A MITEL
PRODUCT
GUIDE

Mitel OpenScape Contact Center V12

Web Manager V12

Manuale di Amministrazione Web Manager

Manuale di Amministrazione
10/2024

A31003-S22C0-M100-01-72A9

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.

Indice

1 Informazioni sul manuale

Questo manuale offre una panoramica dell'applicazione Manager OpenScape Contact Center e guida gli utenti nelle varie attività di amministrazione che occorre eseguire periodicamente.

1.1 A chi è dedicato il manuale

Questo manuale è concepito per gli amministratori del centro contatti, responsabili della manutenzione della configurazione e per i supervisori e i manager che utilizzano gli strumenti di produttività di OpenScape Contact Center.

1.2 Convenzioni di formattazione

Nel presente manuale vengono utilizzate le seguenti convenzioni di formattazione:

Grassetto
Questo formato identifica i componenti, i titoli delle finestre e finestre di dialogo e i nomi degli elementi di OpenScape Contact Center.

Corsivo
Questo formato identifica i riferimenti alla documentazione correlata.

`Tipo di carattere a spaziatura fissa`
Questo formato distingue il testo da digitare o che il computer visualizza in un messaggio.

NOTA: Le note evidenziano informazioni utili ma non essenziali, quali suggerimenti o metodi alternativi per eseguire un'operazione.

IMPORTANTE: Note importanti: le indicazioni di attenzione sottolineano le azioni che potrebbero influire negativamente sul funzionamento dell'applicazione o causare perdite di dati.

1.3 Commenti sulla documentazione

Per notificare problemi in merito al presente documento, rivolgersi al Centro di assistenza clienti.

Al momento di effettuare la chiamata, assicurarsi di poter indicare le informazioni seguenti. Ciò consentirà di identificare il documento pertinente.

- **Titolo:** Manuale di Amministrazione Web Manager
- **Numero d'ordine:** A31003-S22B1-M100-02-72A9

2 Web Manager

2.1 Introduzione

Web Manager è un'applicazione che abilita la configurazione delle funzioni in OpenScape Contact Center tramite un browser web.

2.2 Dettagli di accesso

Web Manager è un'applicazione basata sul browser installata con il pacchetto OpenScape Contact Center Application Server.

Per accedere a Web Manager, è necessario disporre del profilo di accesso utente Amministratore principale.

Con Web Manager è possibile configurare:

- Single Sign-On tramite protocollo SAML2 per Portale agenti Web
- Single Sign-On con Circuiti per Portale agenti Web
- Agenti virtuali per abilitare la funzionalità di chatbot
- REST SDK
- Telefonia

Per accedere a Web Manager, aprire un browser e inserire il seguente url:
https://<OSCC_ApplicationServer_hostname_or_ip>/webmanager

3 Single Sign On tramite il protocollo SAML2

Il formato SAML (Security Assertion Markup Language) è un formato dati open-standard per lo scambio di dati di autenticazione e autorizzazione fra un provider di identità e un provider di servizi.

Poiché molte organizzazioni conoscono già l'identità degli utenti collegati al rispettivo dominio o intranet Active Directory, tali informazioni possono essere utilizzate per gli utenti Single Sign On (SSO) su applicazioni di OpenScape Contact Center. OpenScape Contact Center supporta il protocollo SAML nella versione 2.0 (SAML2).

NOTE: SSO via SAML2 è supportato solo per le applicazioni basate su web del Portale Agenti Web. Queste configurazioni SSO non si applicano ad altre applicazioni come Agent Portal Java, Client Desktop o Manager Desktop, in quanto utilizzano metodi di accesso configurati in Manager Desktop. Web Manager supporta solo il metodo di accesso di OSCC.

Le specifiche del protocollo SAML definiscono i seguenti ruoli:

- **Utente**: Questo ruolo è assegnato al browser web, il quale utilizza l'URL per lanciare l'applicazione sul server applicativo (Application Server).
- **Provider di servizi (Service Provider, SP)**: Questo ruolo è assegnato al server applicativo (Application Server) nel quale viene eseguita l'applicazione.

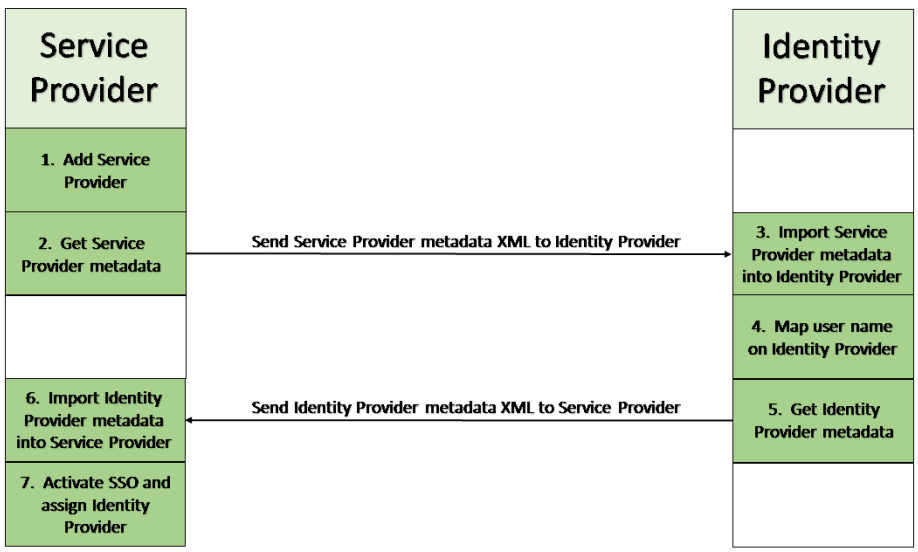
- **Provider di identità (Identity Provider, IdP)**: Questo ruolo è assegnato a un'entità di sistema (autorità di autenticazione) che svolge funzione di autenticazione dell'utente.

NOTE: Esistono numerosi IdP che possono essere utilizzati, ad esempio ADFS o Gluu. In questo manuale è utilizzato Active Directory Federation Services (ADFS) a scopo esemplificativo per descrivere quali informazioni sono necessarie per configurare la funzionalità SSO nella soluzione OpenScape Contact Center. Se si utilizzano altri IdP, è necessario estrarre le stesse informazioni da tali IdP.

NOTE: ADFS è una soluzione SSO offerta da Microsoft. Come componente dei sistemi operativi Windows Server, offre agli utenti un accesso autenticato alle applicazioni attraverso Active Directory (AD).

NOTE: Il servizio di IdP è un'applicazione di terzi non fornita né supportata da Unify. A causa di ciò, gli esempi di configurazione per ADFS presentati in questo documento possono variare.

La funzionalità SSO viene impostata nell'applicazione Web Manager configurando il Provider di servizi sul lato OSCC e il Provider di identità sul lato opposto. Nella figura successiva è illustrata la sequenza dei passaggi per la configurazione:



1. Aggiunta di un Provider di servizi

    1. Eseguire l'accesso all'applicazione Web Manager utilizzando Master Administrator come utente con la password corrispondente. Selezionare **Sign On Configuration** quindi selezionare **Provider di servizi**.
    2. Fare clic su **Aggiungi Provider di servizi**

        - **Host URL**: URL del servizio Portale Agenti Web. Ad esempio:

        `https://<ApplicationServer_hostname_or_ip>/agentportal`

        Questo valore deve essere lo stesso URL configurato nel file di configurazione XML del Portale Agenti Web. Per trovare questo valore, accedere al computer su cui è in esecuzione il server applicativo, quindi aprire il file seguente nella directory di installazione e copiare il contenuto dell'elemento "service-provider-host-url":
        `.\ApplicationServer\ApacheWebServer\conf\webagent.xml`

        - **Certificato**: Un valore opzionale per il Provider di servizi. Consente di inserire un certificato per la crittografia dei messaggi inviati all'IdP.
        - **Chiave pubblica**: Un valore opzionale per la chiave utilizzata nel certificato per convalidare la certificazione con il Provider di servizi. Questo valore deve essere noto al Provider di servizi e all'IdP.

NOTE: Per OpenScape Contact Center, il provider di servizi sarà il servizio del Portale agenti Web stesso. È possibile configurare più di un provider di servizi nel sistema.

---

2. Ottenere metadati del provider di servizi

Mentre si è ancora connessi all'applicazione Web Manager, ottenere i metadati del Provider di servizi e importarli nel servizio Provider d'identità

1. Spostare il puntatore del mouse sul Provider di servizi aggiunto e fare clic su **Ottieni metadati**
2. Fare clic su **Copia negli appunti**, salvare il contenuto in un file di testo sulla propria macchina e rinominare l'estensione del file in "xml". Scegliere il nome del file in modo da rendere evidente il contenuto di metadati del Provider di servizi, ad esempio: `OSCC_<customer>_metadata.xml`

3. Importare i metadati del Provider di servizi nel Provider d'identità

È necessario aggiungere il Provider di servizi come 'relying party' per il Provider d'identità, importandone i metadati. Trasferire il file XML creato nel passaggio 2) in una posizione accessibile al Provider d'identità, quindi accedere al Provider d'identità.

Il seguente esempio illustra il modo in cui i metadati del Provider di servizi vengono importati in Microsoft Active Directory Federation Service (ADFS):

1. Nella Console di gestione ADFS, navigare fino alla cartella: **Trust Relationships > Relying Party Trust**
2. Fare clic su **Aggiungi trust di Relying Party**
3. Compare la schermata **Aggiunta guidata trust di Relying Party**. Fare clic su **Avvia**
4. Selezionare **Importa dati sulla relying party da un file**, quindi scegliere il file XML creato nel passaggio 2). Utilizzare il comando **Sfoglia...** per individuare il file.
5. Fare clic su **Avanti**
6. Inserire un qualsiasi nome nel campo **Nome da visualizzare**
7. Fare clic su **Avanti**
8. Selezionare **Permetti a tutti gli utenti di accedere a questa relying party**
9. Fare clic su **Avanti**
10. Fare clic su **Chiudi**

4. Mappare il nome utente sul Provider d'identità

Aggiungere una regola di richiesta obbligatoria per il trust di Relying Party creato nel passaggio 3).

Le regole di richiesta sono utilizzate per mappare un tipo di richiesta in entrata a un tipo di richiesta in uscita. Nella regola di richiesta viene specificato quale campo del database utente del Provider d'identità corrisponde al nome utente OSCC.

1. Nella Console di gestione ADFS, selezionare i trust di relying party creati e fare clic su **Modifica policy di emissione richieste...**
2. Fare clic su **Aggiungi regola...** per aprire la procedura guidata di creazione della regola di richiesta.

3. Nella finestra **Selezione modello regole**, selezionare **Invia attributi LDAP come richieste** dal menu a tendina.

   NOTE: Nel seguente esempio, il nome utente OSCC viene autenticato utilizzando LDAP.

4. Fare clic su **Avanti**
5. La voce **Mappatura di attributi LDAP a tipi di richiesta in uscita** (Active Directory) sarà utilizzata per l'autenticazione tramite SAML

   NOTE: In questo esempio, il nome di account Windows viene utilizzato per la mappatura del nome utente OSCC, configurato nel server LDAP (Active Directory). Per ADFS, viene inoltre richiesta la mappatura dell'ID del nome.

6. Fare clic su **Fine**

5. Ottenere metadati del Provider d'identità

   Dopo la configurazione del Provider d'identità, importarne i metadati nel Provider di servizi.

   Come visibile nella directory Endpoints della Console di gestione ADFS, i metadati sono accessibili tramite:

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

6. Importare i metadati del Provider d'identità nel Provider di servizi

   1. Eseguire l'accesso all'applicazione Web Manager utilizzandole credenziali utente per Master Administrator. Selezionare **Sign On Configuration** quindi selezionare **Provider d'identità**.

      È possibile aggiungere un Provider d'identità manualmente con il comando **Aggiungi Provider d'identità** oppure aggiungerne uno automaticamente con il comando **Importa da metadati**. Si raccomanda di aggiungere un Provider d'identità mediante importazione. Trasferire il file XML creato nel passaggio 5 in una posizione accessibile al Provider di servizi.

      Se si decide di aggiungere un Provider d'identità manualmente, fare clic su **Aggiungi Provider d'identità**.

      NOTE: Tutte le configurazioni possono essere recuperate dal file dei metadati del Provider d'identità.

- **ID entità**: Identificatore dell'entità IdP (deve essere un URL). Nei metadati, è possibile individuare tale URL cercando l'attributo **entityID**, nel tag **EntityDescriptor**.
- **URL SSO**: Informazioni per l'endpoint SSO dell'IdP. Si tratta dell'URL target dell'IdP in cui l'SP invierà il messaggio di richiesta autenticazione. Nei metadati, tale URL è reperibile all'interno del tag **IDPSSODescriptor** cercando l'attributo **Location (Posizione)**, nel tag **SingleSignOnService**.

NOTE: Utilizzare il valore dell'attributo **Location (Posizione)** dalla riga con il valore "**...HTTP-POST**" nell'attributo **Binding**.

- **Corrispondenza nome utente**: Questo è il parametro restituito dall'IdP, il quale sarà confrontato con l'utente OSCC configurato.

Nei metadati, ad esempio, da ADFS, è stato selezionato il **Nome account Windows** come **Tipo di richiesta in uscita** (vedere passaggio 4 - **Mappare il nome utente sul Provider d'identità - Aggiungi regola**). Nella ricerca del valore del **Nome account Windows** nel file dei metadati, è possibile trovare il valore di **Corrispondenza nome utente** sotto l'attributo **Nome**. In questo esempio, equivale a:

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

In generale, il valore del parametro **Corrispondenza nome utente** deve corrispondere al tipo di richiesta in uscita per la mappatura degli attributi SAML LDAP nell'IdP, vedere passaggio 4) **Mappatura di attributi LDAP a tipi di richiesta in uscita**. Si tratta del valore del parametro LDAP utilizzato da ADFS per identificare (abbinare) l'utente OSCC.

NOTE: Altri IdP avranno una corrispondenza nome utente diversa.

- **URL del servizio Single logout**: URL della posizione dell'IdP a cui l'SP invierà la Richiesta di Single Logout (SLO). Nei metadati, tale URL è reperibile all'interno del tag **IDPSSODescriptor** cercando l'attributo **Location (Posizione)**, nel tag **SingleLogoutService**.

NOTE: Utilizzare il valore dell'attributo **Location (Posizione)** dalla riga con il valore "**...HTTP-POST**" nell'attributo **Binding**.

- **URL di risposta del servizio Single logout**: URL della posizione dell'IdP a cui l'SP invierà la Risposta di Single Logout (SLO). Questo valore è opzionale ed è in genere lasciato vuoto. Se lasciato vuoto, sarà utilizzato lo stesso URL equivalente all'**URL del servizio Single logout**, come informazione di endpoint di risposta SLO dell'IdP. Alcuni IdP utilizzano un URL separato per inviare una richiesta e risposta di logout; utilizzare questa proprietà per impostare l'URL di risposta separato.
- **Certificato x509**: Certificato x509 pubblico dell'IdP. Nei metadati, il valore di questo certificato è reperibile cercando il tag **X509Certificate** all'interno del tag **IDPSSODescriptor**, e all'interno del tag **KeyDescriptor**, con l'attributo **use="signing"**.

NOTE: Quando si inserisce manualmente un certificato, verificare che presenti solo la riga hash; rimuovere eventuali commenti e righe aggiuntive prima o dopo di essa.

- **Impronta digitale certificato**: Invece di utilizzare il certificato x509 intero, è possibile utilizzare un'impronta digitale. Se viene fornita un'impronta digitale, è necessario definire l'Algoritmo dell'impronta digitale per consentire all'OSCC di sapere quale algoritmo è stato utilizzato. Possibili valori sono: SHA1, SHA256, SHA384, SHA512.

Se si decide di aggiungere un Provider d'identità importando metadati, fare clic su **Importa da metadati**, che costituisce l'approccio consigliato per configurare l'IdP.

- **Corrispondenza nome utente**: Questo è il parametro restituito dall'IdP, il quale sarà utilizzato per il confronto con l'utente OSCC configurato.

Nei metadati, ad esempio, da ADFS, è stato selezionato il **Nome account Windows** come **Tipo di richiesta in uscita** (vedere passaggio 4 - **Mappare il nome utente sul Provider d'identità - Aggiungi regola**). Nella ricerca del valore del **Nome account Windows** nel file dei metadati, è possibile trovare il valore di **Corrispondenza nome utente** sotto l'attributo **Nome**. In questo esempio, equivale a:

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

In generale, il valore del parametro **Corrispondenza nome utente** deve corrispondere al tipo di richiesta in uscita per la mappatura degli attributi SAML LDAP nell'IdP, vedere passaggio

4) **Mappatura di attributi LDAP a tipi di richiesta in uscita**. Si tratta del valore del parametro LDAP utilizzato da ADFS per identificare (abbinare) l'utente OSCC.

NOTE: Altri IdP avranno una corrispondenza nome utente diversa.

Dopo aver compilato l'attributo **Corrispondenza nome utente**, selezionare **Carica metadati**, fare clic su **Seleziona file** e selezionare il file di metadati. Fare clic su **Aggiungi**.

Un altro modo è selezionare Digita metadati, modificare o copiare/incollare i metadati nel campo **Contenuto metadati**. Fare clic su **Aggiungi**

7. Attivare SSO e assegnare il Provider d'identità

    1. Dopo l'importazione dei metadati del Provider d'identità nel Provider di servizi, mentre si è ancora connessi all'applicazione Web Manager, fare clic sulla scheda **Tenant**.
    2. Nella scheda **Tenant**, potrebbe essere presente un elenco di tenant. Spostare il puntatore del mouse sul tenant e fare clic su **Modifica**.
    3. Nella finestra **Configura Tenant**, attivare o disattivare le funzionalità **Single Sign On** e **Single Logout**:

        - **Single Sign On**: Consente l'integrazione SAML2
        - **Provider d'identità**: Selezionare il provider d'identità precedentemente configurato nella scheda Provider d'identità nel passaggio 6
        - **Single Logout (SLO)**: Se attivata e l'utente si disconnette dal Portale agenti Web, il sistema eseguirà la disconnessione dal server del Provider d'identità. Se questa opzione è attivata, l'utente sarà disconnesso da ogni altra applicazione che utilizza lo stesso IdP.

NOTE: Se si configura OpenScape Contact Center per Single Tenancy, SSO via SAML2 costituirà una funzionalità con copertura sull'intero sistema. Se si configura OpenScape Contact Center per Multi-Tenancy, è possibile abilitare SSO via SAML2 per ciascun singolo tenant. Per i tenant per cui SSO via SAML2 non è attivata, sono applicabili i metodi di accesso configurati in Manager Desktop.

Dopo il completamento della configurazione Single Sign On, avviare il browser web, accedere al Portale agenti Web e digitare:

`https://<ApplicationServer_hostname_or_ip>/agentportal`

Per la prima autenticazione nella sessione del browser, l'utente sarà indirizzato al Provider d'identità.

1. Immettere <user>@<domain> oppure <domain>\<user>, dove:
   - <domain> è il nome di dominio del cliente
   - <user>è l'utente configurato in Active Directory (nome account)

     NOTE: <user> deve inoltre essere configurato come utente in OpenScape Contact Center

   - Immettere la password Active Directory.

Per ulteriori autenticazioni (log in) nella stessa sessione del browser, sarà attiva la funzionalità SSO è non sarà necessario inserire alcun account e password.

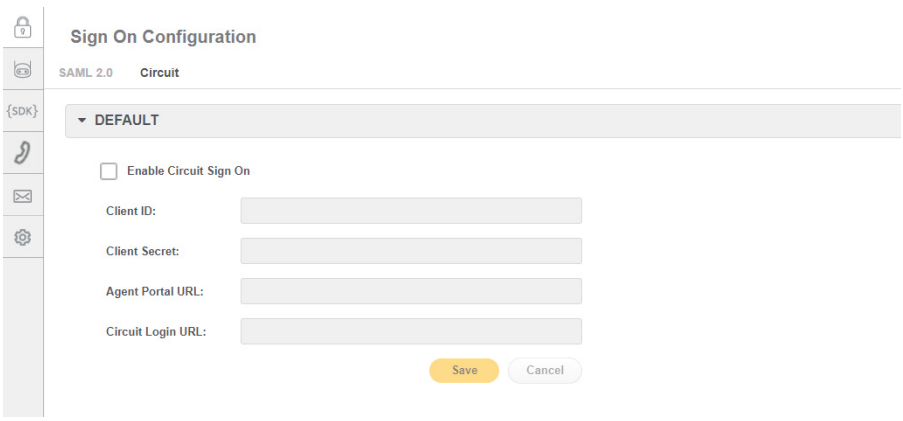
4 Configurazione di Single Sign On con Circuit

Dopo la configurazione dell'applicazione personalizzata su Circuit (vedere *OpenScape Contact Center V10 - Manuale di integrazione della piattaforma di comunicazione*), è necessario sincronizzare le informazioni di ID client e il segreto client con OpenScape Contact Center.

Accedere all'applicazione OSCC Web Manager e accedere con un account manager tenant. In "Sign On Configuration", selezionare la scheda "Circuit" e il tenant OSCC che hanno accesso alla funzione di integrazione di Circuit.

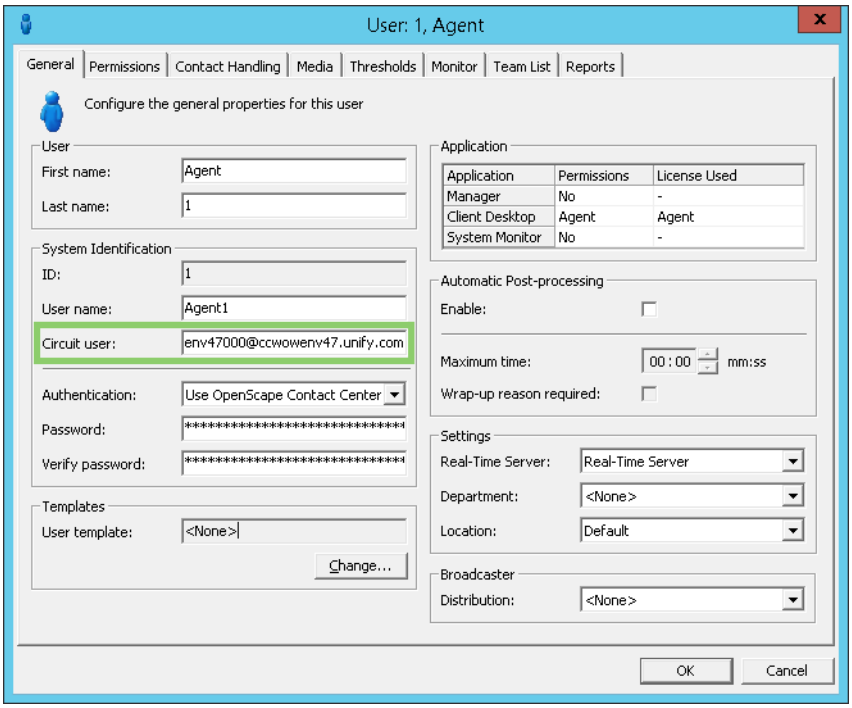
Compilare i campi sottostanti con le informazioni seguenti:

- **Enable Circuit Sign-on** - attivato.
- **Client ID**: identificatore univoco dell'applicazione, ottenuto nel capitolo precedente.
- **Client secret**: chiave segreta per l'applicazione, ottenuta nel capitolo precedente.
- **Agent Portal URL**: URL utilizzato per accedere all'applicazione Agent Portal Web. Seguire lo schema di https://<yourDomain>/agentportal
- **Circuit Login URL**: URL utilizzato per accedere all'applicazione Circuit.



Utilizzando Circuit Sign On per l'autenticazione sulla pagina di accesso di OpenScape Contact Center, è necessario associare un account Circuiti all'utente OpenScape Contact Center. Il nome utente Circuit (URI) è utilizzato per l'associazione.

Nella finestra di configurazione utente, compilare il campo Circuit User con l'URI utilizzato per accedere a Circuit. Due utenti OSCC nello stesso tenant non possono condividere lo stesso utente Circuit.



NOTE: Quando è possibile accedere a Circuit solo tramite un server proxy HTTPS, è necessaria una configurazione speciale in Application Server. Per ulteriori dettagli sulla configurazione, vedere *OpenScape Contact Center V10 - Manuale di installazione*

NOTE: Per informazioni dettagliate sulla configurazione di OpenScape Voice e l'aggiunta di un'applicazione su Circuit, consultare *OpenScape Contact Center V10 - Manuale di integrazione della piattaforma di comunicazione*.

---

5 Agenti virtuali

L'utente Amministratore principale deve accedere all'applicazione Web Manager per configurare agenti virtuali in OpenScape Contact Center.

La funzione Agente virtuale consente di integrare OpenScape Contact Center con un Natural Language Processor (NLP) per includere chatbot.

Il servizio Agente virtuale viene eseguito nel contenitore OSCC Application Server e accede a tutti gli agenti configurati in Web Manager.

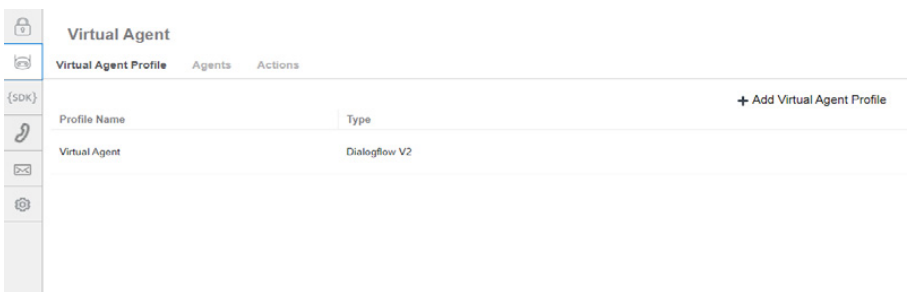
NOTE: L'agente virtuale supporta solo il tipo di password di OpenScape Contact Center. Il sistema non funzionerà con l'accesso a Windows o SAML2 SSO.

NOTE: La funzionalità Agente virtuale è una configurazione a livello di SISTEMA. Se in OpenScape Contact Center è attivato Multi-tenancy, ogni tenant richiede la distribuzione di uno o più CMS per offrire il supporto vocale. Ogni CMS può supportare uno o più profili Agente virtuale. Ogni profilo deve essere configurato con un token GCP diverso. Nell'OSCC Application Server, il file di configurazione `virtualagent.xml` deve avere il nome di unità operativa corretto.

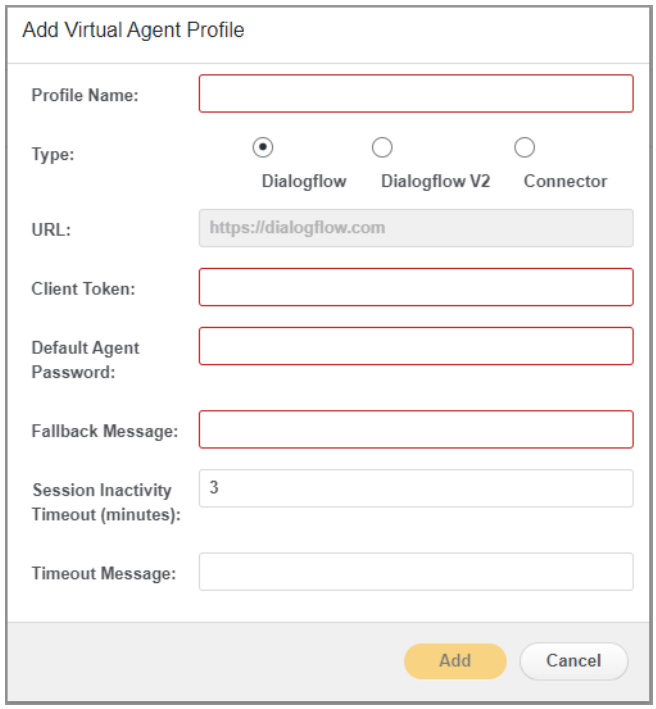
NOTE: Agente virtuale non supporta **Attività di follow-up automatiche** e **Motivo post-elaborazione obbligatoria**. Assicurarsi che queste funzionalità siano state disabilitate nella configurazione dell'utente.

Accedi a Web Manager e attieniti ai seguenti passaggi:

- Andare alla scheda **Agente virtuale**:



- Fare clic su **Aggiungi profilo Agente virtuale**. Viene visualizzata la finestra popup **Aggiungi profilo Agente virtuale**. Questo è il modulo per la configurazione del profilo NLP:



- **Nome profilo**: È un campo obbligatorio. Il nome del profilo NLP Agente virtuale
- **Tipo**: Il tipo di profilo dell'Agente virtuale. È possibile selezionare uno dei seguenti pulsanti di opzione:
  - Dialogflow
  - Dialogflow V2
  - Connettore

A seconda del tipo selezionato, occorre configurare vari parametri.

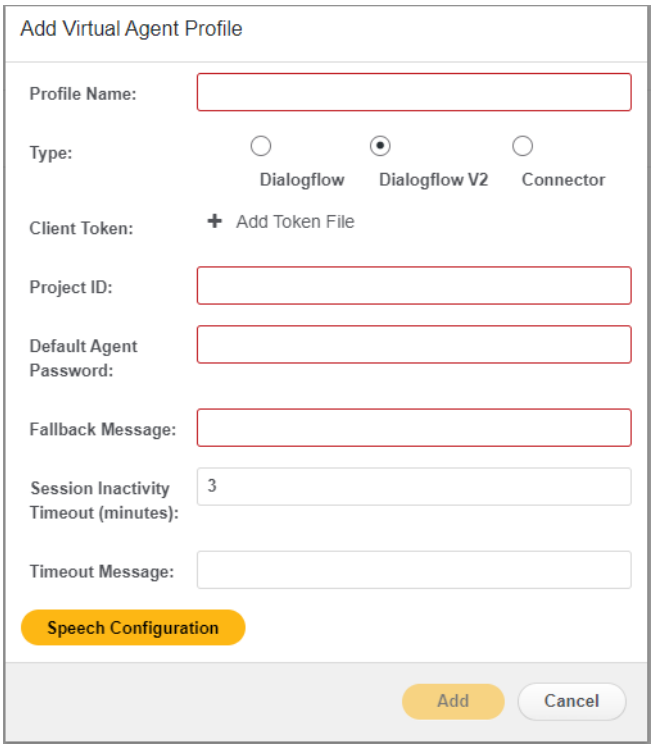
Tipo: Dialogflow

- **URL**: L'URL del motore di Dialogflow. Il valore predefinito è https://dialogflow.com
- **Token client**: Il token client fornito da Dialogflow

- **Password agente predefinita**: La password configurata in Manager per gli utenti configurati perché fungano da Agente virtuale. Importante utilizzare la stessa password per tutte le configurazioni utente di agente virtuale
- **Messaggio fallback**: È un messaggio di fallback del sistema. Se si verifica un errore nel sistema, questo messaggio verrà inviato esternamente per la persona che ha contattato il contact center
- **Timeout per inattività sessione**: Se la sessione contatto corrente è inattiva, la sessione verrà chiusa automaticamente dal sistema in base al periodo di tempo in minuti configurato
- **Messaggio di timeout**: Il messaggio inviato dopo il timeout per inattività della sessione

Tipo: Dialogflow V2

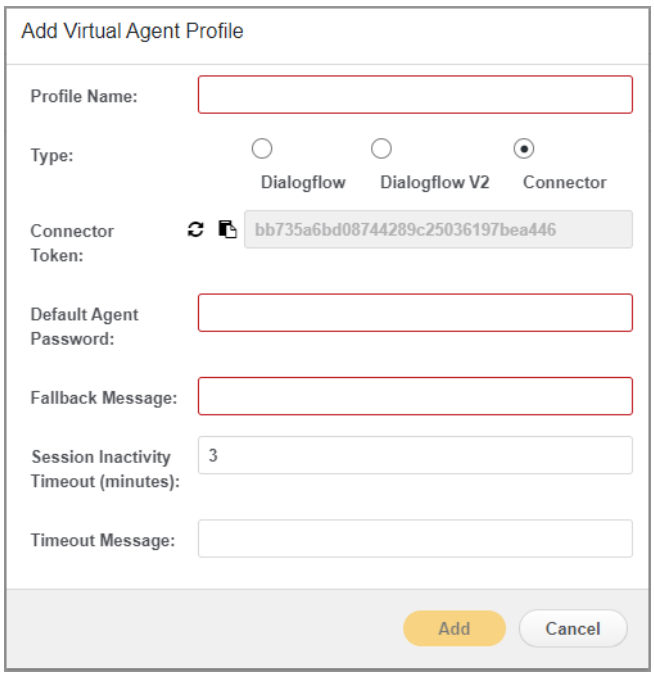
La finestra **Aggiungi profilo Agente virtuale** per la configurazione del profilo NLP si presenterà come segue:



- **Token client**: Fare clic su **Aggiungi file token** e sfogliare il PC per trovare il file Token (il file *.json) da utilizzare
- **ID progetto**: L'ID del progetto
- **Password agente predefinita**: È un campo obbligatorio. La password configurata in Manager per gli utenti configurati perché fungano da Agente virtuale. Importante utilizzare la stessa password per tutte le configurazioni utente di agente virtuale
- **Messaggio fallback**: È un campo obbligatorio. È un messaggio di fallback del sistema. Se si verifica un errore nel sistema, questo messaggio verrà inviato esternamente per la persona che ha contattato il contact center
- **Timeout per inattività sessione**: Se la sessione contatto corrente è inattiva, la sessione verrà chiusa automaticamente dal sistema in base al periodo di tempo in minuti configurato
- **Messaggio di timeout**: Il messaggio inviato dopo il timeout per inattività della sessione
- **Configurazione speech bot**: Questo pulsante consente di configurare lo speech bot

Tipo: Connettore

La finestra **Aggiungi profilo Agente virtuale** per la configurazione del profilo NLP si presenterà come segue

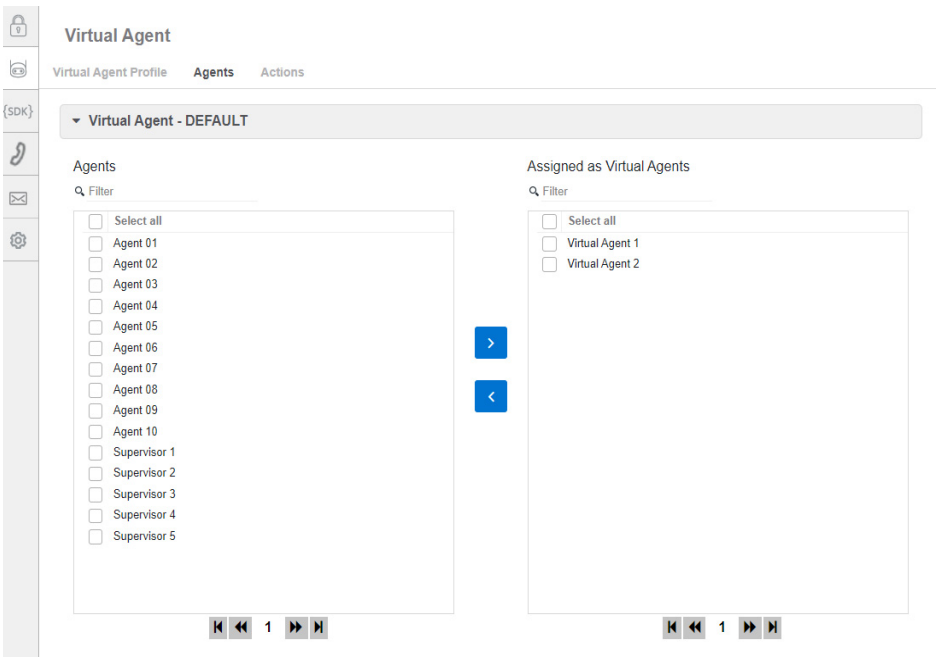


- **Token connettore**: Fare clic sul pulsante **Ricarica** per generare un nuovo token. Il nuovo Token connettore viene visualizzato nel campo in grigio. Fare clic sul pulsante **Appunti** per copiare il token negli Appunti
- **Password agente predefinita**: È un campo obbligatorio. La password configurata in Manager per gli utenti configurati perché fungano da Agente virtuale. Importante utilizzare la stessa password per tutte le configurazioni utente di agente virtuale
- **Messaggio fallback**: È un campo obbligatorio. È un messaggio di fallback del sistema. Se si verifica un errore nel sistema, questo messaggio verrà inviato esternamente per la persona che ha contattato il contact center
- **Timeout per inattività sessione**: Se la sessione contatto corrente è inattiva, la sessione verrà chiusa automaticamente dal sistema in base al periodo di tempo in minuti configurato
- **Messaggio di timeout**: Il messaggio inviato dopo il timeout per inattività della sessione

5.1 Configurazione degli utenti Agente come Agenti virtuali

Per gli agenti virtuali, è necessario assegnare agli utenti il profilo dell'agente registrato in OSCC.

Per assegnare gli utenti, andare alla scheda **Agenti** ed espandere la visualizzazione del profilo:



NOTE: Sono presenti filtri per aiutare nella scelta degli utenti degli agenti nel sistema.

5.2 Configurazione di azioni per Agenti virtuali

La funzione Agente virtuale può elaborare alcune azioni ricevute dal processore NLP.

Di solito un'azione è una stringa di testo inviata dal processore NLP con un set di parametri.

Ci sono varie possibili azioni:

- **Azione di riaccodamento**: Consente al sistema la consegna dall'Agente virtuale a una persona, riaccodando il contatto in un'altra coda.
- **Azione di richiamata**: Consente al sistema la consegna dall'Agente virtuale a una persona, creando una richiamata telefonica su OSCC.
- **Richiesta di sistema esterno**: Consente al sistema di eseguire una query su altri sistemi di terze parti per agevolare la soluzione con una risposta più elegante ai clienti.
- **URL di comunicazione WebInteraction**: Consente al sistema di eseguire una query su altri URL per agevolare la soluzione con una risposta più elegante ai clienti
- **Speech bot Riaccodamento**: Azione per selezionare la destinazione a cui riaccodare

5.2.1 Configurazione di un'azione di riaccodamento per Agenti virtuali

5.2.1.1 Azione di riaccodamento OpenMedia

Per configurare un'azione di riaccodamento OpenMedia, selezionare il Tipo di supporti **OpenMedia** e impostare:

- **Nome azione**: Un valore di testo che deve essere uguale all'azione ricevuta dal sistema NLP. (Obbligatorio)
- **Coda di riaccodamento**: La coda utilizzata per riaccodare il contatto. È un campo obbligatorio. Selezionare un valore dall'elenco e fare clic su **Aggiungi**.

5.2.1.2 Azione di riaccodamento WebInteraction

Per configurare un'azione di riaccodamento WebInteraction, selezionare il Tipo di supporti **WebInteraction** e impostare:

- **Nome azione**: Un valore di testo che deve essere uguale all'azione ricevuta dal sistema NLP. (Obbligatorio)
- **Coda di riaccodamento**: La coda utilizzata per riaccodare il contatto. È un campo obbligatorio. Selezionare un valore dall'elenco e fare clic su **Aggiungi**.

5.2.1.3 Azione di riaccodamento vocale

Per configurare un'azione di riaccodamento vocale, selezionare il Tipo di supporti **Speech bot** e impostare:

- **Nome azione**: Un valore di testo che deve essere uguale all'azione ricevuta dal sistema NLP. (Obbligatorio)
- **Destinazione a cui riaccodare**: La destinazione utilizzata per riaccodare il contatto. È un campo obbligatorio. Selezionare un valore dall'elenco e fare clic su **Aggiungi**.

5.2.2 Configurazione dell'azione di richiamata

Per configurare un'azione di richiamata, selezionare il tipo di azione **Azione di richiamata** e impostare:

- **Nome azione**: Un valore di testo che deve essere uguale all'azione ricevuta dal sistema NLP. (Obbligatorio)
- **Coda richiamate**: La coda utilizzata per creare la richiamata. (Obbligatorio)
- **Nome parametro telefono**: Il nome del parametro per ottenere il numero di telefono dal sistema NLP. (Obbligatorio)
- **Nome parametro ora del piano**: Il nome del parametro per ottenere la data e l'ora del piano richiamata. (Obbligatorio)

5.2.3 Configurazione di una richiesta di sistema esterno per Agenti virtuali

Per configurare un'azione di richiesta di sistema esterno, selezionare il tipo di azione **Richiesta di sistema esterno** e impostare:

- **Nome azione**: Un valore di testo che deve essere uguale all'azione ricevuta dal sistema NLP. (Obbligatorio)
- **Parametro URI sistema esterno**: Il nome di un parametro specificato dal sistema NLP che contiene l'indirizzo URI al quale il sistema Agente virtuale deve inviare la richiesta. (Obbligatorio)

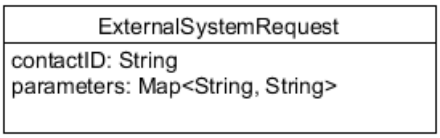
5.2.3.1 Dettagli sulla richiesta di sistema esterno

La funzione di richiesta di sistema esterno è un client di interfaccia REST interno, implementato nel servizio Agente virtuale.

Ogni volta che l'agente virtuale riceve un'azione per effettuare una consultazione esterna da NLP, il sistema invia una richiesta POST all'URI definito nel parametro con un oggetto JSON predefinito.

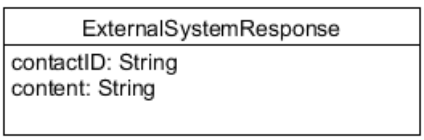
Esistono due oggetti JSON, uno per la richiesta e l'altro per la risposta.

L'oggetto richiesta inviato da agente virtuale è:



- **contactID**: L'attributo contenente il valore contactID di OSCC
- **parameters**: Una raccolta dei parametri ricevuti dal processore NLP composta da un testo chiave/valore. Questi parametri verranno elaborati dal sistema esterno

L'oggetto risposta ricevuto da un agente virtuale deve avere la seguente struttura:



- **contactID**: Questo valore deve essere identico a quello ricevuto dall'oggetto ExternalSystemRequest. (Obbligatorio)
- **content**: Il testo elaborato dal sistema esterno con il contenuto della risposta per la richiesta.

5.2.4 Configurazione di una richiesta Comunica URL WebInteraction per Agenti virtuali

Per configurare un'azione di richiesta Comunica URL WebInteraction, selezionare il tipo di azione **Richiesta URL di comunicazione WebInteraction** e impostare:

- **Nome azione**: Un valore di testo che deve essere uguale all'azione ricevuta dal sistema NLP. (Obbligatorio)
- **Parametro URL di comunicazione**: Il nome di un parametro specificato dal sistema NLP che contiene l'indirizzo URL al quale il sistema Agente virtuale deve inviare la richiesta. (Obbligatorio)

5.3 Configurazione vocale per Agenti virtuali

La funzione Agente virtuale consente di configurare uno speech bot con il pulsante **Configurazione vocale**, che consente a sua volta di configurare i parametri elencati di seguito. Questo pulsante è disponibile solo per il profilo Agente virtuale di tipo Dialog V2.

- **Attiva speech bot**: Parametro per attivare lo speech bot per il profilo selezionato. Valore predefinito: disattivato
- **Indirizzo CMS**: L'indirizzo IP/FQDN per accedere al nodo CMS.
- **Porta CMS**: La porta per accedere al nodo CMS. Valore predefinito: 6017
- **Lingua**: La lingua da utilizzare. Valore predefinito: EN-US
- **Genere**: Il genere della voce del riconoscimento vocale. Valore predefinito: uomo
- **Messaggio di benvenuto**: Il messaggio da riprodurre quando l'Agente virtuale Speechbot risponde alla chiamata.
- **Numero di riaccodamento fallback**: Numero al quale viene instradata la chiamata se CMS non è raggiungibile.

5.4 Informazioni sull'integrazione di Dialogflow

La funzionalità dell'agente virtuale è integrata per impostazione predefinita nel motore Dialogflow per il Natural Language Processor.

NOTE: Il processore NLP predefinito per agente virtuale è il Dialogflow di Google. Per ulteriori informazioni, seguire il collegamento: https://dialogflow.com

---

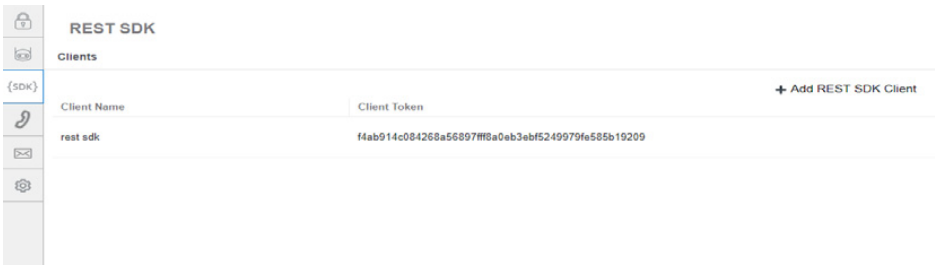
- **Dialogflow Standard Edition** è disponibile gratuitamente sul sito Web di Dialogflow. Fornisce le stesse funzionalità di Dialogflow Enterprise Edition ma le interazioni sono limitate dalle quote di

utilizzo e il supporto è fornito dalla comunità e via e-mail. Dialogflow Standard Edition è ideale per le piccole e medie imprese che desiderano creare interfacce di conversazione o per coloro che desiderano sperimentare Dialogflow.

- **Dialogflow Enterprise Edition** è disponibile come parte di Google Cloud Platform (GCP) e offre interazioni testuali e vocali illimitate, quote di utilizzo di volume maggiore e supporto fornito dall'assistenza di Google Cloud. Dialogflow Enterprise Edition è un'offerta premium, disponibile come servizio pay-as-you-go. Dialogflow Enterprise Edition è ideale per le aziende che necessitano di un servizio di livello aziendale che possa essere facilmente scalato per supportare cambiamenti nella domanda degli utenti.

Per ulteriori informazioni sulle quote, vedere: https://cloud.google.com/dialogflow-enterprise/quotas

6 REST SDK



Il REST SDK Framework permette lo sviluppo di applicazioni multimediali che si integrano con il sistema OpenScape Contact Center.

Il framework è costituito da un'interfaccia REST, che permette l'invio di comandi dall'applicazione a OpenScape Contact Center e l'invio di eventi di monitoraggio da OpenScape Contact Center all'applicazione.

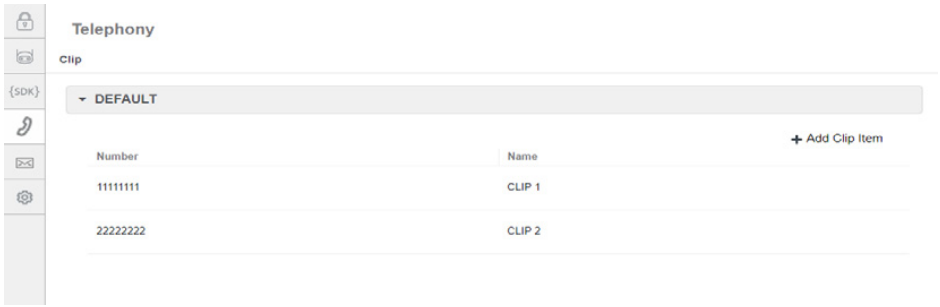
Configurazione

Configurare le istanze REST SDK utilizzando il Web Manager. Per creare una nuova istanza REST SDK:

1. Selezionare la scheda **REST SDK**
2. Fare clic su **Aggiungi REST SDK Client**
3. Appare una finestra popup **Aggiungi REST SDK Client** . Configurare i seguenti parametri:
   - **Nome client**: Il Client Name identifica in modo univoco l'istanza REST SDK ed è una stringa con un massimo di 32 caratteri.
   - **Token client**: Il Client Token è un tipo di password, utilizzato per autenticare il client REST SDK durante il processo di registrazione del client sul server. Il Client Token può essere configurato manualmente o generato automaticamente.

     Fare clic sul pulsante **Reload** per generare automaticamente un nuovo Client Token casuale di 64 byte. Il nuovo Client Token viene mostrato sul campo in grigio. Fare clic sul pulsante **Appunti** per copiare il Token negli appunti.
   - Fare clic su **Aggiungi**
4. È stato creato il nuovo REST SDK Client.

7 CLIP per chiamate in uscita



La funzionalità CLIP (Calling Line Identification Presentation) nel Portale agenti Web, si riferisce all'identificazione della linea chiamante, utilizzata per le chiamate in uscita. La funzionalità CLIP non altera la funzionalità di Callback corrente riguardo alla definizione del numero chiamante. Per ogni tenant, deve essere configurato un elenco di numeri chiamanti. La funzione CLIP è valida per tutte le chiamate in uscita: dal pulsante Effettua chiamata, da Elenco di selezione rapida, da Ricerca nell'elenco e da Registro attività.

È possibile utilizzare Web Manager per configurare CLIP per le chiamate in uscita.

Qui è possibile aggiungere/modificare/eliminare il o i numeri chiamanti per la funzionalità CLIP.

Aggiunta di un nuovo numero

1. Fare clic sulla scheda **Telefonia**
2. Fare clic sul menu a discesa **Default**, che rappresenta il tenant predefinito
3. Fare clic sulla voce **Aggiungi Clip**. È possibile aggiungere fino a dieci numeri per tenant
4. Viene visualizzata una finestra popup **Aggiungi elemento Clip**. Configurare i seguenti parametri:
   - **Numero**: Il numero chiamante. Deve essere costituito da una stringa di caratteri numerici senza nessun carattere speciale. Questo è un campo obbligatorio
   - **Nome**: Il nome associato al numero chiamante. Questo è un campo obbligatorio
5. Fare clic su **Aggiungi**

L'elenco dei numeri CLIP mostra ora il numero appena aggiunto. Questo numero appare anche nei numeri disponibili per la funzionalità CLIP del Portale agenti Web in: **Settings (Impostazioni) > Agent (Agente) > CLIP > Always use this value (Utilizza sempre questo valore)**

Modifica di un numero

1. Fare clic sull'icona **Modifica elemento Clip** accanto al numero CLIP che si desidera modificare

2. Viene visualizzata la finestra popup **Modifica elemento Clip**
3. È possibile modificare il **Numero** e/o il **Nome** del numero chiamante esistente
4. Fare clic su **Aggiorna**

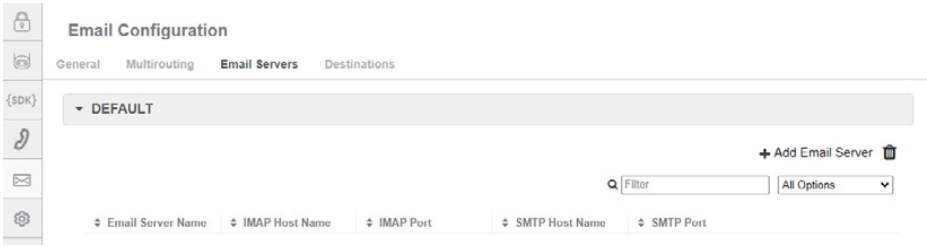
L'elenco mostra ora il numero e/o il nome CLIP aggiornati

Eliminazione di un numero

1. Fare clic sull'icona **Elimina elemento Clip** accanto al numero CLIP che si desidera eliminare

2. Viene visualizzata la finestra popup **Elimina elemento Clip**
3. Fare clic su **OK** per eliminare il numero CLIP o **Annulla** per annullare l'eliminazione

8 Più e-mail per tenant



Questa funzione consente a ciascuna Business Unit di avere più server di posta elettronica o indirizzi e-mail per Business Unit. È possibile configurare i server di posta elettronica e le destinazioni tramite il Web Manager.

NOTE: Ogni Business Unit supporta fino a cinque credenziali configurate di posta elettronica.

Aggiunta di un nuovo server di posta elettronica

1. Fare clic sulla scheda **Configurazione posta elettronica**
2. Fare clic sulla scheda **Email Server (Server di posta elettronica)** e poi su **Tenant Name (Nome tenant)** per espandere la configurazione.
3. Fare clic su **Aggiungi server di posta elettronica**. È possibile configurare lo stesso server di posta elettronica più di una volta, ma con un nome account diverso.
4. Compare una finestra popup **Aggiungi server di posta elettronica**. Configurare i seguenti parametri:
   - **Nome del server di posta elettronica**: Il nome del server. Questo è un campo obbligatorio
   - Fare clic sul menu a discesa **Impostazioni IMAP** e configurare i seguenti parametri:
     - **Nome host**: Il nome host del server. Questo è un campo obbligatorio
     - **Numero porta**: Numero di porta del server. Questo è un campo opzionale
     - **Utilizza SSL**: Attivare questo flag per utilizzare SSL
     - **Nome utente**: Il nome utente dell'account. Questo è un campo obbligatorio

- **Password**: La password dell'account. Questo è un campo obbligatorio
- **Conferma password**: Confermare la password fornita nel parametro precedente. Questo è un campo obbligatorio
- **Numero massimo di sessioni IMAP**: Il numero massimo di sessioni IMAP. Il valore predefinito è 0, questo è un campo opzionale

- Fare clic sul menu a discesa **Impostazioni SMTP** e configurare i seguenti parametri:
  - **Nome host**: Il nome host del server. Questo è un campo obbligatorio
  - **Numero porta**: Numero di porta del server. Questo è un campo obbligatorio
  - **Utilizza SSL**: Attivare questo flag per utilizzare SSL
  - **Autenticazione**: Dal menu a discesa selezionare: "None" (Nessuna), "Use IMAP settings" (Utilizza impostazioni IMAP) e "Use settings below" (Utilizza impostazioni riportate sotto) per autenticare i tre parametri successivi.
  - **Nome utente**: Configurabile solo se si è selezionato "Use settings below" (Utilizza impostazioni riportate sotto) dal parametro Authentication (Autenticazione).
  - **Password**: Configurabile solo se si è selezionato "Use settings below" (Utilizza impostazioni riportate sotto) dal parametro Authentication (Autenticazione).
  - **Conferma password**: Configurabile solo se si è selezionato "Use settings below" (Utilizza impostazioni riportate sotto) dal parametro Authentication (Autenticazione).
  - **Indirizzo e-mail di heartbeat**: L'indirizzo e-mail utilizzato dal sistema per verificare il corretto funzionamento della connessione al server di posta elettronica.
  - **Limite di velocità messaggi**: Il limite di messaggi e-mail inviati all'ora. Il valore predefinito è 0 e indica nessun limite.

5. Fare clic su **Aggiungi**per creare un nuovo server

L'elenco dei server di posta elettronica ora mostra il server appena aggiunto.

Quando la funzione E-mail Multiple Servers (Più server di posta elettronica) è attivata, lo stesso account (server di posta elettronica + nome account) non deve essere utilizzato per tenant diversi. A ogni

invio di un nuovo server di posta elettronica o di una nuova modifica di un server di posta elettronica, verificare se lo stesso account è già configurato per altri tenant.

Modifica di un server di posta elettronica

1. Fare clic sull'icona **Modifica server di posta elettronica** accanto al server di posta elettronica che si desidera modificare

2. Compare la finestra popup **Modifica server di posta elettronica**
3. Modificare i parametri che si desidera modificare. È possibile modificare tutti i parametri.
4. Fare clic su **Salva**

L'elenco ora mostra i parametri aggiornati del server di posta elettronica

Copia di un server di posta elettronica

È possibile copiare i parametri di un server di posta elettronica per crearne uno nuovo con un altro nome.

1. Fare clic sull'icona **Copy Email Server (Copia server di posta elettronica)** accanto al server che si desidera copiare

2. Compare la finestra popup **Copia server di posta elettronica.**
3. Modificare il nome del server.
4. Fare clic su **Aggiungi** per creare il nuovo server.

Eliminazione di un server di posta elettronica

1. Fare clic sull'icona **Elimina server di posta elettronica** accanto al server che si desidera eliminare

2. Compare la finestra popup **Elimina server di posta elettronica**

3. Fare clic su **SI** per eliminare il server di posta elettronica o su **NO** per interrompere l'eliminazione

---

NOTE: Quando si elimina un server di posta elettronica, viene verificato se a esso è associata una destinazione. In questo caso, l'eliminazione del server di posta elettronica non sarà consentita. L'associazione tra le destinazioni e il server di posta elettronica deve essere rimossa prima di eliminare il server di posta elettronica. Se esistono contatti e-mail in sospeso da gestire, non sarà più possibile aprire i messaggi e-mail e dovranno essere scartati.

Aggiunta di una nuova destinazione

Qui è possibile associare le destinazioni con il corrispondente indirizzo e-mail.

1. Fare clic sulla scheda **Configurazione posta elettronica**
2. Fare clic sulla scheda **Destination (Destinazione)** e su **Tenant Name (Nome tenant)** per espandere la configurazione.
3. Fare clic sul menu a discesa **Default**, che rappresenta il tenant predefinito
4. Fare clic su **Aggiungi destinazione**. Compare una finestra popup **Aggiungi destinazione**. Configurare i seguenti parametri:
   - **Nome destinazione**: Il nome della destinazione. Questo è un campo obbligatorio
   - **Indirizzo e-mail**: Digitare l'indirizzo e-mail di destinazione. Questo è un campo obbligatorio.
   - **Descrizione**: Fornire una descrizione della destinazione. Questo è un campo opzionale
   - **Testo per Da**: Digitare un alias per l'indirizzo e-mail di destinazione. Questo alias viene visualizzato nella casella Da quando un utente risponde a un messaggio e-mail.
   - **Monitorata**: Attivare questo flag per monitorare la destinazione. Questo è un campo opzionale
   - **Disponibile per uscita**: Attivare questo flag per rendere disponibile la destinazione per i messaggi e-mail in uscita. Questo è un campo opzionale
   - **Server di posta elettronica**: Selezionare dal menu a discesa il server di posta elettronica a cui si desidera associare la destinazione.
5. Fare clic su **Aggiungi**

6. L'elenco delle destinazioni ora mostra la destinazione appena aggiunta.

Modifica di una destinazione

1. Fare clic sull'icona **Modifica destinazione** accanto alla destinazione che si desidera modificare

2. Compare la finestra popup **Modifica destinazione**
3. Modificare i parametri che si desidera modificare. È possibile modificare tutti i parametri.
4. Fare clic su **Salva**

L'elenco ora mostra i parametri aggiornati della destinazione modificata

Copia di una destinazione

È possibile copiare i parametri di una destinazione per crearne una nuova con un altro nome

1. Fare clic sull'icona **Copy Destination (Copia destinazione)** accanto alla destinazione che si desidera copiare

2. Compare la finestra popup **Copia destinazione**
3. Cambiare il nome della destinazione e l'indirizzo e-mail
4. Fare clic su **Aggiungi** per creare la destinazione

Eliminazione di una destinazione

1. Fare clic sull'icona **Elimina destinazione** accanto alla destinazione che si desidera eliminare

2. Compare la finestra popup **Elimina destinazione**
3. Fare clic su **SI** per eliminare la destinazione o su **NO** per interrompere l'eliminazione

Indice alfabetico