

Document Version: 1.0 – 2017-07-25

GSP Integration FAQ



Typographic Conventions

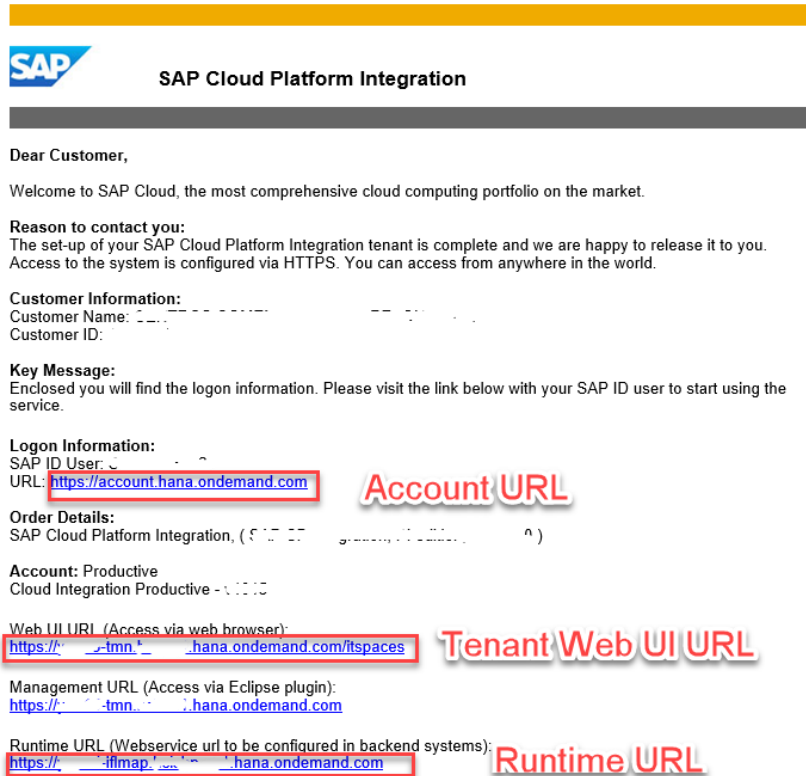
Type Style	Description
<i>Example</i>	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
EXAMPLE	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
Example	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
Example	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE	Keys on the keyboard, for example, F2 or ENTER.

Document History

Version	Date	Change
1.0	2017-07-25	First release

1. How to get the SCP Integration Account URL, Runtime URL and Tenant Web UI URL?

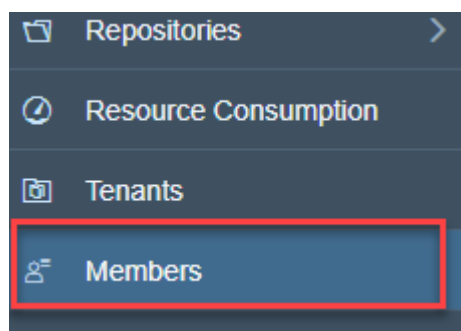
You would have already received a mail from SAP Cloud Platform Integration with the account, logon and tenant URL details that looks as shown below:



2. How to add members to the SAP Cloud Platform Integration account?

To add members to the SAP Cloud platform integration account, follow the below steps:

1. You need to logon to the Account URL with the SAP ID user provided in the mail.
2. You can add members and assign roles on this account by navigating to Members -> Add Members.



3. Assign the Roles.

Assign role *Administrator* to the user who is supposed to have the full permissions of an administrator.

Assign role *Application User Admin* to the user who is supposed to have restricted administrator permissions.

Assign role *Application User Admin* to the user who is supposed to have restricted administrator permissions.

Add Members

Enter up to 100 SAP user IDs. To separate them, you can use commas, spaces, semicolons, or line breaks.

User IDs:

Assign roles:

- Administrator (predefined role)
- Developer (predefined role)
- Support User (predefined role)
- Application User Admin (predefined role)
- Cloud Connector Admin (predefined role)
- CloudConnector

Comment (optional, visible to all members):

Add Members Cancel

3. How to add Authorizations to the existing users?

To add Authorizations to the existing users:

1. Logon to the Account URL with the SAP ID user provided in the mail.
2. In the Navigation Pane, choose Security -> Authorizations
3. Create a Group and Assign the Roles and Assign users for this Group.

The screenshot shows the 'Authorization Management' interface for tenant 'a6690dfad'. The 'Groups' tab is active, showing a table with one group named 'Admin'. Below this, a table lists roles assigned to the group:

Subaccount	Application	Role	Actions	Individual Users
avrddev	...	ESBMessaging send	[Unassign]	
avrddev	...	AuthGroup Administrator	[Unassign]	
avrddev	...	AuthGroup IntegrationD...	[Unassign]	
avrddev	...	AuthGroup BusinessEx...	[Unassign]	

The authorization group AuthGroup.Administrator is designed for the administrator at customer side who administers a (customer-specific) tenant management node.

The authorization group AuthGroup.IntegrationDeveloper has to be assigned on TMN-level. The main difference between the authorization groups AuthGroup.IntegrationDeveloper and AuthGroup.Administrator is the AuthGroup.Administrator group allows in addition to deal with security artifacts.

Note

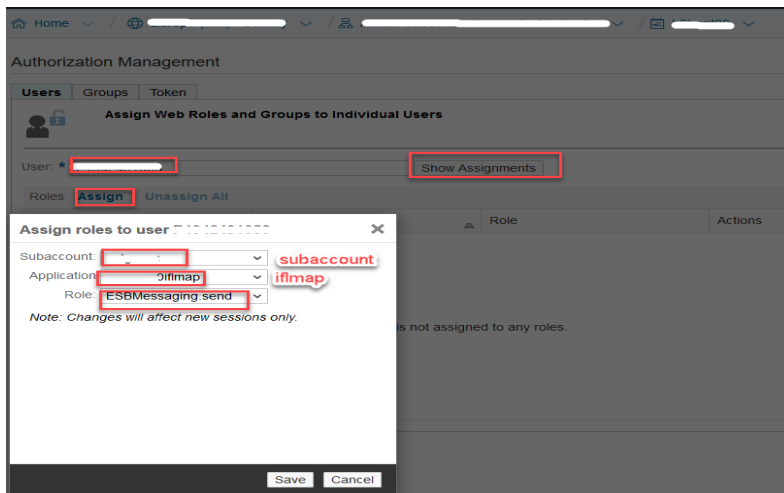
For more details refer [here](#)

4. How to create a service user for communicating from SLH DCS application to GSP Integration Flow?

The communication between the SLH DCS and GSP Integration Flow is done through Basic Authentication.

Perform the below steps to create a service user and assign the necessary role:

1. Register a new user at <https://account.hana.ondemand.com/#/home/welcome>
2. Assign the ESBMessaging.Send role to the user.



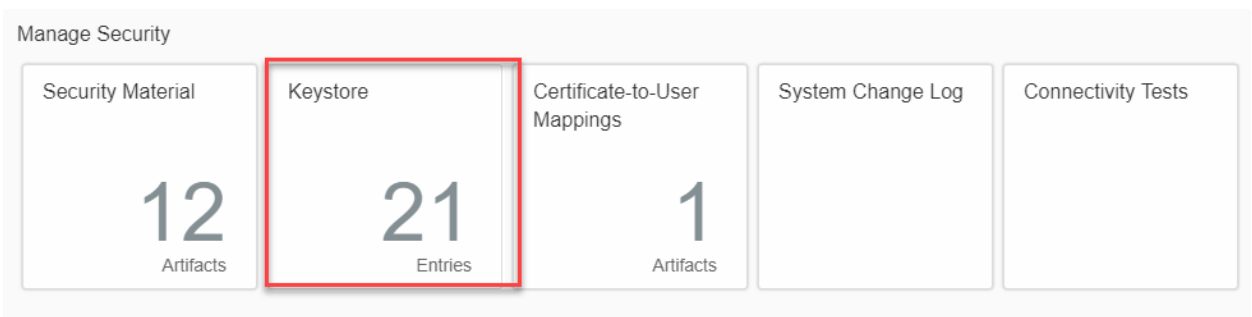
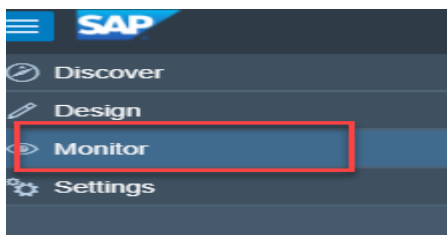
5. How to add new certificates or private keys to the SCP Integration tenants keystore?

You can add the security artifacts like keystore entries following the process mentioned [here](#)

Note

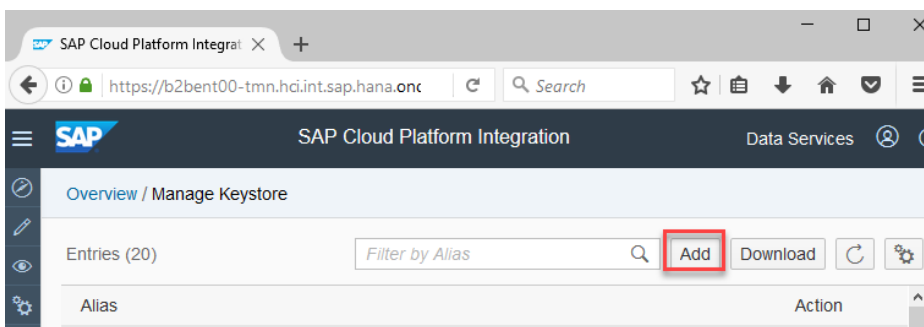
You need to be Tenant Admin (AuthGroup.Administrator role) on the tenant to perform this operation.

1. Navigate to Monitor->Manage Security->Keystore

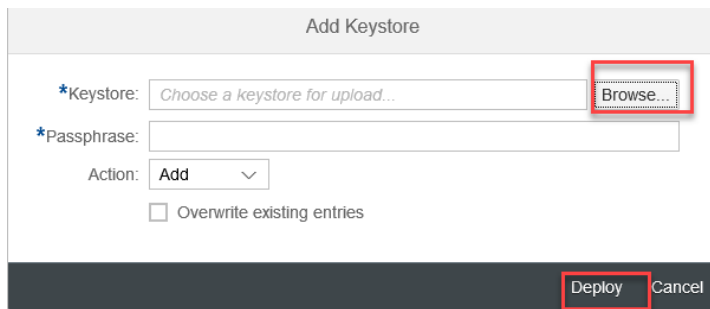


2. Add new Keystore Entry

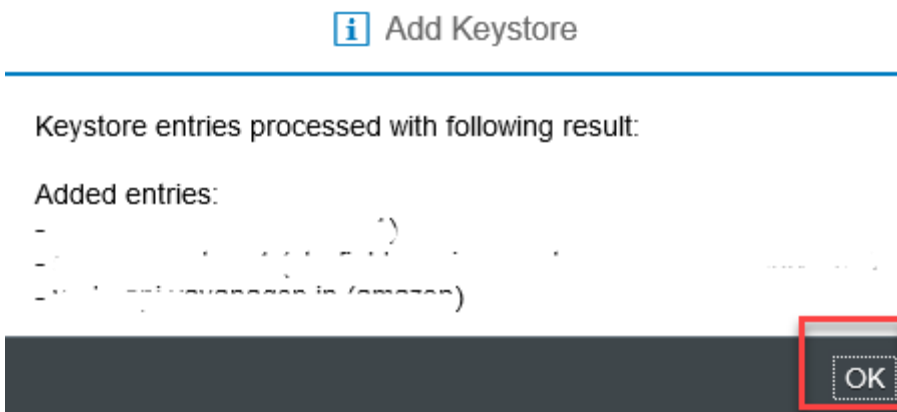
Click on Add button



Browse and deploy new Keystore.



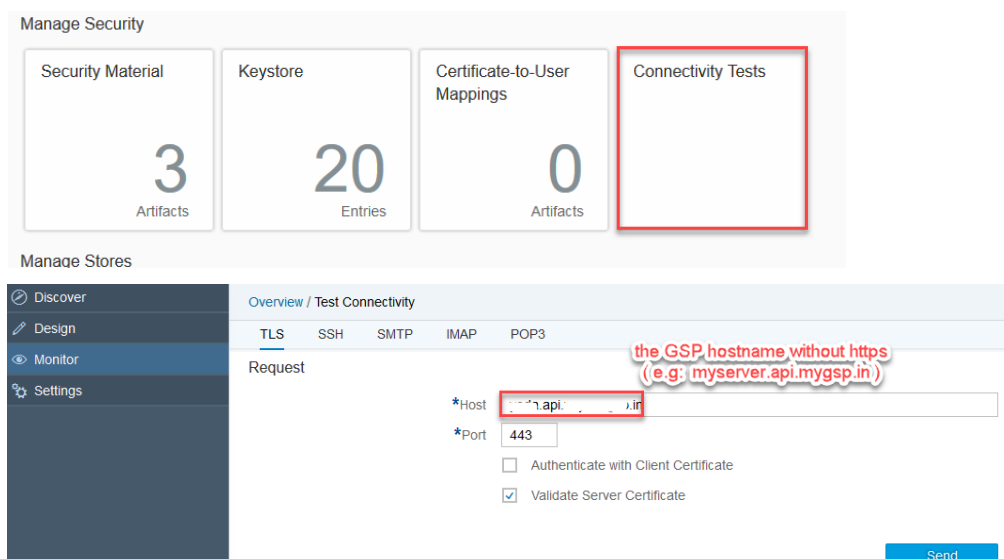
You should get a message as shown below. Click OK.



6. How to perform a connectivity Test?

You can perform the Connectivity test of the receiver by using the feature TLS Connectivity Test as mentioned [here](#).

You can find the connectivity tests under Monitor->Manage Security->Connectivity Tests



You should receive a successful response message.

Response

Successfully reached host at [redacted].api.[redacted].in:443

Client Certificate Used No



www.sap.com/contactsap

© 2016 SAP SE or an SAP 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 or an SAP affiliate company.
SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.

Material Number:

