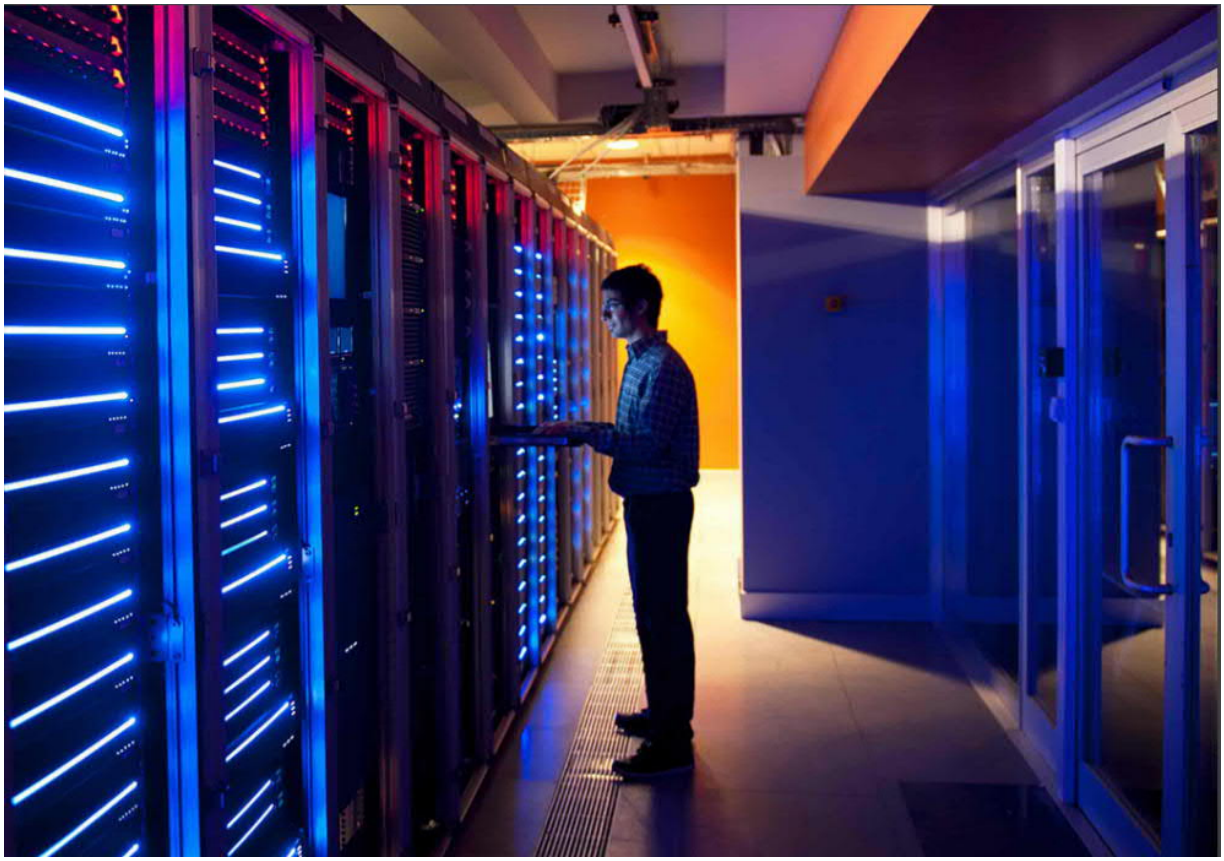


Integration Guide: SAP Access Analysis Service to Target Applications (on-premise and cloud)

Configuring SAP Cloud Identity Access Governance, access analysis service to analyze user access for target applications (on-premise and cloud).

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 the access analysis service and target 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.

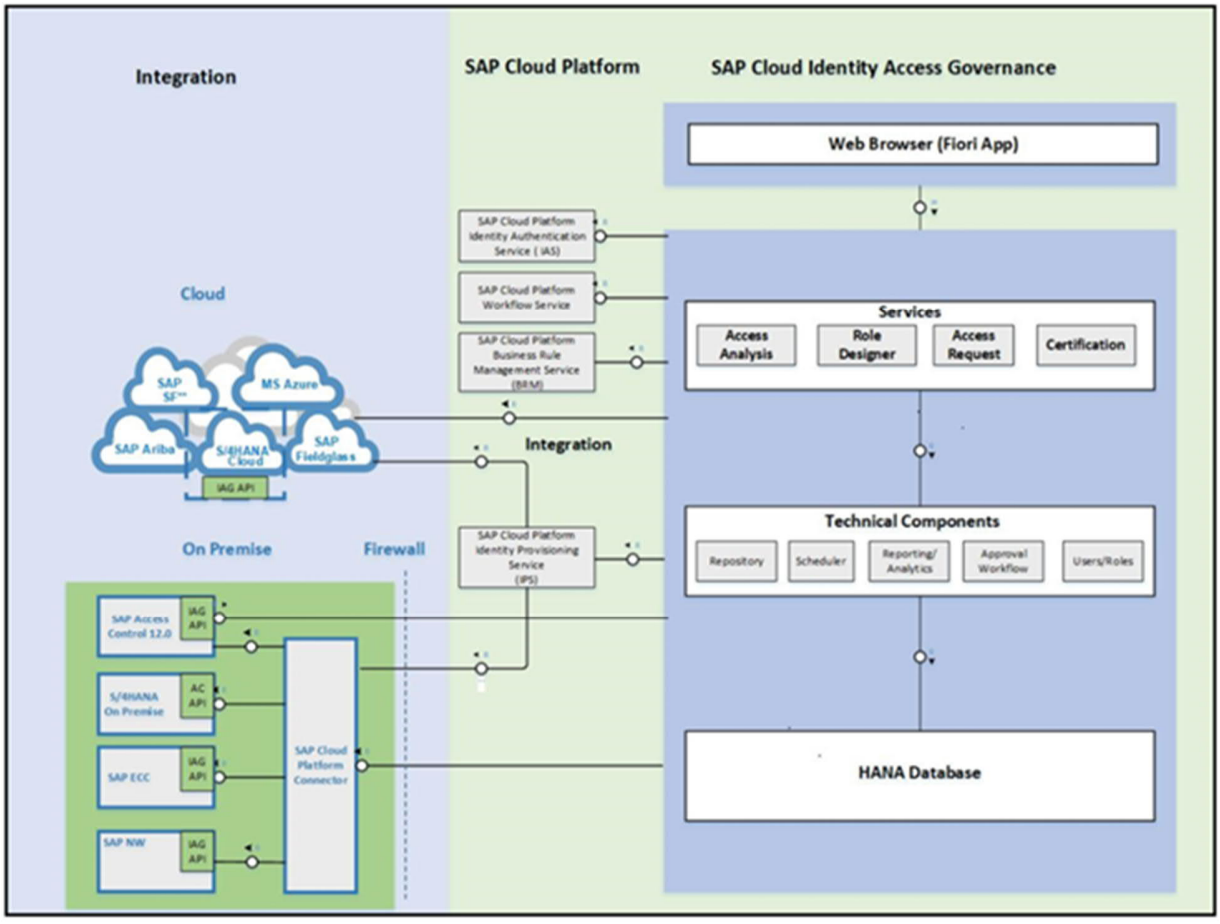
Date	Description
February 28, 2019	Initial version

Table of Contents

Solution Architecture (how everything works together)

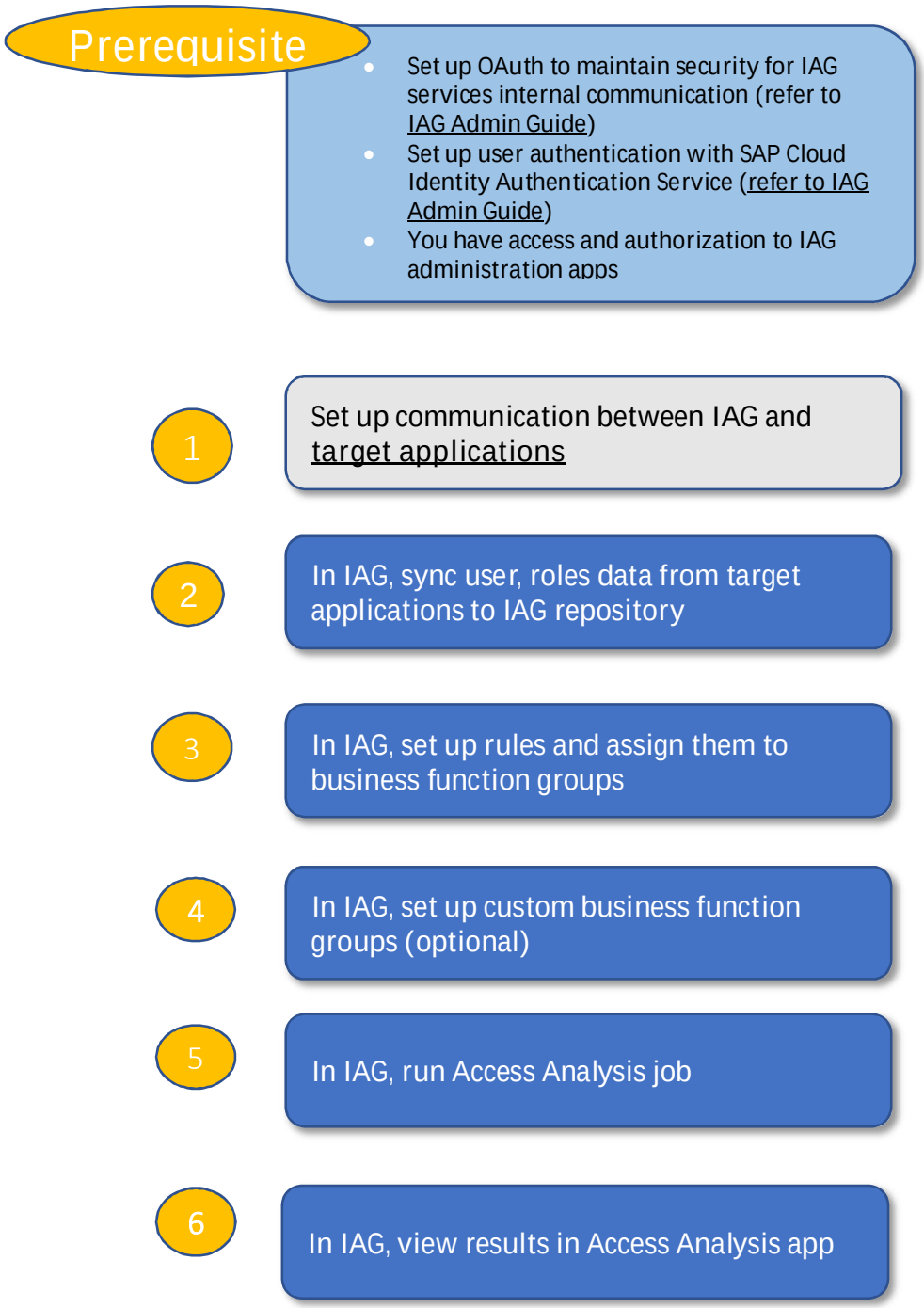
The diagram below illustrates the architectural components of SAP Cloud Identity Access Governance (IAG) solution and services.

The IAG solution is a service on the SAP Cloud Platform. It integrates with other SAP Cloud Platform services and connects with cloud and on-premise target applications.



Integration Process Overview:

This is a summary of the steps for configuring and using IAG Access Analysis



Integration Process Details – including substeps:

This is a detailed description of the steps for configuring and using IAG Access Analysis.

Prerequisites

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

- Working target application (cloud or on-premise)
- In SCP, you have set up OAuth to maintain security for IAG services internal communication (refer to IAG Admin Guide)
- In SCP, you have set up user authentication with SAP Cloud Identity Authentication Service (refer to IAG Admin Guide)
- You have authorization and access to IAG administration apps

1.0 Set Up Communication Between IAG and Target Applications

Use the information in this section to configure communication between IAG and target applications.

> Note: Sections marked (on-premise only) are applicable only for SAP ERP on-premise scenarios. Sections without this tag are applicable for all scenarios. For cloud-only integration scenarios begin at S*ection 1.2 Create Destinations for Target Applications.*

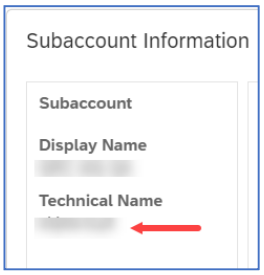
1.1. (on-premise only) Maintain SAP Cloud Connector for SAP ERP Target Applications

This section is applicable only for on-premise SAP ERP target applications. You must install the SAP Cloud Platform Connector to enable communication between the target application and IAG.

Prerequisites

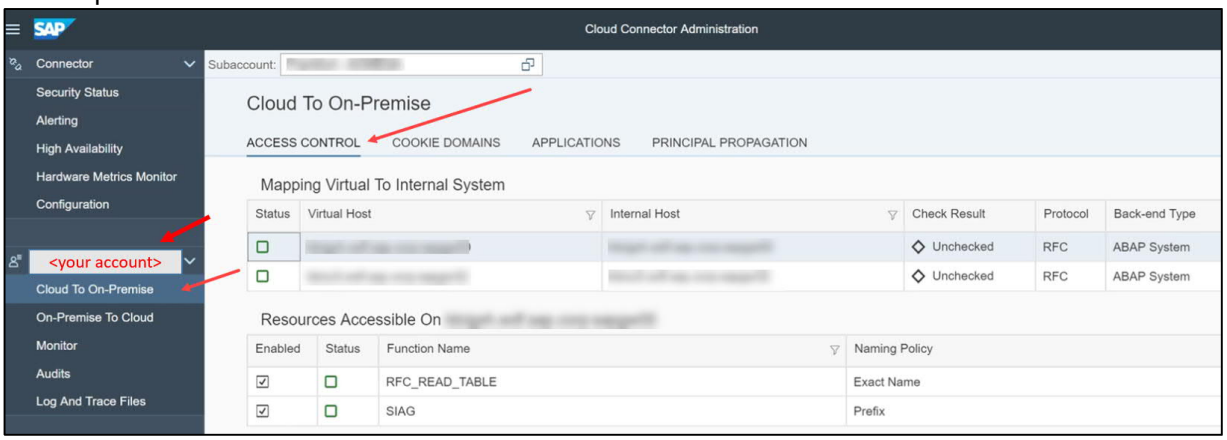
- You have upgraded the target system to one of the supported NetWeaver versions and support packs (see Required NW version and SP)
- You have created the required RFC user allow communication with IAG (see Required RFC User)

1) For each target system, install the SAP Cloud Platform Connector. (see Installing SAP Cloud Platform Connector)
2) Configure the SAP Cloud Platform Connector.
   a. Login to your SAP Cloud Platform Connector and create a new account.
      Go to Account Dashboard and click Add Account.
   b. Enter the following details and save the data:
      - Landscape Host: Enter the URL for the data center for your IAG account.
      - Account Name: Enter the SCP subaccount technical name.
        To locate the name, open SCP, open the subaccount, and navigate to the Subaccount Information section.



      - Display Name: <Company Name>
      - Account User: <S-UserID >
      - Password: <Password created for S-UserID >

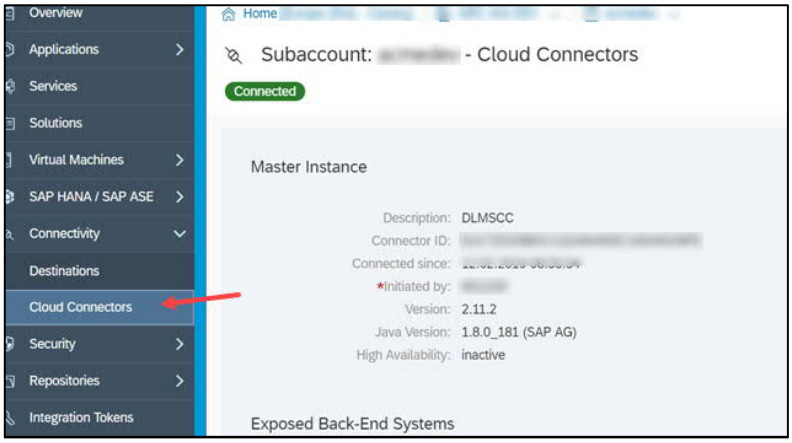
c. In the left pane, select the created account and click Cloud To On-Premise, and on the right pane click Access Control.



d. Add system mapping for each on-premise target system.
For SAP ERP system, enter Back-end Type = ABAP System, Protocol = RFC.

e. Select the above system mapping and add `SIAG` for **Function Module Name**, and `Prefix` for **Naming Policy**

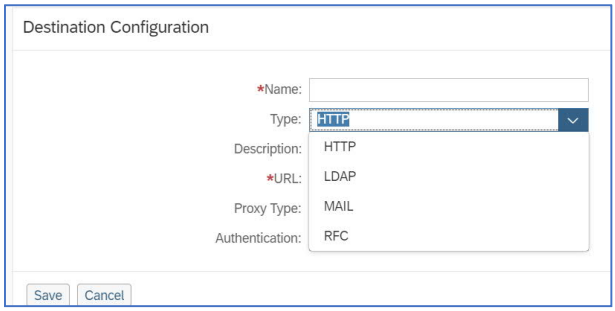
After you save the destination in the Cloud Connector, it automatically creates the same in SCP > Connectivity > Cloud Connector.



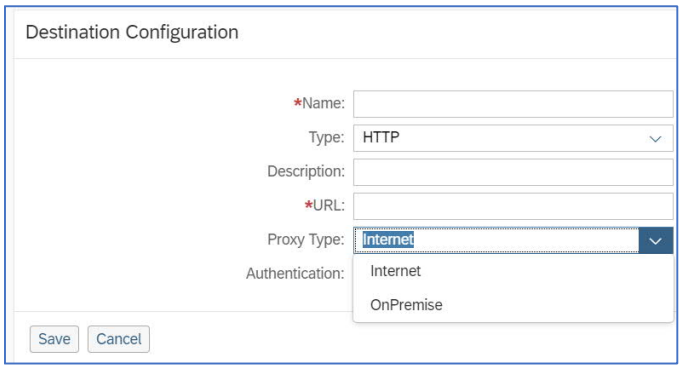
1.2. Create Destinations in SCP for Target Application

The information in this section is applicable for both on-premise and cloud scenarios.

1. In SCP, go to your tenant, and in the left pane click Connectivity > Destinations.
2. Click New Destination.
3. In the Type field, select the communication type you are using.
   - For on-premise, select RFC
   - For cloud applications, select HTTP



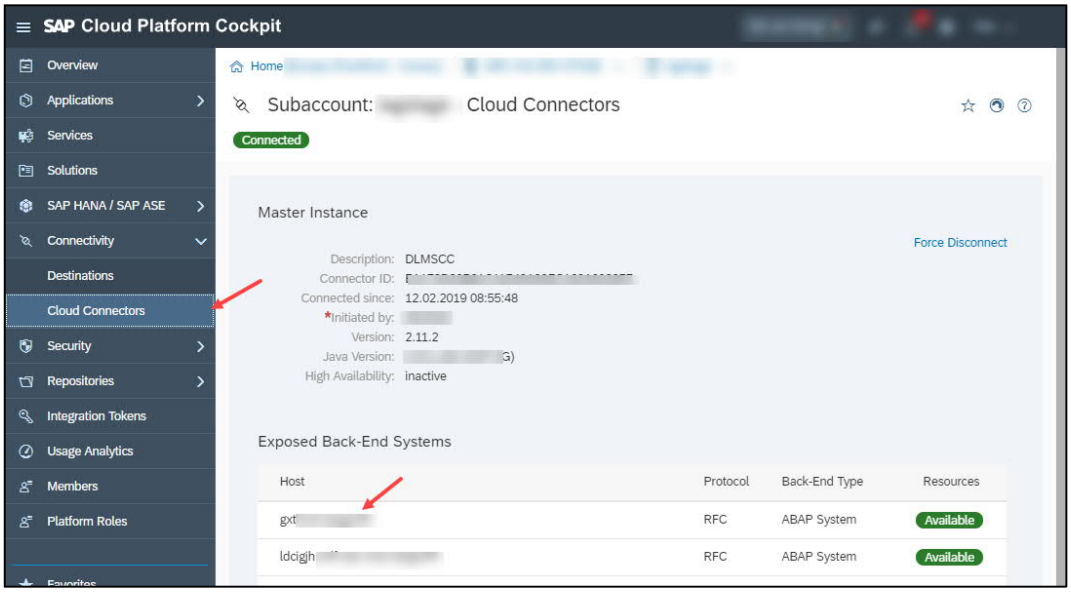
4. In the Proxy Type field, choose:
   - For cloud destinations, select Internet
   - For on-premise destinations, select OnPremise

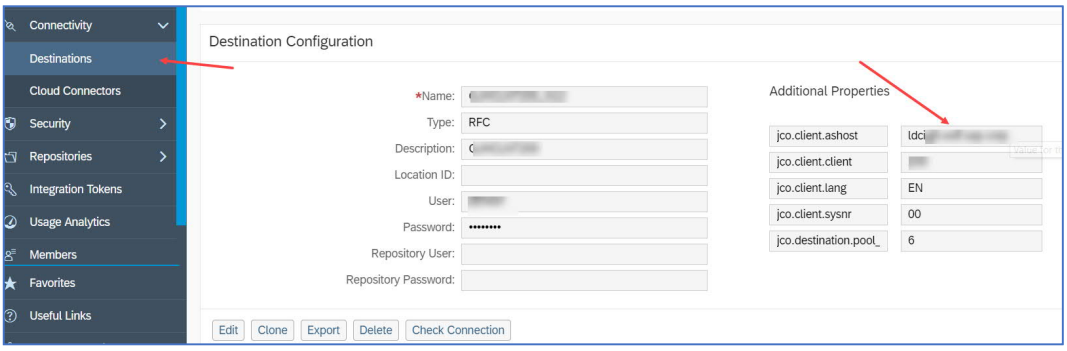


Note: Each type has its own information. For information specific to your implementation, see the Administrator Guide – Integration Scenarios.

(For On-Premise SAP ERP Only)

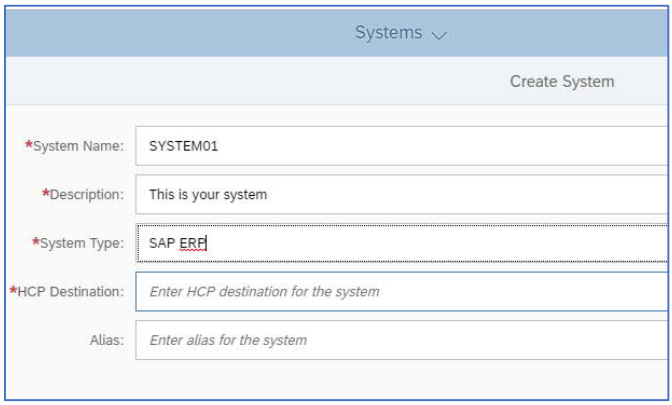
On-premise destinations require the additional jco.client.ashost field. To locate this information, in SCP go to Cloud Connectors. Copy the relevant Host URL. Then, go to Destinations, open the respective destination, and paste it in the jco.client.ashost field.





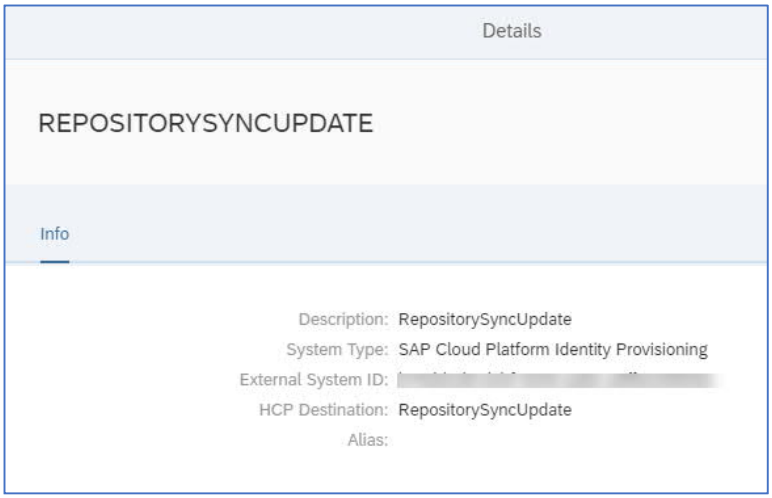
1.3. Create Systems in IAG Launchpad for Target Application

In the IAG launchpad, open the Systems app and add an instance for each of your applications, and save.



1.3.1. (on-premise only) Create REPOSITORYSYNCUPDATE System

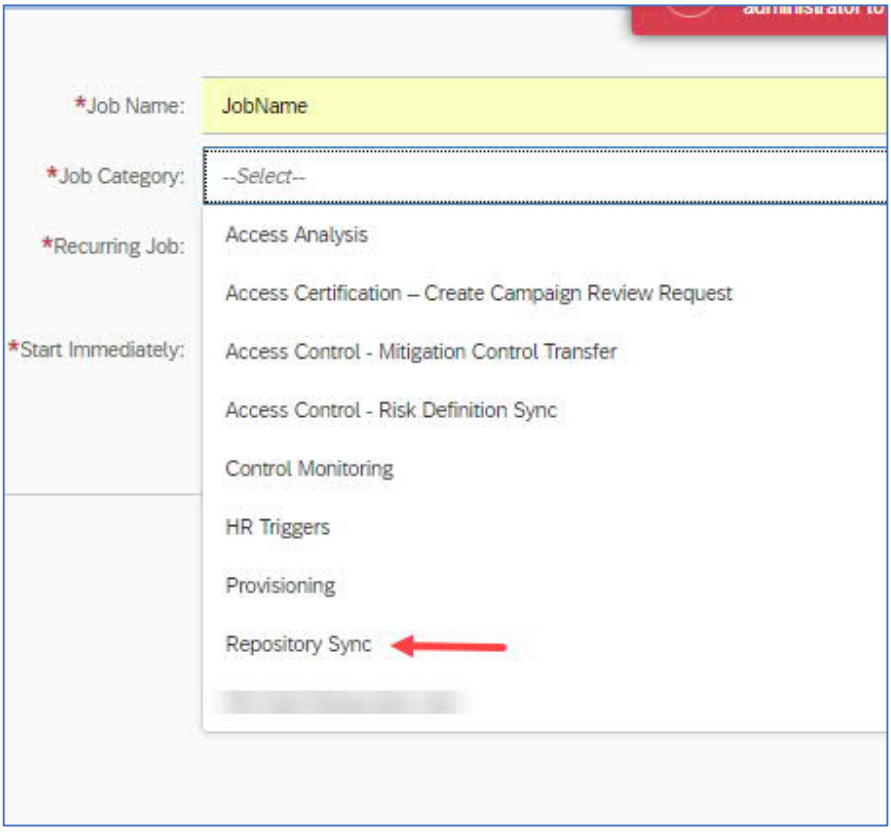
For on-premise applications that use IDM to call IAG, you must also add a System instance as follows. You must enter the Description, System Type, and HCP Destination information as specified below.



2.0 Sync Target Application User Data to IAG Repository

Do the following to sync user data from target applications to the IAG repository.

1. Open the Fiori Launchpad for IAG, and open the Job Scheduler app.
2. Create and run the job of category Repository Sync.

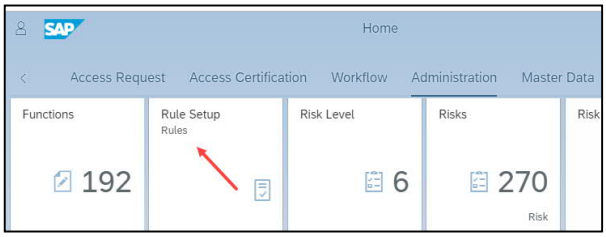


3.0 Set Up Rules

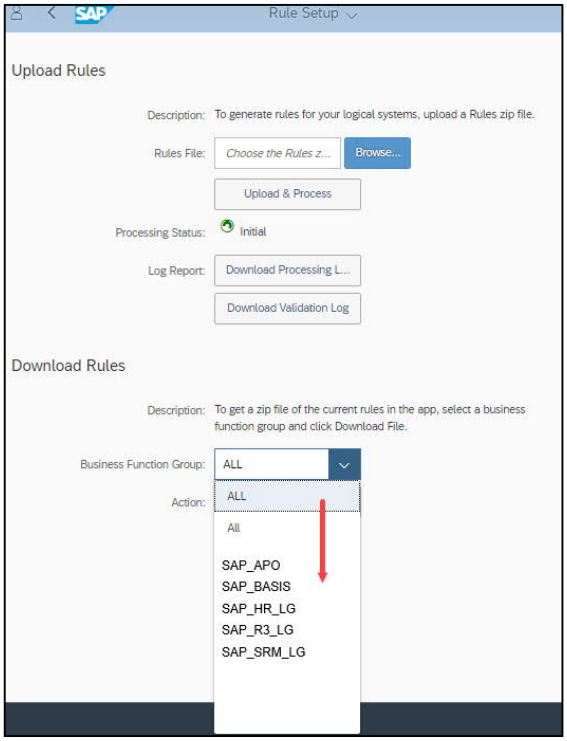
You upload business rules and associate them to business function groups.

> Note: SAP delivers a set of standard business function groups.
> To use the delivered business function groups, follow the steps below to set up rules and assign them to the business function groups. (The delivered group names begin with "SAP_".)
>
> To create your own custom business function groups, go to Step 4 Set Up Custom Business Function Groups (optional). After creating the custom business function groups, follow the instructions in Step 3 to set up rules.

1. On the IAG launchpad, open the Rule Setup app.



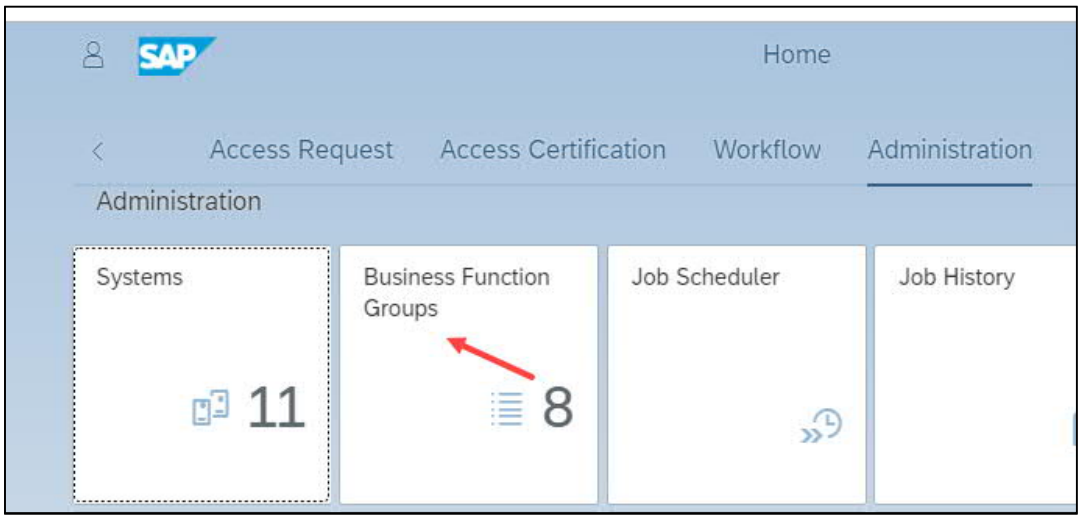
2. To upload the rules set, you have two options:
   A. SAP loads the default standard ruleset on request
   B. You upload your own ruleset following using the delivered template
3. Click the Business Function Group dropdown list and select a group to associate to the rule set.



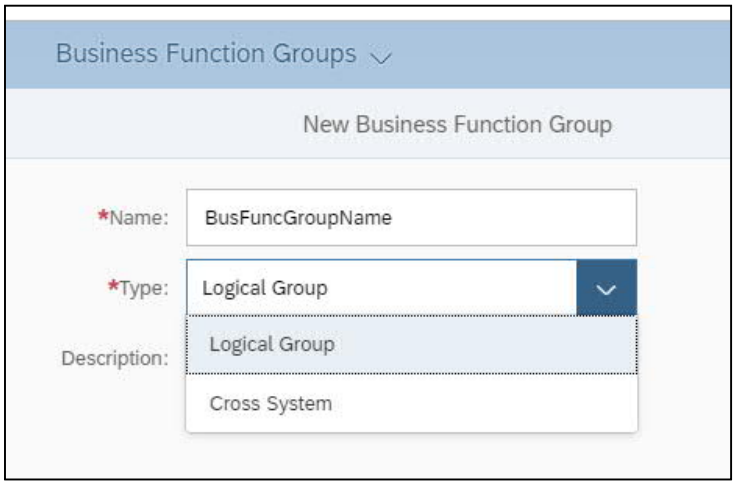
4.0 Set Up Custom Business Function Groups (optional)

You can create your own customer business function groups, and then assign them to business rules.

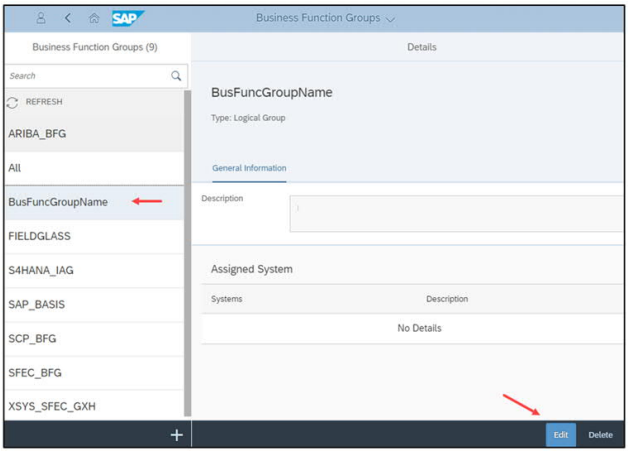
1. In the IAG launchpad, click Business Function Groups app. And click the plus sign (+) to add a business function group.



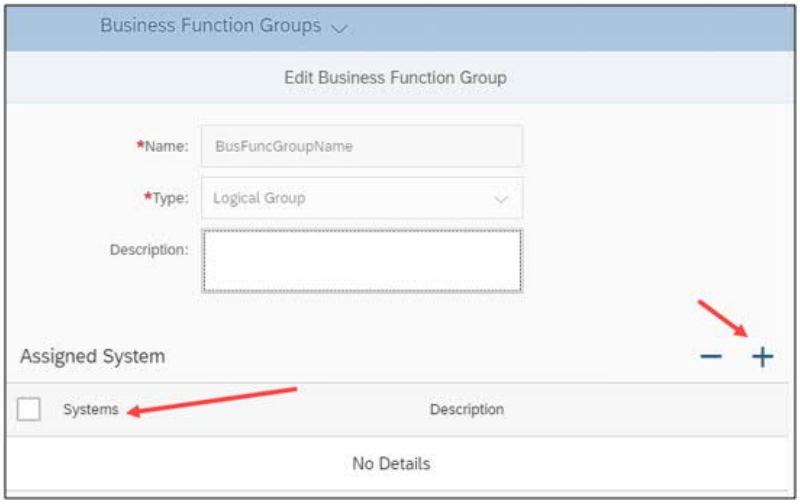
2. Enter information for the business function group and click Save.
   Note: The name is case sensitive.



3. To assign systems and connectors to the group, in the left pane select the business function group, and click Edit.

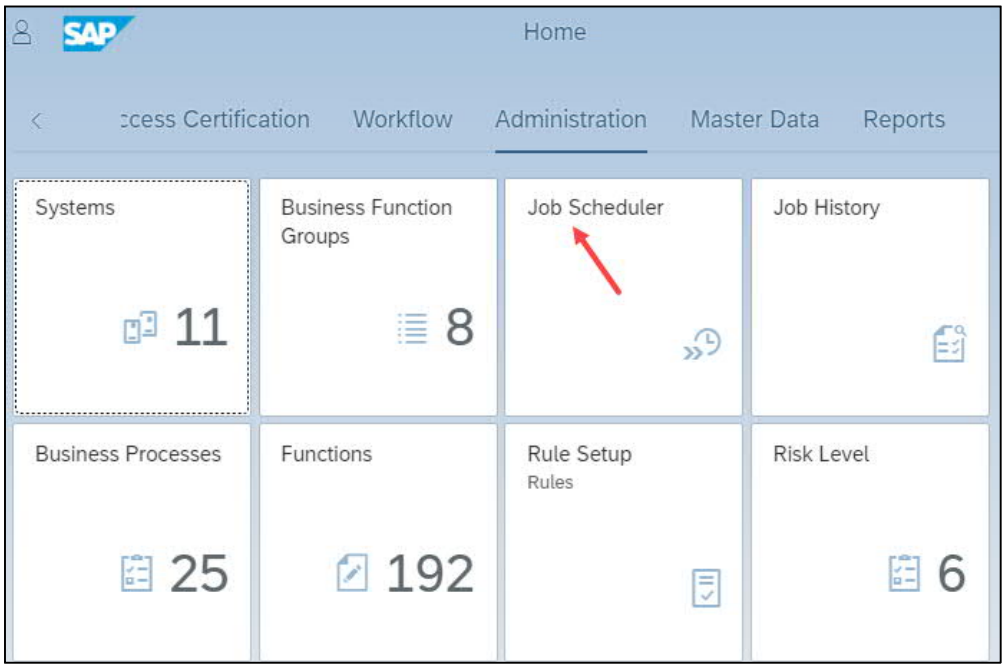


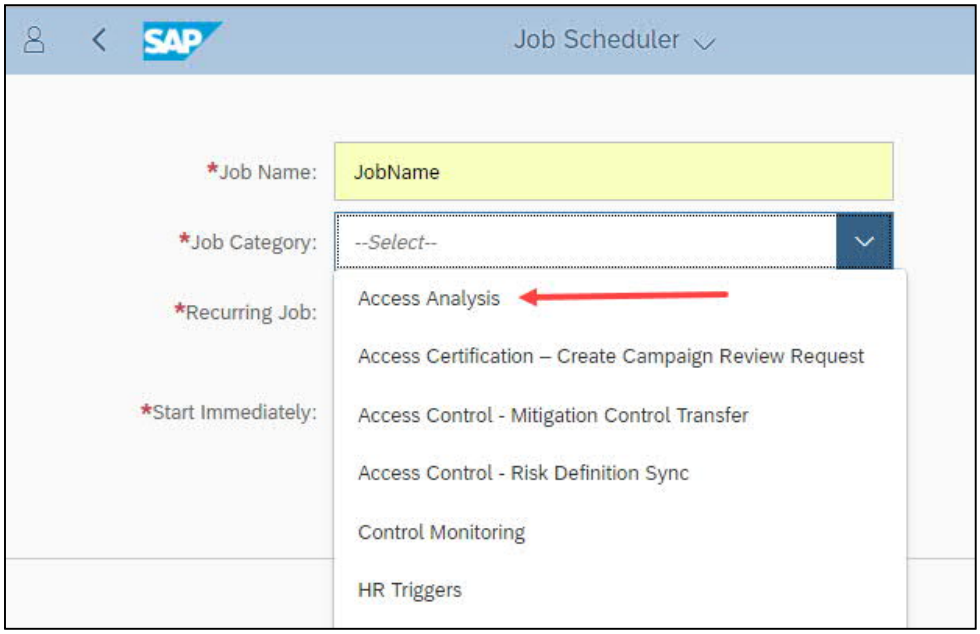
4. On the edit screen, click the plus sign (+), add the systems, and then save.



5.0 Run Access Analysis Job

In the IAG launchpad, open the Job Scheduler app, and run the Access Analysis job.



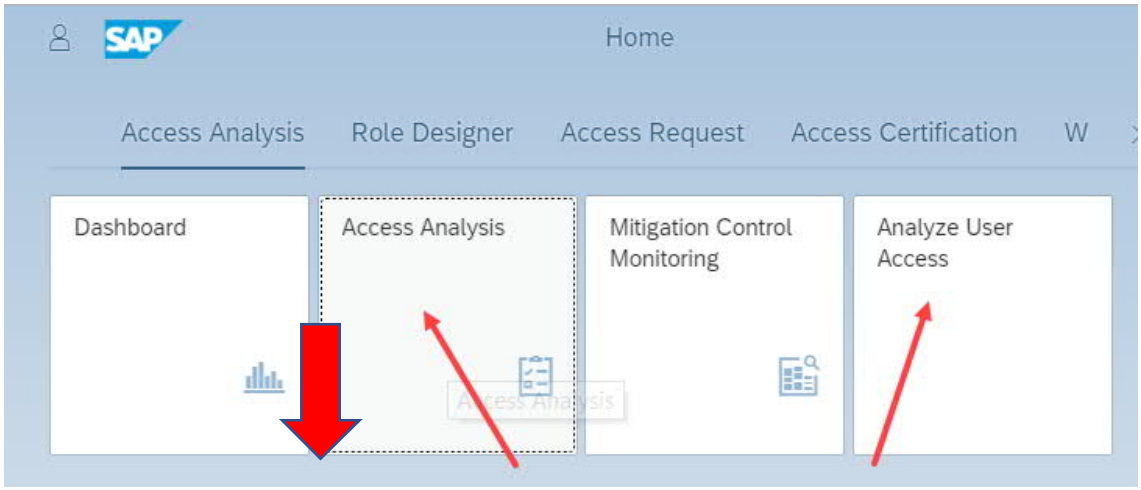


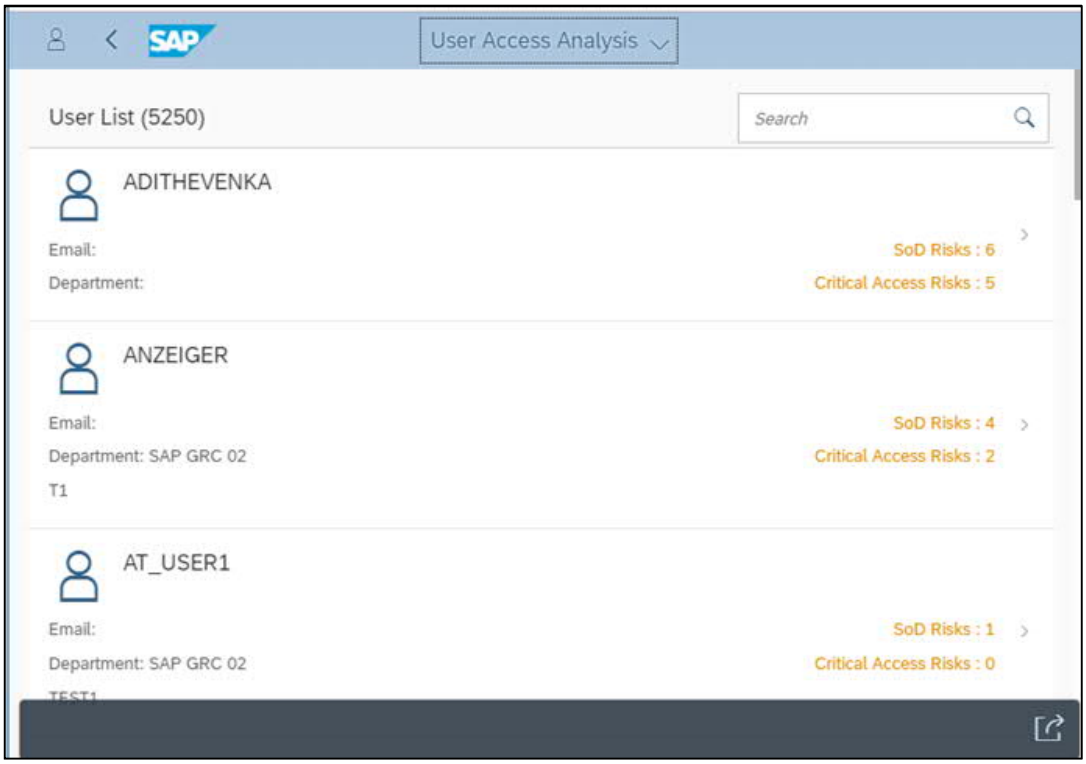
6.0 View Results

In the IAG launchpad, to view results:

- open the Access Analysis app to view access by user and remediate risks
- open the Analyze User Access app to view user access including functions

You can export the results to a spreadsheet.





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.