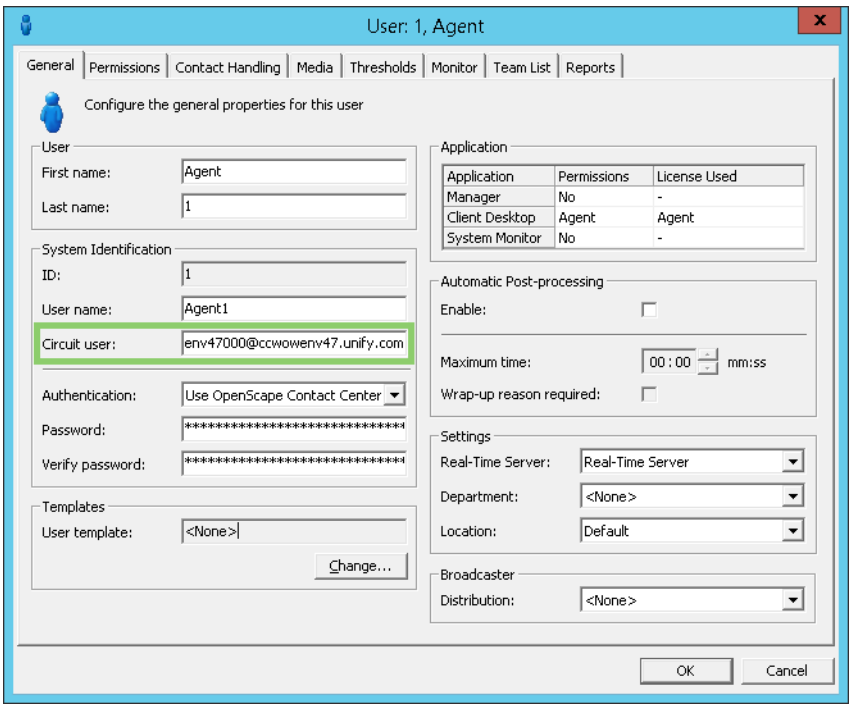
Füllen Sie die unten stehenden Felder mit folgenden Informationen:

- **Circuit Sign On aktivieren** - aktiviert.
- **Client-ID**: Die einmalige Kennung der Anwendung, die im vorherigen Kapitel abgerufen wurde.
- **Geheimer Schlüssel des Client**: Der geheime Schlüssel der Anwendung, der im vorherigen Kapitel abgerufen wurde.
- **Agent Portal URL**: Die URL für den Zugang zur Anwendung Agent Portal Web. Verwenden Sie das Muster `https://<IhreDomain>/agentportal`
- **Circuit-Login-URL**: Die URL für den Zugang zur Circuit-Anwendung.



Wenn Sie sich mit dem Circuit Sign On auf der Anmeldeseite des OpenScape Contact Center authentifizieren, müssen Sie ein Circuit-Konto mit dem OpenScape Contact Center-Benutzer verbinden. Der Circuit-Benutzername (URI) wird für die Zuordnung verwendet.

Geben Sie im Konfigurationsfenster im Feld Circuit-Benutzer die bei der Anmeldung bei Circuit verwendete URI an. Zwei OSCC-Benutzer desselben Mandanten können sich nicht denselben Circuit-Benutzer teilen.



NOTE: Wenn nur über einen HTTPS-Proxy-Server auf Circuit zugegriffen werden kann, ist eine besondere Konfiguration für den Anwendungsserver erforderlich. Weitere Details zur Konfiguration finden Sie im *OpenScape Contact Center V10 Installationshandbuch*.

NOTE: Detaillierte Informationen zur Konfiguration von OpenScape Voice und zum Hinzufügen einer Anwendung zu Circuit finden Sie im *OpenScape Contact Center Enterprise V10 Integrationshandbuch für Kommunikationsplattformen*.

---

5 Virtuelle Agenten

Der Haupt-Administrator-Benutzer muss sich am Web-Manager anmelden, um virtuelle Agenten im OpenScape Contact Center zu konfigurieren.

Die Funktion "Virtueller Agent" ermöglicht die Integration des OpenScape Contact Centers mit einem Natural Language Processor (NLP) zur Einbindung von Chatbots.

Der Dienst Virtual Agent wird im Container des OSCC Application Server ausgeführt und meldet alle im Web Manager konfigurierten Agenten an.

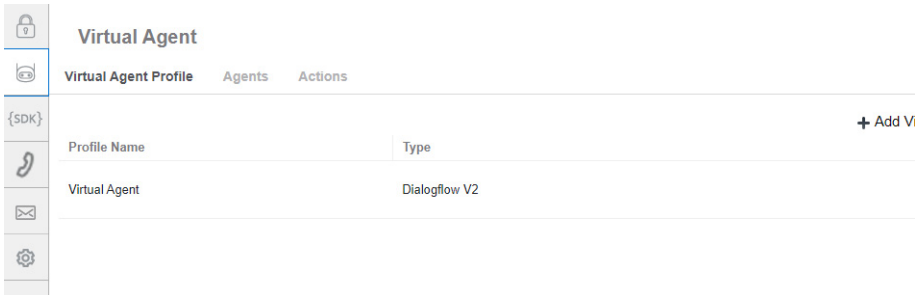
NOTE: Der virtuelle Agent unterstützt nur den Kennworttyp OpenScape Contact Center. Das System funktioniert nicht mit der Windows-Anmeldung oder mit SAML2 SSO.

NOTE: Die Funktionalität des virtuellen Agenten ist eine systemweite Konfiguration. Wenn in OpenScape Contact Center die Mehrinstanzenfähigkeit aktiviert ist, muss jeder Mandant ein oder mehrere CMS bereitstellen, um Sprachausgabeunterstützung bereitzustellen. Jedes CMS kann ein oder mehrere virtuelle Agentenprofile unterstützen. Jedes Profil muss mit einem anderen GCP-Token konfiguriert werden. Auf dem OSCC Application Server muss die Konfigurationsdatei `virtualagent.xml` den korrekten Namen der Geschäftseinheit haben.

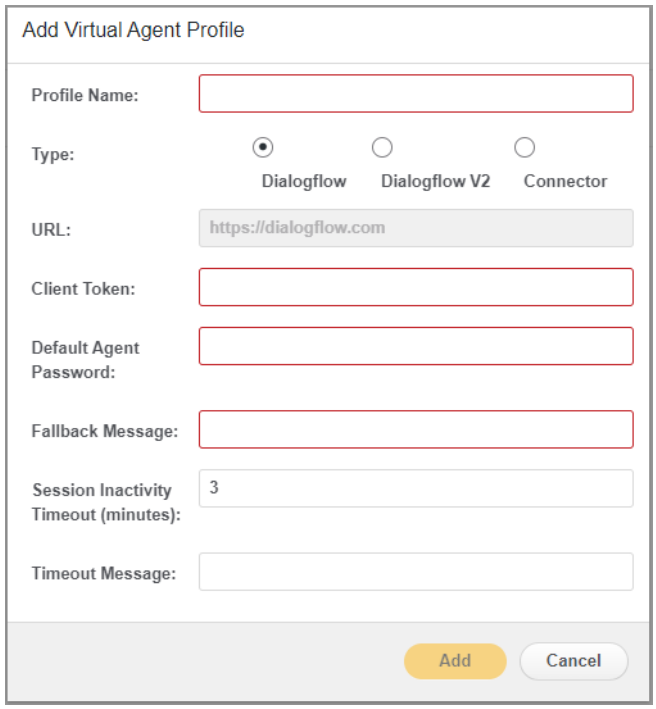
NOTE: **Automatische Nachkontaktaktivitäten** und **Grund für die zwingende Nachbearbeitung** werden vom virtuellen Agenten nicht unterstützt. Achten Sie darauf, dass diese Funktionen in der Benutzerkonfiguration deaktiviert sind.

Melden Sie sich bei Web Manager an und führen Sie die folgenden Schritte aus:

- Gehen Sie zur Registerkarte **Virtueller Agent**:



- Klicken Sie Auf **Virtuelles Agentenprofil hinzufügen**. Es wird das Fenster **Virtuelles Agentenprofil hinzufügen** angezeigt. Dies ist das Formular für die Konfiguration des NLP-Profils:



  - **Profilname**: Das ist ein Pflichtfeld. Name des NLP-Profils des virtuellen Agenten
  - **Typ**: Profiltyp des virtuellen Agenten. Sie können eines der folgenden Optionsfelder auswählen:
    - Dialogflow

- Dialogflow V2
- Connector

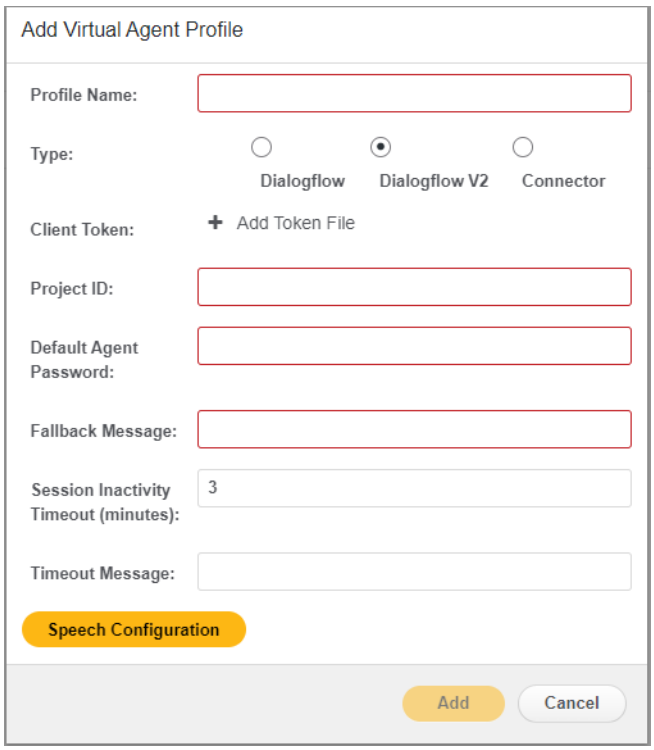
Je nach ausgewähltem Typ müssen Sie verschiedene Parameter konfigurieren.

Typ: Dialogflow

- **URL**: Die Engine-URL des Dialogflow. Standardwert lautet https://dialogflow.com
- **Clienttoken**: Das von Dialogflow bereitgestellte Clienttoken
- **Standard-Agentenkennwort**: Das im Manager konfigurierte Kennwort für die Benutzer, die als virtueller Agent konfiguriert sind. Wichtig ist, dass Sie für die gesamte Benutzerkonfiguration des virtuellen Agenten dasselbe Kennwort verwenden.
- **Rückfall-Meldung**: Das ist eine Rückfall-Meldung des Systems. Wenn ein Fehler im System auftritt, wird diese Nachricht extern an die Person gesendet, die sich an das Kontakt-Center gewandt hat.
- **Zeitüberschreitung wegen Inaktivität der Sitzung**: Wenn die aktuelle Kontaktsitzung inaktiv ist, wird die Sitzung vom System automatisch entsprechend der konfigurierten Zeit in Minuten beendet
- **Zeitüberschreitungsmeldung**: Das ist die Nachricht, die nach der Zeitüberschreitung wegen Inaktivität der Sitzung gesendet wird

Typ: Dialogflow V2

Das Fenster **Virtuelles Agentenprofil hinzufügen** enthält das folgende Formular für die NLP-Profilkonfiguration:

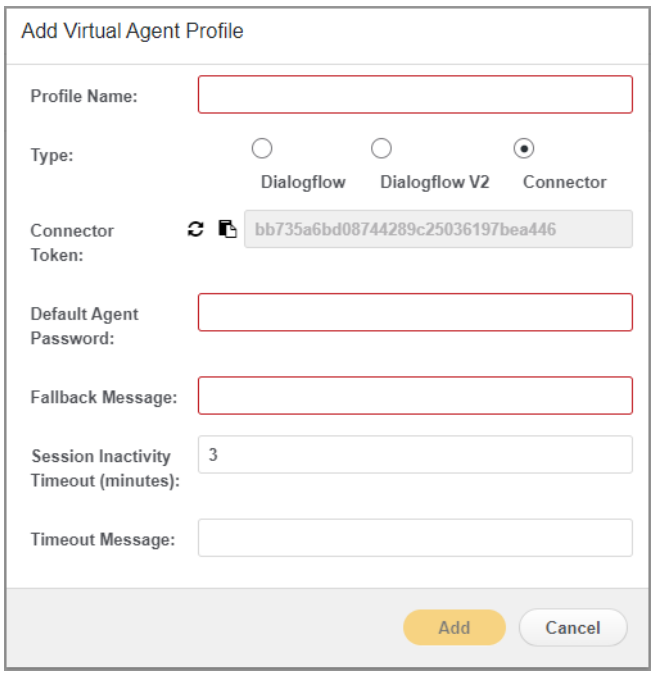


- **Clienttoken**: Klicken Sie auf **Tokendatei hinzufügen** und suchen Sie auf Ihrem PC nach der Tokendatei, einer *.json-Datei, die Sie verwenden möchten
- **Projekt-ID**: ID des Projekts
- **Standard-Agentenkennwort**: Das ist ein Pflichtfeld. Das im Manager konfigurierte Kennwort für die Benutzer, die als virtueller Agent konfiguriert sind. Wichtig ist, dass Sie für die gesamte Benutzerkonfiguration des virtuellen Agenten dasselbe Kennwort verwenden.
- **Rückfall-Meldung**: Das ist ein Pflichtfeld. Das ist eine Rückfall-Meldung des Systems. Wenn ein Fehler im System auftritt, wird diese Nachricht extern an die Person gesendet, die sich an das Kontakt-Center gewandt hat.

- **Zeitüberschreitung wegen Inaktivität der Sitzung**: Wenn die aktuelle Kontaktsitzung inaktiv ist, wird die Sitzung vom System automatisch entsprechend der konfigurierten Zeit in Minuten beendet
- **Zeitüberschreitungsmeldung**: Das ist die Nachricht, die nach der Zeitüberschreitung wegen Inaktivität der Sitzung gesendet wird
- **Sprachausgabekonfiguration**: Mit dieser Schaltfläche können Sie den Speechbot konfigurieren

Typ: Connector

Das Fenster **Virtuelles Agentenprofil hinzufügen** enthält das folgende Formular für die NLP-Profilkonfiguration:



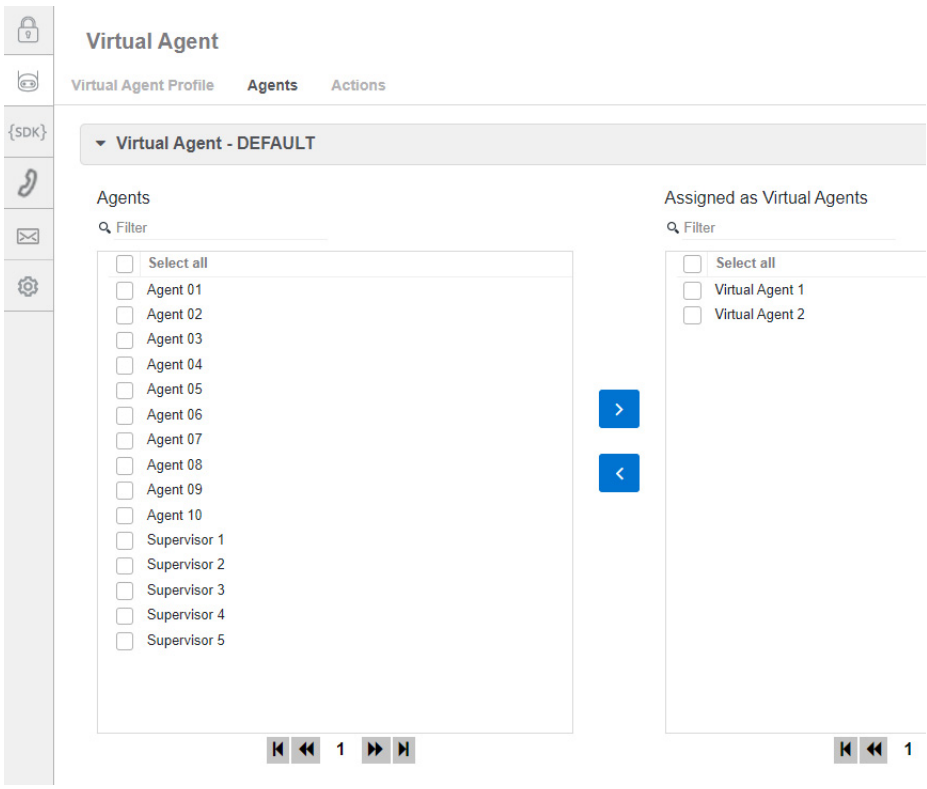
- **Connector-Token**: Klicken Sie auf die Schaltfläche **Neu laden**, um ein neues Token zu generieren. Das neue Connector-Token wird im ausgegrauten Feld angezeigt. Klicken Sie auf die Schaltfläche **Zwischenablage**, um das Token in die Zwischenablage zu kopieren

- **Standard-Agentenkennwort**: Das ist ein Pflichtfeld. Das im Manager konfigurierte Kennwort für die Benutzer, die als virtueller Agent konfiguriert sind. Wichtig ist, dass Sie für die gesamte Benutzerkonfiguration des virtuellen Agenten dasselbe Kennwort verwenden.
- **Rückfall-Meldung**: Das ist ein Pflichtfeld. Das ist eine Rückfall-Meldung des Systems. Wenn ein Fehler im System auftritt, wird diese Nachricht extern an die Person gesendet, die sich an das Kontakt-Center gewandt hat.
- **Zeitüberschreitung wegen Inaktivität der Sitzung**: Wenn die aktuelle Kontaktsitzung inaktiv ist, wird die Sitzung vom System automatisch entsprechend der konfigurierten Zeit in Minuten beendet
- **Zeitüberschreitungsmeldung**: Das ist die Nachricht, die nach der Zeitüberschreitung wegen Inaktivität der Sitzung gesendet wird

5.1 Agentenbenutzer als virtuelle Agenten konfigurieren

Für die virtuellen Agenten ist es notwendig, Benutzer mit dem in OSCC registrierten Agentenprofil zuzuordnen.

Um Benutzer zuzuweisen, wechseln Sie zur Registerkarte **Agenten** und erweitern Sie die Profilansicht:



NOTE: Hier finden Sie Filter, die Ihnen bei der Auswahl der Agentenbenutzer im System helfen.

5.2 Aktionen für virtuelle Agenten konfigurieren

Die Funktion Virtueller Agent kann einige vom NLP-Prozessor empfangene Aktionen verarbeiten.

Üblicherweise ist eine Aktion eine vom NLP-Prozessor gesendete Zeichenkette mit einem Satz von Parametern.

Es gibt mehrere mögliche Aktionen:

- **Aktion Wiedereinreihung**: Ermöglicht dem System die Übergabe vom virtuellen Agenten an eine Person, indem der Kontakt in einer anderen Warteschlange wieder eingereiht wird.

- **Callback-Aktion**: Ermöglicht dem System die Übergabe vom virtuellen Agenten an eine Person durch Erstellen eines Telefonierückrufs in OSCC.
- **Externe Systemanforderung**: Ermöglicht dem System eine Anfrage an andere Drittsysteme, um der Lösung eine elegantere Antwort an die Kunden zu geben.
- **WebInteraction Push URL**: Ermöglicht dem System, eine Anfrage an andere URLs, um der Lösung eine elegantere Antwort an die Kunden zu geben
- **Sprachausgabe**-**Wiedereinreihung**: Aktion zur Auswahl des Ziels der Wiedereinreihung

5.2.1 Konfigurieren einer Wiedereinreihungs-Aktion für virtuelle Agenten

5.2.1.1 Aktion OpenMedia-Wiedereinreihung

Um eine OpenMedia-Wiedereinreihungs-Aktion zu konfigurieren, wählen Sie den Medientyp als **OpenMedia** aus und legen Sie Folgendes fest:

- **Aktionsname**: Ein Textwert, der der vom NLP-System empfangenen Aktion entsprechen muss. (Obligatorisch)
- **Wiedereinreihungs-Warteschlange**: Die Warteschlange, in der der Kontakt wieder eingereiht wird. Das ist ein Pflichtfeld. Wählen Sie einen Wert aus der Liste aus und klicken Sie auf **Hinzufügen**.

5.2.1.2 Aktion WebInteraction-Wiedereinreihung

Um eine WebInteraction-Wiedereinreihungs-Aktion zu konfigurieren, wählen Sie den Medientyp als **WebInteraction** aus und legen Sie Folgendes fest:

- **Aktionsname**: Ein Textwert, der der vom NLP-System empfangenen Aktion entsprechen muss. (Obligatorisch)
- **Wiedereinreihungs-Warteschlange**: Die Warteschlange, in der der Kontakt wieder eingereiht wird. Das ist ein Pflichtfeld. Wählen Sie einen Wert aus der Liste aus und klicken Sie auf **Hinzufügen**.

5.2.1.3 Aktion Sprachausgabe-Wiedereinreihung

Um eine Sprachausgabe-Wiedereinreihungs-Aktion zu konfigurieren, wählen Sie den Medientyp als **Sprachausgabe** aus und legen Sie Folgendes fest:

- **Aktionsname**: Ein Textwert, der der vom NLP-System empfangenen Aktion entsprechen muss. (Obligatorisch)
- **Wiedereinreihungsziel**: Das Ziel, in dem der Kontakt wieder eingereiht wird. Das ist ein Pflichtfeld. Wählen Sie einen Wert aus der Liste aus und klicken Sie auf **Hinzufügen**.

5.2.2 Konfigurieren von Callback-Aktionen

Um eine Callback-Aktion zu konfigurieren, wählen Sie den Aktionstyp als **Callback-Aktion** aus und legen Sie Folgendes fest:

- **Aktionsname**: Ein Textwert, der der vom NLP-System empfangenen Aktion entsprechen muss. (Obligatorisch)
- **Callback-Warteschlange**: Die Warteschlange, die zum Erstellen des Rückrufs verwendet wird. (Obligatorisch)
- **Name des Telefonparameters**: Der Parametername, um die Telefonnummer vom NLP-System zu erhalten. (Obligatorisch)
- **Name des Zeitplanparameters**: Der Parametername, um das Datum und die Uhrzeit für den Callback-Plan zu erhalten. (Obligatorisch)

5.2.3 Konfigurieren einer externen Systemanforderung für virtuelle Agenten

Um eine externe Systemanforderung zu konfigurieren, wählen Sie den Aktionstyp **Externe Systemanforderung** aus und legen Sie Folgendes fest:

- **Aktionsname**: Ein Textwert, der der vom NLP-System empfangenen Aktion entsprechen muss. (Obligatorisch)
- **URI-Parameter des externen Systems**: Ein vom NLP-System definierter Parametername, der die URI-Adresse enthält, an die das System des virtuellen Agenten die Anforderung senden muss. (Obligatorisch)

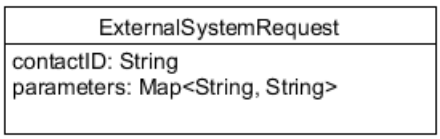
5.2.3.1 Details zu externen Systemanforderungen

Die Funktion Externe Systemanforderung ist ein interner REST-Schnittstellen-Client, der in den virtuellen Agentendienst implementiert ist.

Sobald der virtuelle Agent eine Aktion für eine externe Konsultation von NLP erhält, sendet das System eine POST-Anfrage an den im Parameter definierten URI mit einem vordefinierten JSON-Objekt.

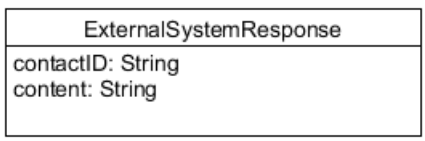
Es gibt zwei JSON-Objekte - eines für die Anforderung und eines für die Antwort.

Das vom virtuellen Agenten gesendete Anforderungsobjekt lautet:



- **contactID**: Das Attribut, das den Wert der OSCC contactID enthält
- **Parameter**: Eine Sammlung von Parametern, die vom NLP-Prozessor empfangen wurden und aus einem Schlüssel-/Wertetext zusammengesetzt sind. Diese Parameter werden durch das externe System verarbeitet

Das vom virtuellen Agenten empfangene Antwortobjekt muss die folgende Struktur aufweisen:



- **contactID**: Dieser Wert muss dem Wert entsprechen, der im Objekt ExternalSystemRequest empfangen wurde. (Obligatorisch)
- **Inhalt**: Der vom externen System verarbeitete Text mit dem Antwortinhalt für die Anforderung.

5.2.4 Konfigurieren einer WebInteraction-Push-URL-Anforderung für virtuelle Agenten

Um eine Webinteraction-Push-URL-Anforderungs-Aktion zu konfigurieren, wählen Sie den Aktionstyp **WebInteraction Push URL** aus und legen Sie Folgendes fest:

- **Aktionsname**: Ein Textwert, der der vom NLP-System empfangenen Aktion entsprechen muss. (Obligatorisch)
- **Push-URL-Parameter**: Ein vom NLP-System definierter Parametername, der die URL-Adresse enthält, an die das System des virtuellen Agenten die Anforderung senden muss. (Obligatorisch)

5.3 Sprachausgabe für virtuelle Agenten konfigurieren

Mit der Funktion Virtueller Agent können Sie einen Speechbot über die Schaltfläche **Sprachausgabekonfiguration** konfigurieren, auf der Sie die folgenden Parameter konfigurieren können. Diese Schaltfläche ist nur für den Profiltyp Dialog V2 des virtuellen Agenten verfügbar.

- **Sprachausgabe**aktivieren: Ein Parameter, um den Speechbot für das ausgewählte Profil zu aktivieren. Standardwert: Deaktiviert
- **CMS-Adresse**: IP-Adresse/FQDN für den Zugriff auf den CMS-Knoten.
- **CMS-Port**: Port für den Zugriff auf den CMS-Knoten. Standardwert: 6017
- **Sprache**: Die zu verwendende Sprache. Standardwert: EN-US
- **Geschlecht**: Geschlecht der Text-zu-Sprache-Stimme. Standardwert: Männlich
- **Willkommensnachricht**: Nachricht, die wiedergegeben wird, wenn der Anruf vom virtuellen Speechbot-Agenten angenommen wird.
- **Nummer der Rückfall-Wiedereinreihung**: Nummer, an die der Anruf weitergeleitet wird, wenn das CMS nicht erreichbar ist.

5.4 Info zur Dialogflow-Integration

Die Funktion Virtueller Agent ist standardmäßig in das Dialogflow-Modul für den Natural Language Processor integriert.

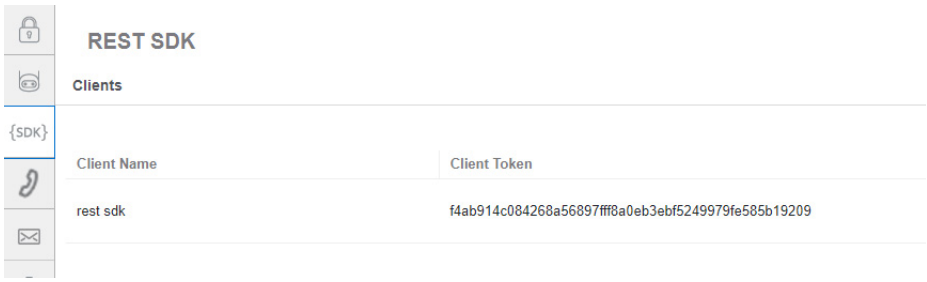
NOTE: Der standardmäßige NLP-Prozessor für den virtuellen Agenten ist der Dialogflow von Google. Für weitere Informationen folgen Sie dem Link: https://dialogflow.com

---

- **Dialogflow Standard Edition** ist kostenlos auf der Dialogflow-Webseite erhältlich. Es bietet dieselben Funktionen wie Dialogflow Enterprise Edition, aber die Interaktionen sind durch Nutzungsquoten begrenzt und der Support wird durch die Community und per E-Mail bereitgestellt. Dialogflow Standard Edition ist ideal für kleine und mittlere Unternehmen, die Konversationsschnittstellen erstellen oder mit Dialogflow experimentieren möchten.
- **Dialogflow Enterprise Edition** ist als Teil der Google Cloud Platform (GCP) erhältlich und bietet unbegrenzte Text- und Sprachinteraktionen, höhere Mengenquoten und Unterstützung durch den Support von Google Cloud. Dialogflow Enterprise Edition ist ein Premium-Angebot, das als Pay-as-you-go-Service erhältlich ist. Dialogflow Enterprise Edition ist ideal für Unternehmen, die einen unternehmensweiten Service benötigen, der leicht skalierbar ist, um Änderungen der Benutzeranforderungen zu unterstützen.

Weitere Informationen zu Quoten finden Sie unter: https://cloud.google.com/dialogflow-enterprise/quotas

6 REST SDK



Das REST SDK-Framework ermöglicht die Entwicklung von Multimedia-Anwendungen, die in das OpenScape Contact Center-System integriert werden können.

Das Framework besteht aus einer REST-Schnittstelle, die das Senden von Befehlen aus der Anwendung an das OpenScape Contact Center und das Senden von Überwachungsereignissen aus dem OpenScape Contact Center an die Anwendung ermöglicht.

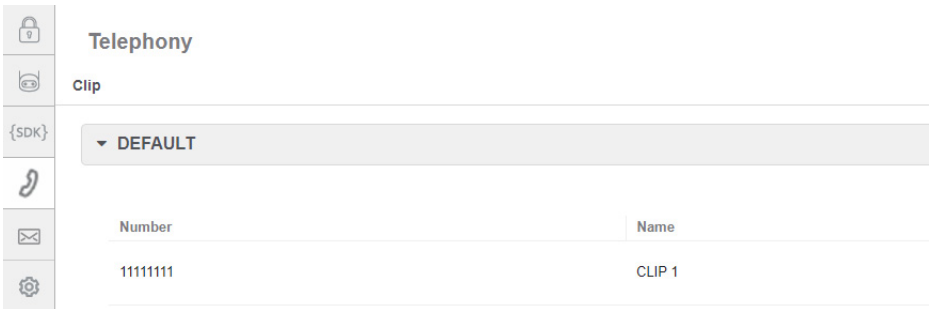
Configuration

Konfigurieren Sie die REST SDK-Instanzen über den Web Manager. So erstellen Sie eine neue REST SDK-Instanz:

1. Wählen Sie die Registerkarte **REST SDK**
2. Klicken Sie auf **+ REST SDK Client hinzufügen**
3. Ein Popup-Fenster **REST SDK Client hinzufügen** erscheint. Konfigurieren Sie die folgenden Parameter:
   - **Client-Name**: Der Client Name identifiziert die REST SDK-Instanz eindeutig und ist ein String mit bis zu 32 Zeichen.
   - **Client-Token**: Das Client Token ist ein Typ eines Passworts, mit dem der REST SDK-Client während des Registrierungsprozesses des Clients auf dem Server authentifiziert wird. Das Client Token kann entweder manuell konfiguriert oder automatisch generiert werden.

     Klicken Sie auf die Schaltfläche **Erneut laden**, um automatisch ein neues 64-Byte-Client Token zufällig zu generieren. Das neue Client Token wird auf dem ausgegrauten Feld angezeigt. Klicken Sie auf die Schaltfläche **Zwischenablage**, um das Token in die Zwischenablage zu kopieren.
   - Klicken Sie auf **Hinzufügen**
4. Der neue REST SDK-Client wurde erstellt.

7 CLIP für abgehende Anrufe



Calling Line Identification Presentation (CLIP) im Agenten-Portal-Web bezieht sich auf die für abgehende Anrufe verwendete Rufnummernübermittlung des Anrufers. CLIP beeinflusst nicht die aktuelle Funktionalität von Callback in Bezug auf die Definition der Anrufernummer. Eine Liste der Rufnummern muss pro Mandant konfiguriert werden. CLIP ist gültig für alle abgehenden Anrufe: von Anruftaste, Kurzwahlliste, Verzeichnissuche und Aktivitätsprotokoll.

Sie können CLIP für abgehende Anrufe über den Web Manager konfigurieren.

Hier können Sie die Rufnummer(n) für die CLIP-Funktionalität hinzufügen/ bearbeiten/löschen.

Neue Nummer hinzufügen

1. Klicken Sie auf die Registerkarte Telefonie
2. Klicken Sie auf das Dropdown-Menü Standard, das der Standardmandant ist
3. Klicken Sie auf Clip-Element hinzufügen. Sie können bis zu zehn Nummern pro Mandant hinzufügen
4. Ein Popup-Fenster Clip-Element hinzufügen erscheint. Konfigurieren Sie die folgenden Parameter:
   - Nummer: Die Rufnummer. Sie muss eine Reihe von Zahlen und keine Sonderzeichen haben. Dies ist ein Pflichtfeld
   - Name: Der Name der Rufnummer. Dies ist ein Pflichtfeld
5. Klicken Sie auf Hinzufügen

Die Liste der CLIP-Nummern zeigt jetzt die Zahl, die Sie gerade hinzugefügt haben. Diese Nummer erscheint auch in den verfügbaren Nummern in der CLIP-Funktionalität von Agenten-Portal-Web in: Einstellungen > Agent > CLIP > Immer diesen Wert verwenden

Nummer bearbeiten

1. Klicken Sie auf das Symbol Clip-Element bearbeiten neben der CLIP-Nummer, die Sie bearbeiten möchten

2. Das Popup-Fenster Clip-Element bearbeiten erscheint
3. Sie können die Nummer und/oder den Namen der vorhandenen Rufnummer ändern
4. Klicken Sie auf Aktualisieren

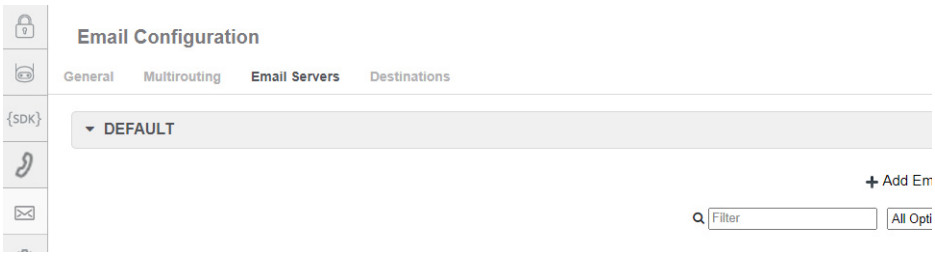
Die Liste zeigt nun die aktualisierte CLIP-Nummer und/oder den Namen

Nummer löschen

1. Klicken Sie auf das Symbol Clip-Element löschen neben der CLIP-Nummer, die Sie löschen möchten

2. Das Popup-Fenster Clip-Element löschen erscheint
3. Klicken Sie auf OK, um die CLIP-Nummer zu löschen oder auf Abbrechen, um das Löschen abzubrechen

8 Mehrere E-Mails pro Mandant



Mit dieser Funktion kann jede Unternehmenseinheit über mehrere E-Mail-Server oder E-Mail-Adressen pro Unternehmenseinheit verfügen. Sie können die E-Mail-Server und die Ziele über den Web Manager konfigurieren.

NOTE: Jede Unternehmenseinheit unterstützt bis zu fünf konfigurierte E-Mail-Anmeldeinformationen .

Hinzufügen eines neuen E-Mail-Servers

1. Klicken Sie auf die Registerkarte **E-Mail-Konfiguration**
2. Klicken Sie auf die Registerkarte **E-Mail-Server** und dann auf **Mandantenname**, um die Konfiguration zu erweitern.
3. Klicken Sie auf **E-Mail-Server hinzufügen**. Sie können den gleichen E-Mail-Server mehr als einmal konfigurieren, aber mit einem anderen Kontonamen.
4. Ein Popup-Fenster **E-Mail-Server hinzufügen** erscheint. Konfigurieren Sie die folgenden Parameter:
   - **Name des E-Mail-Servers**: Der Name des Servers. Dies ist ein Pflichtfeld
   - Klicken Sie auf das Dropdown-Menü **IMAP-Einstellungen** und konfigurieren Sie die folgenden Parameter:
     - **Hostname**: Der Hostname des Servers. Dies ist ein Pflichtfeld
     - **Portnummer**: Portnummer des Servers. Dies ist ein optionales Feld
     - **SSL verwenden**: Aktivieren Sie dieses Flag, um SSL zu verwenden
     - **Benutzername**: Der Benutzername des Kontos. Dies ist ein Pflichtfeld

- **Passwort**: Das Passwort des Kontos. Dies ist ein Pflichtfeld
- **Passwort bestätigen**: Bestätigen Sie das Passwort, das Sie im vorherigen Parameter angegeben haben. Dies ist ein Pflichtfeld
- **Max. IMAP-Sitzungen**: Die maximale Anzahl von IMAP-Sitzungen. Standardwert ist 0. Dies ist ein optionales Feld

- Klicken Sie auf das Dropdown-Menü **SMTP-Einstellungen** und konfigurieren Sie die folgenden Parameter:
  - **Hostname**: Der Hostname des Servers. Dies ist ein Pflichtfeld
  - **Portnummer**: Portnummer des Servers. Dies ist ein Pflichtfeld
  - **SSL verwenden**: Aktivieren Sie dieses Flag, um SSL zu verwenden
  - **Authentifizierung**: Wählen Sie aus dem Dropdown-Menü: "Keine", "IMAP-Einstellungen verwenden" und "Einstellungen unten verwenden", um die nächsten drei Parameter zu authentifizieren.
  - **Benutzername**: Nur konfigurierbar, wenn Sie „Einstellungen unten verwenden" aus dem Authentifizierungsparameter ausgewählt haben.
  - **Passwort**: Nur konfigurierbar, wenn Sie „Einstellungen unten verwenden" aus dem Authentifizierungsparameter ausgewählt haben.
  - **Passwort bestätigen**: Nur konfigurierbar, wenn Sie „Einstellungen unten verwenden" aus dem Authentifizierungsparameter ausgewählt haben.
  - **E-Mail-Adresse Systemüberw.**: Die vom System verwendete E-Mail-Adresse überprüft, ob die Verbindung zum E-Mail-Server ordnungsgemäß funktioniert.
  - **Max. Nachrichtenrate**: Die maximale Zahl der pro Stunde gesendeten E-Mail-Nachrichten. Der Standardwert ist 0 und bedeutet kein Limit.

5. Klicken Sie auf **Hinzufügen** , um einen neuen Server zu erstellen

Die Liste der E-Mail-Server zeigt nun den Server, den Sie gerade hinzugefügt haben.

Wenn die Funktion E-Mail an mehrere Server aktiviert ist, darf das gleiche Konto (E-Mail-Server + Kontoname) nicht für verschiedene Mandanten verwendet werden. Überprüfen Sie jedes Mal, wenn ein neuer E-Mail-Server oder die Änderung eines E-Mail-Servers gemeldet, ob das gleiche Konto bereits für andere Mandanten konfiguriert ist.

E-Mail- Server bearbeiten

1. Klicken Sie auf das Symbol **E-Mail Server** neben dem E-Mail-Server, den Sie bearbeiten möchten

2. Das Popup-Fenster **E-Mail-Server bearbeiten** wird angezeigt.
3. Wählen Sie den Parameter aus, die Sie ändern wollen. Sie können alle Parameter ändern.
4. Klicken Sie auf **Speichern**

Die Liste zeigt nun die aktualisierten Parameter des E-Mail-Servers an

E-Mail-Server kopieren

Sie können die Parameter eines E-Mail-Servers kopieren, um einen neuen mit einem anderen Namen zu erstellen.

1. Klicken Sie auf das Symbol **E-Mail-Server kopieren** neben dem Server, den Sie kopieren möchten

2. Das Popup-Fenster **E-Mail-Server kopieren** wird angezeigt..
3. Ändern Sie den Namen des Servers.
4. Klicken Sie auf **Hinzufügen**, um den neuen Server zu erstellen.

E-Mail-Server löschen

1. Klicken Sie auf das Symbol **E-Mail-Server löschen** neben dem Server, den Sie löschen möchten

2. Das Popup-Fenster **E-Mail-Server löschen** wird angezeigt.

3. Klicken Sie auf **JA**, um den E-Mail-Server zu löschen oder auf **NEIN**, um das Löschen abzubrechen

---

NOTE: Beim Löschen eines E-Mail-Servers wird überprüft, ob ein Ziel damit verbunden ist. In diesem Fall ist das Löschen des E-Mail-Servers nicht erlaubt. Die Verbindung zwischen den Zielen und dem E-Mail-Server muss vor dem Löschen des E-Mail-Servers entfernt werden. Wenn noch E-Mail-Kontakte zu bearbeiten sind, ist es nicht mehr möglich, die E-Mails zu öffnen und sie müssen verworfen werden.

Neues Ziel hinzufügen

Hier können Sie die Ziele mit der entsprechenden E-Mail-Adresse verbinden.

1. Klicken Sie auf die Registerkarte **E-Mail-Konfiguration**
2. Klicken Sie auf die Registerkarte **Ziel** und dann auf **Mandantenname**, um die Konfiguration zu erweitern.
3. Klicken Sie auf das Dropdown-Menü **Standard**, das der Standardmandant ist
4. Klicken Sie auf **Ziel hinzufügen**. Ein Popup-Fenster **Ziel hinzufügen** erscheint. Konfigurieren Sie die folgenden Parameter:
   - **Zielname**: Der Name des Ziels. Dies ist ein Pflichtfeld
   - **E-Mail-Adresse**: Geben Sie die Ziel-E-Mail-Adresse ein. Dies ist ein Pflichtfeld.
   - **Beschreibung**: Geben Sie eine Beschreibung für das Ziel ein. Dies ist ein optionales Feld
   - **Von-Text**: Geben Sie einen Alias für die Ziel-E-Mail-Adresse ein. Dieser Aliasname erscheint im Feld Von, wenn ein Benutzer auf eine E-Mail-Nachricht antwortet.
   - **Überwacht**: Aktivieren Sie dieses Flag, um das Ziel zu überwachen. Dies ist ein optionales Feld
   - **Verfügbar für gehend**: Aktivieren Sie dieses Flag, um das Ziel für ausgehende E-Mails zur Verfügung zu stellen. Dies ist ein optionales Feld
   - **E-Mail-Server**: Wählen Sie im Dropdown-Menü den E-Mail-Server aus, mit dem Sie das Ziel verbinden möchten.
5. Klicken Sie auf **Hinzufügen**

6. Die Liste der Ziele zeigt jetzt das Ziel, das Sie gerade hinzugefügt haben.

Ziel bearbeiten

1. Klicken Sie auf das Symbol **Ziel bearbeiten** neben dem Ziel, das Sie bearbeiten möchten

2. Das Popup-Fenster **Ziel bearbeiten** erscheint
3. Wählen Sie den Parameter aus, die Sie ändern wollen. Sie können alle Parameter ändern.
4. Klicken Sie auf **Speichern**

Die Liste zeigt nun die aktualisierten Parameter des geänderten Ziels an

Ziel kopieren

Sie können die Parameter eines Ziels kopieren, um ein neues mit einem anderen Namen zu erstellen

1. Klicken Sie auf das Symbol **Ziel kopieren** neben dem Ziel, das Sie kopieren möchten

2. Das Popup-Fenster **Ziel kopieren** erscheint
3. Ändern Sie den Namen des Ziels und die E-Mail-Adresse
4. Klicken Sie auf **Hinzufügen**, um das Ziel zu erstellen

Ziel löschen

1. Klicken Sie auf das Symbol **Ziel löschen** neben dem Ziel, das Sie löschen möchten

2. Das Popup-Fenster **Ziel löschen** erscheint
3. Klicken Sie auf **JA**, um das Ziel zu löschen oder auf **NEIN**, um das Löschen abzubrechen

Stichwörter