CA Single Sign-On

Integration of CA Single Sign-On with Amazon Alexa

technologies

This Documentation, which includes embedded help systems and electronically distributed materials (hereinafter referred to as the “Documentation”), is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2018 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contents

Integrate CA Single Sign-On with Amazon Alexa

This document describes how to integrate CA Single Sign-On (CA SSO) with Amazon Alexa services using its account linking capability.

A knowledge of CA SSO, Amazon Alexa, and OpenID Connect is required to understand this integration.

Important! *CA Technologies offers this document as is as of May 04, 2018. This document does not represent or include any commitment from CA Technologies to provide a formal, ongoing support of the content in this document by CA Technologies.*

Overview of Amazon Alexa Account Linking

The account linking capability of Amazon Alexa allows voice-controlled devices like Amazon Echo to establish an identity with third-party systems and to consume its services with ease.

A user's Amazon Alexa account is connected to his/her corresponding user account in CA SSO through OIDC **Access Token**. Access Token identifies the user uniquely in CA SSO. The Amazon Alexa service stores this token and includes it in requests that are sent to the Amazon Alexa skills service. The skill uses the token to authenticate with CA SSO on behalf of the user.

As an example, let us see how this feature works in a financial institution.

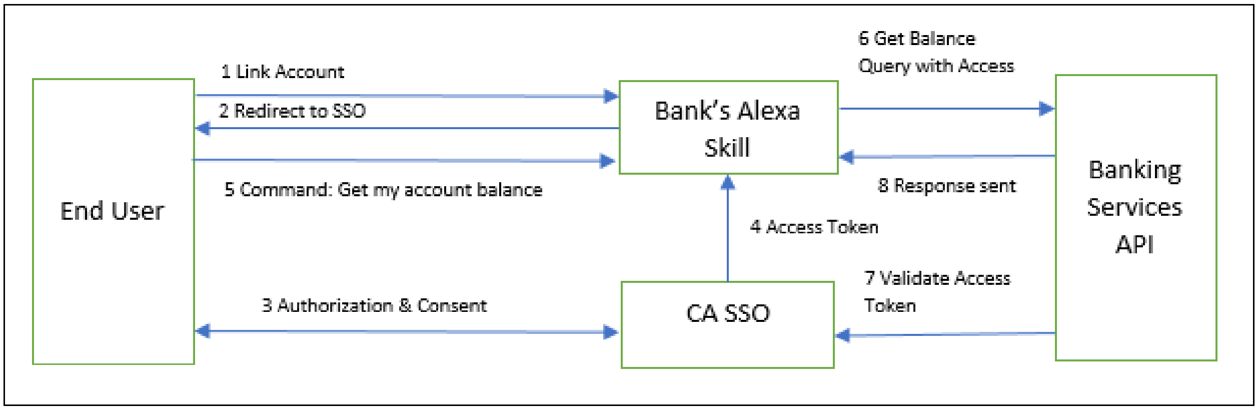
Account Linking in Financial Institution

A financial institution such as a bank can use Amazon Alexa to enhance the digital experience of its customers. Building specific Amazon Alexa skills allows users to check account balances, pay bills, and find information such as interest rates. These services provide the bank an opportunity to connect with users to complete bank transactions at home, and thus simplifying the banking experience of customers.

However, the question is how to trust an Amazon Alexa end user account, allow it to connect and utilize secured banking services. The answer is the account linking capability of Amazon Alexa. It allows secure linking of an Amazon Alexa end user account with an enterprise account.

A financial institution or a bank that secures its environment using CA SSO can leverage CA SSO's OIDC capabilities to establish account linking with an Amazon Alexa end user account. Amazon Alexa end users authenticate with CA SSO to link with their corresponding user account in CA SSO, which is deployed at the bank.

The following diagram details how CA SSO can work with Amazon Alexa:



The following process explains how CA SSO works with Amazon Alexa:

1. User initiates the Amazon Alexa Account to Bank Account linking process.
2. Bank's Amazon Alexa skill redirects the user to CA SSO authorization page that is deployed at Bank.
3. User authenticates with his/her credentials and provides the consent to allow the Bank's Amazon Alexa skill to use Bank's account information on his/her behalf.
4. CA SSO generates and sends an access token with the consented scopes to Bank's Amazon Alexa Skill.
5. End user asks Amazon Alexa to fetch the account balance.
6. Amazon Alexa skill provides the access token to Banking Services API and triggers a request to fetch the account balance.
7. Banking Services API validates the access token with CA SSO that is deployed at Bank.
8. If the access token is valid, Banking Services API provides an appropriate response to Amazon Alexa skill, which delivers an audio message to the end user with the information received.

Configure CA SSO

Configure CA SSO as an OIDC Provider using Authorization Code Flow.

Follow these steps:

1. Open Administrative UI.
2. Create an Authorization Provider.

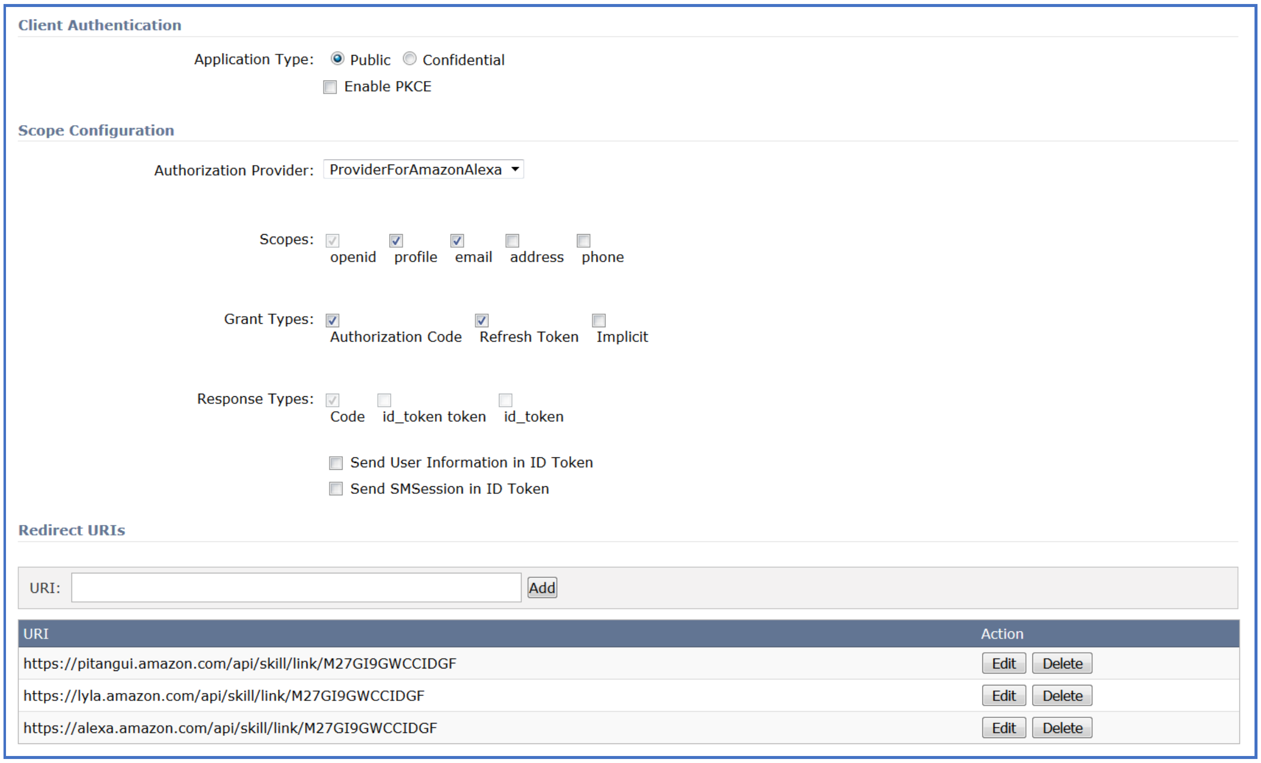
   Define all the necessary fields such as scopes, authorization URL, minimum authentication level, and so on.

   For information, see Configure CA Single Sign-On as OpenID Connect Provider.
3. Create an OIDC Client.

   Define all the necessary fields.

   Select **Authorization Code flow**.

   Enable **Refresh Token**.



Client Authentication

Application Type: ● Public ○ Confidential

□ Enable PKCE

Scope Configuration

Authorization Provider: ProviderForAmazonAlexa

Scopes: ☑ openid ☑ profile ☑ email □ address □ phone

Grant Types: ☑ Authorization Code ☑ Refresh Token □ Implicit

Response Types: ☑ Code □ id_token token □ id_token

□ Send User Information in ID Token

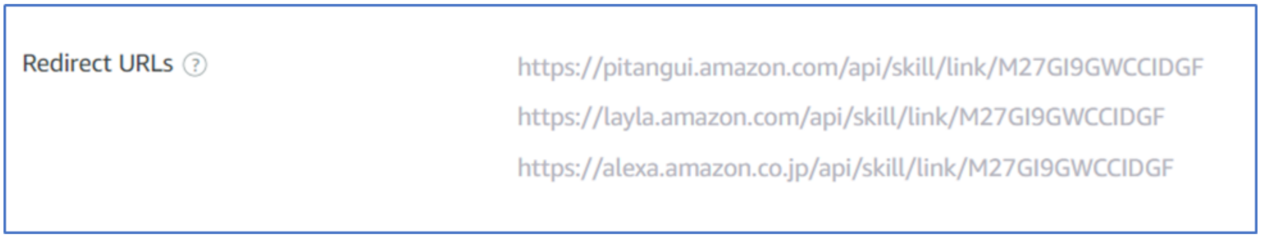
□ Send SMSession in ID Token

Redirect URIs

URI: Add

URI	Action
https://pitangui.amazon.com/api/skill/link/M27GI9GWCCIDGF	Edit Delete
https://lyla.amazon.com/api/skill/link/M27GI9GWCCIDGF	Edit Delete
https://alexa.amazon.com/api/skill/link/M27GI9GWCCIDGF	Edit Delete

Specify Redirect URLs that are provided in the respective Amazon Alexa Skill's Developer page as shown in the following example:



Redirect URLs ?

https://pitangui.amazon.com/api/skill/link/M27GI9GWCCIDGF

https://layla.amazon.com/api/skill/link/M27GI9GWCCIDGF

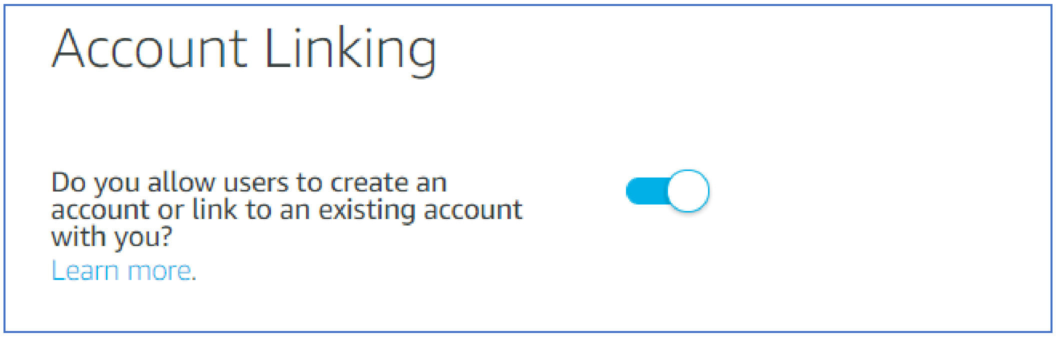
https://alexa.amazon.co.jp/api/skill/link/M27GI9GWCCIDGF

For information, see Configure CA Single Sign-On as OpenID Connect Provider.

Configure Amazon Alexa Skill

Follow these steps:

1. Navigate to https://developer.amazon.com/alexa/console/.
2. Enable Account Linking.

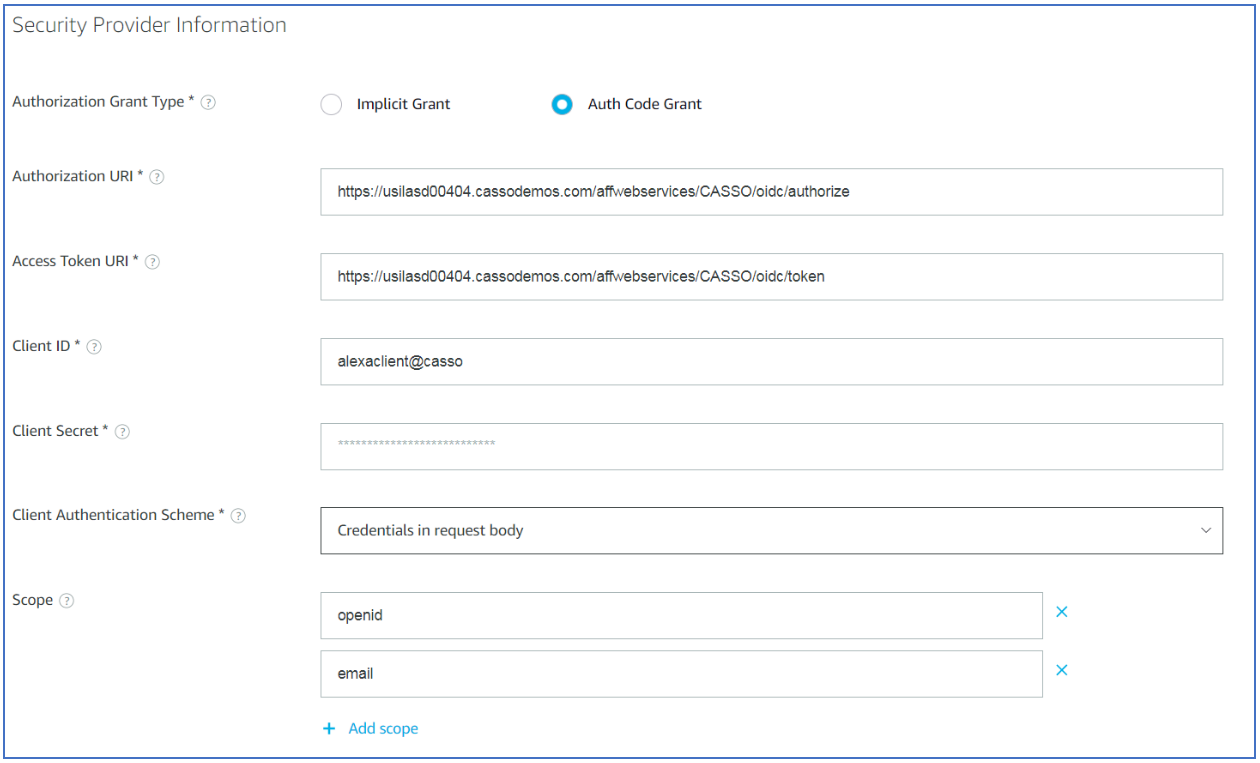


Account Linking

Do you allow users to create an account or link to an existing account with you?

Learn more.

3. Gather the following values from the Clients dialog CA SSO Administrative UI, and fill them in the Security Provider Information:
   - Authorization URL
   - Access Token URL
   - Client ID
   - Client Secret
   - Scopes



Security Provider Information

Authorization Grant Type * ○ Implicit Grant ● Auth Code Grant

Authorization URI * https://usilasd00404.cassodemos.com/affwebservices/CASSO/oidc/authorize

Access Token URI * https://usilasd00404.cassodemos.com/affwebservices/CASSO/oidc/token

Client ID * alexaclient@casso

Client Secret * ****************************

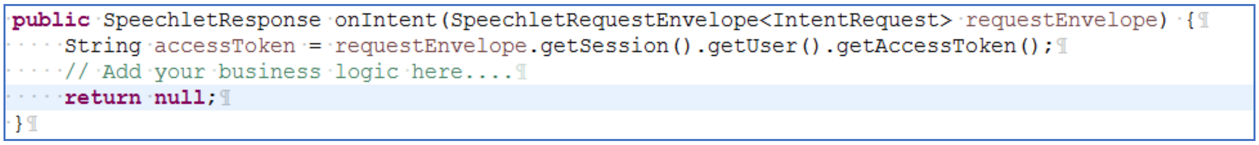
Client Authentication Scheme * Credentials in request body

Scope openid, email

4. Add the domain of the CA SSO OIDC Authorization URL to the **Domain White List** to enable the communication between Amazon Alexa Service and CA SSO.

Retrieve Access Token Programmatically in the Amazon Alexa Skill

Access token can be obtained from the user session as shown:



```
public SpeechletResponse onIntent(SpeechletRequestEnvelope<IntentRequest> requestEnvelope) {
    String accessToken = requestEnvelope.getSession().getUser().getAccessToken();
    // Add your business logic here....
    return null;
}
```

Additional Resources

For further information on Amazon Alexa Skills and Amazon Alexa Account Linking, see the following URLs:

- https://developer.amazon.com/docs/custom-skills/link-an-alexa-user-with-a-user-in-your-system.html
- https://developer.amazon.com/post/Tx3CX1ETRZZ2NPC/Alexa-Account-Linking-5-Steps-to-Seamlessly-Link-Your-Alexa-Skill-with-Login-wit