**Sign Up Configuration Using Amazon**

**To use Amazon for social login we must:**

1. Obtain an Amazon developer account from [https://developer.amazon.com](https://developer.amazon.com/).
2. Do one of the following:
   * Open a previously-created Amazon application and copy the client ID and client secret.
   * Create a new application and copy the client ID and client secret.
3. Use the Social Login Engage Dashboard and the Amazon client ID and client secret to configure Amazon as a social login provider.

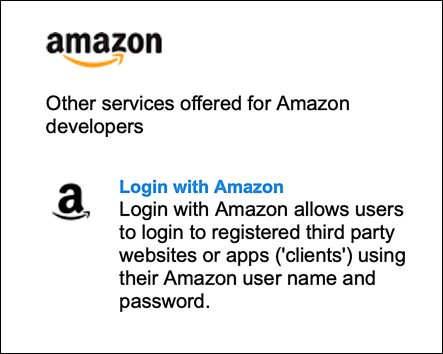
This section walks you through the process of creating an Amazon application for social login. If you already have an application, see the [Using an Existing Amazon Application for Social Login](https://janrain-education-center.knowledgeowl.com/home/amazon-social-login-configuration-guide" \l "using" \o ")section of this documentation.

To create an Amazon application, complete the following procedure:

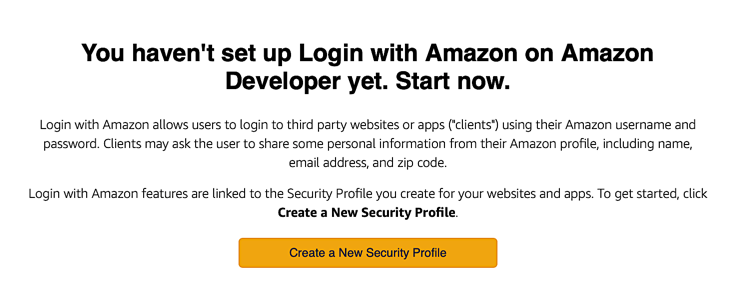
1. Log on to the Amazon developers center ([https://developer.amazon.com](https://developer.amazon.com/)).
2. On the developer home page, in the upper right corner, click **Developer Console:**



1. On the **Developer Console** home page, click **Login with Amazon:**



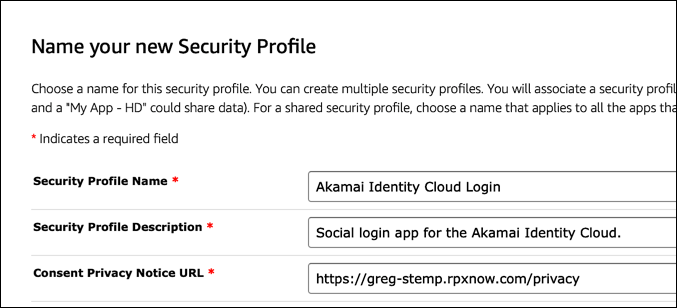
4. On the **Login with Amazon** home page, click **Create a New Security Profile**



5 .On the Name your new Security Profilepage:

* Enter the name of your app in the **Security Profile Name** field.
* Enter a brief description of your app in the **Security Profile Description**field.
* Enter the URL for your privacy policy in the **Consent Privacy Notice URL** field.

For example:



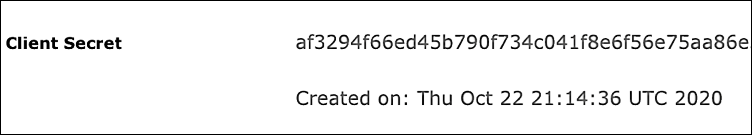
1. Click Save.
2. On the home page for your new app. click the configuration icon in the Manage column and then click Web Settings:



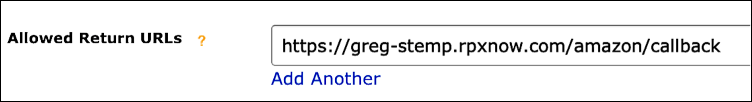
In the **Web Settings** section, copy the **Client ID:**



Click **Show Secret** and then copy the client secret



1. Both the client ID and the client secret are required to configure Amazon as a social login provider.
2. Click the Edit button, enter your Amazon redirect URI in the AllowedReturns URLs field, and then click Save. If you are using a standard Identity Cloud domain your redirect URL will look similar to this: *https://greg-stemp.rpxnow.com/amazon/callback*. For example:



1. Log off from the Amazon developers center.

**Password:**  We can set a custom password policy on our AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. If we don't set a custom password policy, IAM user passwords must meet the default AWS password policy.

**Rules for setting a password policy:** The IAM password policy does not apply to the AWS account root user password or IAM user access keys. If a password expires, the IAM user can't sign in to the AWS Management Console but can continue to use their access keys.

When we create or change a password policy, most of the password policy settings are enforced the next time our users change their passwords. However, some of the settings are enforced immediately. For example:

* When the minimum length and character type requirements change, these settings are enforced the next time that our users change their passwords. Users are not forced to change their existing passwords, even if the existing passwords do not adhere to the updated password policy.
* When we set a password expiration period, the expiration period is enforced immediately. For example, assume that you set a password expiration period of 90 days. In that case, the password expires for all IAM users whose existing password is older than 90 days. Those users are required to change their password the next time that they sign in.
* We can't create a "lockout policy" to lock a user out of the account after a specified number of failed sign-in attempts. For enhanced security, we recommend that you combine a strong password policy with multi-factor authentication (MFA).

## Permissions required to set a password policy

We must configure permissions to allow an IAM entity (user or role) to view or edit their account password policy. You can include the following password policy actions in an IAM policy:

* iam:GetAccountPasswordPolicy – Allows the entity to view the password policy for their account
* iam:DeleteAccountPasswordPolicy – Allows the entity to delete the custom password policy for their account and revert to the default password policy
* iam:UpdateAccountPasswordPolicy – Allows the entity to create or change the custom password policy for their account.

## Default password policy

If an administrator does not set a custom password policy, IAM user passwords must meet the default AWS password policy. The default password policy enforces the following conditions:

* Minimum password length of 8 characters and a maximum length of 128 characters
* Minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & \* ( ) \_ + - = [ ] { } | ' symbols
* Not be identical to your AWS account name or email address

## Custom password policy options

When we configure a custom password policy for your account, you can specify the following conditions:

* Password minimum length – We can specify a minimum of 6 characters and a maximum of 128 characters.
* Password strength – We can select any of the following check boxes to define the strength of your IAM user passwords:
  + Require at least one uppercase letter from Latin alphabet (A–Z)
  + Require at least one lowercase letter from Latin alphabet (a–z)
  + Require at least one number
  + Require at least one nonalphanumeric character ! @ # $ % ^ & \* ( ) \_ + - = [ ] { } | '
* Enable password expiration – We can select and specify a minimum of 1 and a maximum of 1,095 days that IAM user passwords are valid after they are set. For example, after 90 days a user's password expires and they must set a new password before accessing the AWS Management Console. The AWS Management Console warns IAM users when they are within 15 days of password expiration. IAM users can change their password at any time if they have permission. When they set a new password, the expiration period for that password starts over. An IAM user can have only one valid password at a time.
* Password expiration requires administrator reset – Select this option to prevent IAM users from updating their own passwords after the password expires. Before you select this option, confirm that your AWS account has more than one user with administrative permissions to reset IAM user passwords. Also consider providing access keys to allow administrators to reset IAM user passwords programmatically. If you clear this check box, IAM users with expired passwords must still set a new password before they can access the AWS Management Console.
* Allow users to change their own password – We can permit all IAM users in your account to use the IAM console to change their own passwords, as described in Permitting IAM users to change their own passwords. Alternatively, you can allow only some users to manage passwords, either for themselves or for others. To do so, you clear this check box. For more information about using policies to limit who can manage passwords, see Permitting IAM users to change their own passwords.
* Prevent password reuse – We can prevent IAM users from reusing a specified number of previous passwords. We can specify a minimum number of 1 and a maximum number of 24 previous passwords that can't be repeated.

## Setting a password policy (console)

We can use the AWS Management Console to create, change, or delete a custom password policy.

**To create a custom password policy (console)**

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Account settings.
3. In the Password policy section, choose Change password policy.
4. Select the options that you want to apply to your password policy and choose Save changes.

**To change a custom password policy (console)**

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Account settings.
3. In the Password policy section, choose Change.
4. Select the options that you want to apply to your password policy and choose Save changes.

**To delete a password policy (console)**

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Account settings.
3. In the Password policy section, choose Delete.
4. Confirm that you want to delete the custom password policy by choosing Delete custom.