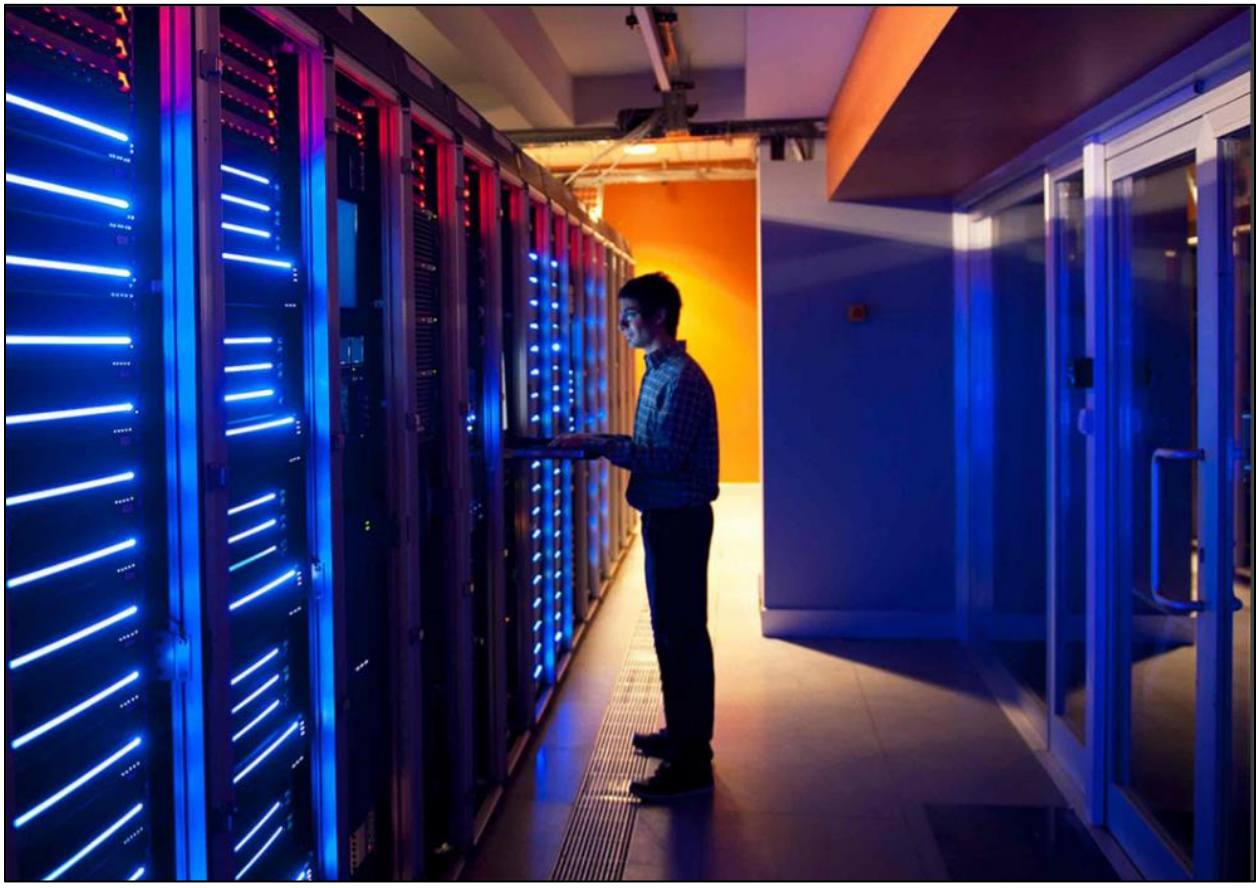


Integration Guide: AC 12.0 – IAG Bridge Scenario

Using SAP Cloud Identity Access Governance as a bridge to enable creation of access requests from SAP Access Control on-premise to cloud applications

PUBLIC

TARGET AUDIENCE: Administrators

2019_Feb_28

THE BEST RUN SAP

About This Guide

This guide is intended for administrators to assist in setup and integration of SAP Access Control 12.0 on-premise with the SAP Cloud Identity Access Governance solution and target cloud applications. This guide is to be used in conjunction with the SAP Cloud Identity Access Governance administrator guide.

Document History

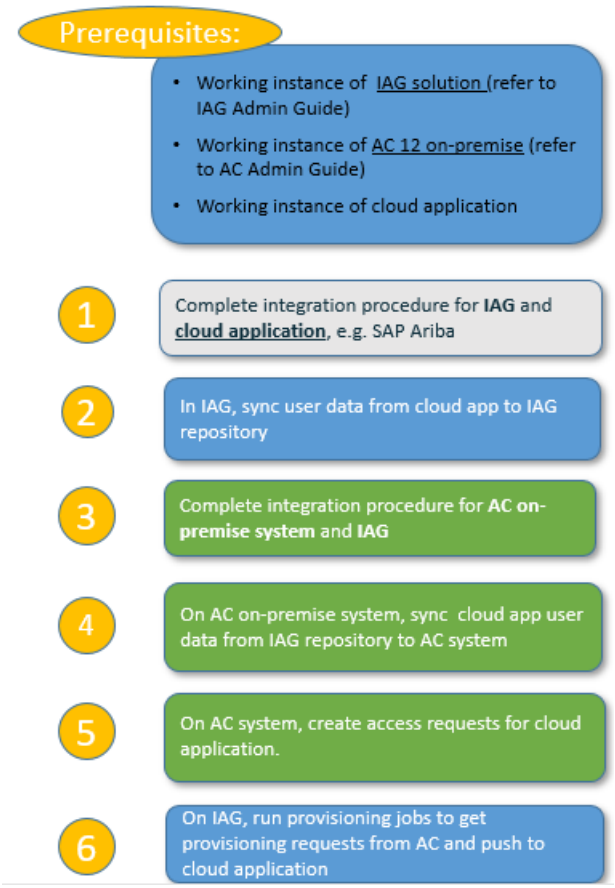
Provides details about the changes made in each version of this document.

Date	Description
February 28, 2019	Initial version
November 26, 2019	Minor corrections (subsection 3.1)
March 06, 2020	Minor corrections (subsections 1.3 and 3.4)

Table of Contents

About This Guide 2
Document History 2
Integration Process: AC on-premise -to- IAG -to- Cloud Apps (overview) 4
Integration Process: AC on-premise -to- IAG -to- Cloud App (including sub steps) 5
1.0 Complete Integration for IAG and Target Cloud Application 5
2.0 Sync Target Cloud Application User Data to IAG repository 6
3.0 Complete Integration of AC on-premise to IAG 7
3.1. Install SAP Cloud Connector 7
3.2. Maintain RFC Destination for the IAGTRIGGER App 8
3.3. Configure Parameters for Cloud Integration 9
3.4. Create Connector and Connector Group 10
3.5. Create Destinations for IAG Service: IAG_PROVISION_STATUS_UPDATE_SRV 11
4.0 Sync Cloud Application User Data from IAG repository to AC system 17
5.0 Create Access Requests for Cloud Applications 17
6.0 Run Provisioning Jobs 17
Important Disclaimers and Legal Information 18

Integration Process: AC on-premise -to- IAG -to- Cloud Apps (overview)



Integration Process: AC on-premise -to- IAG -to- Cloud App (including sub steps)

Prerequisites
Ensure the following are setup and working before starting the integration procedure:

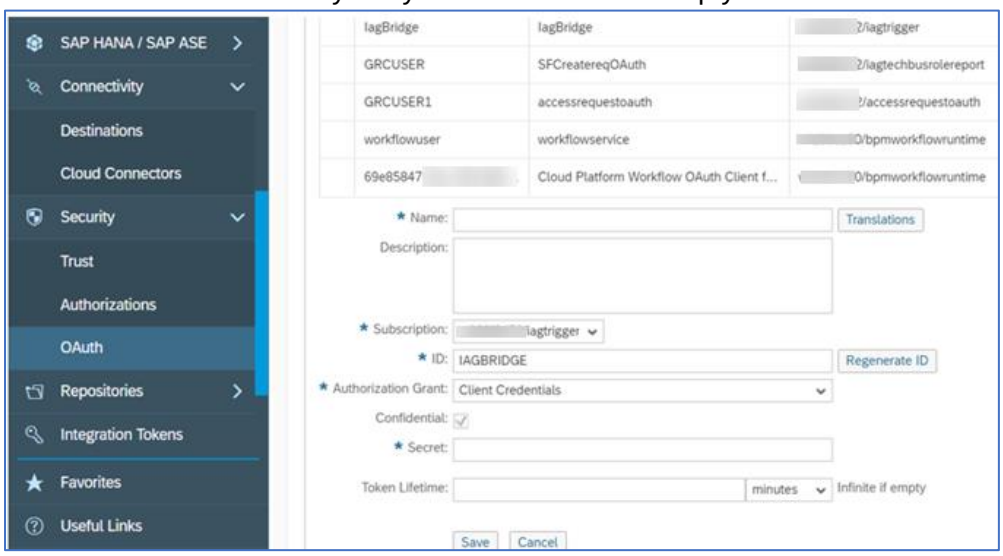
- Working instance of **IAG** solution (refer to IAG Admin Guide)
- Working **AC 12 on-premise** system (refer to AC Admin Guide)
- Working instance of **target cloud application**

1.0 Complete Integration for IAG and Target Cloud Application

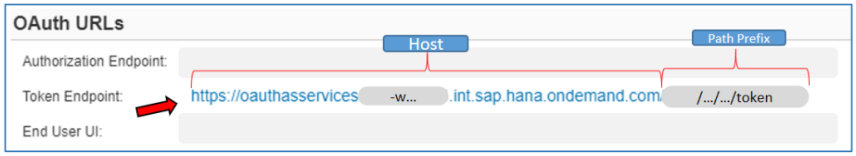
This enables communication and data sync between IAG and the target cloud application. (The information in this section refers to the IAG Admin Guide.)

1.1. In SCP, create destinations for your specific target cloud applications, e.g. SAP Ariba. (see IAG Admin Guide – Integration Scenarios)
   1. Go to your subaccount and open **Connectivity** > **Destinations** > **New Destinations.**
   2. Create destinations as specified in the Admin Guide.

1.2. In SCP, create **OAuth client** for IAG bridge security. (see Configuration Steps)
   1. Navigate to **Security** > **OAuth**. On the **Clients** tab click **Register New Client**.
   2. Fill in the required fields as shown below.
      - **Subscription:** select *<provider tenant ID>/iagtrigger*
      - **ID:** enter *IAGBRIDGE*
      - **Authorization Grant:** select *Client Credentials*
      - **Secret:** enter the password for the service
      - **Token Lifetime:** delete any entry and leave the field empty



3. On the **Branding** tab, take note of the **Token Endpoint URL**. You will need it in the step to create connectors on the access control system.



1.3. In **Fiori Launchpad** for IAG, add a system for the cloud application destination.

Open the **Systems** app and click the plus (**+**) to create a system. Use information from the destination you created in SCP to fill in the fields. (See IAG Admin Guide – Integration Scenarios – Add [cloud app] Instance)

Note: For a successful integration of SAP Access Control with SAP Identity Access Governance, the Systems and Business Function Group apps created in SAP Identity Access Governance must have 10 characters or less.

This completes the communication setup between IAG and the target cloud application.

2.0 Sync Target Cloud Application User Data to IAG repository

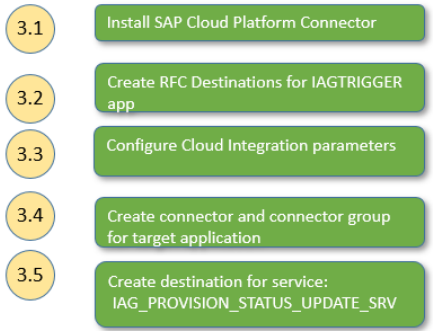
To synch user data from the cloud application to IAG repository, open the IAG Launchpad, and open the **Job Scheduler** app. Schedule and run the job: **Repository Sync**.

3.0 Complete Integration of AC on-premise to IAG

This enables communication and data synch between IAG and the AC system.

(The information in this section refers to the IAG Admin Guide > Integration Scenarios > SAP ABAP on-premise.)

This section contains the following tasks:



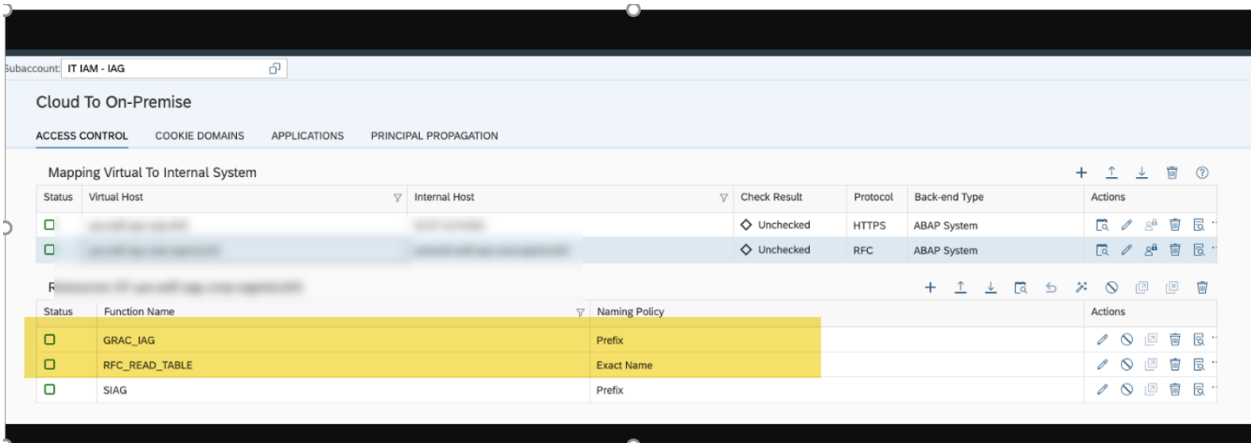
Prerequisites

- You have upgraded the target system to one of the supported NetWeaver versions and support packs (see *Required NW version and SP*)
- You have created the required RFC user allow communication with IAG (see *Required RFC User*)

3.1. Install SAP Cloud Connector

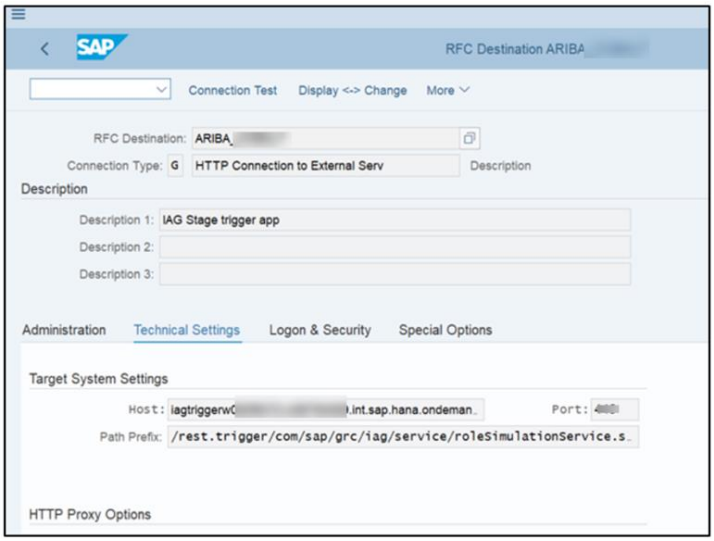
On the AC system, install and configure the *SAP Cloud Platform Connector* to enable communication between on-premise systems and the SAP Cloud Platform, and maintain destinations for each target system. (For detail steps, see Maintaining Cloud Connector)

After performing the steps mentioned in the link above, enter the **Function Name** and the **Naming Policy** for the on-premise system added to the cloud connector.

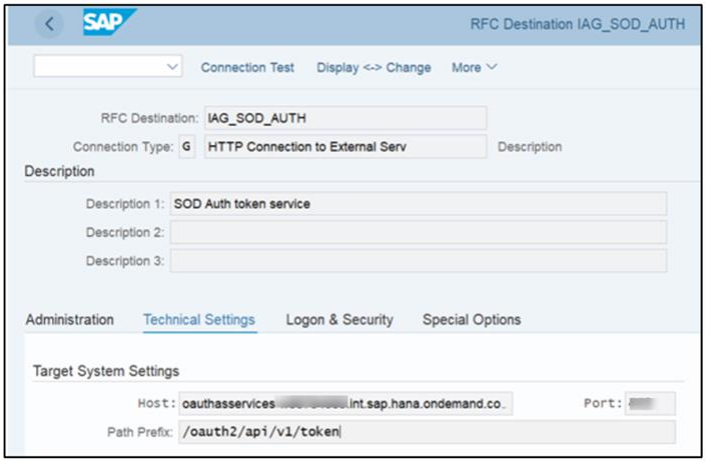


3.2. Maintain RFC Destination for the IAGTRIGGER App

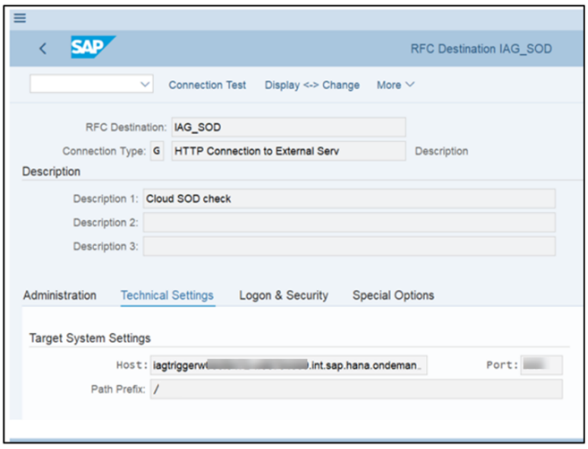
1. Go to *SPRO* **>** *Governance, Risk and Compliance* **>** *Common Component Settings* **>** *Integration Framework* **>** *Create Connectors.*
2. Create an **HTTP Connections to External Server**.
   For **Host** enter the URL for the IAGtrigger Java app.
   For **Path Prefix** enter this URL as IAG requires this exact URL to communicate with IAG services:
   /rest.trigger/com/sap/grc/iag/service/roleSimulationService.svc/



3. Create IAG_SOD_AUTH Connector (see Create IAG_SOD_AUTH Connector)

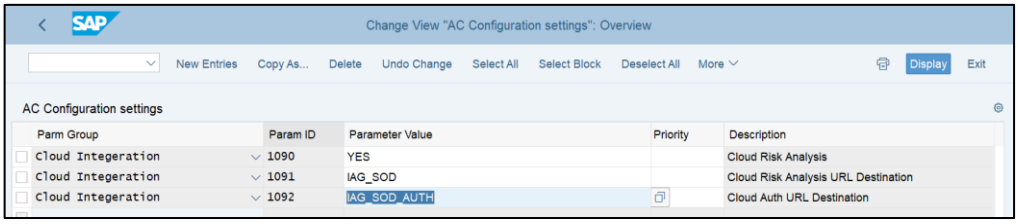


4. Create IAG_SOD_CHECK Connector (see Create IAG_SOD_CHECK Connector)



3.3. Configure Parameters for Cloud Integration

1. Go to SPRO **>** Governance, Risks and Compliance **>** Access Control **>** Maintain Configuration Settings.
2. Maintain the following parameters and values.
   (For more information, see Configure Parameters for IAG)

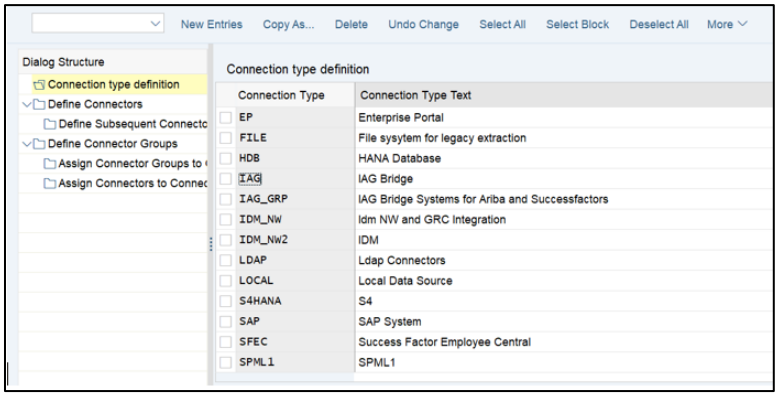


3.4. Create Connector and Connector Group

Create connectors and connector groups for the target cloud application.

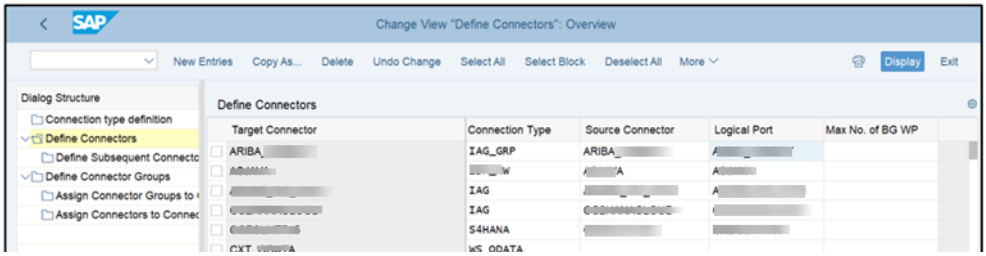
1. Go to *SPRO* **>** *Governance, Risk and Compliance* **>** *Common Component Settings* **>** *Integration Framework* **>** **Maintain Connectors and Connection Types**

2. Create *Connection Type Definition*: **IAG** and **IAG_GRP**.

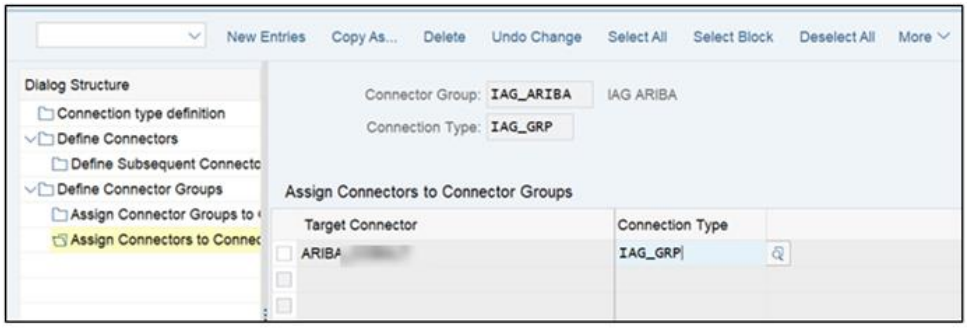


Note: For steps 3 and 4 below, the Systems and Business Function Group apps in SAP Identity Access Governance must have 10 characters or less, as SAP Access Control supports only 10 characters.

3. Define the Connectors for the target cloud applications.



4. Assign Connectors to Connector Groups.

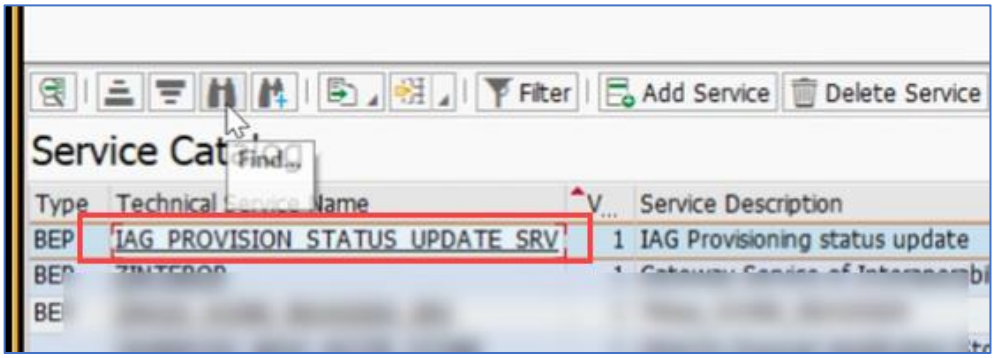


3.5. Create Destinations for IAG Service: IAG_PROVISION_STATUS_UPDATE_SRV

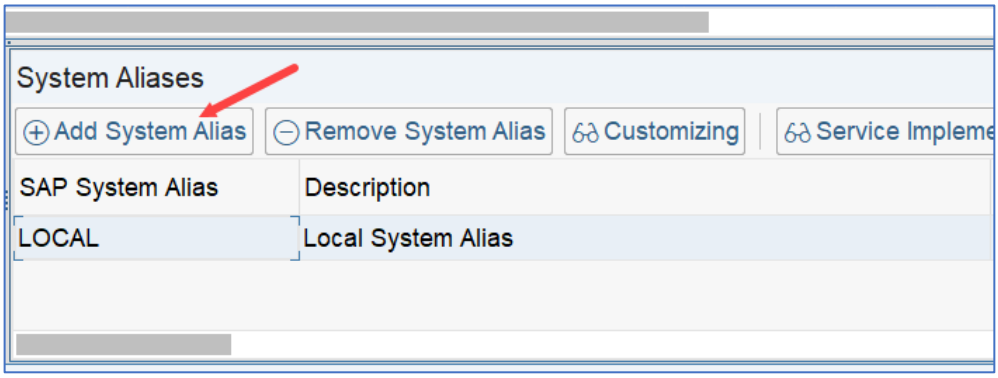
This delivered service is used by IAG to push status updates from the cloud target applications to access control. This enables the proper and accurate display of provisioning status for access requests.

1. On the AC system, go to SPRO > SAP NetWeaver > SAP Gateway > Administration > General Settings > **Activate and Maintain Services**.

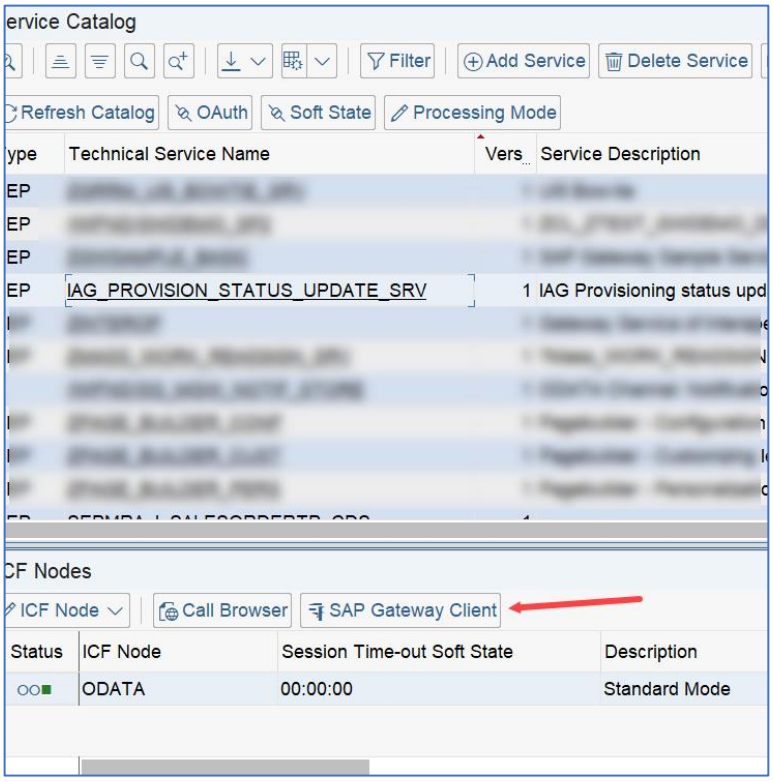
2. In the Service Catalog screen, select **IAG_PROVISION_STATUS_UPDATE_SRV** and activate it.



3. In the **System Aliases** pane, click **Add System Alias**, and add it as *local host*, and Save.

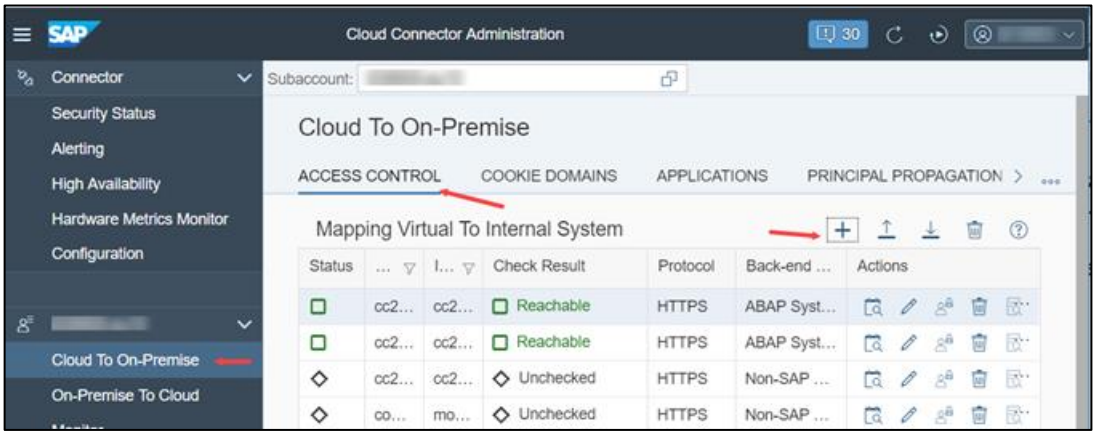


4. In the **ICF Nodes** pane, click **SAP Gateway Client**, and then **Execute**.

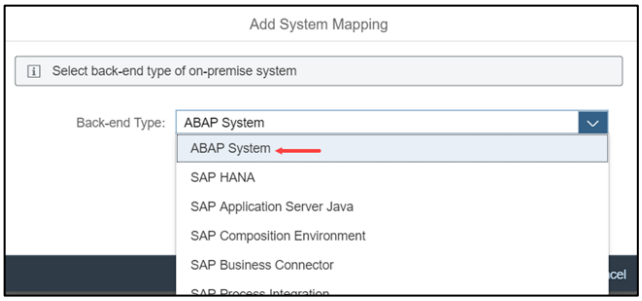


5. In the html pane, copy the href link. You will need it for the next step.

6. In the **Cloud Connector**, create a system mapping for the provisioning status update service.
   1) Open the SAP Cloud Platform Connector, select the subaccount, and click **Cloud To On-Premise**.
   2) Go to the **Access Control tab** and click the plus (**+**) sign to add a new system mapping.



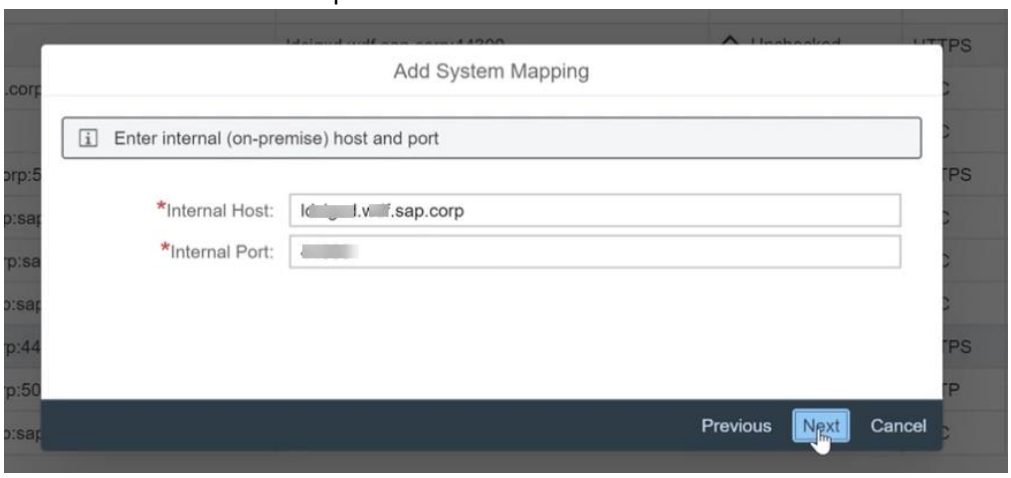
   3) For **Back-end Type**, select *ABAP System* and click **Next**.



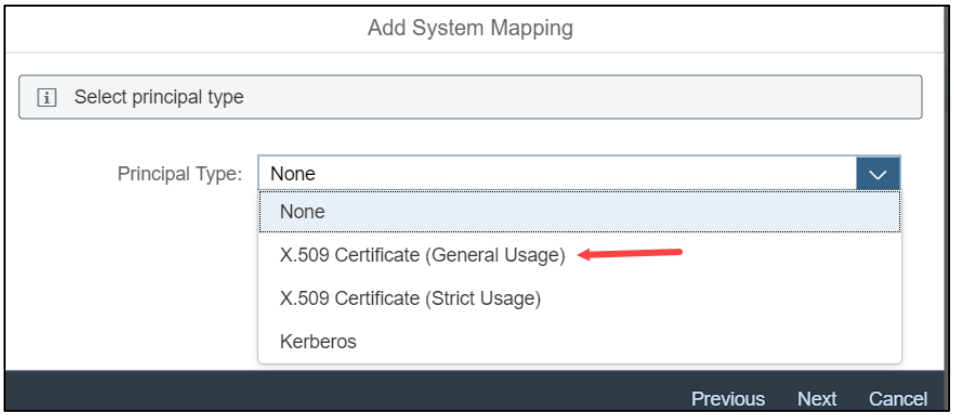
   4) For **Protocol**, select **HTTPS**, and click **Next**.

5) Enter the internal host and port information and **Next**.
You can copy this information from the services URL.

- For Internal Host: enter the root URL; do not include the protocol
- For Internal Port: enter the port number

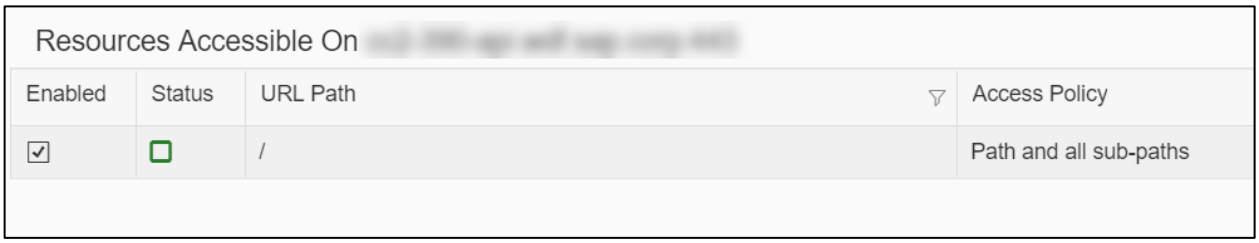


6) For **Principal Type**, select **X.509 Certificate (General Usage)** and click **Next**.

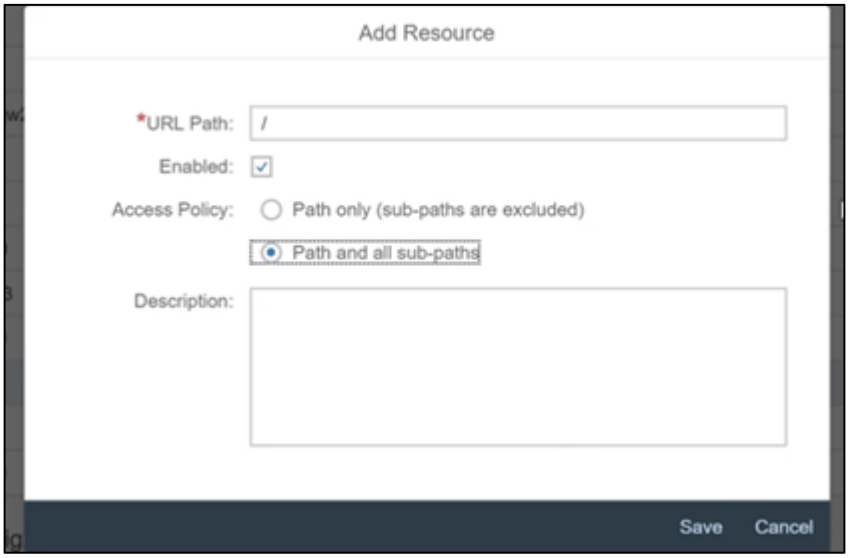


7) Select the **Check the Internal Host** box and click **Finish**.

8) Add a resource path. In the **Mapping Virtual To Internal System** table, select the new mapping. In the **Resources Accessible On** section, click the pencil icon to edit it.



In the **URL Path** field, make sure only a **/** is entered, and save.



9) Test the configuration. In the **Mapping Virtual To Internal System** table, select the new mapping, and click the check-availability icon.

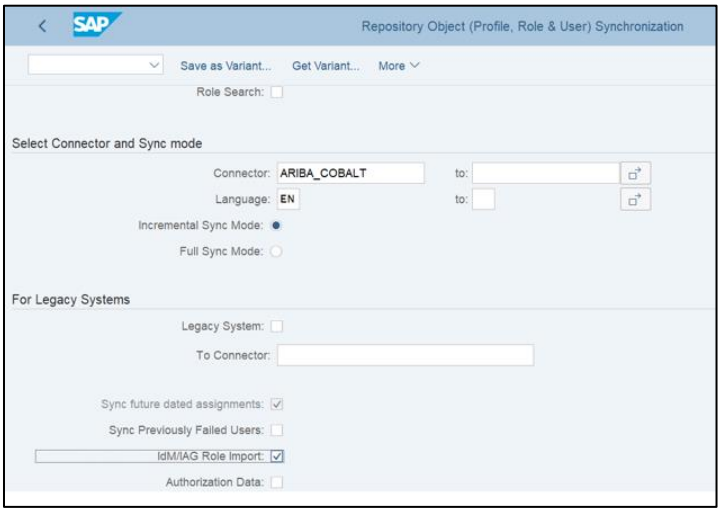
7. In SCP, create a destination for the IAG Provisioning Status Update virtual mapping.

   1) Go to **Connectivity** > **Destinations** and click the plus sign (**+**) to add a destination.
      Add the destination. Enter the name as **IAGProvisionStatusUpdate**.
   2) For the URL field, copy and paste the URL from the services configuration step.

   3) Save.

4.0 Sync Cloud Application User Data from IAG repository to AC system

On the AC system, go to SPRO > Governance, Risk and Compliance > Synchronization Jobs and run the **Repository Object Sync**.



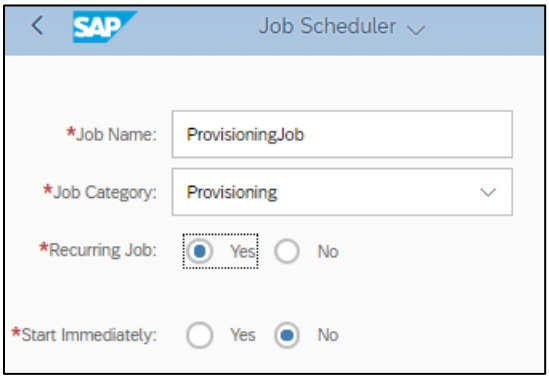
5.0 Create Access Requests for Cloud Applications

Use AC on-premise to create access requests for the target cloud applications.

6.0 Run Provisioning Jobs

In the Fiori Launchpad for IAG, run the provisioning job to retrieve provisioning requests from AC and push them to the target cloud application.

1. In the Fiori Launchpad for IAG open *Job Scheduler* app.
2. In the *Job Category* field, select **Provisioning**.
   We recommend setting this as a recurring job.



Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information. About the icons:

● Links with the  icon: You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:

- The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
- SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.

● Links with the  icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up. The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.