A MITEL
PRODUCT
GUIDE

Unify OpenScape Contact Center V11 R1

Web Manager V11 R1

Guide d’Administration de Web Manager

Guide d’Administration
09/2024

A31003-S22B1-M100-02-77A9

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.

Sommaire

1 A propos de ce guide 5
1.1 A qui ce guide est-il destiné? 5
1.2 Conventions de formats 5
1.3 Commentaires sur la documentation 6
2 Web Manager 7
2.1 Mise en route 7
2.2 Informations d'accès 7
3 Authentification unique à l'aide du protocole SAML2 9
4 Configuration de Single Sign-On avec Circuit 19
5 Agents virtuels 21
5.1 Configuration d'agents utilisateurs en tant qu'agents virtuels 26
5.2 Configuration d'actions pour les agents virtuels 26
5.2.1 Configuration d'une action de remise en file d'attente pour les agents virtuels 27
5.2.2 Configuration d'une action de rappel 28
5.2.3 Configuration d'une requête système externe pour les agents virtuels 28
5.2.4 Configuration d'une demande de poussée d'URL WebInteraction pour les agents virtuels 30
5.3 Configuration vocale pour les agents virtuels 30
5.4 À propos de l'intégration Dialogflow 31
6 REST SDK 33
7 CLIP pour les appels sortants 35
8 Plusieurs e-mails par client 37
Index 43

Sommaire

1 A propos de ce guide

Ce guide contient une vue d'ensemble de l'application OpenScape Contact Center Manager et présente aux utilisateurs les différentes tâches administratives devant être exécutées régulièrement.

1.1 A qui ce guide est-il destiné?

Ce guide est destiné aux administrateurs des centres de contacts, aux spécialistes de la maintenance de la configuration et aux superviseurs et responsables qui utilisent les outils de productivité de OpenScape Contact Center.

1.2 Conventions de formats

Les conventions de formats utilisées dans ce guide sont les suivantes :

Gras
Identifie les composants OpenScape Contact Center, les titres des fenêtres et des boîtes de dialogue et les noms d'éléments.

Italique
Cette police identifie les références à une documentation connexe.

`Police monospace`
Caractérise la police du texte que vous entrez ou que l'ordinateur affiche dans un message.

REMARQUE : Les remarques soulignent des informations qui sont utiles sans être essentielles, par exemple, des conseils ou d'autres méthodes pour exécuter une tâche.

IMPORTANT : Les remarques importantes sont destinées à attirer l'attention sur des actions qui pourraient entraver le bon fonctionnement de l'application ou entraîner une perte de données.

1.3 Commentaires sur la documentation

Pour signaler un problème avec ce document, veuillez appeler le centre de support clientèle.

Quand vous appelez, veuillez avoir l'obligeance d'inclure les informations suivantes. Ceci nous aidera à repérer le document qui vous pose problème.

- **Titre :** Guide d'Administration de Web Manager
- **Référence :** A31003-S22B1-M100-02-77A9

2 Web Manager

2.1 Mise en route

Web Manager est une application qui permet de configurer des fonctionnalités dans OpenScape Contact Center via un navigateur Web.

2.2 Informations d’accès

Web Manager est une application basée sur navigateur installée avec le pack du serveur d’application OpenScape Contact Center.

Pour accéder à Web Manager, vous devez disposer du profil d’administrateur central.

Web Manager permet de configurer les éléments suivants :

- authentification unique à l’aide du protocole SAML2 pour le Portail agent Web ;
- authentification unique avec Circuit pour le Portail agent Web ;
- Agents virtuels pour activer la fonctionnalité chatbot
- REST SDK
- Téléphonie

Pour accéder à Web Manager, ouvrez un navigateur et saisissez l’URL suivante :
https://<OSCC_ApplicationServer_hostname_or_ip>/webmanager

3 Authentification unique à l'aide du protocole SAML2

Security Assertion Markup Language (SAML) est un format de données ouvert à base XML destiné à l'échange de données d'identification et d'autorisation entre un fournisseur d'identité et un fournisseur de service.

La plupart des organisations connaissant déjà l'identité des utilisateurs connectés à leur domaine Active Directory ou à leur intranet, ces informations peuvent être utilisées pour connecter les utilisateurs SSO (*Single Sign On* ou authentification unique) aux applications OpenScape Contact Center. OpenScape Contact Center prend en charge le SAML dans la version 2.0 (SAML2).

NOTE: Le protocole SSO, via SAML2, n'est supporté que sur l'application en ligne du Portail agent Web. Ces configurations SSO ne s'appliquent pas à d'autres applications telles que le Portail agent Java, Client Desktop ou Manager Desktop utilisant des méthodes de connexion paramétrées dans Manager Desktop. Web Manager prend uniquement en charge la méthode de connexion OSCC.

La spécification SAML définit les rôles suivants :

- **Utilisateur** : ce rôle est affecté au navigateur Web, qui utilise l'URL pour exécuter l'application sur le serveur d'application.
- **Fournisseur de service** : ce rôle est affecté au serveur d'application, qui exécute l'application.

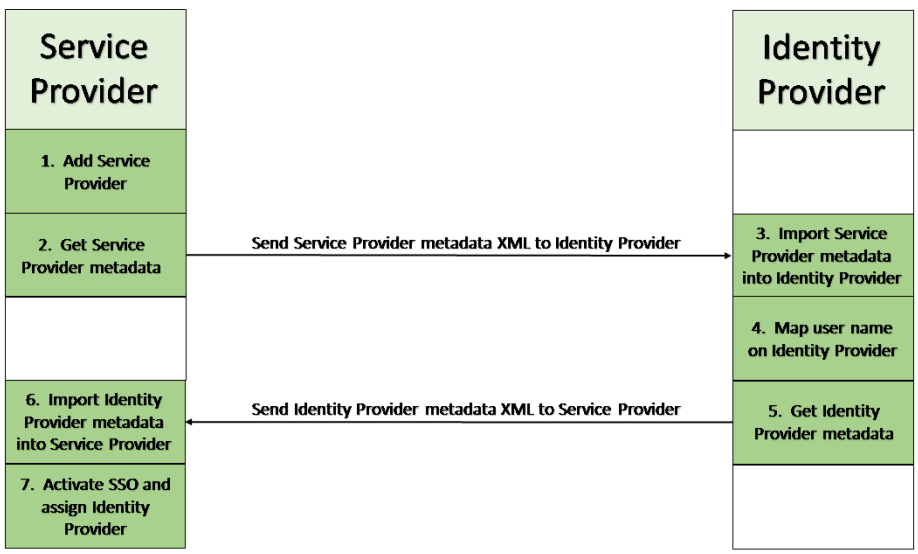
- **Fournisseur d'identité** : ce rôle est affecté à une entité système (autorité d'identification) permettant l'authentification de l'utilisateur.

NOTE: De nombreux fournisseurs d'identité, comme ADFS ou Gluu, peuvent être utilisés. Dans cet exemple, nous utilisons Active Directory Federation Services (ADFS) pour exposer les informations nécessaires à la configuration du SSO dans la solution OpenScape Contact Center. Ces mêmes informations doivent être extraites, quel que soit le fournisseur d'identité utilisé.

NOTE: ADFS est une solution SSO proposée par Microsoft. En tant que composante des systèmes d'exploitation Windows Server, elle fournit aux utilisateurs un accès authentifié aux applications en passant par Active Directory (AD).

NOTE: La fourniture d'identité est un service tiers qui n'est ni fourni ni pris en charge par Unify. De ce fait, les exemples de configuration ADFS mentionnés dans ce document peuvent être sujets à modifications.

Pour paramétrer le SSO dans l'application Web Manager, configurez le fournisseur de service du côté OSCC et le fournisseur d'identité de l'autre. La figure suivante illustre les différentes étapes de configuration :



1. Ajoutez un fournisseur de service

    1. Connectez-vous à l'application Web Manager avec le compte utilisateur de l'administrateur central ainsi que son mot de passe. Sélectionnez **Configuration de l'authentification**, puis **Fournisseur de service**.
    2. Cliquez sur **Ajouter un fournisseur de service**.

        - **URL de l'hôte** : l'URL du service Portail agent Web. Par exemple :

        `https://<ApplicationServer_hostname_or_ip>/agentportal`

        Cette valeur doit être la même URL que celle configurée dans le fichier de configuration XML du Portail agent Web. Pour la trouver, accédez à l'ordinateur sur lequel est installé le serveur d'application et ouvrez le fichier suivant dans le répertoire d'installation. Copiez ensuite le contenu de l'élément « service-provider-host-url » :
        `.\ApplicationServer\ApacheWebServer\conf\webagent.xml`

        - **Certificat** : valeur facultative pour le fournisseur de service. Elle vous permet d'insérer un certificat cryptant les messages envoyés au fournisseur d'identité.
        - **Clé publique** : valeur facultative pour la clé utilisée par le certificat pour valider l'authentification avec le fournisseur de service. Cette valeur doit être connue du fournisseur de service et du fournisseur d'identité.

NOTE: Pour OpenScape Contact Center, le fournisseur de service sera le Portail agent Web lui-même. Vous pouvez configurer plusieurs fournisseurs de services dans le système.

---

2. Obtenez les métadonnées des fournisseurs de service

Sans vous déconnecter de l'application Web Manager, récupérez les données du fournisseur de service et importez-les dans le fournisseur d'identité

1. Survolez le nom du fournisseur de service que vous avez ajouté et cliquez sur **Obtenir les métadonnées**
2. Cliquez sur **Copier dans le presse-papiers**, enregistrez le contenu dans un fichier texte sur votre ordinateur et renommez-le avec une extension « xml ». Choisissez un nom de fichier qui vous permet d'afficher clairement qu'il contient les métadonnées du fournisseur de service, par exemple :
`OSCC_<customer>_metadata.xml`

3. Importez les métadonnées du fournisseur de service dans le fournisseur d'identité

   Vous devez ajouter le fournisseur de service en tant que partie utilisatrice du fournisseur d'identité en important ses métadonnées. Transférez le fichier XML créé à l'étape 2) à un emplacement auquel le fournisseur d'identité peut avoir accès et connectez-vous à ce dernier.

   L'exemple ci-dessous montre comment les métadonnées du fournisseur de service sont importées dans l'Active Directory Federation Service (ADFS) de Microsoft :

   1. Dans la console de gestion ADFS, naviguez jusqu'au dossier :
      Relations de confiance > Parties utilisatrices de confiance
   2. Cliquez sur **Ajouter une partie utilisatrice de confiance**
   3. L'écran de l'**assistant Ajouter une partie utilisatrice de confiance** s'affiche. Cliquez sur **Démarrer**
   4. Sélectionnez **Importer des données concernant la partie utilisatrice à partir d'un fichier**, puis le fichier XML créé à l'étape 2). Utilisez **Parcourir...** pour trouver le fichier.
   5. Cliquez sur **Suivant**
   6. Indiquez le nom de votre choix dans le champ **Nom d'affichage**
   7. Cliquez sur **Suivant**
   8. Sélectionnez **Autoriser tous les utilisateurs à accéder à cette partie utilisatrice**
   9. Cliquez sur **Suivant**
   10. Cliquez sur **Fermer**

Ajoutez une règle de réclamation pour la partie utilisatrice de confiance créée à l'étape 3).

Les règles de réclamation sont utilisées pour associer un type de réclamation entrant à un type de réclamation sortant. Dans la règle de réclamation, spécifiez le champ de la base de données utilisateur du fournisseur d'identité correspondant au nom de l'utilisateur OSCC.

1. Dans la Console de gestion ADFS, sélectionnez les parties utilisatrices de confiance créées et cliquez sur **Modifier les règles de réclamation...**
2. Cliquez sur **Ajouter une règle...** pour ouvrir l'assistant des règles de réclamation.
3. Dans le menu déroulant de la fenêtre **Sélectionner un modèle de règle**, choisissez **Utiliser les attributs LDAP envoyés comme règles de réclamation**.

   NOTE: Dans l'exemple suivant, le nom d'utilisateur OSCC est authentifié à l'aide du protocole LDAP.

4. Cliquez sur **Suivant**
5. **Associez les attributs LDAP aux types de réclamations sortants** (Active Directory) qui seront utilisés pour l'authentification SAML

   NOTE: Dans cet exemple, le nom d'utilisateur OSCC, qui est configuré dans le serveur LDAP (Active Directory), est associé au nom du compte Windows. Dans le cas de l'ADFS, le mappage de l'ID du nom est également requis.

6. Cliquez sur **Terminer**

4. Obtenez les métadonnées du fournisseur d'identité

   Après avoir configuré le fournisseur d'identité, importez ses métadonnées dans le fournisseur de service.

   Comme on peut le voir dans le répertoire Endpoints de la console de gestion ADFS, les métadonnées sont accessibles sur :

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

5. Importez les métadonnées du fournisseur d'identité dans le fournisseur de services

   1. Connectez-vous à l'application Web Manager à l'aide des informations d'identification de l'administrateur central. Sélectionnez **Configuration de l'authentification**, puis **Fournisseur d'identité**.

      Vous pouvez ajouter un fournisseur d'identité manuellement en sélectionnant **Ajouter un fournisseur d'identité** ou automatiquement en choisissant **Importer des métadonnées**.

Il est recommandé d'utiliser l'importation automatique. Transférez le fichier XML créé à l'étape 5 à un emplacement auquel le fournisseur de service peut avoir accès.

Si vous optez pour l'ajout manuel, cliquez sur **Ajouter un fournisseur d'identité**

NOTE: Toutes les configurations peuvent être récupérées dans le fichier de métadonnées du fournisseur d'identité.

- **ID de l'entité** : identifiant de l'entité Fournisseur d'identité (doit être une URL). Dans les métadonnées, on trouve cette URL en recherchant l'attribut **entityID**, dans la balise **EntityDescriptor**.
- **URL SSO** : informations d'authentification unique du fournisseur d'identité. Il s'agit de l'URL cible du fournisseur d'identité auquel le fournisseur de service envoie le message de demande d'authentification. Dans les métadonnées, cette URL se situe dans l'étiquette **IDPSSODescriptor**, que vous trouverez en recherchant l'attribut **Emplacement**, dans l'étiquette **SingleSignOnService**.

NOTE: Utilisez la valeur **Emplacement** de la ligne affichant la valeur « **...HTTP-POST** » dans l'attribut **Association**.

- **Correspondance du nom d'utilisateur** : Il s'agit du paramètre, renvoyé par le fournisseur d'identité, qui sera comparé à l'utilisateur OSCC configuré.

Dans les métadonnées, par exemple dans l'ADFS, le **Nom du compte Windows** a été sélectionné en tant que **Type de réclamation sortante** (voir l'étape 4, **Associer le nom d'utilisateur au fournisseur d'identité, Règles d'ajout**). Quand vous recherchez la valeur **Nom du compte Windows** dans le fichier de métadonnées, la valeur **Correspondance du nom d'utilisateur** peut être trouvée sous l'attribut **Nom**. Dans cet exemple :

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

En règle générale, la valeur du paramètre **Correspondance du nom d'utilisateur** doit correspondre au Type de réclamation sortant configuré pour le mappage des attributs SAML LDAP dans le fournisseur d'identité, voir étape 4) **Association des**

attributs LDAP sortants aux types de réclamations. Il s'agit de la valeur du paramètre LDAP utilisé par l'ADFS pour identifier (faire correspondre) l'utilisateur OSCC.

NOTE: Les autres fournisseurs d'identité auront un nom d'utilisateur différent.

- **URL du service de déconnexion unique** : emplacement de l'URL du fournisseur d'identité auquel le fournisseur de service enverra la Requête de déconnexion unique (SLO). Dans les métadonnées, cette URL se situe dans l'étiquette **IDPSSODescriptor**, que vous trouverez en recherchant l'attribut **Emplacement** dans l'étiquette **SingleLogoutService**.

NOTE: Utilisez la valeur **Emplacement** de la ligne affichant la valeur « **...HTTP-POST** » dans l'attribut **Association**.

- **URL de réponse du service de déconnexion unique** : emplacement de l'URL du fournisseur d'identité auquel le fournisseur de services enverra la Réponse de déconnexion unique (SLO). Cette valeur est facultative et est généralement laissée vide. Si vous choisissez de procéder ainsi, l'URL utilisée pour envoyer la réponse SLO au fournisseur d'identité sera la même que celle du **service de déconnexion unique** employée pour la requête. Certains fournisseurs d'identité utilisent des URL séparées pour envoyer les demandes et les réponses de déconnexion et se servent de cette propriété pour définir une URL de réponse distincte.
- **Certificat x509** : le certificat x509 public du fournisseur d'identité. Dans les métadonnées, vous trouverez la valeur de ce certificat en recherchant l'étiquette **X509Certificate**, dans l'étiquette **IDPSSODescriptor**, puis dans **KeyDescriptor** avec l'attribut **use="signing".**

NOTE: Lorsque vous saisissez un certificat manuellement, vérifiez qu'il comporte uniquement la ligne de hachage ; supprimez les commentaires et les lignes supplémentaires avant ou après.

- **Certificat empreinte digitale** : plutôt que de recourir au certificat x509 complet, vous pouvez utiliser une empreinte digitale. Dans ce cas, l'algorithme d'empreinte est nécessaire pour qu'OSCC sache quel algorithme a été utilisé. Voici les valeurs possibles : SHA1, SHA256, SHA384, SHA512.

Si vous décidez d'ajouter un fournisseur d'identité en important ses métadonnées, cliquez sur **Importer à partir des métadonnées**. Il est recommandé d'utiliser cette méthode pour configurer le fournisseur d'identité.

- **Correspondance du nom d'utilisateur** : il s'agit du paramètre, renvoyé par le fournisseur d'identité, qui permettra la comparaison avec l'utilisateur OSCC configuré.

Dans les métadonnées, par exemple dans l'ADFS, le **Nom du compte Windows** a été sélectionné en tant que **Type de réclamation sortante** (voir l'étape 4, **Associer le nom d'utilisateur au fournisseur d'identité, Règles d'ajout**). Quand vous recherchez la valeur **Nom du compte Windows** dans le fichier de métadonnées, la valeur **Correspondance du nom d'utilisateur** peut être trouvée sous l'attribut **Nom**. Dans cet exemple :

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

En règle générale, la valeur du paramètre **Correspondance du nom d'utilisateur** doit correspondre au Type de réclamation sortant configuré pour le mappage des attributs SAML LDAP dans le fournisseur d'identité, voir étape 4) **Association des attributs LDAP sortants aux types de réclamations**. Il s'agit de la valeur du paramètre LDAP utilisé par l'ADFS pour identifier (faire correspondre) l'utilisateur OSCC.

NOTE: Les autres fournisseurs d'identité auront un nom d'utilisateur différent.

Après avoir rempli la **Correspondance du nom d'utilisateur**, cliquez sur **Télécharger les métadonnées**, puis sur **Choisir le fichier** et sélectionnez le fichier de métadonnées désiré. Cliquez sur **Ajouter**.

Une autre solution consiste à sélectionner Saisir les métadonnées et à modifier ou copier/coller les métadonnées dans le champ **Contenu des métadonnées**. Cliquez sur **Ajouter**

6. Activez le protocole SSO et assignez le fournisseur d'identité

1. Après avoir importé les métadonnées du fournisseur d'identité dans le fournisseur de service, sans vous déconnecter de l'application Web Manager, cliquez sur l'onglet **Client** (Tenant).
2. Vous y trouverez probablement une liste des **Clients**. Survolez le nom du client et cliquez sur **Modifier**.
3. Dans la fenêtre **Configurer le client**, activez ou désactivez les fonctionnalités **Authentification unique** et **Déconnexion unique** :
   - **Authentification unique** : active l'intégration SAML2
   - **Fournisseur d'identité** : sélectionnez le fournisseur d'identité précédemment configuré dans l'onglet Fournisseur d'identité de l'étape 6
   - **Déconnexion unique (SLO)** : lorsque cette option est activée, le système se déconnecte du serveur du fournisseur d'identité lorsque vous mettez fin à votre connexion et l'utilisateur est déconnecté de toutes les autres applications utilisant le même fournisseur d'identité.

NOTE: Lorsque vous configurez OpenScape Contact Center pour un environnement Monosociété, la fonctionnalité SSO via SAML2 opère à l'échelle du système. Lorsque vous configurez OpenScape Contact Center pour un environnement Multisociétés, le SSO via SAML2 peut être activé pour chaque client. Dans ce cas, quand le SSO via SAML2 n'est pas activé, les méthodes de connexion configurées dans Manager Desktop peuvent être appliquées.

Une fois la configuration de l'authentification unique terminée, démarrez le navigateur Web, connectez-vous au Portail agent Web et tapez :

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

Lors de la première authentification dans cette session du navigateur, vous serez redirigé vers le fournisseur d'identité.

1. Entrez les expressions <utilisateur>@<domaine> ou <domaine>\<utilisateur>, dans lesquelles :
   - <domaine> représente le nom de domaine du client

- <utilisateur>désigne l’utilisateur configuré dans Active Directory (Nom du compte)

  NOTE: <user> doit également être configuré en tant qu’utilisateur dans OpenScape Contact Center

- Entrez le mot de passe Active Directory.

Lorsqu’une autre authentification (connexion) a lieu dans la même session du navigateur, le SSO est exécuté et il n’est pas nécessaire de saisir de nouveau les identifiants de compte ainsi que le mot de passe.

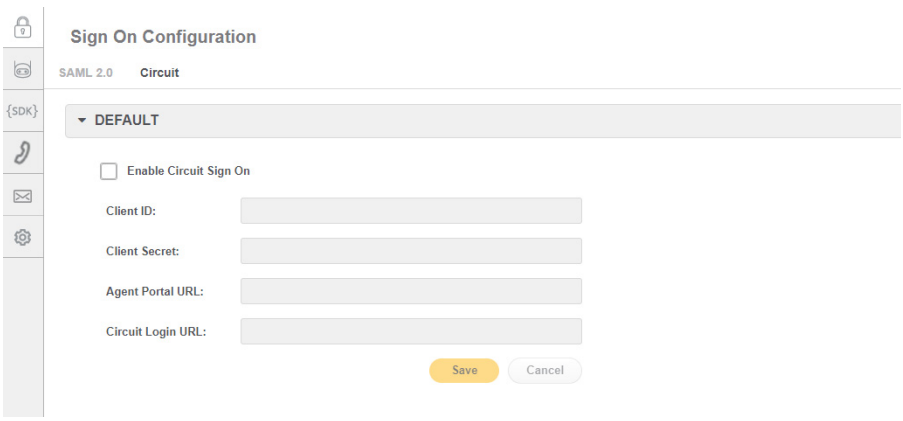
4 Configuration de Single Sign-On avec Circuit

Une fois la configuration de l'application personnalisée sur Circuit terminée (cf. le *Guide d'intégration des plates-formes de communication OpenScape Contact Center V10*), il est nécessaire de synchroniser l'identifiant client et les informations secrètes client à l'aide d'OpenScape Contact Center.

Accédez à l'application Web Manager de l'OSCC et connectez-vous avec un compte de responsable de client. Dans « Configuration de l'authentification », sélectionnez l'onglet « Circuit » et le client OSCC qui a accès à la fonctionnalité d'intégration de Circuit.

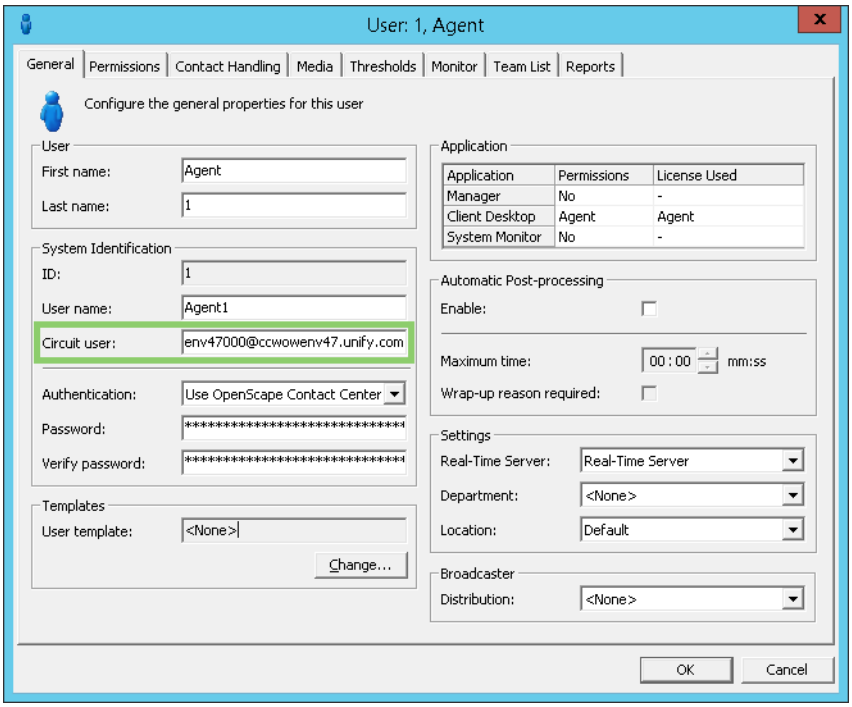
Remplissez les champs ci-dessous avec les informations suivantes :

- **Activer Circuit Sign-on** - activé.
- **Identifiant client** : L'identifiant unique de l'application, obtenu au chapitre précédent.
- **Clé secrète client** : La clé secrète de l'application, obtenue au chapitre précédent.
- **URL de l'Agent Portal** : L'URL utilisée pour accéder à l'application de l'Agent Portal Web. Suivez le modèle de https://<yourDomain>/agentportal
- **URL de connexion à Circuit** : L'URL utilisée pour accéder à l'application Circuit.



Quand vous utilisez l'authentification Circuit pour vous identifier sur la page de connexion d'OpenScape Contact Center, il est nécessaire d'associer un compte Circuit à l'utilisateur d'OpenScape Contact Center. Le nom utilisateur de Circuit (URI) est utilisé pour l'association.

Dans la fenêtre de configuration de l'utilisateur, remplissez le champ Utilisateur Circuit avec l'URI utilisé pour vous connecter à Circuit. Deux utilisateurs d'OSCC dans le même client ne peuvent pas partager le même utilisateur Circuit.



NOTE: Lorsque Circuit est uniquement accessible par l'intermédiaire d'un serveur proxy HTTPS, une configuration spéciale est requise dans le serveur d'application. Pour plus d'informations sur la configuration, veuillez consulter le *Guide d'installation OpenScape Contact Center V10*

NOTE: Pour plus d'informations sur la configuration d'OpenScape Voice et l'ajout d'une application sur Circuit, veuillez consulter le *Guide d'intégration des plates-formes de communication OpenScape Contact Center V10*.

5 Agents virtuels

L’administrateur central doit se connecter au Web Manager pour configurer des agents virtuels dans OpenScape Contact Center.

La fonctionnalité Agent virtuel permet d’intégrer OpenScape Contact Center à un processeur de langage naturel (NLP) pour inclure des chatbots.

Le service d’agent virtuel est exécuté dans le conteneur de serveur d’application OSCC et connectera tous les agents configurés dans le Web Manager.

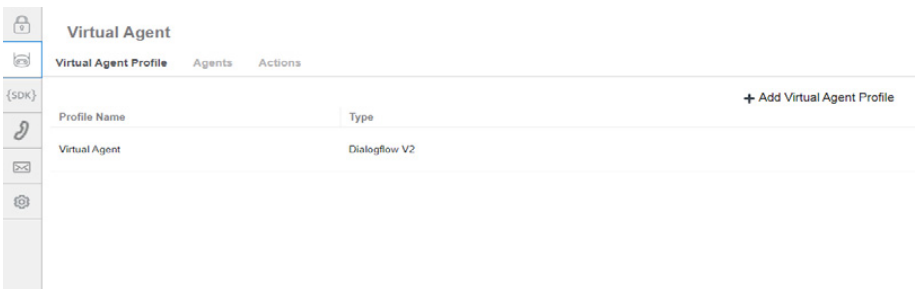
NOTE: L’agent virtuel prend seulement en charge le type de mot de passe OpenScape Contact Center. Le système ne fonctionnera pas avec la connexion Windows ou SSO SAML2.

NOTE: La fonctionnalité d’agent virtuel est une configuration s’appliquant à l’ensemble du SYSTÈME. Si la fonction Multisociétés est activée dans OpenScape Contact Center, chaque locataire exige un ou plusieurs CMS déployés pour fournir le support vocal. Chaque CMS peut prendre en charge un ou plusieurs profils d’agent virtuel. Chaque profil doit être configuré avec un autre jeton GCP. Sur le serveur d’application OSCC, le fichier de configuration `virtualagent.xml` doit porter le bon nom d’unité opérationnelle.

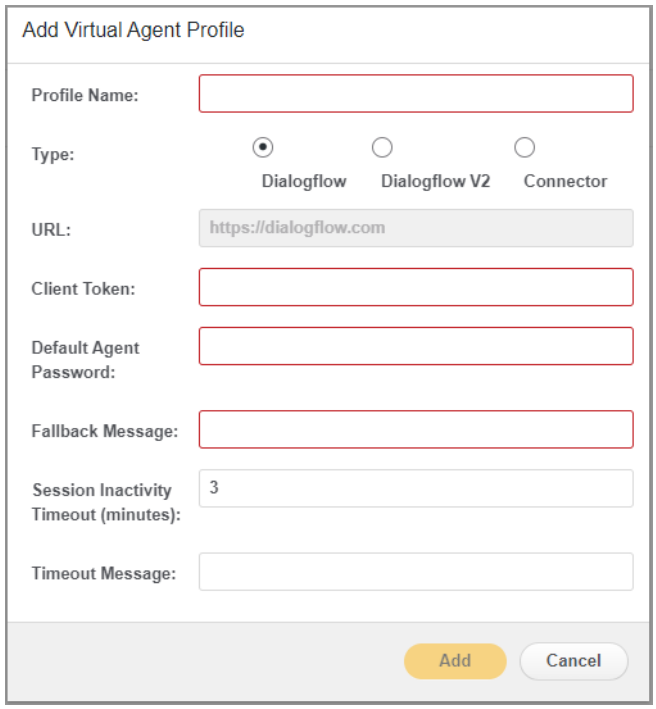
NOTE: Le **suivi-activité automatique** et le **motif de post-traitement obligatoire** ne sont pas pris en charge par l’agent virtuel. Veillez à ce que ces fonctionnalités soient désactivées dans la configuration de l’utilisateur.

Connectez-vous à Web Manager et suivez les étapes ci-après :

- Allez à l’onglet **Agent virtuel** :



- Cliquez sur **Ajouter un profil d'agent virtuel**. La fenêtre **Ajouter un profil d'agent virtuel** s'affiche. Voici le formulaire pour la configuration de profil NLP :



  - **Nom du profil** : Il s'agit d'un champ obligatoire. Le nom du profil NLP d'agent virtuel
  - **Type** : Type de profil d'agent virtuel. Vous pouvez sélectionner l'un des boutons suivants :
    - Dialogflow
    - Dialogflow V2
    - Connecteur

  Selon le type sélectionné, vous devez configurer différents paramètres.

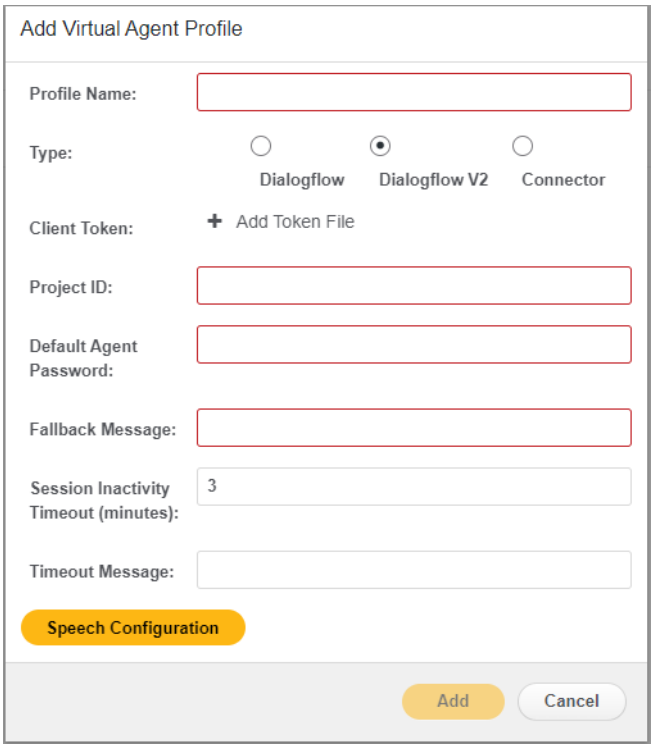
  Type : Dialogflow

  - **URL** : L'URL du moteur Dialogflow. La valeur par défaut est https://dialogflow.com
  - **Jeton de client** : Le jeton de client fourni par Dialogflow

- **Mot de passe d'agent par défaut** : Le mot de passe configuré dans le gestionnaire pour les utilisateurs configurés comme agents virtuels. Important pour utiliser le même mot de passe pour toutes les configurations d'utilisateur d'agent virtuel
- **Message de secours** : Il s'agit d'un message de secours du système. Si une erreur se produit sur le système, ce message sera envoyé en externe pour la personne qui a contacté le centre de contact
- **Délai d'inactivité de session** : Si la session actuelle du contact n'est pas active, le système met fin à la session automatiquement selon la durée configurée en minutes
- **Message d'expiration** : Il s'agit du message envoyé une fois que le délai d'inactivité de la session est écoulé

Type : Dialogflow V2

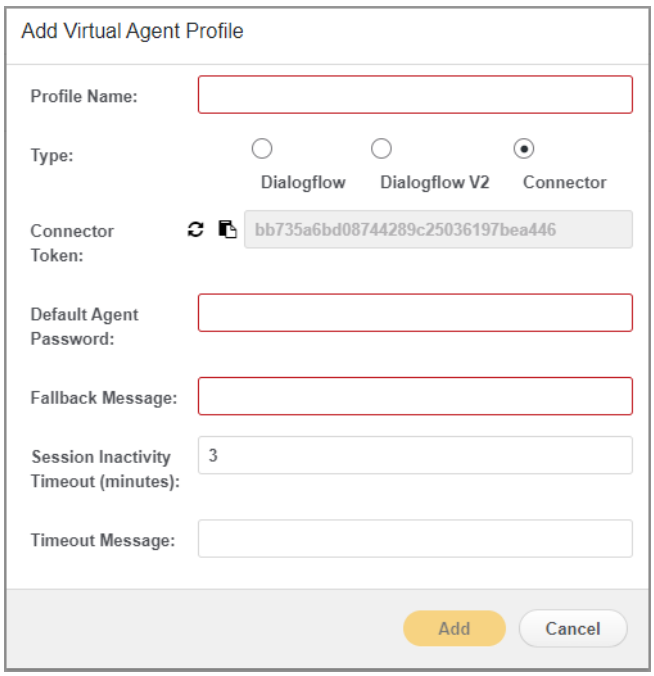
La fenêtre **Ajouter un profil d'agent virtuel** contient le formulaire suivant pour la configuration de profil NLP :



- **Jeton de client** : Cliquez sur **Ajouter un fichier jeton** et naviguez sur votre PC pour trouver le fichier de jeton (fichier *.json) que vous souhaitez utiliser
- **ID du projet** : L'ID du projet
- **Mot de passe d'agent par défaut** : Il s'agit d'un champ obligatoire. Le mot de passe configuré dans le gestionnaire pour les utilisateurs configurés comme agents virtuels. Important pour utiliser le même mot de passe pour toutes les configurations d'utilisateur d'agent virtuel
- **Message de secours** : Il s'agit d'un champ obligatoire. Il s'agit d'un message de secours du système. Si une erreur se produit sur le système, ce message sera envoyé en externe pour la personne qui a contacté le centre de contact
- **Délai d'inactivité de session** : Si la session actuelle du contact n'est pas active, le système met fin à la session automatiquement selon la durée configurée en minutes
- **Message d'expiration** : Il s'agit du message envoyé une fois que le délai d'inactivité de la session est écoulé
- **Configuration vocale** : Ce bouton vous permet de configurer le Speechbot

Type : Connecteur

La fenêtre **Ajouter un profil d'agent virtuel** contient le formulaire suivant pour la configuration de profil NLP

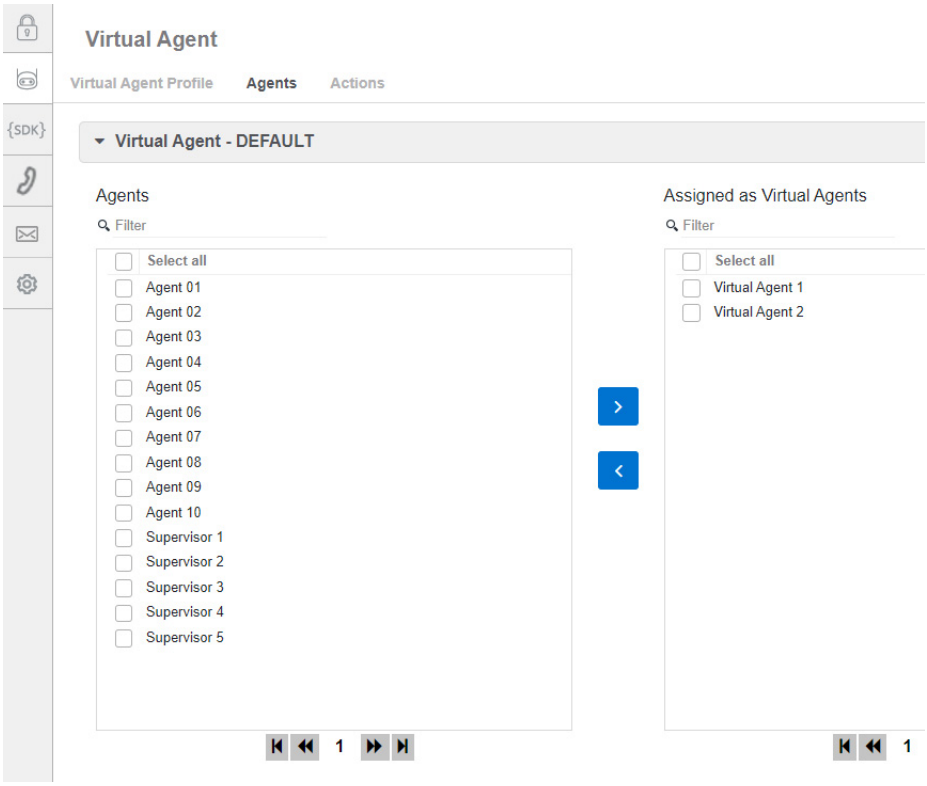


- **Jeton de connecteur** : Cliquez sur le bouton **Recharger** pour générer un nouveau jeton. Le nouveau jeton de connecteur est affiché dans le champ grisé. Cliquez sur le bouton **Presse-papier** pour copier le jeton dans le presse-papier
- **Mot de passe d'agent par défaut** : Il s'agit d'un champ obligatoire. Le mot de passe configuré dans le gestionnaire pour les utilisateurs configurés comme agents virtuels. Important pour utiliser le même mot de passe pour toutes les configurations d'utilisateur d'agent virtuel
- **Message de secours** : Il s'agit d'un champ obligatoire. Il s'agit d'un message de secours du système. Si une erreur se produit sur le système, ce message sera envoyé en externe pour la personne qui a contacté le centre de contact
- **Délai d'inactivité de session** : Si la session actuelle du contact n'est pas active, le système met fin à la session automatiquement selon la durée configurée en minutes
- **Message d'expiration** : Il s'agit du message envoyé une fois que le délai d'inactivité de la session est écoulé

5.1 Configuration d’agents utilisateurs en tant qu’agents virtuels

Pour les agents virtuels, il est nécessaire d’associer des utilisateurs à un profil d’agent enregistré dans OSCC.

Pour attribuer des utilisateurs, accédez à l’onglet **Agents** et développez la vue de profil :



NOTE: Il existe des filtres pour vous aider quant au choix des utilisateurs d’agent dans le système.

5.2 Configuration d’actions pour les agents virtuels

La fonctionnalité d’agent virtuel peut traiter certaines actions reçues de la part du processeur NLP.

Une action est généralement une chaîne de texte envoyée par le processeur NLP avec un ensemble de paramètres.

Il existe plusieurs actions possibles :

- **Action de remise en file d'attente** : Permet au système de transférer l'agent virtuel à une personne en replaçant le contact vers une autre file d'attente.
- **Action de rappel** : Permet au système de transférer l'agent virtuel à une personne en créant un rappel téléphonique sur OSCC.
- **Demande de système externe** : Permet au système d'envoyer une requête à d'autres systèmes pour aider la solution à répondre plus élégamment aux clients.
- **Poussée d'URL WebInteraction** : Permet au système d'envoyer une requête à d'autres adresses URL pour aider la solution à répondre plus élégamment aux clients.
- **Remise en file d'attente vocale** : Action pour sélectionner la destination de remise en file d'attente

5.2.1 Configuration d'une action de remise en file d'attente pour les agents virtuels

5.2.1.1 Action de remise en file d'attente OpenMedia

Pour configurer une action de remise en file d'attente OpenMedia, sélectionnez le type de média **OpenMedia** et définissez :

- **Nom de l'action** : Valeur de texte qui doit être égale à l'action reçue par le système NLP. (Obligatoire)
- **File de remise en file d'attente** : La file d'attente utilisée pour remettre le contact en file d'attente. Il s'agit d'un champ obligatoire. Sélectionnez une valeur dans la liste et cliquez sur **Ajouter**.

5.2.1.2 Action de remise en file d'attente WebInteraction

Pour configurer une action de remise en file d'attente WebInteraction, sélectionnez le type de média **WebInteraction** et définissez :

- **Nom de l'action** : Valeur de texte qui doit être égale à l'action reçue par le système NLP. (Obligatoire)
- **File de remise en file d'attente** : La file d'attente utilisée pour remettre le contact en file d'attente. Il s'agit d'un champ obligatoire. Sélectionnez une valeur dans la liste et cliquez sur **Ajouter**.

5.2.1.3 Action de remise en file d’attente vocale

Pour configurer une action de remise en file d’attente vocale, sélectionnez le type de média **Vocale** et définissez :

- **Nom de l’action** : Valeur de texte qui doit être égale à l’action reçue par le système NLP. (Obligatoire)
- **Destination de remise en file d’attente** : La cible utilisée pour remettre le contact en file d’attente. Il s’agit d’un champ obligatoire. Sélectionnez une valeur dans la liste et cliquez sur **Ajouter**.

5.2.2 Configuration d’une action de rappel

Pour configurer une action de rappel, sélectionnez **Action de rappel** comme type d’action et définissez :

- **Nom de l’action** : Valeur de texte qui doit être égale à l’action reçue par le système NLP. (Obligatoire)
- **File d’attente de rappels** : La file d’attente utilisée pour créer le rappel. (Obligatoire)
- **Nom du paramètre de téléphone** : Le nom du paramètre pour obtenir le numéro de téléphone du système NLP. (Obligatoire)
- **Nom du paramètre de temps de planification** : Le nom du paramètre pour obtenir la date et l’heure de la planification des rappels. (Obligatoire)

5.2.3 Configuration d’une requête système externe pour les agents virtuels

Pour configurer une action de requête système externe, sélectionnez **Demande de système externe** comme type d’action et définissez :

- **Nom de l’action** : Valeur de texte qui doit être égale à l’action reçue par le système NLP. (Obligatoire)
- **Paramètres de l‘URI du système externe** : Un nom de paramètre défini par le système NLP qui contient l’adresse URI à laquelle le système d’agent virtuel doit envoyer la requête. (Obligatoire)

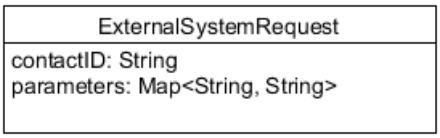
5.2.3.1 Détails concernant la requête système externe

La fonctionnalité de requête système externe est un client d'interface REST, implémenté dans le service d'agent virtuel.

Chaque fois que l'agent virtuel reçoit une action pour effectuer une consultation externe de NLP, le système envoie une requête POST à l'URI défini dans le paramètre avec un objet JSON prédéfini.

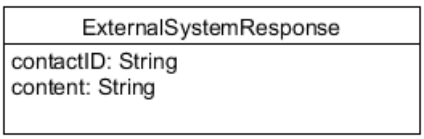
Il existe deux objets JSON : l'un pour la requête et l'autre pour la réponse.

L'objet de requête envoyé par l'agent virtuel est le suivant :



- **contactID** : L'attribut contenant la valeur de l'ID de contact OSCC
- **parameters**: Ensemble de paramètres reçus du processeur NLP composé par un texte clé/valeur. Ces paramètres seront traités par le système externe

L'objet de réponse reçu par l'agent virtuel doit avoir la structure suivante :



- **contactID** : Cette valeur doit être la même que pour l'objet ExternalSystemRequest. (Obligatoire)
- **content**: Texte traité par le système externe avec le contenu de réponse de la demande.

5.2.4 Configuration d'une demande de poussée d'URL WebInteraction pour les agents virtuels

Pour configurer une demande de poussée d'URL WebInteraction, sélectionnez **Poussée d'URL** comme type d'action et définissez :

- **Nom de l'action** : Valeur de texte qui doit être égale à l'action reçue par le système NLP. (Obligatoire)
- **Paramètre Poussée d'URL** : Un nom de paramètre défini par le système NLP qui contient l'adresse URL à laquelle le système d'agent virtuel doit envoyer la requête. (Obligatoire)

5.3 Configuration vocale pour les agents virtuels

La fonction d'agent virtuel vous permet de configurer un speechbot à l'aide du bouton **Configuration vocale**, vous permettant de configurer les paramètres suivants. Ce bouton est uniquement disponible pour le type de profil d'agent virtuel Dialog V2.

- **Activer la voix** : Paramètre permettant d'activer le speechbot pour le profil sélectionné. Valeur par défaut : désactivé
- **Adresse CMS** : Adresse IP/FQDN pour accéder au nœud CMS.
- **Port CMS** : Port pour accéder au nœud CMS. Valeur par défaut : 6017
- **Langue** : La langue à utiliser. Valeur par défaut : EN-US
- **Homme/Femme** : Le sexe de la voix utilisée. Valeur par défaut : Homme
- **Message de bienvenue** : Message à lire lorsque l'appel reçoit une réponse de l'agent virtuel Speechbot.
- **Numéro de remise en file d'attente de secours** : Numéro vers lequel l'appel est acheminé si le CMS n'est pas joignable.

5.4 À propos de l'intégration Dialogflow

La fonctionnalité d'agent virtuel est intégrée par défaut au moteur Dialogflow pour le processeur de langage naturel.

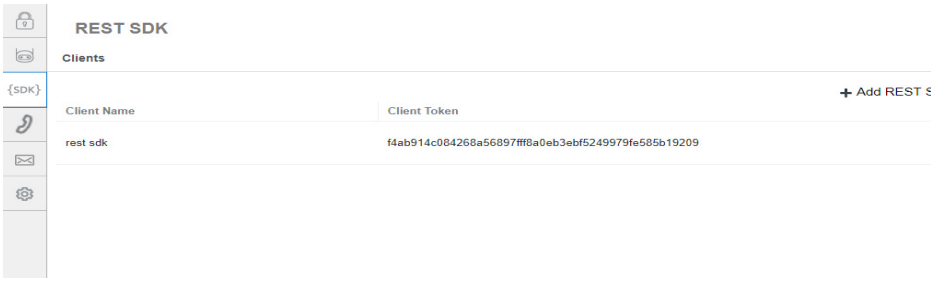
NOTE: Le processeur NLP par défaut pour l'agent virtuel est le Dialogflow de Google. Pour plus d'informations, suivez ce lien : https://dialogflow.com

---

- **Dialogflow Standard Edition** est disponible gratuitement sur la page web de Dialogflow. Il offre les mêmes fonctionnalités que Dialogflow Enterprise Edition mais les interactions sont limitées par des quotas d'utilisation et l'assistance est assurée par la communauté et par e-mail. Dialogflow Standard Edition est idéal pour les petites et moyennes entreprises qui veulent créer des interfaces de conversation ou pour les personnes qui veulent essayer Dialogflow.
- **Dialogflow Enterprise Edition** est disponible au sein de Google Cloud Platform (GCP) et fournit des interactions de texte et vocales illimitées, des quotas d'utilisation de volume plus élevés et une assistance du support Google Cloud. Dialogflow Enterprise Edition est une offre premium, disponible sous forme de service à la carte. Dialogflow Enterprise Edition est idéal pour les entreprises ayant besoin de services de niveau professionnel pouvant facilement évoluer pour s'adapter aux changements dans la demande des utilisateurs.

Pour plus d'informations sur les quotas, veuillez vous reporter à la page suivante :
https://cloud.google.com/dialogflow-enterprise/quotas

6 REST SDK



Le cadre REST SDK permet le développement d'applications multimédia qui s'intègrent au système OpenScape Contact Center.

Le cadre consiste en une interface REST, qui permet d'envoyer des commandes de l'application à OpenScape Contact Center et des événements de surveillance d'OpenScape Contact Center à l'application.

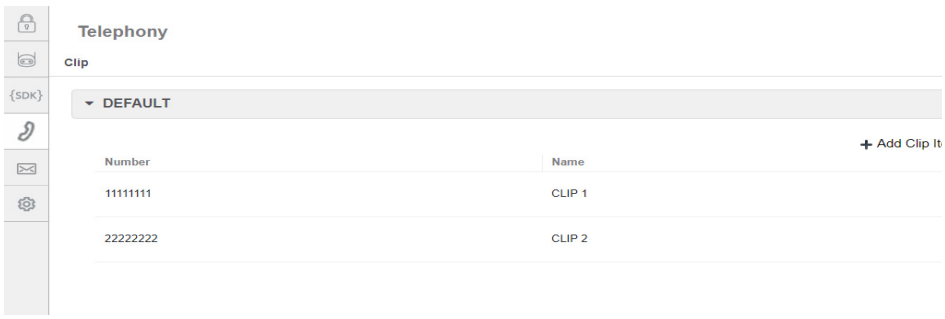
Configuration

Configurez les instances REST SDK en utilisant le Web Manager. Pour créer une nouvelle instance REST SDK :

1. Sélectionnez l'onglet **REST SDK**
2. Cliquez sur **+ Ajouter un client REST SDK**
3. Une fenêtre contextuelle **Ajouter un client REST SDK** apparaît. Configurez les paramètres suivants :
   - **Nom du client** : Le nom du client identifie de manière unique l'instance REST SDK en une chaîne de 32 caractères maximum.
   - **Jeton du client** : Le jeton client est un type de mot de passe utilisé pour authentifier le client REST SDK pendant le processus d'enregistrement du client sur le serveur. Le jeton client peut être configuré manuellement ou généré automatiquement.

     Cliquez sur le bouton **Recharger** pour générer automatiquement un nouveau jeton client aléatoire de 64 octets. Le nouveau jeton client apparaît dans le champ grisé. Cliquez sur le bouton **Presse-papiers** pour copier le jeton dans le presse-papiers.
   - Cliquez sur **Ajouter**
4. Le nouveau client REST SDK a été créé.

7 CLIP pour les appels sortants



Dans le Portail agent Web, la présentation de la ligne appelante (CLIP) correspond à l'identification de la ligne appelante utilisée pour les appels sortants. La fonctionnalité CLIP n'affecte pas la fonctionnalité de rappel en vigueur concernant la définition du numéro de l'appelant. Une liste de numéros appelants doit être configurée par client. La fonctionnalité CLIP est valable pour tous les appels sortants : à partir du bouton Passer un appel, de la Liste de numérotation rapide, de la Recherche de répertoire et du Journal d'activité.

Vous pouvez configurer la fonctionnalité CLIP pour les appels sortants en utilisant le Web Manager.

Ici, vous pouvez ajouter/modifier/supprimer le(s) numéro(s) appelant(s) pour la fonctionnalité CLIP.

Ajout d'un nouveau numéro

1. Cliquez sur l'onglet **Téléphonie**
2. Cliquez sur le menu déroulant **Défaut**, qui est le client par défaut
3. Cliquez sur **Ajouter un élément CLIP**. Vous pouvez ajouter jusqu'à dix numéros par client
4. Une fenêtre contextuelle intitulée **Ajouter un élément CLIP** apparaît. Configurez les paramètres suivants :
   - **Numéro** : Numéro appelant. Doit comporter une chaîne de chiffres et aucun caractère spécial. Ce champ est obligatoire
   - **Nom** : Nom de l'appelant. Ce champ est obligatoire
5. Cliquez sur **Ajouter**

La liste des numéros CLIP indique maintenant le numéro que vous venez d'ajouter. Ce numéro apparaît également dans les numéros disponibles dans la fonctionnalité CLIP du Portail agent Web dans : **Paramètres > Agent > CLIP > Toujours utiliser cette valeur**

Modification d’un numéro

1. Cliquez sur l’icône **Modifier un élément CLIP** à côté du numéro CLIP que vous souhaitez modifier

2. La fenêtre contextuelle **Modifier un élément CLIP** apparaît
3. Vous pouvez modifier le **numéro** et/ou le **nom** du numéro appelant existant
4. Cliquez sur **Mettre à jour**

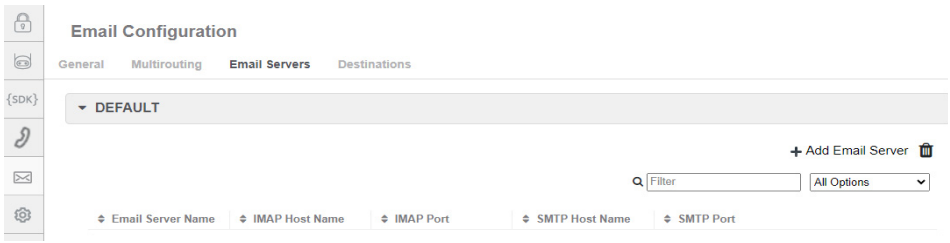
La liste indique maintenant le numéro et/ou le nom CLIP mis à jour

Suppression d’un numéro

1. Cliquez sur l’icône **Supprimer un élément CLIP** à côté du numéro CLIP que vous souhaitez supprimer

2. La fenêtre contextuelle **Supprimer un élément CLIP** apparaît
3. Cliquez sur **OK** pour supprimer le numéro CLIP ou sur **Annuler** pour interrompre la suppression

8 Plusieurs e-mails par client



Cette fonctionnalité permet à chaque unité opérationnelle d'avoir plusieurs serveurs e-mail ou adresses e-mail. Vous pouvez configurer les destinations et les serveurs e-mail par le biais du Web Manager.

NOTE: Chaque unité opérationnelle prend en charge jusqu'à cinq identifiants de messagerie configurés.

Ajout d'un nouveau serveur e-mail

1. Cliquez sur l'onglet **Configuration de messagerie**
2. Cliquez sur l'onglet **Serveurs e-mail**, puis sur le **Nom du client** pour ouvrir la configuration.
3. Cliquez sur **Ajouter un serveur e-mail**. Vous pouvez configurer le même serveur e-mail plusieurs fois, mais avec un nom de compte différent.
4. Une fenêtre contextuelle **Ajouter un serveur e-mail** apparaît. Configurez les paramètres suivants :
   - **Nom du serveur e-mail** : Nom du serveur. Ce champ est obligatoire
   - Cliquez sur le menu déroulant **Paramètres IMAP** et configurez les paramètres suivants :
     - **Nom d'hôte** : Nom d'hôte du serveur. Ce champ est obligatoire
     - **Num. de port** : Numéro de port du serveur. Ce champ est facultatif
     - **Utiliser SSL** : Activer cet indicateur pour utiliser le SSL
     - **Nom d'utilisateur** : Nom de l'utilisateur du compte. Ce champ est obligatoire

- **Mot de passe** : Mot de passe du compte. Ce champ est obligatoire
- **Confirmer mot de passe** : Confirmez le mot de passe que vous avez donné dans le paramètre précédent. Ce champ est obligatoire
- **Sessions IMAP maximum** : Nombre maximum de sessions IMAP. La valeur par défaut est 0, et ce champ est facultatif

- Cliquez sur le menu déroulant **Paramètres SMTP** et configurez les paramètres suivants :
  - **Nom d'hôte** : Nom d'hôte du serveur. Ce champ est obligatoire
  - **Num. de port** : Numéro de port du serveur. Ce champ est obligatoire
  - **Utiliser SSL** : Activer cet indicateur pour utiliser le SSL
  - **Authentification** : Choisissez dans le menu déroulant : « Aucun », « Utiliser les paramètres IMAP » et « Utiliser les paramètres ci-dessous » pour authentifier les trois paramètres suivants.
  - **Nom d'utilisateur** : Seulement paramétrable si vous avez sélectionné « Utiliser les paramètres ci-dessous » dans le paramètre Authentification.
  - **Mot de passe** : Seulement paramétrable si vous avez sélectionné « Utiliser les paramètres ci-dessous » dans le paramètre Authentification.
  - **Confirmer mot de passe** : Seulement paramétrable si vous avez sélectionné « Utiliser les paramètres ci-dessous » dans le paramètre Authentification.
  - **Adresse e-mail de surveillance** : Adresse e-mail utilisée par le système pour vérifier si la connexion au serveur e-mail fonctionne correctement.
  - **Limite du débit de message** : Limite des messages électroniques envoyés par heure. La valeur par défaut est 0 et signifie qu'il n'y a pas de limite.

5. Cliquez sur **Ajouter** pour créer un nouveau serveur

La liste des serveurs e-mail indique maintenant le serveur que vous venez d'ajouter.

Lorsque la fonction Plusieurs serveurs e-mail est activée, le même compte (Serveurs e-mail + Nom du compte) ne doit pas être utilisé pour différents clients. Chaque fois qu'un nouveau serveur e-mail ou une modification de serveur e-mail est envoyée, vérifiez si le même compte est déjà configuré pour d'autres clients.

Modification d'un serveur e-mail

1. Cliquez sur l'icône **Modifier le serveur e-mail** à côté du serveur e-mail que vous souhaitez modifier

2. La fenêtre contextuelle **Modifier le serveur e-mail** apparaît
3. Sélectionnez les paramètres à modifier. Vous pouvez modifier tous les paramètres.
4. Cliquez sur **Enregistrer**

La liste indique maintenant les paramètres mis à jour du serveur e-mail

Copie d'un serveur e-mail

Vous pouvez copier les paramètres d'un serveur e-mail pour en créer un nouveau avec un autre nom.

1. Cliquez sur l'icône **Copier le serveur e-mail** à côté du serveur que vous voulez copier

2. La fenêtre contextuelle **Copier le serveur e-mail** apparaît.
3. Modifiez le nom du serveur.
4. Cliquez sur **Ajouter** pour créer le nouveau serveur.

Suppression d'un serveur e-mail

1. Cliquez sur l'icône **Supprimer le serveur e-mail** à côté du serveur que vous souhaitez supprimer

2. La fenêtre contextuelle **Supprimer le serveur e-mail** apparaît

3. Cliquez sur **OUI** pour supprimer le serveur e-mail ou sur **NON** pour annuler la suppression

---

NOTE: Lors de la suppression d'un serveur e-mail, il sera vérifié si une destination lui est associée. Dans ce cas, la suppression du serveur e-mail ne sera pas autorisée. L'association entre les destinations et le serveur e-mail doit être supprimée avant de supprimer le serveur e-mail. S'il y a des contacts e-mail en attente à traiter, il ne sera plus possible d'ouvrir les e-mails et ils devront être jetés.

Ajout d'une nouvelle destination

Ici, vous pouvez associer les destinations à l'adresse e-mail correspondante.

1. Cliquez sur l'onglet **Configuration de messagerie**
2. Cliquez sur l'onglet **Destination**, puis sur le **Nom du client** pour ouvrir la configuration.
3. Cliquez sur le menu déroulant **Défaut**, qui est le client par défaut
4. Cliquez sur **Ajouter une destination**. Une fenêtre contextuelle **Ajouter une destination** apparaît. Configurez les paramètres suivants :
   - **Nom de la destination** : Nom de la destination. Ce champ est obligatoire
   - **Adresse e-mail** : Saisissez l'adresse e-mail de la destination. Ce champ est obligatoire.
   - **Description** : Donnez une description de la destination. Ce champ est facultatif
   - **À partir du texte** : Saisissez un alias pour l'adresse e-mail de destination. Cet alias apparaît dans le champ De quand un utilisateur répond à un message email.
   - **Surveillé** : Activez cet indicateur pour surveiller la destination. Ce champ est facultatif
   - **Disponible pour la sortie** : Activez cet indicateur pour rendre la destination disponible pour les e-mails sortants. Ce champ est facultatif
   - **Serveur e-mail** : Sélectionnez dans le menu déroulant le serveur e-mail auquel vous souhaitez associer la destination.
5. Cliquez sur **Ajouter**

6. La liste des destinations indique maintenant la destination que vous venez d'ajouter.

Modification d'une destination

1. Cliquez sur l'icône **Modifier la destination** à côté de la destination que vous souhaitez modifier

2. La fenêtre contextuelle **Modifier la destination** apparaît
3. Sélectionnez les paramètres à modifier. Vous pouvez modifier tous les paramètres.
4. Cliquez sur **Enregistrer**

La liste indique maintenant les paramètres mis à jour de la destination modifiée

Copie d'une destination

Vous pouvez copier les paramètres d'une destination pour en créer une nouvelle avec un autre nom

1. Cliquez sur l'icône **Copier la destination** à côté de la destination que vous souhaitez copier

2. La fenêtre contextuelle **Copier la destination** apparaît
3. Modifiez le nom de la destination et l'adresse e-mail
4. Cliquez sur **Ajouter** pour créer la destination

Suppression d'une destination

1. Cliquez sur l'icône **Supprimer la destination** à côté de la destination que vous souhaitez supprimer

2. La fenêtre contextuelle **Supprimer la destination** apparaît
3. Cliquez sur **OUI** pour supprimer la destination ou sur **NON** pour annuler la suppression

Index

A
Agents virtuels 21

D
documentation
    apport de commentaire 6
    conventions de formats 5
    public visé 5

R
REST SDK 33

T
Téléphonie CLIP 35, 37

W
Web Manager 7