A MITEL
PRODUCT
GUIDE

Unify OpenScape Contact Center

Web Manager V11

Administration Guide
10/2024

A31003-S22B0-M102-02-76A9

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.

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Contents

1 About this guide . . . 5
1.1 Who should use this guide . . . 5
1.2 Formatting conventions . . . 5
1.3 Documentation feedback . . . 6
2 Web Manager . . . 7
2.1 Getting Started . . . 7
2.2 Access Details . . . 7
3 Single Sign On using SAML2 protocol . . . 9
4 Single Sign On with Circuit . . . 25
5 Virtual Agents . . . 27
5.1 Configuring Agent Users as Virtual Agents . . . 32
5.2 Configuring Actions for Virtual Agents . . . 32
5.2.1 Configuring a Requeue Action for Virtual Agents . . . 33
5.2.1.1 OpenMedia Requeue Action . . . 33
5.2.1.2 WebInteraction Requeue Action . . . 33
5.2.1.3 Speech Requeue Action . . . 33
5.2.2 Configuring Callback Action . . . 34
5.2.3 Configuring an External System Request for Virtual Agents . . . 34
5.2.3.1 Details about External System Request . . . 34
5.2.4 Configuring a WebInteraction Push URL Request for Virtual Agents . . . 35
5.3 Configuring Speech for Virtual Agents . . . 36
5.4 About Dialogflow Integration . . . 36
6 REST SDK . . . 39
7 CLIP for Outgoing Calls . . . 41
8 Multiple e-mails per tenant . . . 43
8.1 OAuth 2.0 Authentication . . . 47
8.1.1 Microsoft Azure configuration . . . 48
8.1.2 E-mail Account Configuration on OSCC Web Manager . . . 51
Index . . . 56

Contents

1 About this guide

This guide provides an overview of the OpenScape Contact Center Web Manager application and walks users through the various administration tasks that need to be performed on an ongoing basis.

1.1 Who should use this guide

This guide is intended for contact center administrators, who are responsible for configuration maintenance, and for supervisors and managers, who use the OpenScape Contact Center productivity tools.

1.2 Formatting conventions

The following formatting conventions are used in this guide:

Bold
This font identifies OpenScape Contact Center components, window and dialog box titles, and item names.

Italic
This font identifies references to related documentation.

`Monospace Font`
This font distinguishes text that you should type, or that the computer displays in a message.

NOTE: Notes emphasize information that is useful but not essential, such as tips or alternative methods for performing a task.

IMPORTANT: Important notes draw special attention to actions that could adversely affect the operation of the application or result in a loss of data.

1.3 Documentation feedback

To report an issue with this document, call the Customer Support Center.

When you call, be sure to include the following information. This will help identify which document you are having issues with.

- **Title:** Web Manager
- **Order Number:** A31003-S22B0-M102-02-76A9

2 Web Manager

2.1 Getting Started

Web Manager is an application that enables feature configuration in OpenScape Contact Center via a web browser.

2.2 Access Details

Web Manager is a browser-based application installed with the OpenScape Contact Center Application Server package.

To access the Web Manager, you must have the Master Administrator user logon profile.

With Web Manager you can configure:

- Single Sign On by using SAML2 protocol for Agent Portal Web
- Single Sign On with Circuit for Agent Portal Web
- Virtual Agents to enable chatbot functionality
- REST SDK
- CLIP for Outgoing Calls
- Email Configuration

To access the Web Manager, open a browser and enter the following url: *https://<OSCC_ApplicationServer_hostname_or_ip>/webmanager*

3 Single Sign On using SAML2 protocol

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between an identity provider and a service provider.

As most organizations already know the identity of users logged on to their Active Directory domain or intranet, this information can be used to Single Sign On (SSO) users to OpenScape Contact Center applications. OpenScape Contact Center supports SAML in the version 2.0 (SAML2).

NOTE: SSO via SAML2 is only supported for the web-based application Agent Portal Web. These SSO configurations do not apply to other applications, such as Agent Portal Java, Client Desktop or Manager Desktop, as they use the logon methods configured in Manager Desktop. Web Manager only supports OSCC logon method.

The SAML specification defines the following roles:

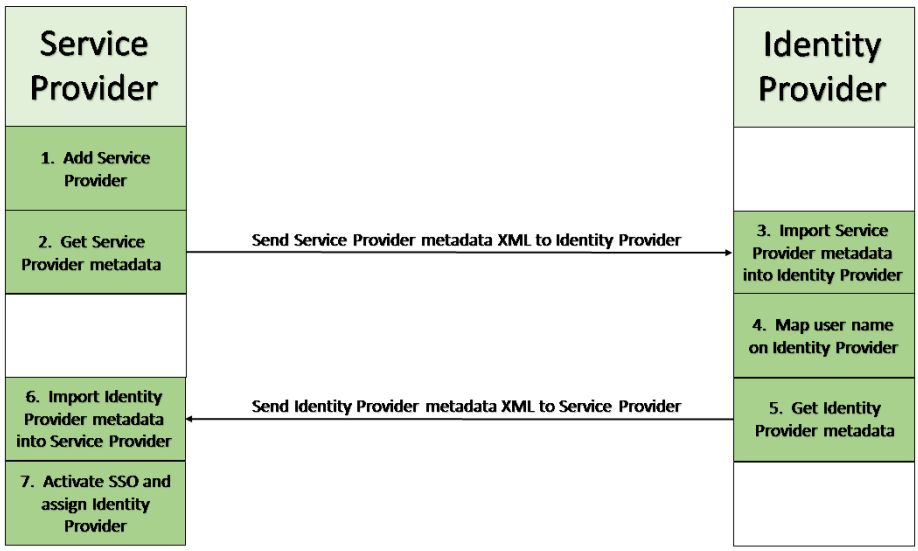
- **Service Provider (SP)**: This role is assigned to the Application Server, which runs the application.
- **Identity Provider (IdP)**: This role is assigned to a system entity (authentication authority) that offers the user authentication.
- **Tenant**: This role is assigned to the web browser, which uses the URL to run the application on the Application Server.

NOTE: There are many IdPs that can be used, for example ADFS or Gluu. Here we use Active Directory Federation Services (ADFS) as example to describe which information is needed to configure SSO in the OpenScape Contact Center solution. When other IdPs are used, the same information must be extracted from such IdPs.

NOTE: ADFS is an SSO solution offered by Microsoft. As a component of the Windows Server operating systems, it provides users with authenticated access to applications through Active Directory (AD).

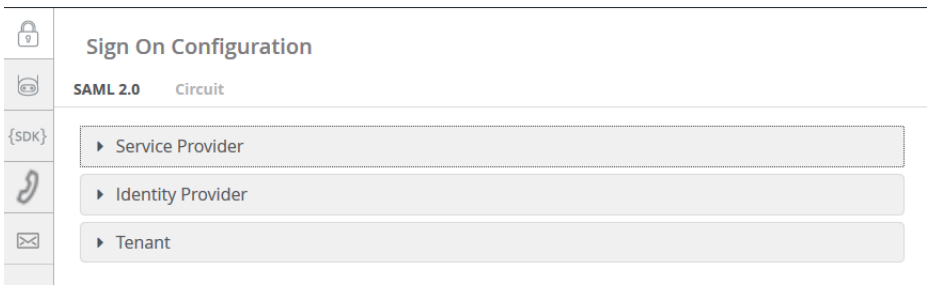
NOTE: The IdP service is a 3rd party application, which is not provided or supported by Unify. Due to this, the configuration examples for ADFS mentioned in this document may change.

The SSO is set-up in the Web Manager application by configuring the Service Provider on the OSCC side and by configuring the Identity Provider on the other side. The next figure shows the sequence of configuration steps:

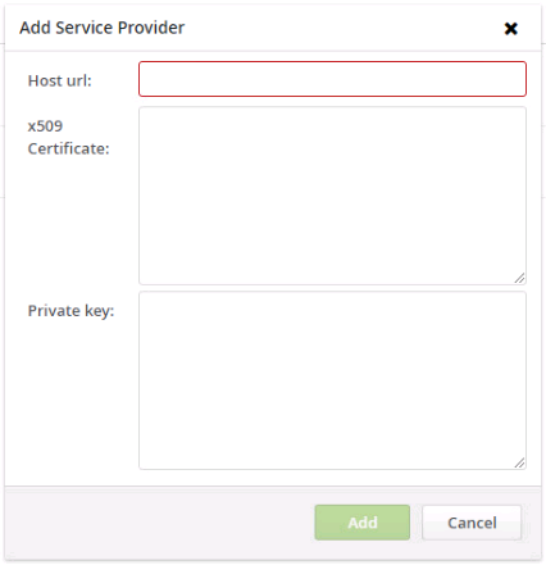


1. Add a Service Provider

    1. Login to the Web Manager application using the Master Administrator user and the corresponding password. Select **Sign On Configuration** and then select **Service Provider**.



2. Click **Add Service Provider** and the following window will pop-up:



- **Host url**: The URL of the Agent Portal Web service. For example:

  `https://<ApplicationServer_hostname_or_ip>/agentportal`

  This value must be the same URL as configured in the Agent Portal Web XML configuration file. To find this value, go to the machine where the application server is running and open the following file from the installation directory and copy the content of the element "service-provider-host-url":
  `.\ApplicationServer\ApacheWebServer\conf\webagent.xml`

- **Certificate**: An optional value for the Service Provider. It allows you to insert a certificate that will encrypt the messages sent to the IdP.

- **Public key**: An optional value for the key used in the certificate to validate the certification with the Service Provider. This value must be known on the Service Provider and the IdP.

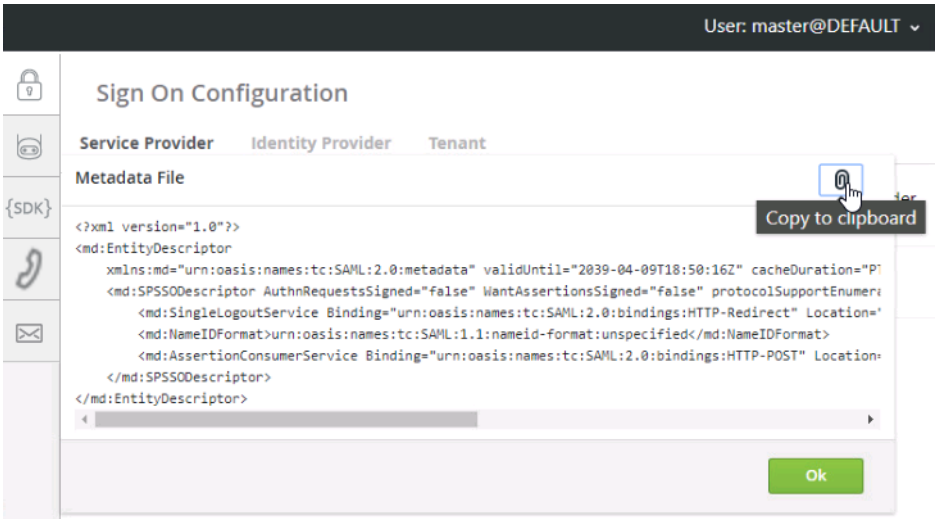
NOTE: For OpenScape Contact Center, the service provider will be the Agent Portal Web service itself. You can configure more than one Service Provider in the system.

---

2. Get Service Provider metadata

While still logged in the Web Manager application, get the Service Provider's metadata and import it to the Identity Provider service

1. Hover over the added Service Provider and click **Get Metadata**
2. Click **Copy to clipboard**, save the content to a text file on your machine and rename the file extension to "xml". Choose the file name in a way that it becomes clear that it contains the Service Provider metadata, for example:
   `OSCC_<customer>_metadata.xml`

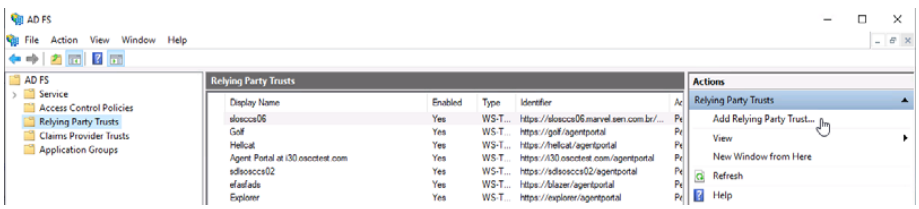


3. Import Service Provider metadata into the Identity Provider

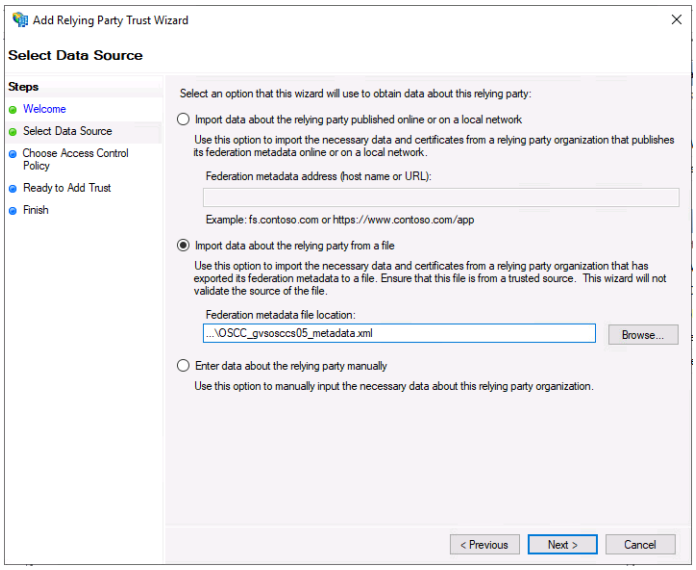
   You have to add the Service Provider as relying party to the Identity Provider by importing its metadata. Transfer the XML file created in step 2) to a location accessible by the Identity Provider and access the Identity Provider.

   The example below shows how the Service Provider metadata is imported into the Microsoft Active Directory Federation Service (ADFS):

   1. In the ADFS Management Console navigate to the folder: **Trust Relationships > Relying Party Trusts**
   2. Click **Add Relying Party Trust**

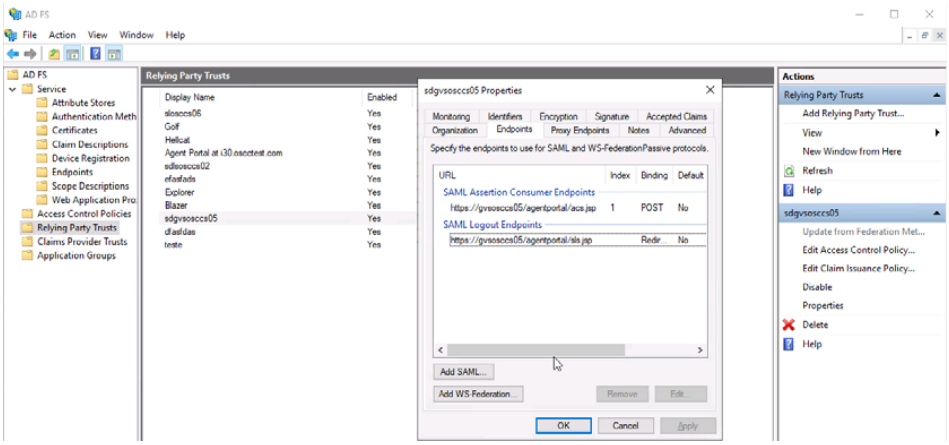


3. The **Add Relying Party Trust Wizard** screen appears. Click **Start**
4. Select **Import data about the relying party from a file** and select the XML file which was created in step 2). Use **Browse...** to locate the file.



5. Click **Next**
6. Give any name in the **Display name** field
7. Click **Next**
8. Select **Permit all users to access this relying party**
9. Click **Next**
10. Click **Close**

The figure below shows the system with the new relying party trust.

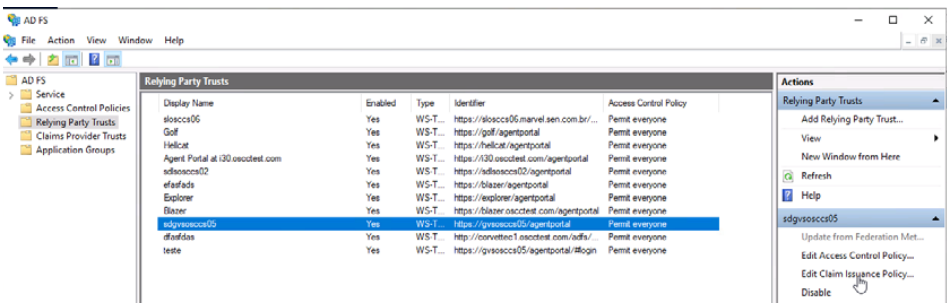


4. Map user name on Identity Provider

Add a claim rule must for the relying party trust created in step 3).

Claim rules are used to map an incoming claim type to an outgoing claim type. In the claim rule you specify which field in the user database of the Identity Provider matches the OSCC user name.

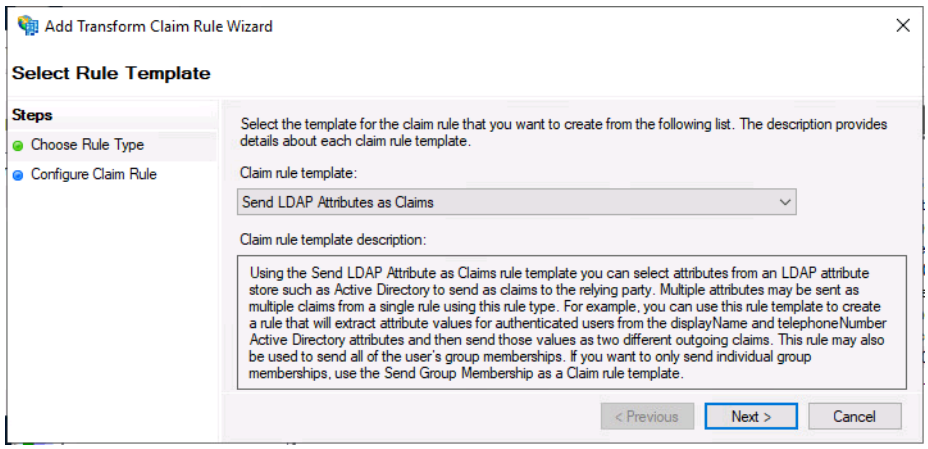
1. In the ADFS Management Console, select the relying party trusts created and click **Edit Claim Issuance Policy...**



2. Click **Add Rule...** to open the claim rule wizard.

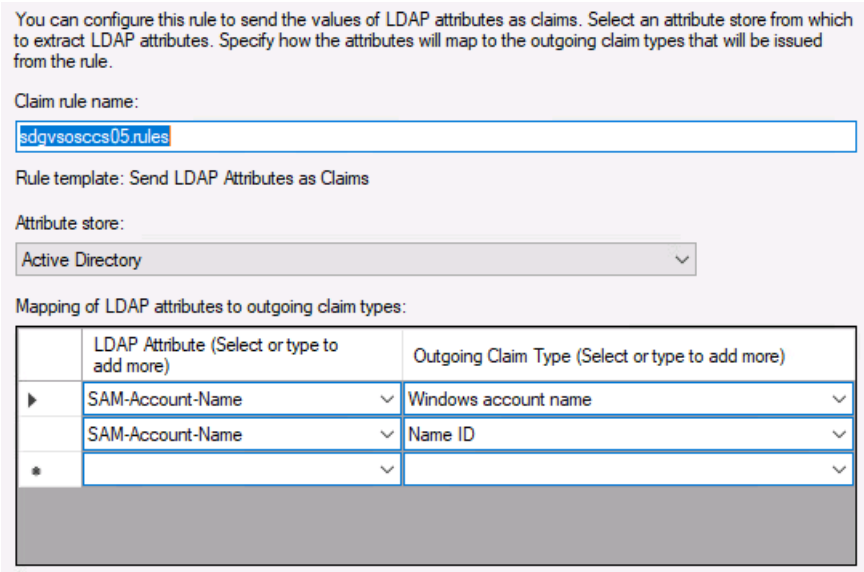
3. In the **Select Rule Template** window, select **Send LDAP Attributes as Claims** from the drop-down menu.

NOTE: In the following example, the OSCC user name is being authenticated by using LDAP.



4. Click **Next**

5. **Mapping of LDAP attributes to outgoing claim types** (Active Directory) which will be used for authentication by SAML



NOTE: In this example, the Windows account name is being used to map the OSCC user name, which is configured in the LDAP (Active Directory) server. For ADFS, the Name ID mapping is additionally required.

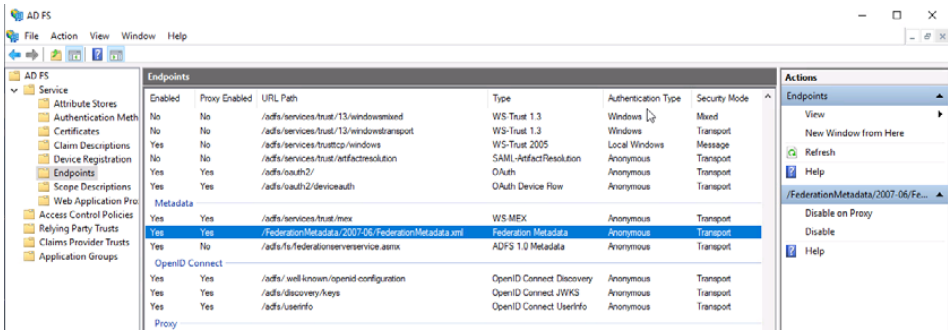
6. Click **Finish**

5. Get Identity Provider Metadata

   After configuring the Identity Provider, import its metadata into the Service Provider.

   As can be seen from the Endpoints directory of the ADFS Management Console the metadata is accessible through:

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



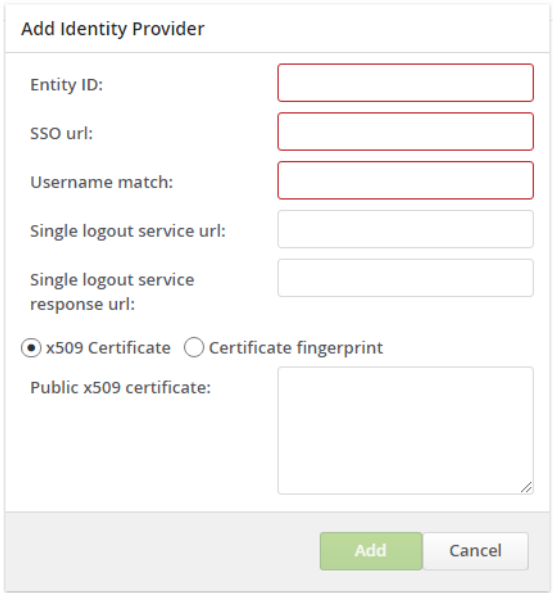
Create a copy of the FederationMetadata.xml file on your machine.

6. Import Identity Provider metadata into Service Provider

   1. Login to the Web Manager application using the Master Administrator user credentials. Select **Sign On Configuration** and then select **Identity Provider**.

      You can either add an Identity provider manually via **Add Identity Provider** or add one automatically via **Import from metadata**. It is recommended to add an identity provider by import. Transfer the XML file created in step 5 to a location accessible by the Service Provider.

If you decide to add an Identity Provider manually, click **Add Identity Provider** and a pop-up window will appear with the following configuration:



NOTE: All configurations can be retrieved from the Identity Provider metadata file.

- **Entity ID**: Identifier of the IdP entity (must be a URL). In the metadata, this URL is found by searching the attribute **entityID**, in tag **EntityDescriptor**.
- **SSO url**: SSO endpoint information of the IdP. This is the URL target of the IdP where the SP sends the Authentication Request Message. In the metadata, this URL is found inside the tag **IDPSSODescriptor** by searching the attribute **Location**, in tag **SingleSignOnService**.

NOTE: Use the **Location** value from the line that has value "**...HTTP-POST**" in the attribute **Binding**.

- **Username match**: This is the parameter returned by IdP which will be compared with the configured OSCC user.

In the metadata, for example from ADFS, the **Windows account name** as **Outgoing Claim Type** was selected (see step 4 - **Map user name on Identity Provider - Add Rule**). When searching for the **Windows account name** value in the metadata file, the **Username match** value can be found under the attribute **Name**. In this example it is:

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

In general, the value of the **Username match** parameter has to match to the outgoing claim type configured for mapping SAML LDAP attributes in the IdP, see step 4) **Mapping of LDAP attributes to outgoing claim types**. It is the LDAP parameter value used by ADFS to identify (match) the OSCC user.

NOTE: Other IdPs will have a different user name match.

- **Single logout service URL**: The URL Location of the IdP where the SP will send the Single Logout (SLO) Request to. In the metadata, this URL is found inside the tag **IDPSSODescriptor** by searching the attribute **Location**, in the tag **SingleLogoutService**.

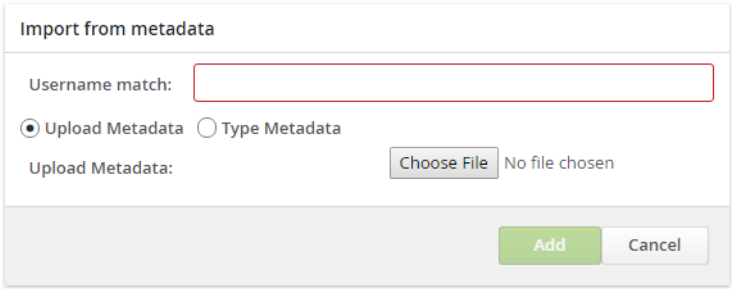
NOTE: Use the **Location** value from the line that has value "**...HTTP-POST**" in the attribute **Binding**.

- **Single logout service response URL**: The URL Location of the IdP where the SP will send the Single Logout (SLO) Response. This value is optional, and it is usually left blank. By leaving it blank, the same URL as **Single logout service URL** will be used as the SLO response endpoint information of the IdP. Some IdPs use a separate URL for sending a logout request and response, use this property to set the separate response URL.
- **x509 Certificate**: The public x509 certificate of the IdP. In the metadata, this certificate value is found by searching the tag **X509Certificate**, inside the tag **IDPSSODescriptor**, and inside the tag **KeyDescriptor** with attribute **use="signing"**.

NOTE: When you are entering a certificate manually, make sure it has only the hash line; remove any comments and extra lines before or after it.

- **Certificate fingerprint**: Instead of using the whole x509 certificate you can use a fingerprint. When a fingerprint is provided, then the Fingerprint Algorithm is required to let the OSCC know which Algorithm was used. Possible values are: SHA1, SHA256, SHA384, SHA512.

If you decide to add an Identity Provider by importing metadata, click **Import from metadata**, which is the recommended approach to configure the IdP.



- **Username match**: This is the parameter returned by IdP which will be used to compare with the configured OSCC user.

In the metadata, for example from ADFS, the **Windows account name** as **Outgoing Claim Type** was selected (see step 4 - **Map user name on Identity Provider - Add Rule**). When searching for the **Windows account name** value in the metadata file, the **Username match** value can be found under the attribute **Name**. In this example it is:

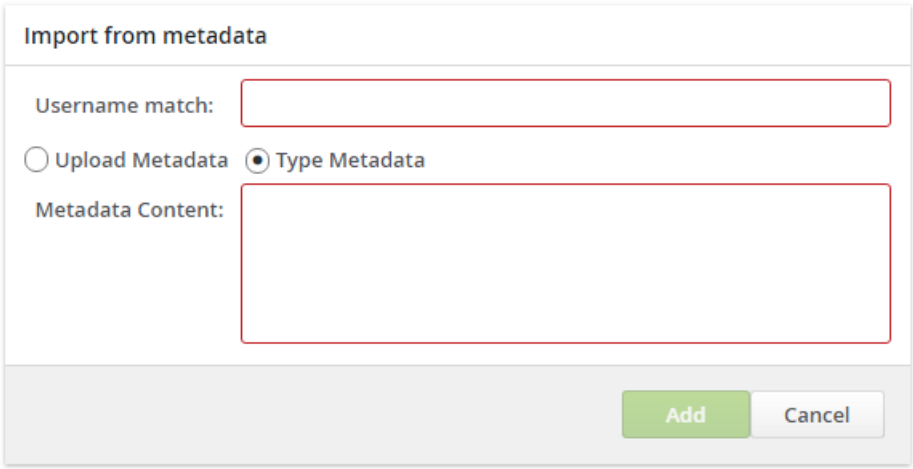
```
http://schemas.microsoft.com/ws/2008/06/identity/
claims/windowsaccountname
```

In general, the value of the **Username match** parameter has to match to the outgoing claim type configured for mapping SAML LDAP attributes in the IdP, see step 4) **Mapping of LDAP attributes to outgoing claim types**. It is the LDAP parameter value used by ADFS to identify (match) the OSCC user.

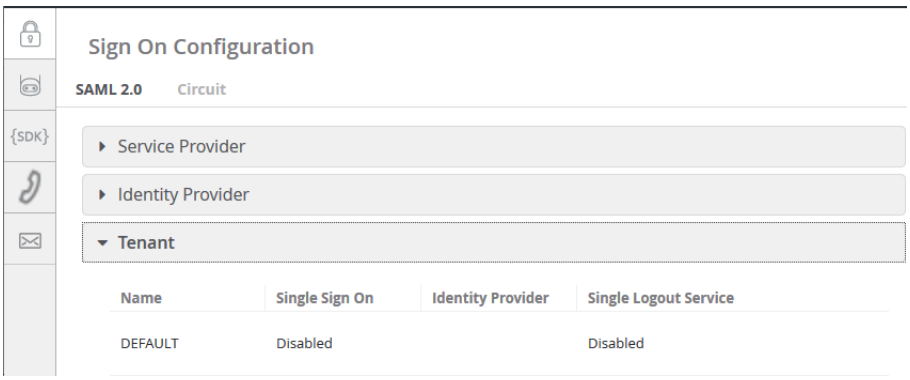
NOTE: Other IdPs will have a different user name match.

After filling **Username match**, select U**pload Metadata**, click **Choose File** and select the metadata file. Click **Add**.

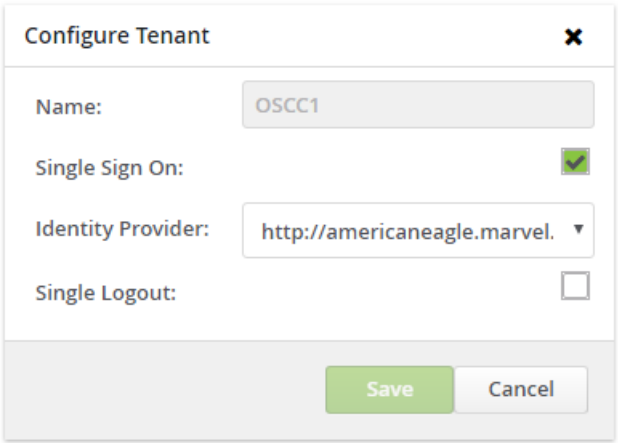
Another way is to select Type Metadata, edit or copy/paste metadata in the **Metadata Content** field. Click **Add**



7. Activate SSO and assign Identity Provider
    1. After importing the Identity Provider metadata into the Service Provider, still logged in the Web Manager application, click the **Tenant** tab.
    2. On the **Tenant** tab, there may be a list of tenants. Hover over the tenant and click **Edit**.



3. In the **Configure Tenant** window, enable or disable the **Single Sign On** and **Single Logout** functionalities:



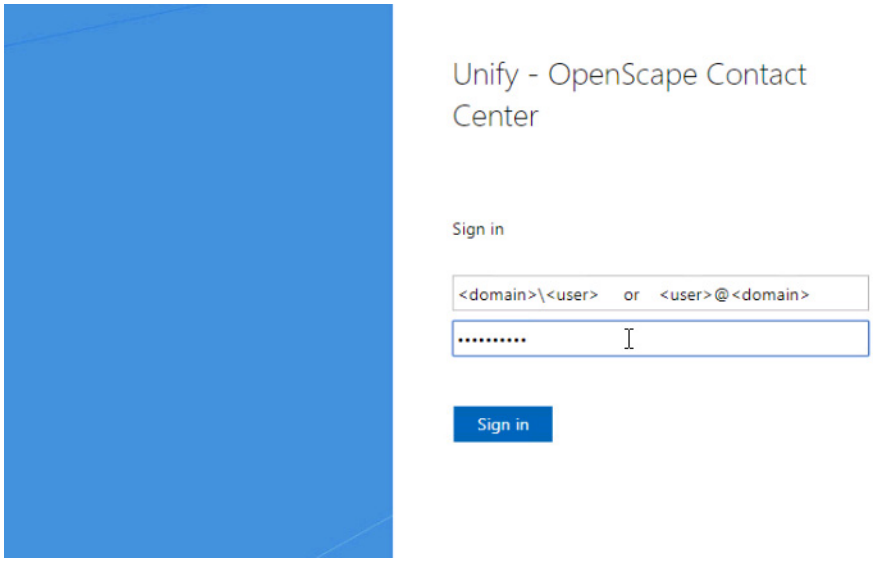
- **Single Sign On**: Enables the SAML2 integration
- **Identity Provider**: Select the identity provider previously configured on the Identity Provider tab in step 6
- **Single Logout (SLO)**: When enabled and you log out from the Agent Portal Web, the system will logout from the Identity Provider server. When this option is enabled, the user is logged off from every other application using the same IdP.

NOTE: When you configure the OpenScape Contact Center for Single Tenancy, SSO via SAML2 is a system wide functionality. When you configure the OpenScape Contact Center for Multitenancy, SSO via SAML2 can be enabled per tenant. For those tenants where SSO via SAML2 is not enabled, the logon methods configured in Manager Desktop are applicable.

After the Single Sign On configuration has been completed, start the web browser and log in to the Agent Portal Web and type:

`https://<ApplicationServer_hostname_or_ip>/agentportal`

For the first authentication in that browser session, you will be redirected to the Identity Provider, as shown in the figure below:



1. Enter <user>@<domain> or <domain>\<user>, where:
   - <domain> is the customer domain name
   - <user>is the user configured in the Active Directory (Account Name)

     NOTE: <user> must also be configured as a user in OpenScape Contact Center

   - Enter the Active Directory password.

For further authentications (log in) in the same browser session, SSO will occur and no account and password need to be entered.

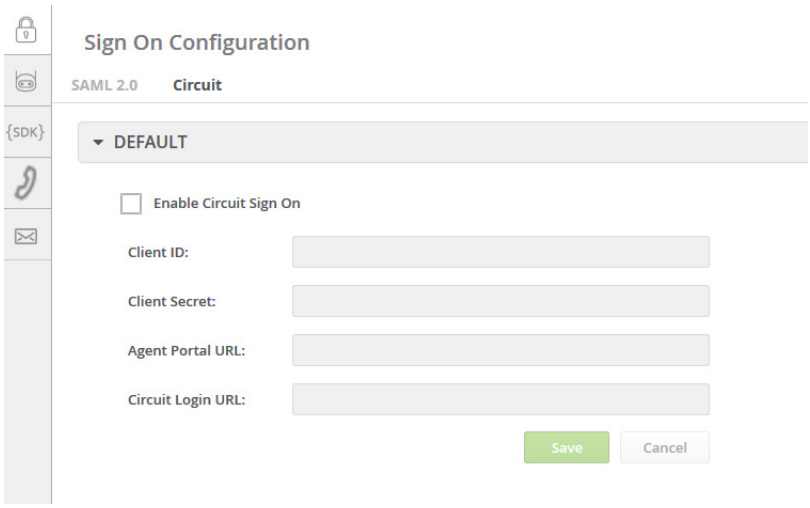
4 Single Sign On with Circuit

After configuring the custom application on Circuit (see *OpenScape Contact Center V11 Communication Platform Integration Guide*), it is necessary to synchronize the client ID and client secret information with OpenScape Contact Center.

Access the OSCC Web Manager application and log in with a tenant manager account. On "Sign On Configuration", select the "Circuit" tab and the OSCC tenant that have access to the Circuit integration feature.

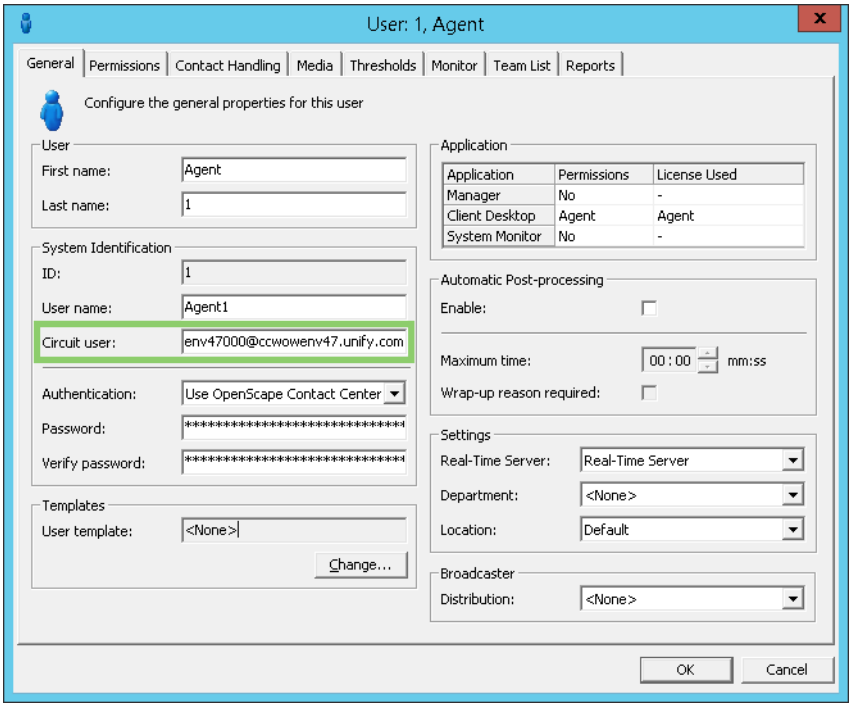
Fill in the fields below with the following information:

- **Enable Circuit Sign-on** - enabled.
- **Client ID**: The unique identifier of the application, obtained in the previous chapter.
- **Client secret**: Secret key for the application, obtained in the previous chapter.
- **Agent Portal URL**: The URL used to access the Agent Portal Web application. Follow the pattern of `https://<yourDomain>/agentportal`
- **Circuit Login URL**: The URL used to access the Circuit application.



Using the Circuit Sign On to authenticate on the OpenScape Contact Center login page, it is necessary to associate a Circuit account with the OpenScape Contact Center user. The Circuit user name (URI) is used for the association.

On the user configuration window, fill in the **Circuit User** field with the URI used to log in to Circuit. Two OSCC users in the same tenant cannot share the same Circuit user.



NOTE: When Circuit can only be accessed via an HTTPS proxy server, a special configuration is required in the Application Server. For more details on the configuration, see *OpenScape Contact Center V11 Installation Guide*

NOTE: For detailed information about the configuration of the OpenScape Voice and the addition of an application on Circuit, refer to the *OpenScape Contact Center V11 Communication Platform Integration Guide*.

5 Virtual Agents

The Master Administrator user must logon to the Web Manager for configuring Virtual Agents in OpenScape Contact Center.

The Virtual Agent feature enables the integration of the OpenScape Contact Center with a Natural Language Processor (NLP) to include chatbots.

The Virtual Agent service runs into the OSCC Application Server container, and will logon all agents configured in the Web Manager.

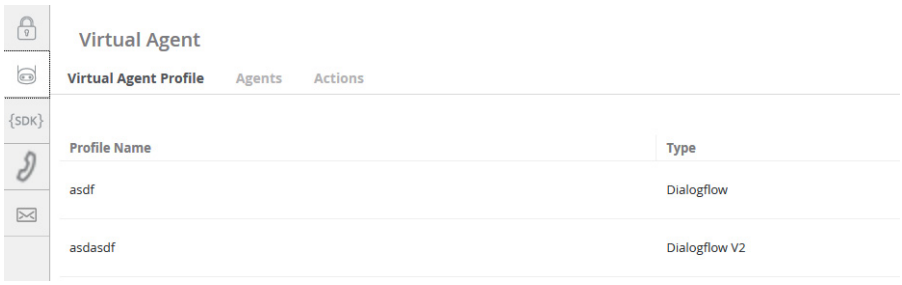
NOTE: The Virtual Agent only supports the OpenScape Contact Center password type. The system will not work with Windows logon or SAML2 SSO.

NOTE: The Virtual Agent functionality is a SYSTEM wide configuration. If OpenScape Contact Center has Multitenancy enabled, each tenant demands one or more CMS deployed to provide speech support. Each CMS can support one ore more Virtual Agent profiles. Each profile must be configured with a different GCP token. In the OSCC Application Server, the `virtualagent.xml` configuration file must have the correct business unit name.

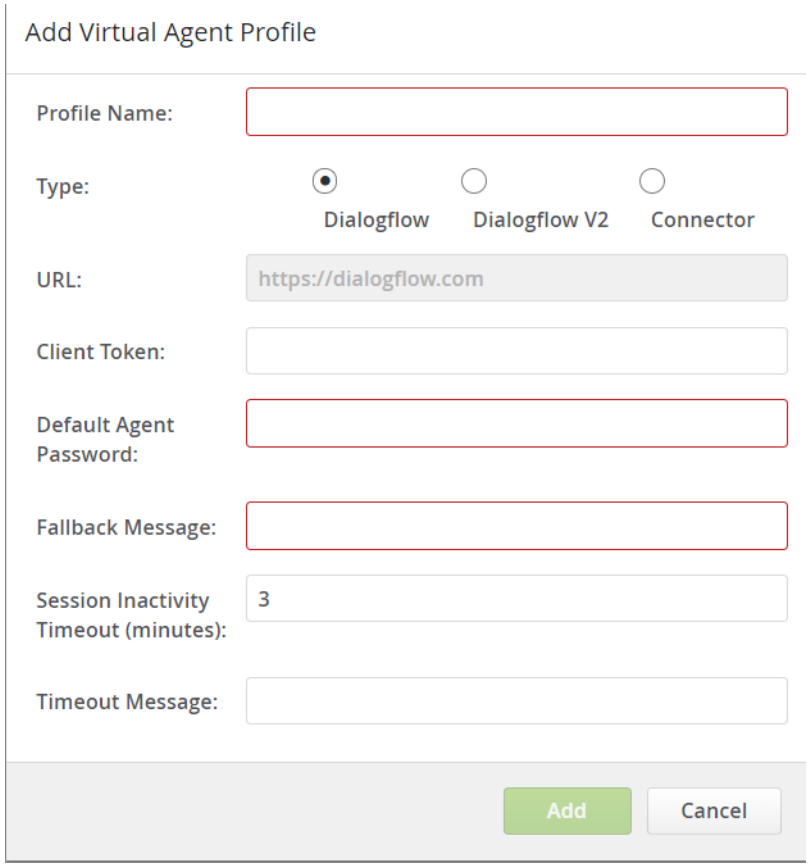
NOTE: **Automatic Post-processing** and **Mandatory wrap-up reason** are not supported by Virtual Agent. Be sure that these features were disabled in the user's configuration.

Login to Web Manager and follow the steps below:

- Go to the **Virtual Agent** tab:



- Click **Add Virtual Agent Profile**. The **Add Virtual Agent Profile** window will pop up. This is the form for the NLP profile configuration:



  - **Profile Name**: This is a mandatory field. The name of Virtual Agent NLP profile
  - **Type**: The Virtual Agent's Profile type. You can select one of the following radio buttons:
    - Dialogflow
    - Dialogflow V2
    - Connector

  Depending on the selected Type, you have to configure different parameters.

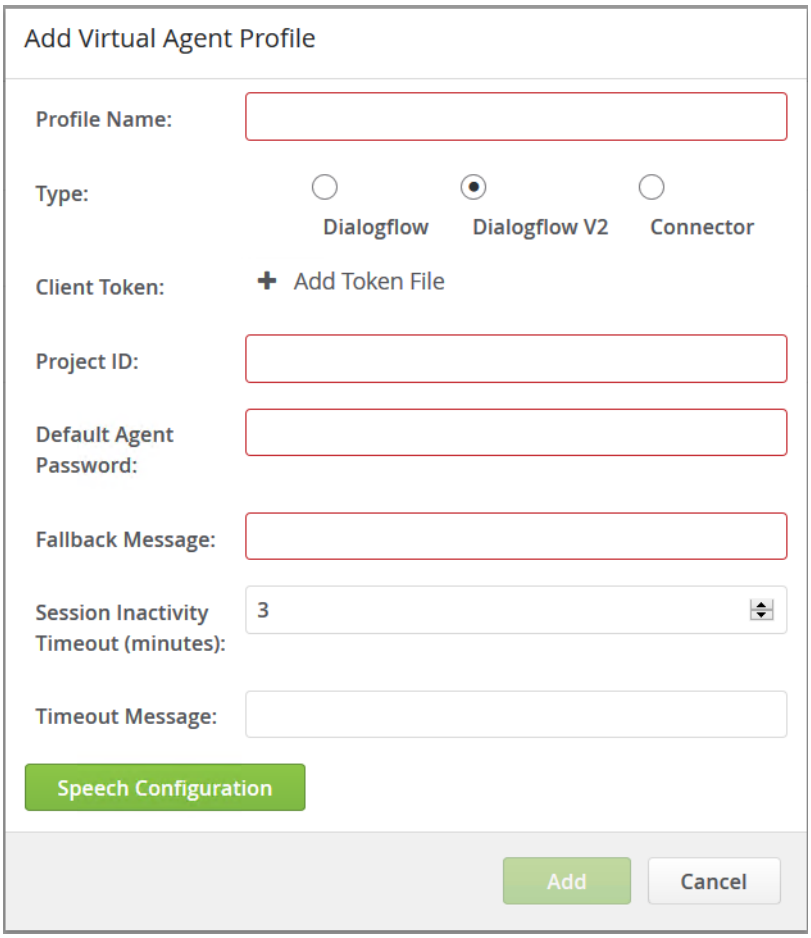
  Type: Dialogflow

  - **URL**: The Dialogflow's engine URL. Default value is https://dialogflow.com
  - **Client Token**: The client token provided by Dialogflow

- **Default Agent Password**: The password configured in manager for the users that are configured to behave as a Virtual Agent. Important to use the same password for all Virtual Agent user configuration
- **Fallback Message**: This is a system fallback message. If some error occurs to the system, this message will be sent externally for the person who has reached the contact center
- **Session Inactivity Timeout**: If the current contact session is inactive, the session will be finished automatically by the system according to the configured time in minutes
- **Timeout Message**: This is the message sent after the session's inactivity timeout

Type: Dialogflow V2

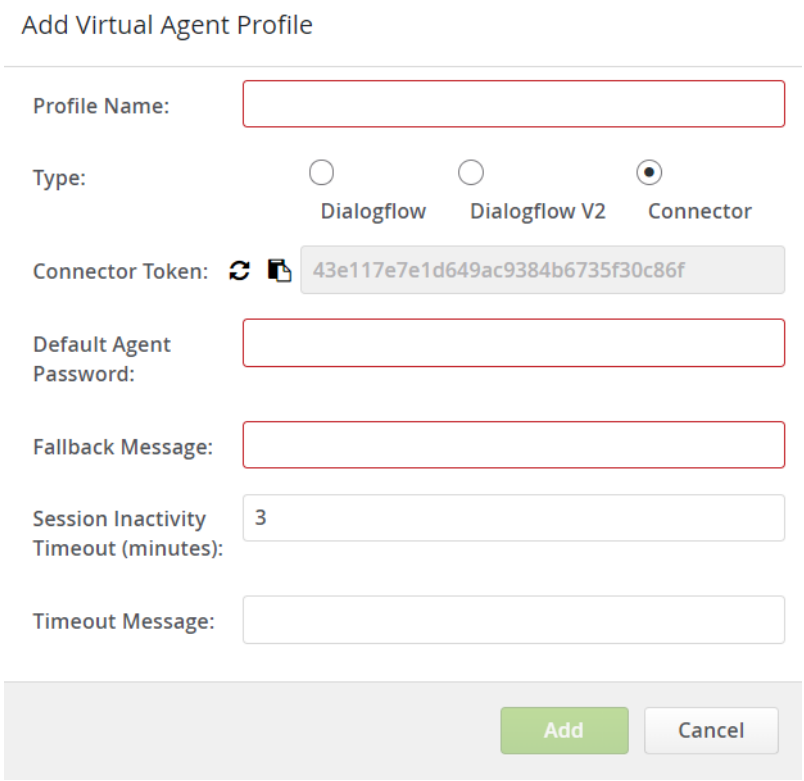
The **Add Virtual Agent Profile** window will have the following form for the NLP profile configuration:



- **Client Token**: Click **Add Token File** and browse on your pc to find the Token file, a *.json file, you want to use
- **Project ID**: The ID of the project
- **Default Agent Password**: This is a mandatory field. The password configured in manager for the users that are configured to behave as a Virtual Agent. Important to use the same password for all Virtual Agent user configuration
- **Fallback Message**: This is a mandatory field. This is a system fallback message. If some error occurs to the system, this message will be sent externally for the person who has reached the contact center
- **Session Inactivity Timeout**: If the current contact session is inactive, the session will be finished automatically by the system according to the configured time in minutes
- **Timeout Message**: This is the message sent after the session's inactivity timeout
- **Speech Configuration**: This button allows you to configure the Speechbot

Type: Connector

The **Add Virtual Agent Profile** window will have the following form for the NLP profile configuration

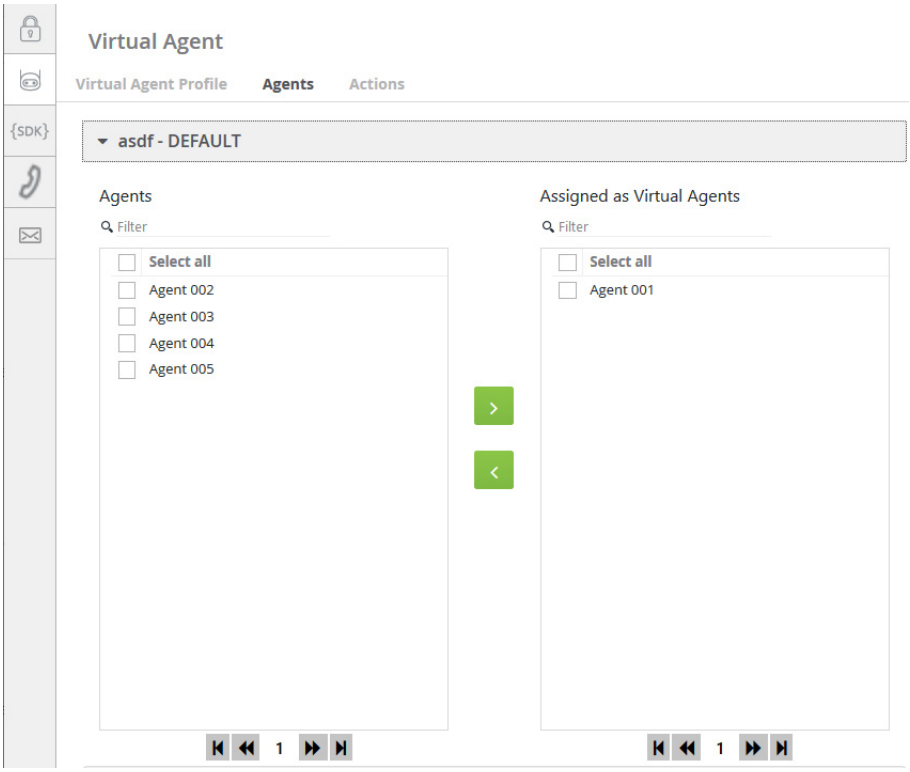


- **Connector Token**: Click the **Reload** button to generate a new Token. The new Connector Token is shown on the greyed out field. Click the **Clipboard** button to copy the Token to clipboard
- **Default Agent Password**: This is a mandatory field. The password configured in manager for the users that are configured to behave as a Virtual Agent. Important to use the same password for all Virtual Agent user configuration
- **Fallback Message**: This is a mandatory field. This is a system fallback message. If some error occurs to the system, this message will be sent externally for the person who has reached the contact center
- **Session Inactivity Timeout**: If the current contact session is inactive, the session will be finished automatically by the system according to the configured time in minutes
- **Timeout Message**: This is the message sent after the session's inactivity timeout

5.1 Configuring Agent Users as Virtual Agents

For the virtual agents, it is necessary to assign users with the Agent profile registered in OSCC.

To assign users, go to the **Agents** tab and expand the profile view:



NOTE: There are filters to help on the choice of agent users in the system.

5.2 Configuring Actions for Virtual Agents

The Virtual Agent feature can process some actions received from the NLP processor.

Usually an action is a text string sent by the NLP processor with a set of parameters.

There are several possible actions:

- **Requeue Action**: Enables the system to handover from the Virtual Agent to a person by requeueing the contact to another queue.

- **Callback action**: Enables the system to handover from the Virtual Agent to a person by creating a telephony callback on OSCC.
- **External System Request**: Enables the system to make a query to other third party systems to help the solution with a more elegant reply to customers.
- **WebInteraction Push URL**: Enables the system to make a query to other URLs to help the solution with a more elegant reply to customers
- **Speech Requeue**: Action to select the Requeue target

5.2.1 Configuring a Requeue Action for Virtual Agents

5.2.1.1 OpenMedia Requeue Action

To configure an OpenMedia requeue action, select the Media Type as **OpenMedia** and set:

- **Action Name**: A text value that must be equal to the action received from the NLP system. (Mandatory)
- **Requeue Queue**: The queue used to requeue the contact. This is a mandatory field. Select a value from the list and click **Add**.

5.2.1.2 WebInteraction Requeue Action

To configure an WebInteraction requeue action, select the Media Type as **WebInteraction** and set:

- **Action Name**: A text value that must be equal to the action received from the NLP system. (Mandatory)
- **Requeue Queue**: The queue used to requeue the contact. This is a mandatory field. Select a value from the list and click **Add**.

5.2.1.3 Speech Requeue Action

To configure an Speech requeue action, select the Media Type as **Speech** and set:

- **Action Name**: A text value that must be equal to the action received from the NLP system. (Mandatory)

- **Requeue Target**: The target used to requeue the contact. This is a mandatory field. Select a value from the list and click **Add**.

5.2.2 Configuring Callback Action

To configure a callback action, select the action type as **Callback Action** and set:

- **Action Name**: A text value that must be equal to the action received from the NLP system. (Mandatory)
- **Callback Queue**: The queue used to create the callback. (Mandatory)
- **Phone Parameter Name**: The parameter name to get the phone number from the NLP system. (Mandatory)
- **Schedule Time Parameter Name**: The parameter name to get the Date and Time for the callback schedule. (Mandatory)

5.2.3 Configuring an External System Request for Virtual Agents

To configure an external system request action, select the action type as **External System Request** and set:

- **Action Name**: A text value that must be equal to the action received from the NLP system. (Mandatory)
- **External System URI Parameter**: A parameter name defined by the NLP system that contains the URI address to where the Virtual Agent system must send the request. (Mandatory)

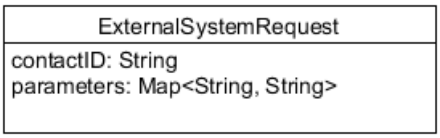
5.2.3.1 Details about External System Request

The External system request feature is an internal REST interface client, implemented into the Virtual Agent service.

Every time the Virtual Agent receives an action to make an external consultation from NLP, the system will send a POST request to the URI defined in the parameter with a pre-defined JSON object.

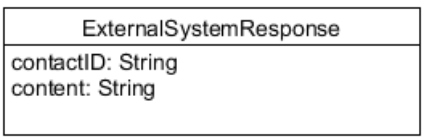
There are two JSON objects, one for the request and the other for the response.

The request object sent by Virtual Agent is:



- **contactID**: The attribute containing the OSCC contactID value
- **parameters**: A collection of parameters received from the NLP processor composed by a key/value text. These parameters will be processed by the external system

The response object received by Virtual Agent must have the following structure:



- **contactID**: This value must be the same received on the ExternalSystemRequest object. (Mandatory)
- **content**: The text processed by the external system with the response content for the request.

5.2.4 Configuring a WebInteraction Push URL Request for Virtual Agents

To configure a Webinteraction Push URL request action, select the action type as **WebInteraction Push URL** and set:

- **Action Name**: A text value that must be equal to the action received from the NLP system. (Mandatory)
- **Push URL Parameter**: A parameter name defined by the NLP system that contains the URL address to where the Virtual Agent system must send the request. (Mandatory)

5.3 Configuring Speech for Virtual Agents

The Virtual Agent feature allows you to configure a speechbot through the **Speech Configuration** button, where you can configure the following parameters. This button is only available for Virtual Agent profile type Dialog V2.

- **Enable speech**: A parameter to enable the speechbot for the selected profile. Default value: disabled
- **CMS address**: IP address/FQDN to access the CMS node.
- **CMS port**: Port to access the CMS node. Default value: 6017
- **Language**: The language to be used. Default value: EN-US
- **Gender**: The gender of the Text-to-Speech voice. Default value: male
- **Welcome message**: Message to be played when the call is answered by the Speechbot Virtual Agent.
- **Fallback requeue number**: Number to which the call is routed if the CMS is not reachable.

5.4 About Dialogflow Integration

The Virtual Agent feature is by default integrated to the Dialogflow engine for the Natural Language Processor.

NOTE: The default NLP processor for Virtual Agent is the Google's Dialogflow. For more information, follow the link: https://dialogflow.com

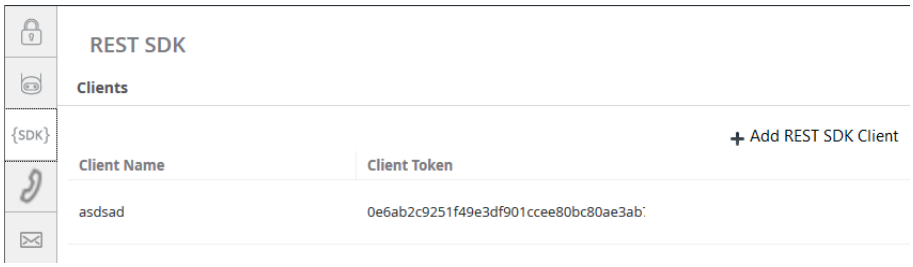
---

- **Dialogflow Standard Edition** is available for free at the Dialogflow’s web page. It provides the same features as Dialogflow Enterprise Edition but the interactions are limited by usage quotas and support is provided by the community and by e-mail. Dialogflow Standard Edition is ideal for small to medium businesses that want to build conversational interfaces or those who want to experiment with Dialogflow.
- **Dialogflow Enterprise Edition** is available as part of the Google Cloud Platform (GCP) and provides unlimited text and voice interactions, higher volume usage quotas, and support from Google Cloud support. Dialogflow Enterprise Edition is a premium offering,

available as a pay-as-you-go service. Dialogflow Enterprise Edition is ideal for businesses that need an enterprise-grade service that can easily scale to support changes in user demand.

For more information about the quotas, see: https://cloud.google.com/dialogflow-enterprise/quotas

6 REST SDK



The REST SDK Framework allows the development of multimedia applications that integrate with the OpenScape Contact Center system.

The framework consists of a REST interface, which allows sending commands from the application to the OpenScape Contact Center and sending monitoring events from the OpenScape Contact Center to the application.

Configuration

Configure the REST SDK instances by using the Web Manager. To create a new REST SDK instance:

1. Select the tab **REST SDK**
2. Click **+ Add REST SDK Client**
3. A pop-up window **Add REST SDK Client** appears. Configure the following parameters:
   - **Client Name**: The Client Name uniquely identifies the REST SDK instance and is a string with up to 32 characters.
   - **Client Token**: The Client Token is a type of a password, used to authenticate the REST SDK client during the registration process of the client on the server. The Client Token can be either manually configured or automatically generated.

     Click the **Reload** button to automatically generate a random 64 bytes new Client Token. The new Client Token is shown on the greyed out field. Click the **Clipboard** button to copy the Token to clipboard.
   - Click **Add**
4. The new REST SDK Client has been created.

7 CLIP for Outgoing Calls

The Calling Line Identification Presentation (CLIP) in the Agent Portal Web, refers to the calling line identification, used for outgoing calls. CLIP does not affect the current functionality of Callback regarding the definition of the Caller number. A list of calling numbers must be configured per tenant. CLIP is valid for all outgoing calls: from Make Call button, from Speed List, Directory Search and Activity Log.

You can configure CLIP for Outgoing Calls by using the Web Manager.

Here you can add/edit/delete the calling number(s) for the CLIP functionality.

Adding a new number

1. Click the **Telephony** tab
2. Click the **Default** drop-down menu, which is the default tenant
3. Click **Add Clip** Item. You can add up to ten numbers per tenant
4. A pop-up window **Add Clip Item** appears. Configure the following parameters:
   - **Number**: The calling number. It must have a string of numbers and no special characters. This is a mandatory field
   - **Name**: The name of the calling number. This is a mandatory field
5. Click **Add**

The list of CLIP numbers now shows the number you have just added. This number also appears in the available numbers in the CLIP functionality of Agent Portal Web in: **Settings > Agent > CLIP > Always use this value**

Editing a number

1. Click the **Edit Clip Item** icon next to the CLIP number you want to edit

2. The **Edit Clip Item** pop-up window appears
3. You can change the **Number** and/or the **Name** of the existing Calling number
4. Click **Update**

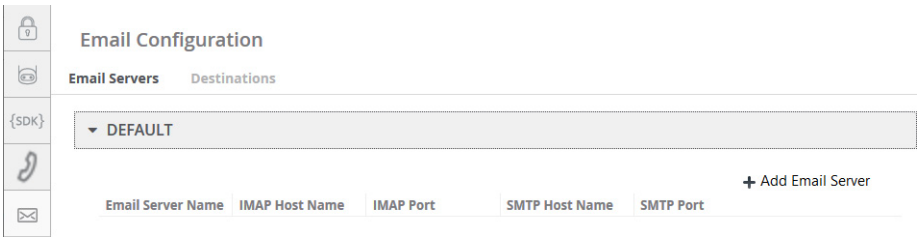
The list now shows the updated CLIP Number and/or Name

Deleting a number

1. Click the **Delete Clip Item** icon next to the CLIP number you want to delete

2. The **Delete Clip Item** pop-up window appears
3. Click **OK** to delete the CLIP number or **Cancel** to abort deletion

8 Multiple e-mails per tenant



This feature allows each Business Unit to have multiple E-mail Servers or E-mail addresses per Business Unit. You can configure the e-mail servers and the destinations through the Web Manager.

NOTE: Each Business Unit supports up to five e-mail configured credentials .

Adding a new E-mail Server

1. Click the **Email Configuration** tab
2. Click the **Email Servers** tab and then click the **Tenant Name** to expand the configuration.
3. Click **Add Email Server**. You can configure the same E-mail Server more than once, but with a different account name.
4. A pop-up window **Add Email Server** appears. Configure the following parameters:
   - **Email Server Name**: The name of the server. This is a mandatory field
   - Click the **IMAP Settings** drop-down menu and configure the following parameters:
     - **Host name**: The host name of the server. This is a mandatory field
     - **Port number**: The port number of the server. This is an optional field
     - **Use SSL**: Enable this flag to use SSL
     - **User name**: The user name of the account. This is a mandatory field
     - **Password**: The password of the account. This is a mandatory field

- **Confirm Password**: Confirm the password you gave in the previous parameter. This is a mandatory field
- **Maximum IMAP sessions**: The maximum number of IMAP sessions. Default value is 0, This is an optional field

- Click the **SMTP Settings** drop-down menu and configure the following parameters:
  - **Host name**: The host name of the server. This is a mandatory field
  - **Port number**: The port number of the server. This is an mandatory field
  - **Use SSL**: Enable this flag to use SSL
  - **Authentication**: Select from the drop-down menu: "None", "Use IMAP settings" and "Use settings below" to authenticate the next three parameters.
  - **User name**: Only configurable, when you have selected "Use settings below" from the Authentication parameter.
  - **Password**: Only configurable, when you have selected "Use settings below" from the Authentication parameter.
  - **Confirm Password**: Only configurable, when you have selected "Use settings below" from the Authentication parameter.
  - **Heartbeat E-mail Address**: The e-mail address used by the system to check whether the connection to the E-mail Server is working properly.
  - **Message rate limit**: The limit of e-mail messages sent per hour. The default value is 0 and means no limit.

5. Click **Add** to create a new server

The list of E-mail servers now shows the server you have just added.

When the feature E-mail Multiple Servers is enabled, the same account (E-mail Servers + Account Name) must not be used for different tenants. Every time a new e-mail server or a change to an e-mail server is submitted, verify whether the same account is already configured for other tenants.

Editing an E-mail Server

1. Click the **Edit Email Server** icon next to the Email server you want to edit

2. The **Edit E-mail Server** pop-up window appears
3. Modify the parameters you want to change. You can modify all parameters.
4. Click **Save**

The list now shows the updated parameters of the E-mail server

Copying an E-mail Server

You can copy an e-mail server’s parameters to create a new one with another name.

1. Click the **Copy Email Server** icon next to the server you want to copy

2. The **Copy E-mail Server** pop-up window appears.
3. Change the name of the server.
4. Click **Add** to create the new server.

Deleting an E-mail Server

1. Click the **Delete E-mail Server** icon next to the server you want to delete

2. The **Delete E-mail Server** pop-up window appears

3. Click **YES** to delete the E-mail Server or **NO** to abort deletion

---

NOTE: When deleting an E-mail Server, there will be a verification whether a destination is associated to it. In this case, the deleting the E-mail Server will not be allowed. The association between the destinations and the E-mail Server must be removed before deleting the E-mail Server. If there are pending e-mail contacts to be handled, it will not be possible to open the e-mails anymore and they must be discarded.

Adding a new Destination

Here you can associate the destinations with the corresponding E-mail Address.

1. Click the **Email Configuration** tab
2. Click the **Destination** tab and then click the **Tenant Name** to expand the configuration.
3. Click the **Default** drop-down menu, which is the default tenant
4. Click **Add Destination**. A pop-up window **Add Destination** appears. Configure the following parameters:
   - **Destination Name**: The name of the destination. This is a mandatory field
   - **Email Address**: Type the destination e-mail address. This is a mandatory field.
   - **Description**: Give a description to the destination. This is an optional field
   - **From Text**: Type an alias for the destination e-mail address. This alias appears in the From box when a user replies to an e-mail message.
   - **Monitored**: Enable this flag to monitor the destination. This is an optional field
   - **Available for outgoing**: Enable this flag to make the destination available for outgoing e-mails. This is an optional field
   - **Email server**: Select from the drop-down menu the e-mail server you want to associate the destination with.
5. Click **Add**
6. The list of destinations now shows the destination you have just added.

Editing a Destination

1. Click the **Edit Destination** icon next to the Destination you want to edit

2. The **Edit Destination** pop-up window appears
3. Modify the parameters you want to change. You can modify all parameters.
4. Click **Save**

The list now shows the updated parameters of the modified Destination

Copying a Destination

You can copy a Destination's parameters to create a new one with another name

1. Click the **Copy Destination** icon next to the Destination you want to copy

2. The **Copy Destination** pop-up window appears
3. Change the name of the Destination and the Email Address
4. Click **Add** to create the Destination

Deleting a Destination

1. Click the **Delete Destination** icon next to the Destination you want to delete

2. The **Delete Destination** pop-up window appears
3. Click **YES** to delete the Destination or **NO** to abort deletion

8.1 OAuth 2.0 Authentication

Starting with V11R0.1.0, the Open Scape Contact Center E-mail Server supports OAuth 2.0 Authentication.

8.1.1 Microsoft Azure configuration

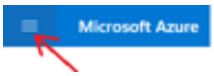
To create and configure the Microsoft Azure application, proceed with the following steps:

1. Open the Microsoft Azure portal: https://portal.azure.com/

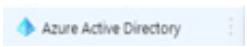
   To login, use the office365 account.

   Example: urus_365@8mdh07.onmicrosoft.com

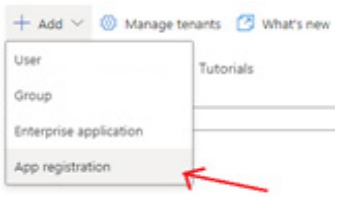
2. Click on the **Show Portal Menu** button, located in the top left corner.



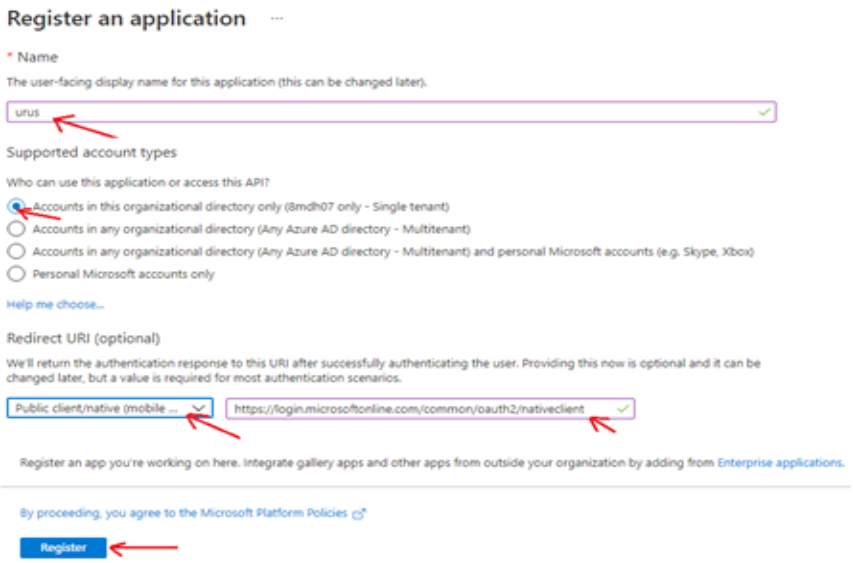
3. Click on the **Azure Active Directory** button.



4. Navigate to **Add -> App registration**

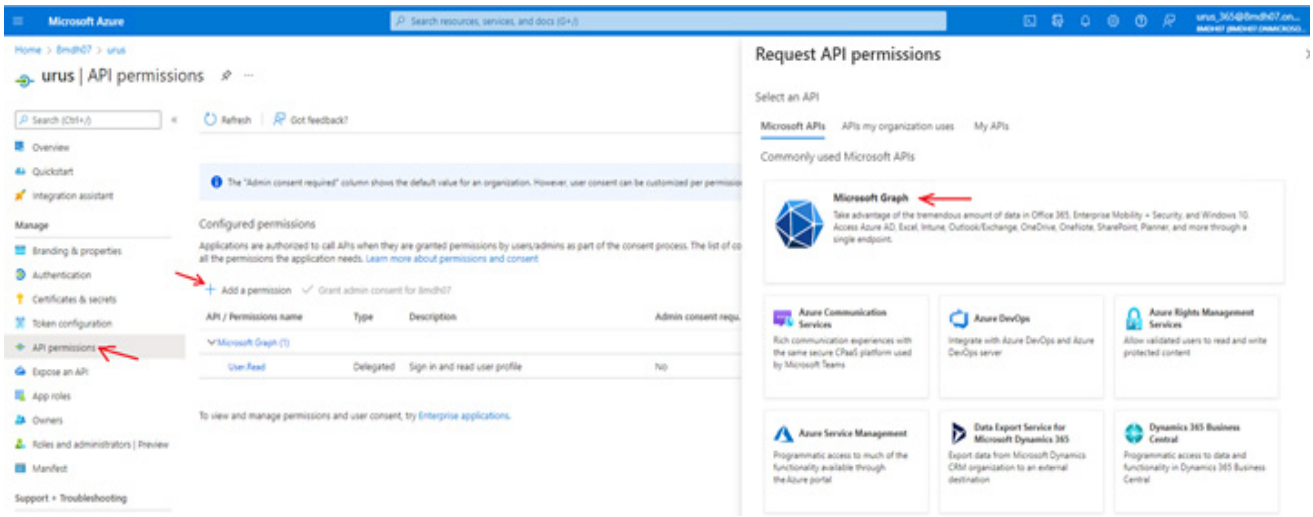


5. Register the application as shown below:



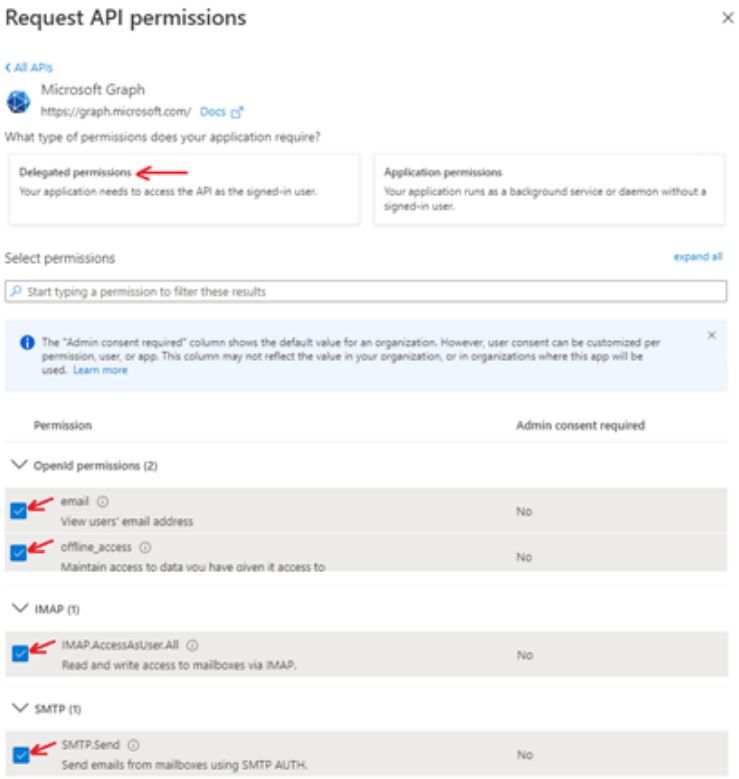
Finally, click the **Register** button.

6. Navigate to **API permissions -> Add Permission -> Microsoft Graph** and configure permissions for the registered application.



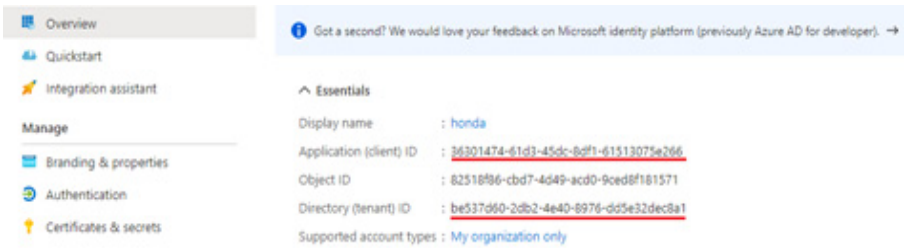
Configure the **Delegated permissions**:

- OpenId permissions:
  - email
  - offline_access
- IMAP
  - IMAP.AccessAsUser.All
- SMTP
  - SMTP.Send



Click the **Add permissions** button to save the configuration.

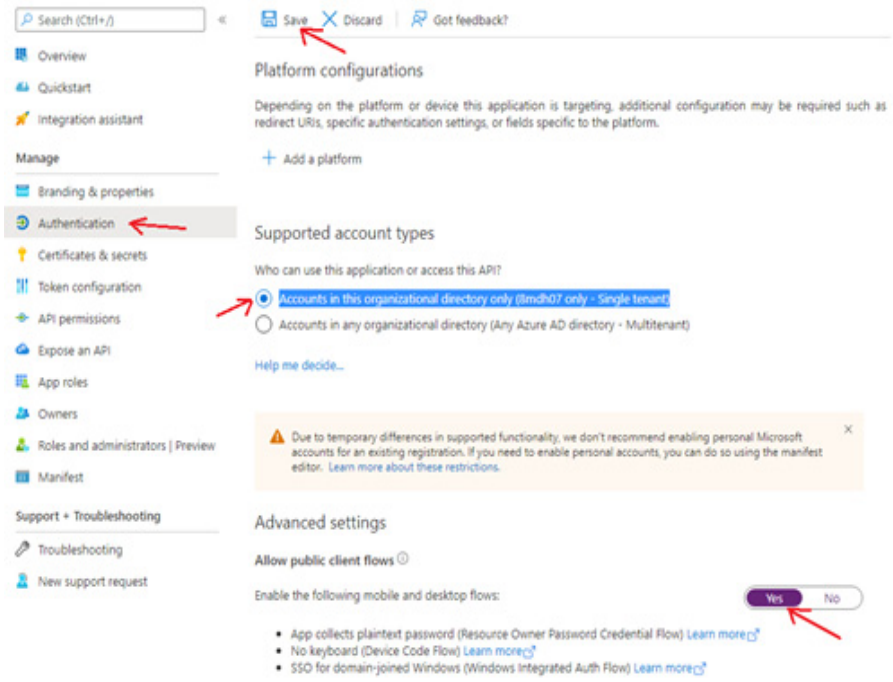
7. Navigate to **Overview** and copy the **Application (client) ID** and the **Directory (tenant) ID**.



NOTE: The **Application (client) ID** and **the Directory (tenant) ID** will be used for the OpenScape Contact Center Web Manager configuration.

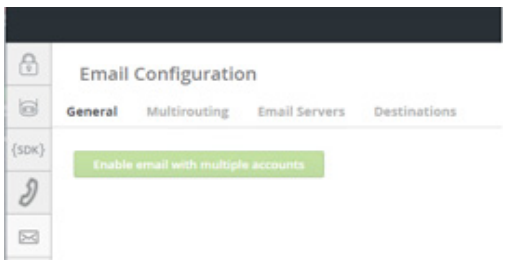
8. Navigate to **Authentication** and check the "Accounts in this organizational directory only (8mdh07 only - Single tenant)" option in the **Supported account types** section.

In the **Advanced settings** area, choose **Yes** for "Enable the following mobile and desktop flows" option.



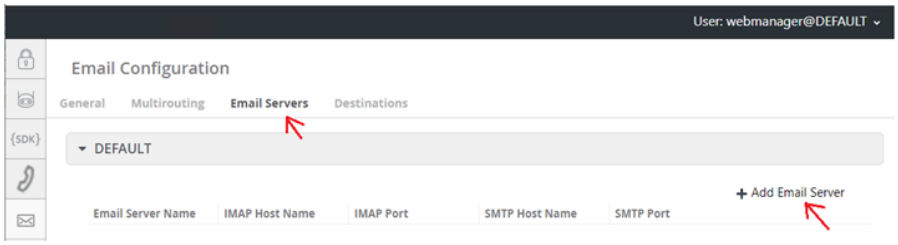
8.1.2 E-mail Account Configuration on OSCC Web Manager

1. Open the OpenScape Contact Center Web Manager: https://<OSCC Application Server>/webmanager



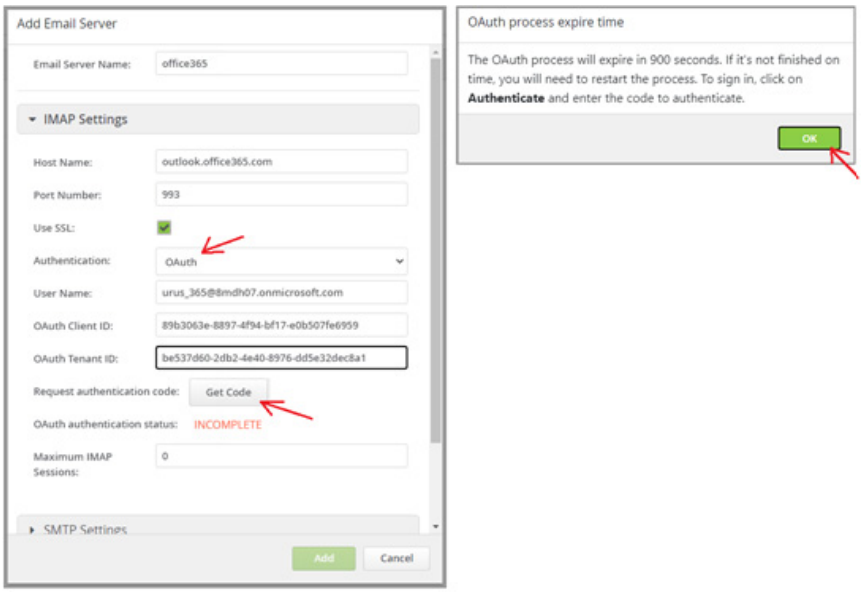
NOTE: E-mail with Multiple Accounts must be enabled. To enable the Multiple Accounts feature, see chapter Chapter 8, "Multiple e-mails per tenant".

2. Click on **Email Servers** and add an e-mail server, by clicking the **Add Email Server** button.

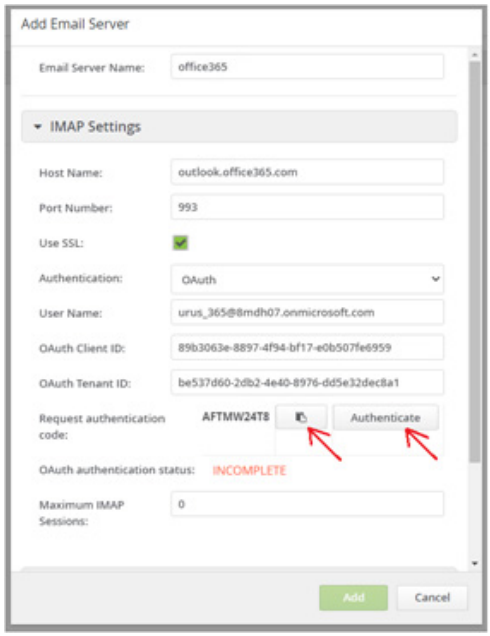


3. Configure the IMAP settings

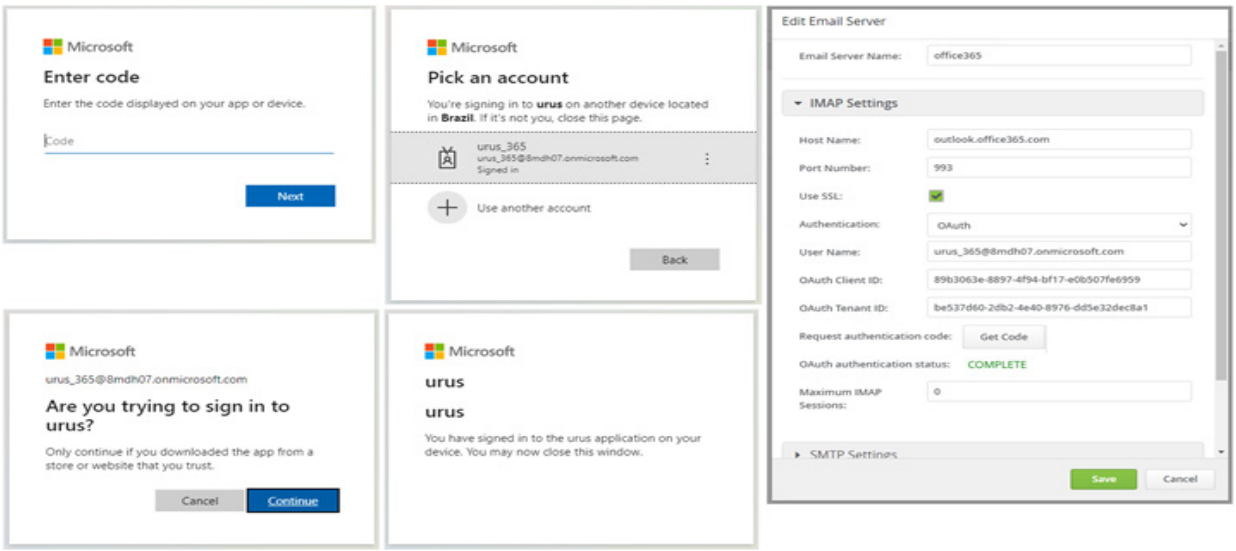
   – Enter the IMAP Account information and select OAuth in the Authentication field and click the **Get Code** button.



– Copy the generated code and click the **Authenticate** button.

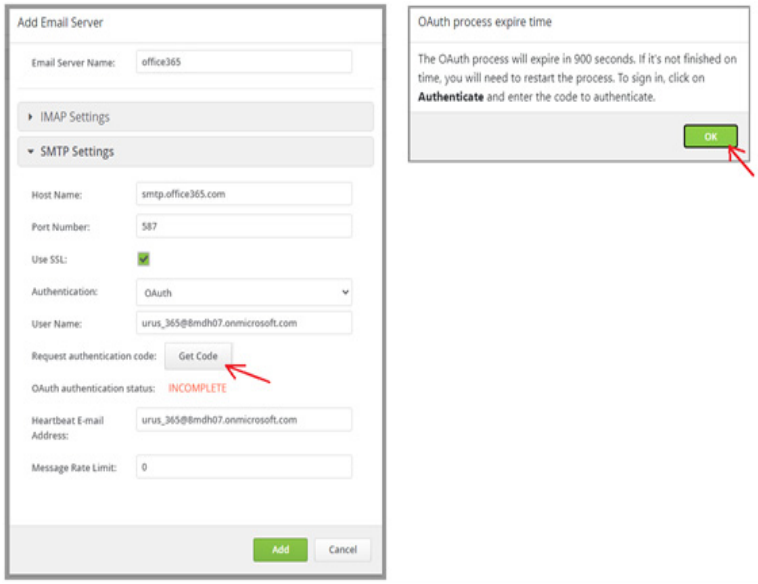


– Enter the code in the requested field and sign in the account.

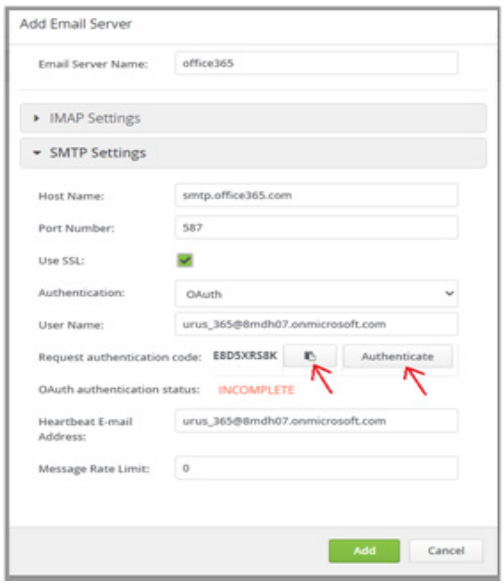


4. Configure the SMTP settings

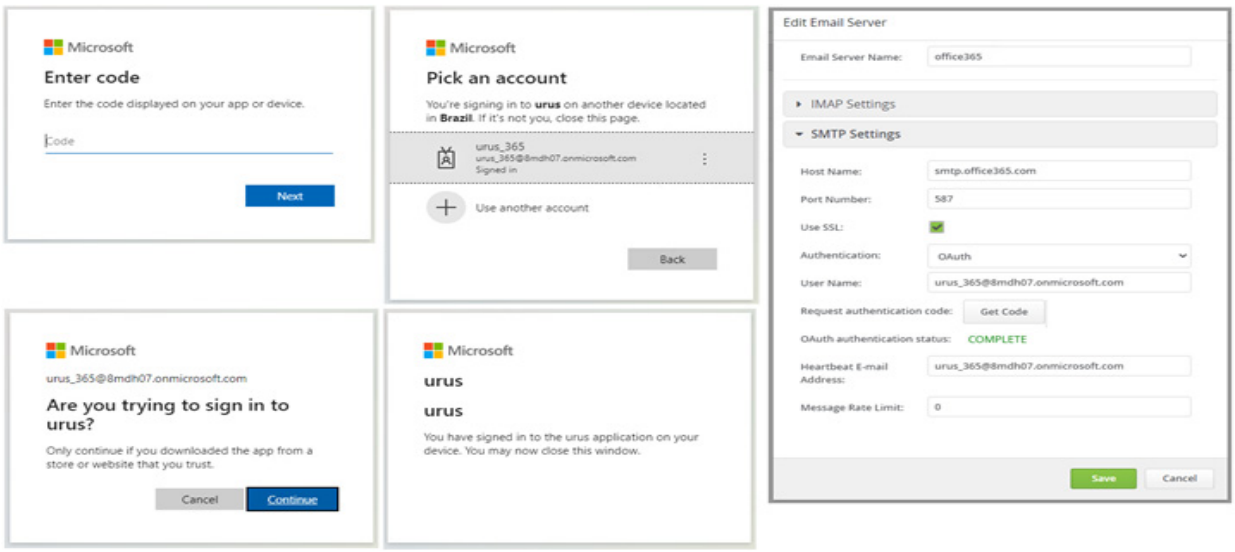
– Enter the SMTP account information, select the **OAuth** option in the Authentication field and click the **Get Code** button.



– Copy the generated code and click the **Authenticate** button.

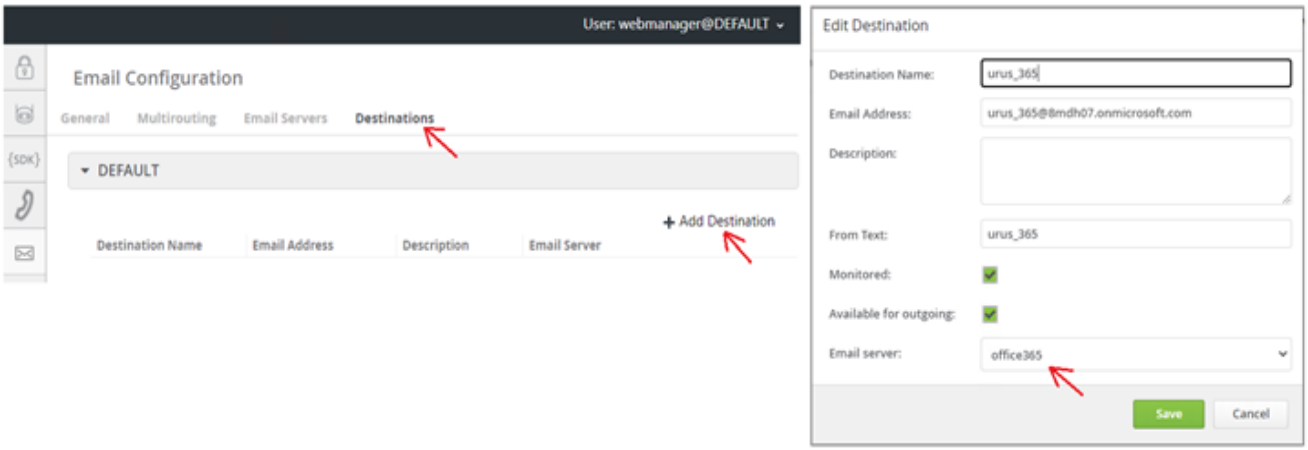


– Enter the code in the requested field and sign in the account.



5. Click on **Destinations** and create a new Destination by clicking the **Add Destination** button.

   Associate the new destination with the OAuth account.



Index

C
CLIP Telephony 41, 43

D
documentation
formatting conventions 5
intended audience 5
providing feedback 6

R
REST SDK 39

S
Single Sign On
using SAML2 protocol 9

V
Virtual Agents 27

W
Web Manager 7

© 2024 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.