

## Setting up the connectivity between C4C and HCP Application

---

### **Applies to:**

Cloud For Customer

### **Summary**

SAP Cloud for Customer (C4C) supports OData services. C4C provided standard OData services which has business entities like Account, Opportunities, Leads, Service Request, and Employee etc. Partners and customer can build extension applications using HANA Cloud Platform (HCP) by consuming these OData services. You need to configure connectivity to consume OData APIs from C4C. Depending on your scenario you can either use Basic or OAuth2.0 authentication for accessing C4C resources from extension solution.

**Author(s): Prabhat Raman**

**Company: SAP Labs, Palo Alto**

**Created on:** 25<sup>th</sup> August 2015

# Table of Contents

Prerequisites .....	3
Business Context .....	3
Setup OAuth2.0 Authentication .....	3
Setup Basic Authentication .....	8
Copyright .....	9

## Prerequisites

1. HCP account - you should have access to HCP trial or production account
2. You should have access to SAP Cloud for Customer with Admin authorization

## Business Context

To use SAP Cloud for Customer (C4C) OData APIs user has to configure the connectivity between C4C and HANA Cloud Platform (HCP). If your scenario requires the support of Single Sign-On (SSO), you register an OAuth2.0 client in the SAP Cloud for Customer system, and create and configure an HTTP destination with OAuth2.0 authentication in the SAP Cloud Platform account.

To setup the OAuth2.0 authentication following two steps are needed

1. Create and configure OAuth2.0 client in SAP Cloud for Customer to access OData
2. Configure the HTTP destination of "OAuth2SAMLBearerAssertion" Authentication type in HCP

If your scenario does not require SSO (for example, if you do not need ID federation or UI integration) you can use an HTTP destination with Basic Authentication. This scenario is possible if the SAP HANA Cloud Platform extension application can use a technical user.

To setup the Basic authentication following step is needed

1. Configure the HTTP destination of "BasicAuthentication" Authentication type in HCP

## Setup OAuth2.0 Authentication

### Create and configure OAuth2.0 client in SAP Cloud for Customer to access OData

Use this procedure to configure OAuth2.0 client in SAP Cloud for Customer OData for OData access to configure the connectivity to APIs.

1. Logon to the SAP HANA Cloud Platform cockpit, select the account, and then choose TRUST
  - a. On the Local Service Provider tap page, copy the entry in the Local Provider Name field.

Note - In case you don't find Local Provider Name click on Edit button and change Configuration Type to Custom. Here you will find the Local Service Provider entry. But don't save this setting.

- b. On the Local Service Provider tap page, copy the entry in the Signing Certificate field, and save it in the following format <account>\_signing.cer format.



- b. Specify the client secret (any password of your choice), client description, and token lifetime (in seconds).
- c. In the Issuer Name field, use the dropdown list to specify the identity provider that you created on step 2.
- d. Copy the entry in the Client ID field. You will need it later when creating the HTTP destination for the connectivity to the SAP Cloud for Customer OData APIs.
- e. In the Scope list, select the scopes to which you need access. Select UIWC:CC\_HOME
- f. Choose Save and Close.

#### OAuth 2.0 CLIENT REGISTRATION

Save and Close Close

Client ID:

\*Client Secret:

\*Description:

\*Issuer Name:

\*Token Lifetime (Seconds):

Scope

Scope ID	Description	Selected
UIWC.COD_MARKETING		<input type="checkbox"/>
UIWC.COD_PRODUCTDATA		<input type="checkbox"/>
UIWC.COD_SALES_WCF		<input type="checkbox"/>
UIWC.COD_SEOD_AGENT_QUEUE_WCF		<input type="checkbox"/>
UIWC.CC_HOME		<input checked="" type="checkbox"/>

## Configure the HTTP destination of “OAuth2SAMLBearerAssertion” Authentication type in HCP

Use this procedure to configure the HTTP destination in SAP HANA Cloud Platform account. You can create and configure the destinations on account level using the Destinations editor in SAP HANA Cloud Platform cockpit.

1. In the cockpit, go to the Account dropdown menu and choose your account.
2. To open the Destinations editor, choose Destinations in the navigation panel.
3. Create an HTTP destination as follows:
  - a. To enable per user authorization, create an OAuth2SAMLBearerAssertion HTTP destination and configure its settings as follows:
    - i. Configure the basic settings:

Parameter	Value
Name	Enter a meaningful name
Type	<b>HTTP</b>
Description	(Optional) Enter a meaningful description

Parameter	Value
URL	<b>https://</b> <b>&lt;my_SAP_Cloud_for_Customer_system_name&gt;.crm.ondemand.com</b>
Proxy Type	<b>Internet</b>
Cloud Connector Version	2
Authentication	<b>OAuth2SAMLBearerAssertion</b>
Audience	Enter the host name of your SAP HANA Cloud for Customer system, for example <b>&lt;my_SAP_Cloud_for_Customer_system_name&gt;.crm.ondemand.com</b>
Client Key	Paste the entry you have copied from the Client ID field when configuring the OAuth client. For more information, see the <i>Configuring the OAuth Client for OData Access</i> section in this guide.
Token Service URL	<b>https://</b> <b>&lt;my_SAP_Cloud_for_Customer_system_name&gt;.crm.ondemand.com/sap/bc/sec/oauth2/token</b>

Token Service User	Client ID  Paste the entry you have copied from the Client ID field when configuring the OAuth client in the <i>Administrator</i> work center of SAP Cloud for Customer. For more information, see the <i>Configuring the OAuth Client for OData Access</i> section in this guide.
Token Service Password	Client secret  Enter the client secret you have specified when configuring the OAuth client in the <i>Administrator</i> work center of SAP Cloud for Customer. For more information, see the <i>Configuring the OAuth Client for OData Access</i> section in this guide.

- i. Configure the required additional properties. To do so, in the Additional Properties panel, choose New Property, and enter the following properties:

Parameter	Value
authnContextClassRef	<code>urn:oasis:tc:SAML:2.0:ac:classes:PreviousSession</code>
nameIdFormat	<code>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</code>

Parameter	Value
scope	<p>Enter the Scope ID of the scope you have selected when configuring the OAuth client in the <i>Administrator</i> work center of SAP Cloud for Customer. For more information, see the <i>Configuring the OAuth Client for OData Access</i> section in this guide.</p> <p>For each of the selected scopes, you need to configure a separate <code>nameIdFormat</code> additional property.</p>
userIdSource	email

4. Select the Use default JDK truststore checkbox.
5. Save your entries.

## Result

Use the created destination in the HCP application to use logged in user authorizations for making OData API calls.

# Setup Basic Authentication

To use basic authentication, create a Basic Authentication HTTP destination and configure its settings as follows and save your entries:

Parameter	Value
Name	Enter a meaningful name
Type	<b>HTTP</b>
Description	(Optional) Enter a meaningful description
URL	<b>https://</b> <b>&lt;my_SAP_Cloud_for_Customer_system_name</b> <b>&gt;.crm.ondemand.com</b>
Proxy Type	<b>Internet</b>
Cloud Connector Version	2
Authentication	<b>BasicAuthentication</b>
User	Enter the name of the SAP Cloud for Customer user who should have access to the extension applications. This user will be used as a technical user
Password	Enter the password of the SAP Cloud for Customer user who should have access to the extension applications

## Result

Use the created destination in the HCP application to use technical user for making OData API calls.

Note - It takes some time for the system to activate the destination.

## Copyright

© 2014 SAP SE or an SAP SE affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE and its affiliated companies ("SAP SE Group") for informational purposes only, without representation or warranty of any kind, and SAP SE Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP SE and other SAP SE products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE in Germany and other countries.

Please see

<http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark>

for additional trademark information and notices.