amazon business

Single Sign-on (SSO) Integration with Amazon Business

Contents

Overview

This document provides guidance and reference material to IT professionals to establish a Single Sign-on (SSO) integration with Amazon Business. SSO with Amazon Business is no different from any other SSO integration you may have done with other apps.

SSO benefits

Single Sign-on integration allows you to set up SSO with a variety of identity providers such as Okta, OneLogin, Microsoft Entra ID, Google Workspace (gSuite), Microsoft ADFS, AWS SSO, OpenAM, and Shibboleth using SAML 2.0. The key benefits of this feature are:

Streamline onboarding

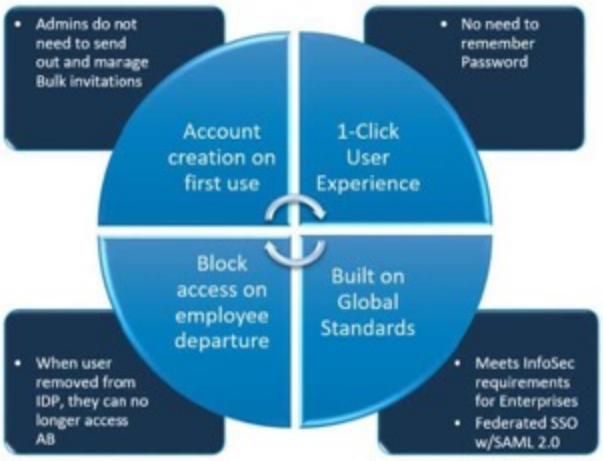
- Get started easily on Amazon Business without the need to manually invite new users.
- Just-In-Time (JIT) provisioning allows employees to join as a user to their organization's Amazon Business account and start purchasing immediately the first time they visit the Amazon Business store.

Improve security & reduce risk

- Automatically block access to Amazon Business when an employee leaves and is offboarded by IT.

One-click access

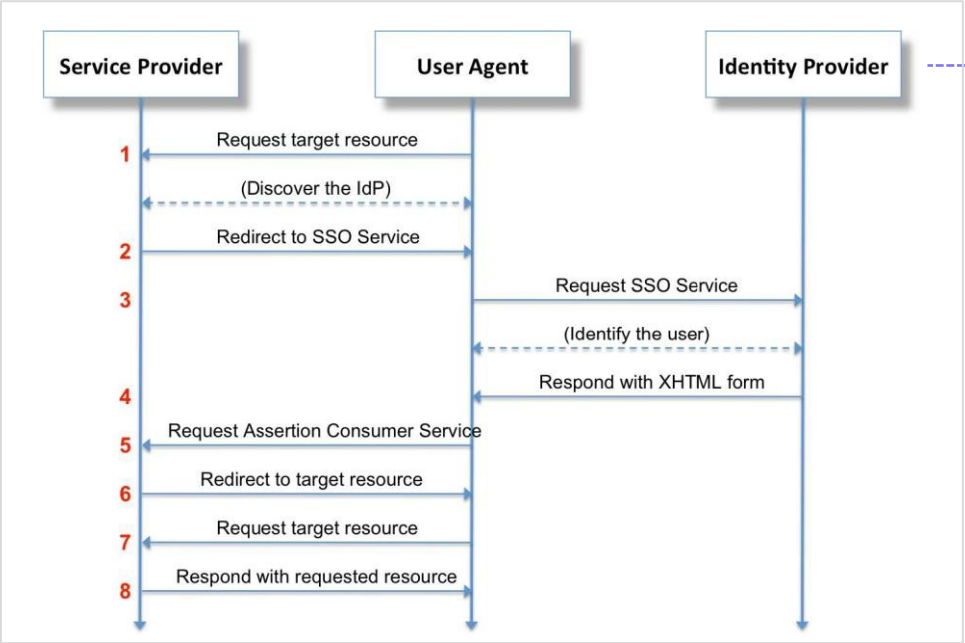
- "Direct access" users don't need to enter an Amazon Business password when signing in to the website.
- Punchout users won't be prompted to create a password when viewing order history or processing returns.



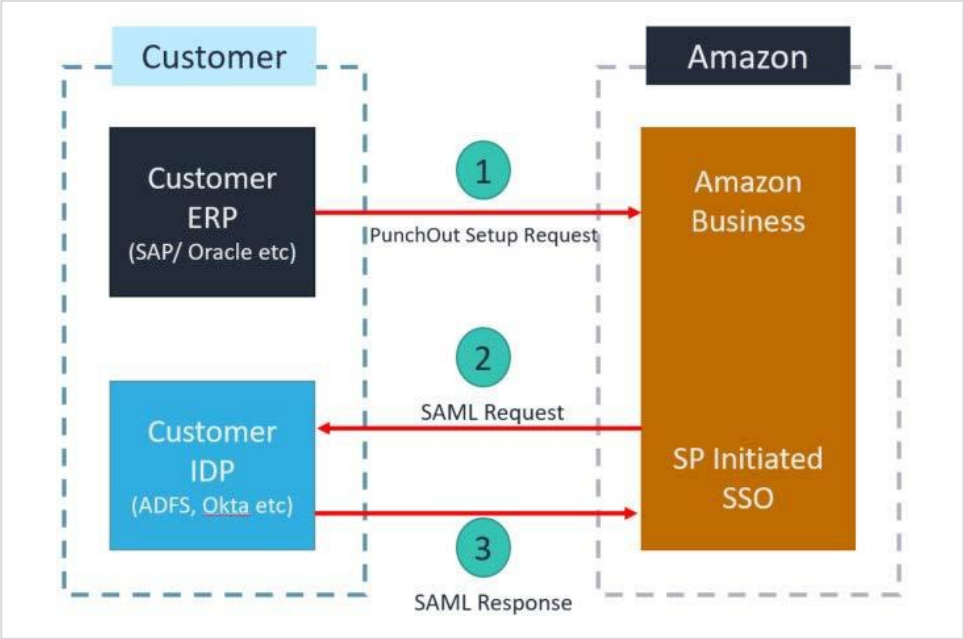
Process Flow

Below is the SSO connectivity flow.

- Identity Provider is customer's IdP.
- Service provider is Amazon Business.



Below is the Punchout flow with SSO.



Self-Service Setup on Amazon Business

SSO with Amazon Business is similar to any other SSO integration that customers may have done with other applications such as Concur, Tableau, Salesforce, ADP, etc.

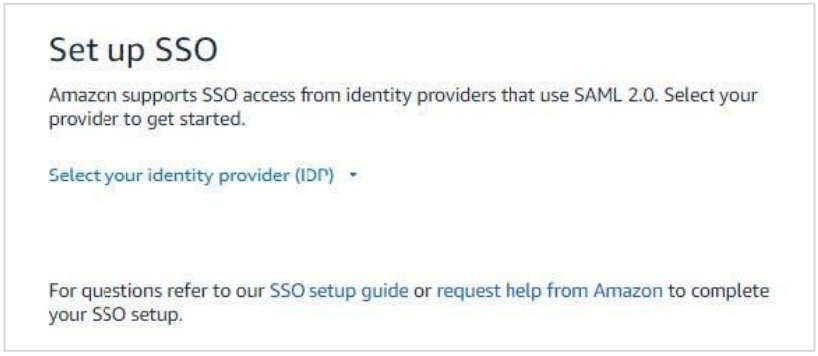
Log in to your organization's Amazon Business account.

- NOTE: If you don't yet have access to the account, reach out to your Amazon Business Admin to get invited as an "Admin" or "Tech" user. The invitation will come from business@amazon.com.

To get started, click self-service. You can also find the below screen at this path in your Amazon Business account:

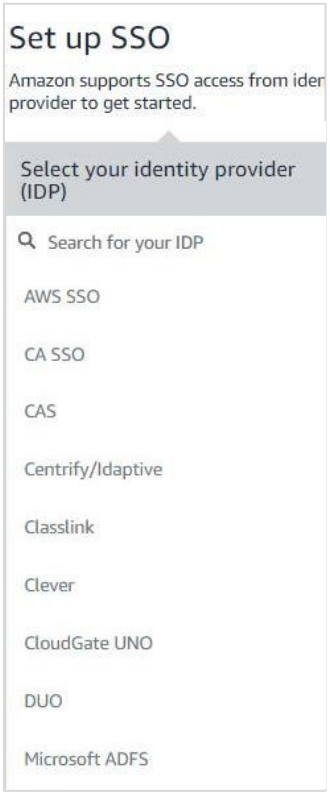
- *Hello, NAME > Business Settings > Single Sign-On (SSO)* (in the *System integrations* section).

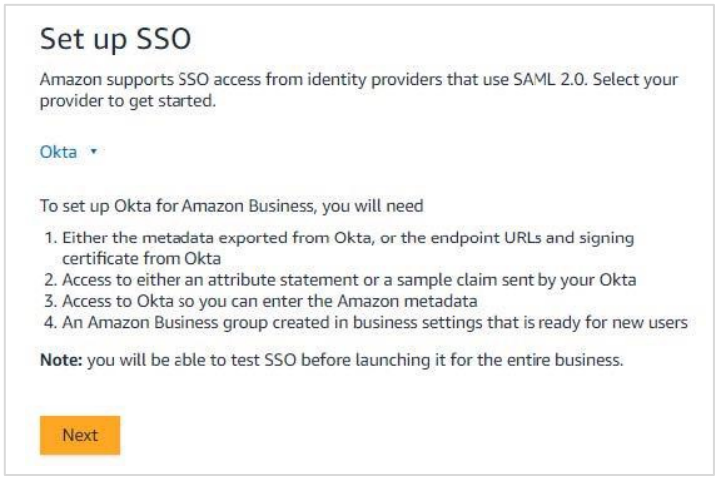
To get started, visit self-service.



Select your IdP provider name from the drop down. If you do not see your IdP in the list, search using the search bar. Once it is selected, download the configuration guide for the selected IdP and select **Next**. If you still do not see your IdP in the list, select **Other** as the IdP. While we currently only support the IdPs identified on our list, Amazon Business regularly adds support for new IdPs based on customer feedback. Your feedback is very important and will help inform that process. To share your feedback, select **Request help from Amazon**.

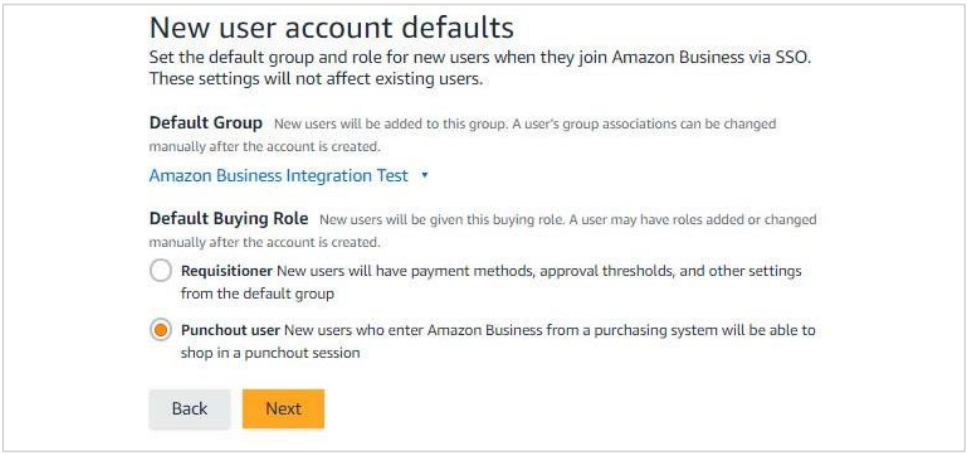
Select the **Default Group** and **Default Buying Role**. Select **Next**.



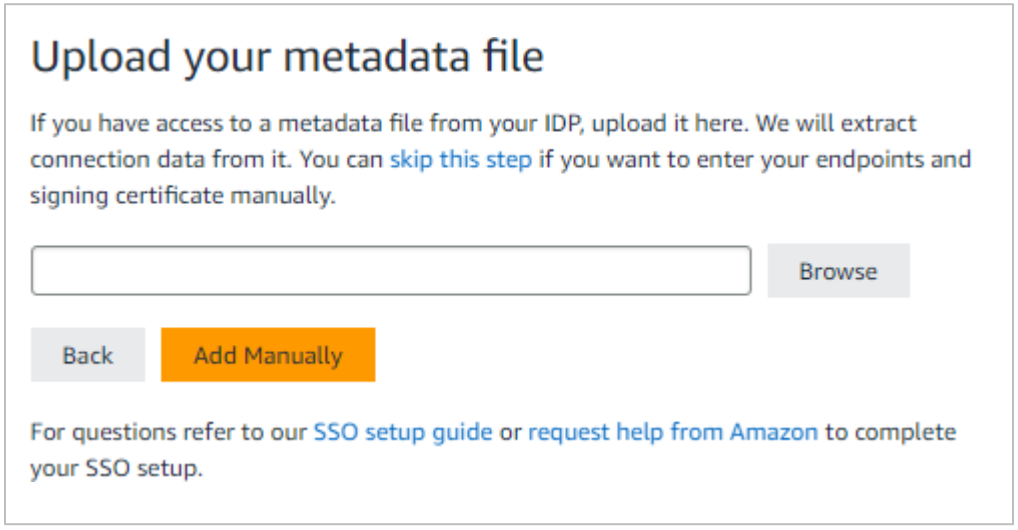


- **Default Group:** Determines where newly ("Just-In-Time") provisioned users land.
    - This group must be created in *Business Settings > Groups*.
    - You can disable purchasing in this group if users should be moved before they can start buying.
    - NOTE: Users who join your account by punching out from an eProcurement system will be provisioned in both the Punchout group and the default SSO group if they're different groups. Amazon Business suggests choosing the Punchout group here if you want all orders to be placed via Punchout.
- **Default Buying Role:** Set the default role for new users: *Requisitioner* (Direct Access) or *Punchout user*.
    - If you chose a Punchout group above, choose *Punchout user* here. Otherwise, choose *Requisitioner*.

P.S: You must ensure PPI setup is complete before setting up SSO if selecting "Punchout User".



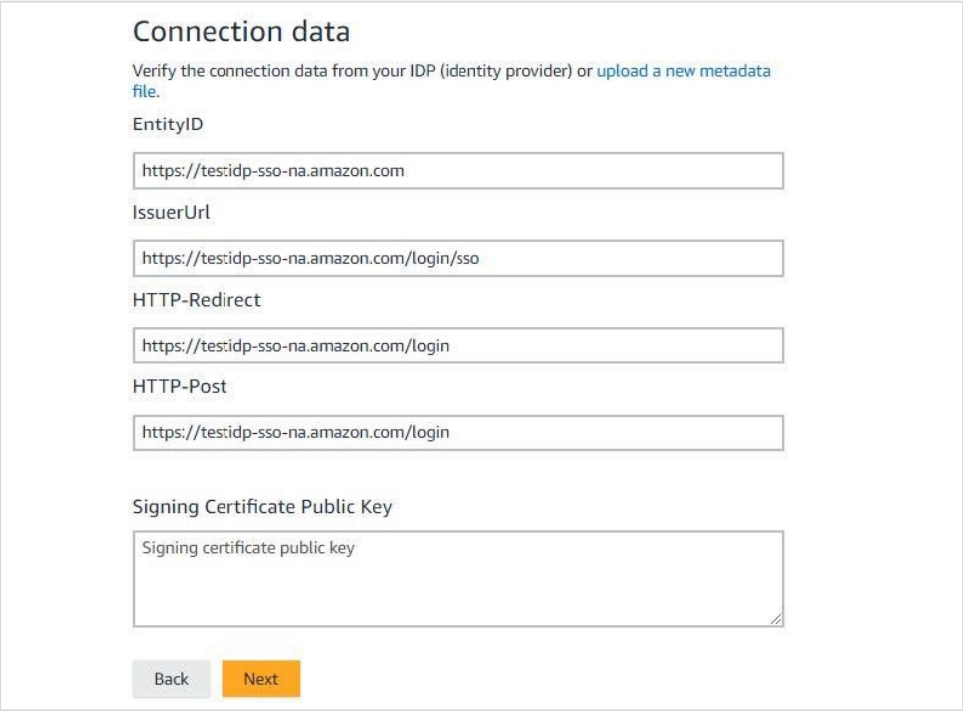
Provide Amazon Business with your IdP metadata. If your IdP provides SAML metadata for export, download it from your IdP. Then, upload the file in the Amazon Business SSO setup page. We will automatically parse the file for the necessary information. Alternatively, you can manually enter on the next page by selecting **Skip**.



Enter the following information. Please reach out to your SSO administrator if you have any questions.

- **EntityID**: A globally unique URL provided by your IdP. The standard value is regional (see below).
    - North America: https://www.amazon.com
    - EU: https://www.amazon.de
    - India: https://www.amazon.in
    - Japan and Australia: https://www.amazon.co.jp
- **IssuerURL**: A URL that uniquely identifies your SAML identity provider.
- **HTTP-Redirect URL**: This determines how a browser redirects a user to your IdP for authentication.
- **Signing certificate**: This allows you to verify signatures and establish trust in the messages that have been exchanged. Ensure that you correctly provide the complete certificate without any missing characters.

Note: If you are setting up SSO for an Australian Amazon Business account, use the entity ID for the JP marketplace.

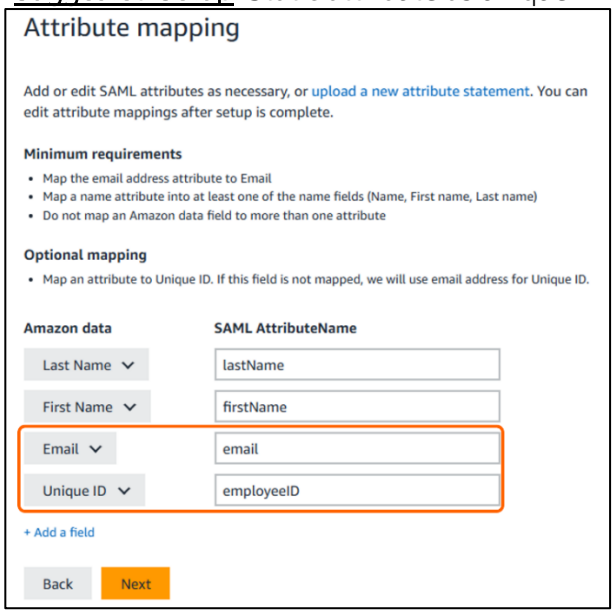


Provide Amazon Business with your attribute statement mapping. You'll need to provide the user attributes that will be provided as part of the SAML response. If you have a sample claim or attribute statement, you can upload it and we'll parse the information. Otherwise, you can enter the following values manually on the next page by clicking on **Skip**.

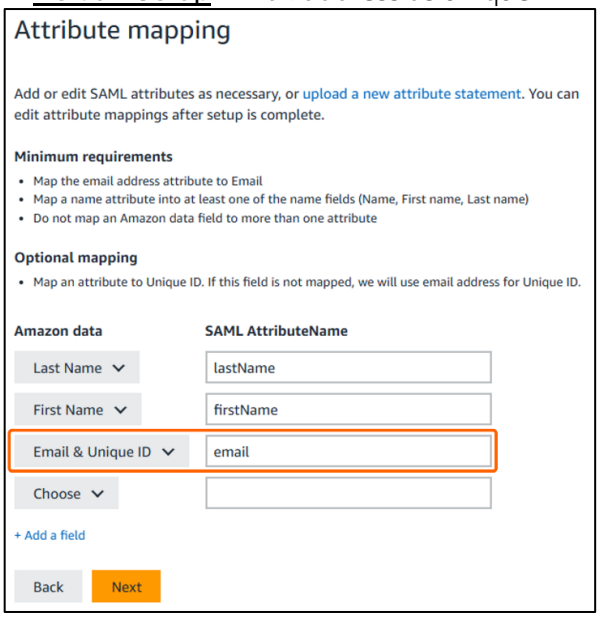
On the *Attribute Mapping* page, map "Amazon data" (data required to provision users) to the relevant "SAML AttributeNames". NOTE: SAML attribute names must be **exact matches** to what's in the SAML response.

- **Mandatory attributes**: *Email address*, *First Name*, *Last Name*. Optionally, the name can also be sent in one "Full Name" attribute instead of separate attributes for first and last names.
- **Unique identifier**: Indicate which attribute Amazon Business should use as the unique ID for each user. **Amazon Business suggests using something less likely to change than email address, such as employee number. In this example, the unique ID is set to "employeeID". See the following.**

Suggested Setup: Static attribute as unique ID

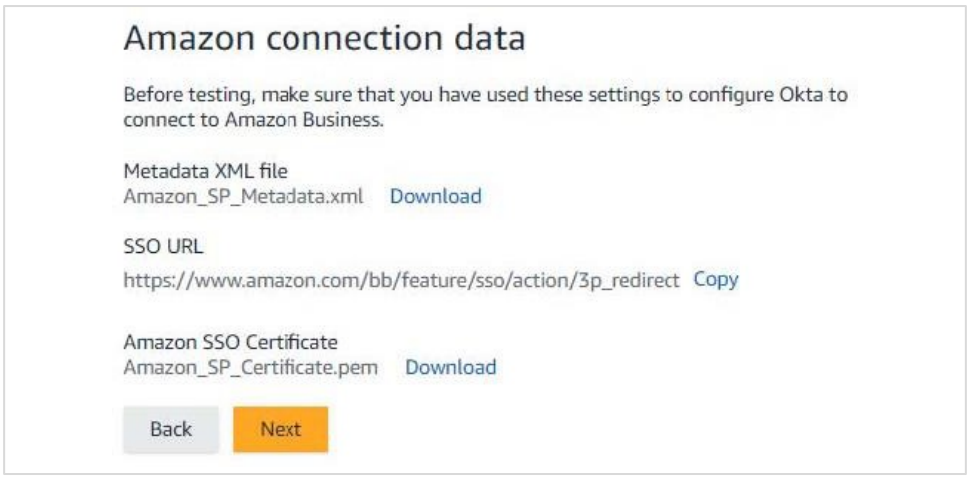


Default Setup: Email address as unique ID

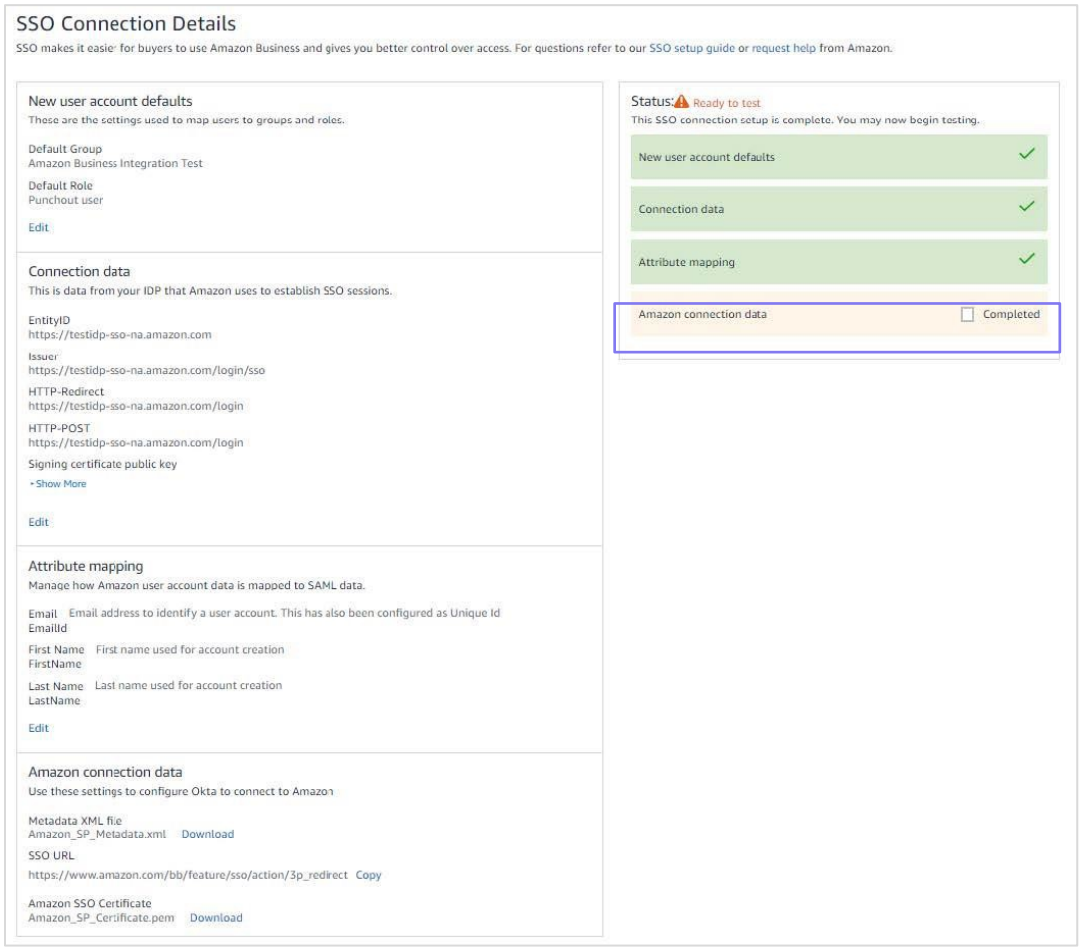


Configure your IdP with Amazon Business metadata.

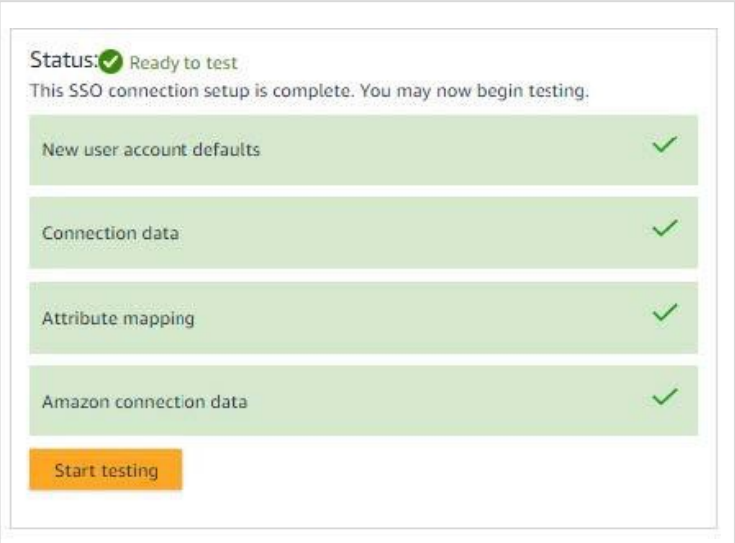
- Search for Amazon Business in your IdP's application catalog. If you do not find it, create a new custom application, and enter your IdP.
- Do one of the following, depending on whether the Amazon Business application you created supports SAML metadata import:
    A. If your application supports SAML metadata import, you can download the SAML metadata file from the Amazon connection data section and import it into your application.
    B. If your application does not support SAML metadata import, you need to enter the SSO configuration information using the steps given below:
        1. Download the Amazon metadata XML file from the application configuration page. Open the file and copy the entityID, HTTP_POST URL and configure these in your application as required.
        2. Download the Amazon certificate. Upload the certificate in your application.
- With the information provided in the SSO Connection page, configure the application with the URL and Amazon metadata.
- Ensure that the SAML responses are signed with any algorithm such as SHA56.
- If your IdP supports SAML assertion encryption, we recommend encrypting using the x509 certificate provided in the Amazon metadata. If your IdP does not support SAML assertion encryption or encryption using third-party certificates, then you do not need encrypt the assertion.
- Provide the attribute mappings for the application to match the attributes you provided on Amazon Business.



Select **Completed** once you verify Connection Data and Attribute mapping.



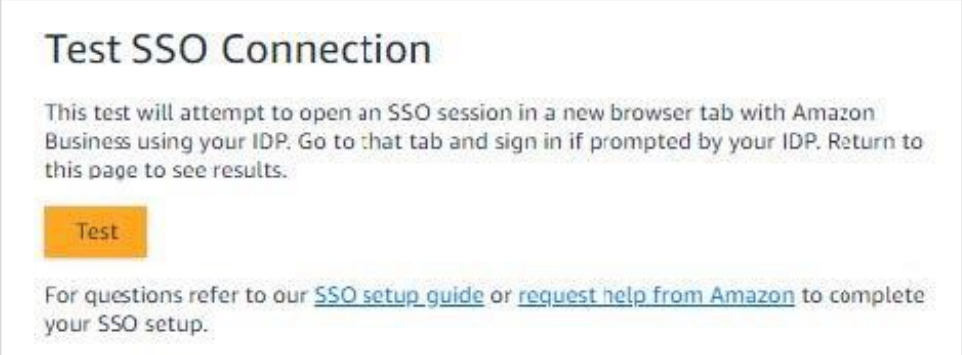
You should be ready to test the connection now. Select **Start Testing**.



Testing

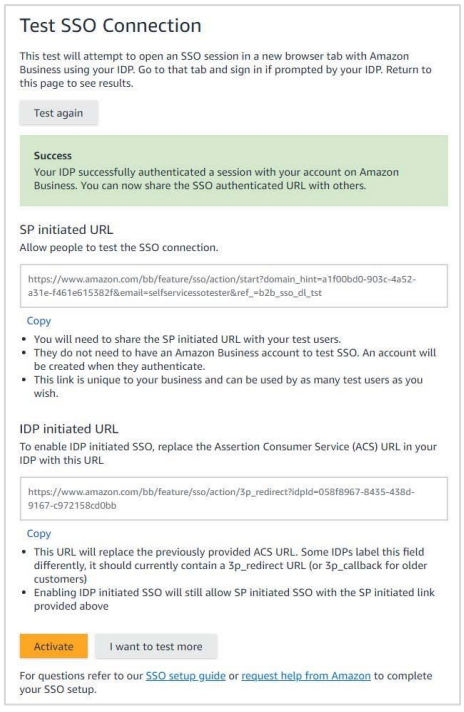
Before you start testing, please make sure the administrator who selects **Start Testing** is added to your IdP server.

A new window will open with **Test** button. Select **Test**. A new browser tab will open that will redirect you to your IdP for authentication. In the IdP portal, sign in as a user who has been granted access to the Amazon Business application. If you are already authenticated with your IdP, then we will attempt to federate you using SSO into Amazon Business. Once you are successfully authenticated, you will be able to land on Amazon.com.



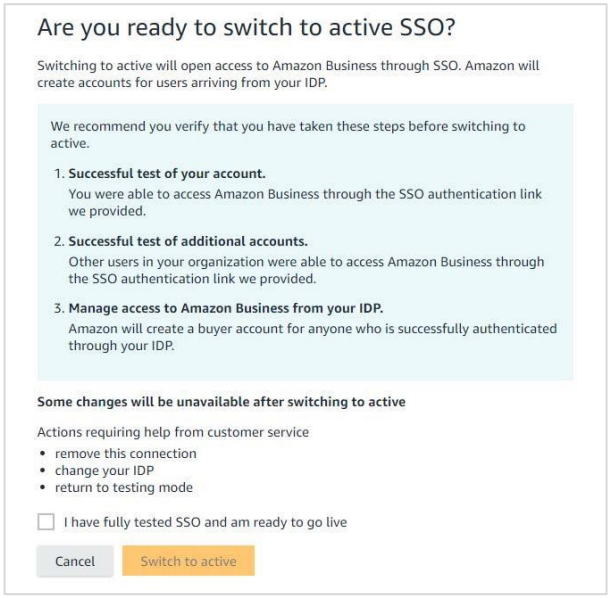
On the SSO testing page, you will see whether the test was successful or not. If your test was successful, you will be federated into Amazon Business.

- If you want other users to test, you can share the SSO SP-login link on the Test page with those users. Please ensure that those users can authenticate using your IdP.
- If you are ready to enable SSO for all users, select **Activate**.



Select the checkbox confirming all testing has been completed and select **Switch to active**. The first time someone signs into Amazon Business using SSO, they will automatically be given an Amazon Business account.

To turn off SSO for your account, navigate to the SSO page in your Amazon Business account by going to **Hello, NAME > Business Settings > Single Sign-on (SSO)** in the "System integrations" section, and select **Disable SSO**.



Once SSO is active, please follow the below process depending on your use case. Ensure that only the right users or groups have access to Amazon Business through your IdP. Users accessing Amazon Business through your e-procurement system through SSO will have to authenticate with your IdP. Ensure that the users have access to Amazon Business through your IdP.

Instructions for your End Users - Punchout

- The way users access Punchout will remain the same even with SSO. They have to start Punchout from your e-procurement system.
- Users accessing Amazon Business through your e-procurement system through SSO will have to authenticate with your IdP. Ensure that the users have access to Amazon Business through your IdP.

Instructions for your End Users – Direct Buy

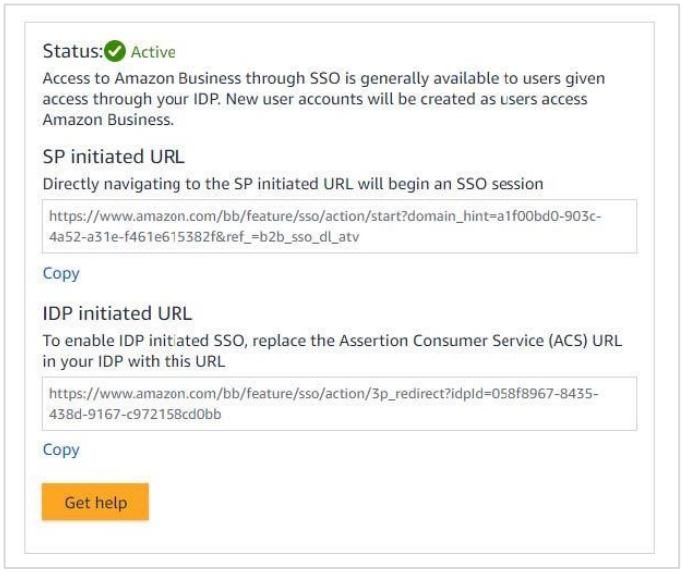
- **SP-Initiated URL**: You can host the SSO SP-link provided on the connection page anywhere within your systems so that your users can access the URL and federate to Amazon Business. If you use an IdP such as Okta, you can also set up a Bookmark application and embed the SP-login URL. You can also share the URL directly with user so that they can bookmark in their browser.
- **IdP-initiated URL**: If your IdP supports it, you will be given an IdP initiated URL which can be used to enable ID-initiated SSO. To use IdP initiated SSO, the URL must be used to replace the Assertion Consumer Service (ACS) URL in your IdP.

- Direct Access: If your users try to access Amazon.com, they will be routed to your SSO server immediately once they enter their email address. This currently works only for existing users.

The ACS can be labelled differently in different IdPs. If you are having trouble finding the field to replace, check your IdP's documentation. This field should have a URL ending in 3p_redirect or 3p_callback if you have access to the IdP initiated URL.

- User logs in to the e-procurement system and clicks on the Amazon Business tile.

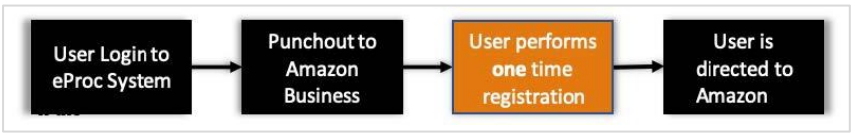
Enabling IdP initiated SSO will not impact the usage of Service Provider (SP) initiated SSO through the link provided.

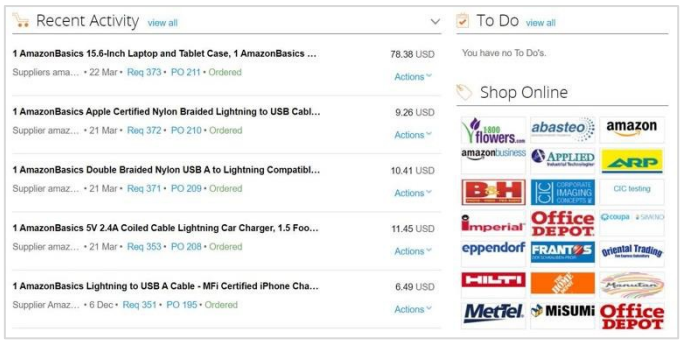


User Experience

User Experience without SSO:

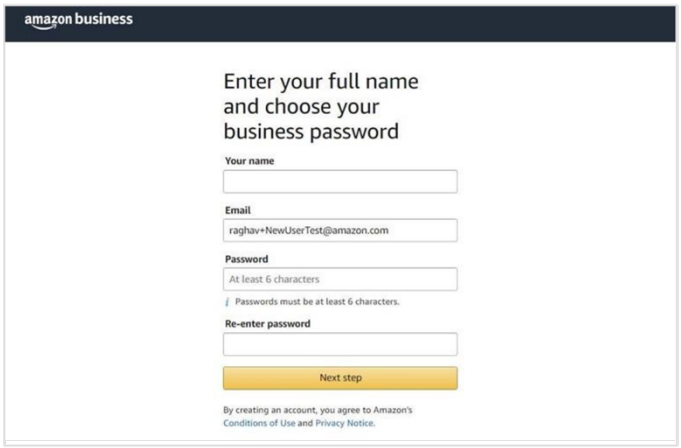
- If the user doesn't have an existing Amazon account tied to their work email address, the user will be provided step-by-step instructions to create a new account log-in in your organization's Amazon Business account. Details like Name and Password need to be entered by the user.

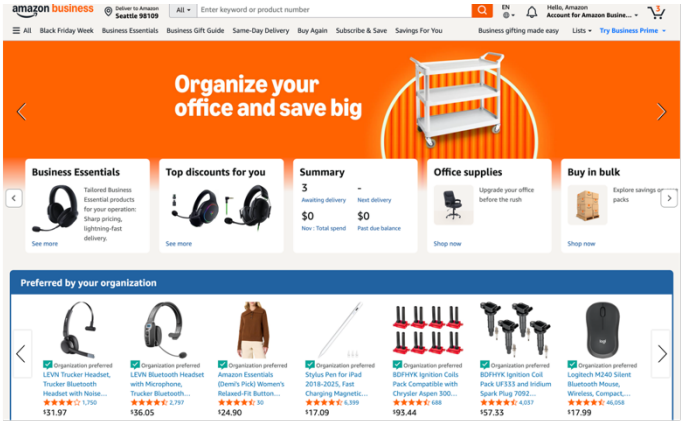




- You will be logged in to Amazon Business.

- Click on "Get Started" to create an account. Enter your Name and set a password. Please do not change the email address.



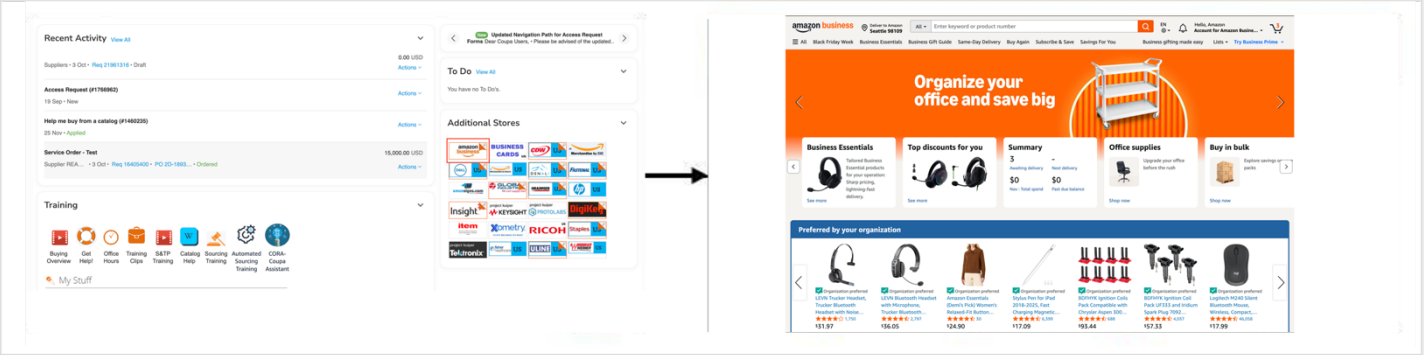


User Experience with SSO:

Use Case 1:

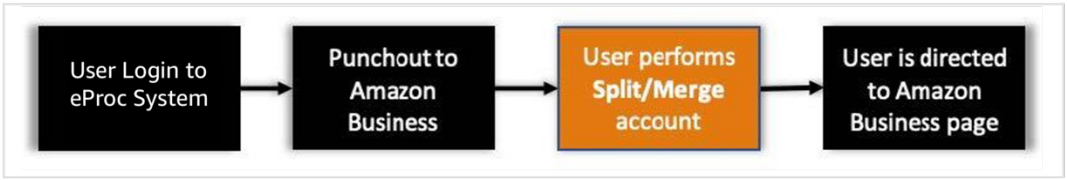
- If the user doesn't have an existing Amazon account tied to the work email address, Amazon Business SSO will leverage customer identity provider and fetch the required details to create a new account log-in automatically in the organization's Amazon Business account.
- The user will be automatically routed to Amazon Business homepage.

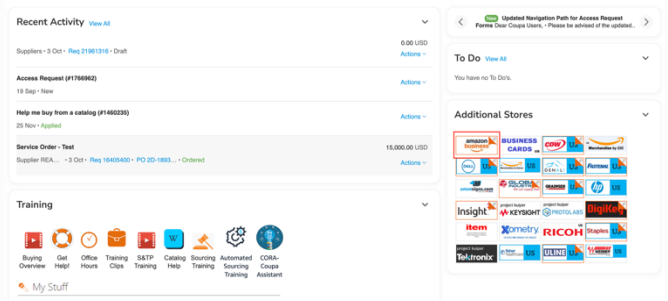
- The user logs into e-procurement system and clicks on the Amazon Business tile.

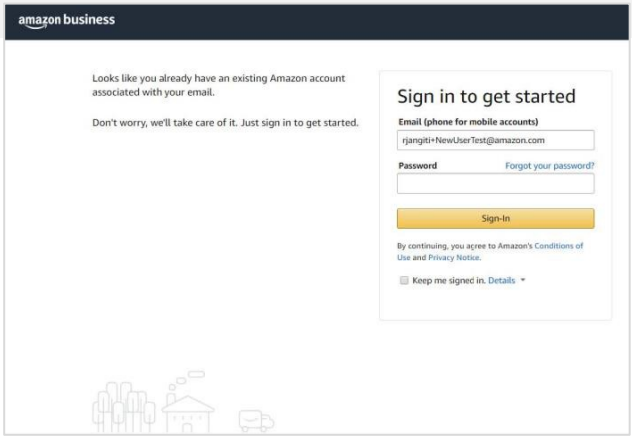


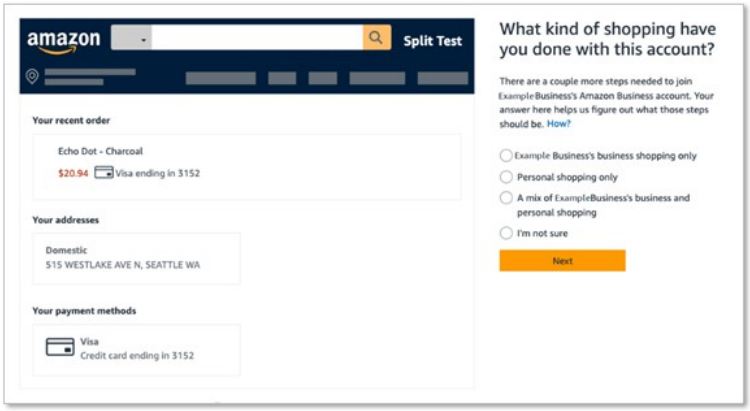
Use Case 2:

- If the user has an existing Amazon personal account tied to the work email address, Amazon Business SSO will present the option to split/merge the personal account from your business account.









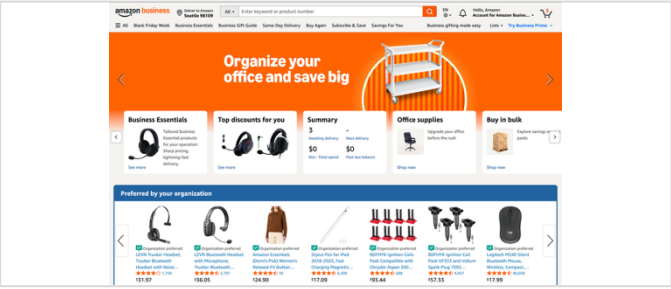
- Create a separate business user account: This option separates your personal account with your business account. Enter your personal email address and continue. You can login to your personal account with new email id and same old password.

- You will then be added to the business account with your work email address.

OR

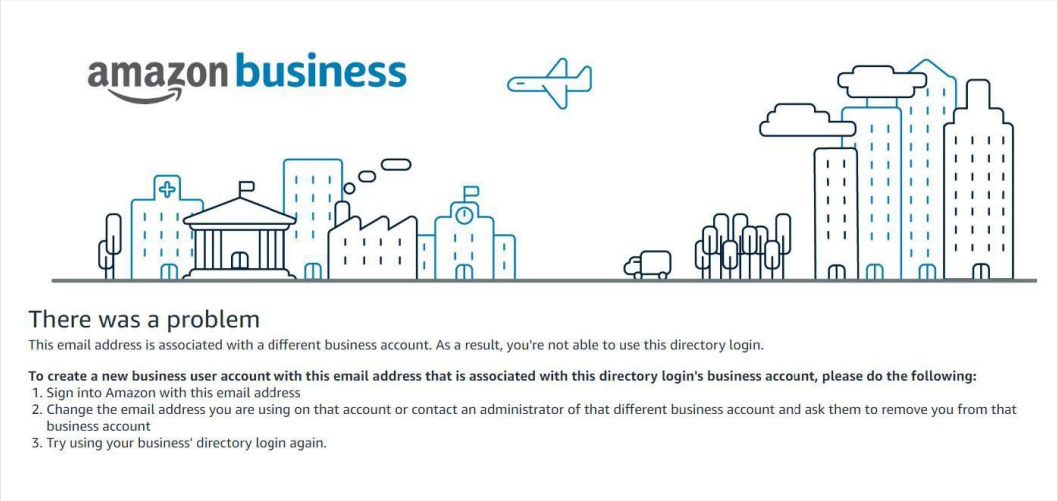
- Convert my existing Amazon account: This option converts your existing personal account into the business account.
- Converting your account will move all of your order history, addresses and payments in to the business account. Your business account administrator will have access to your order history.

  Choose the option that best fits the kind of shopping you have done using your personal Amazon Business account and follow the remaining prompts to complete the convert/split workflow.



- Once completed, you will be logged in to Amazon Business.

- If the user has an existing Amazon Business account tied to the same work email address, you will have to change the email address on your existing business account or reach out to your administrator of previous business account.



Provisioning Users to Multiple groups

Customers can now provision new users in different groups.

Prerequisites

- Customer should be able to create and send a new attribute in the SAML assertion.
- Customer should have some mapping between their existing system and Amazon Business i.e. their Amazon Business structure reflects departments, business units, cost centers, etc.
- Punchout customers will still need to send User Business Unit (UBU) Value in Punchout cXML as an extrinsic.

There are two ways this can be set up:

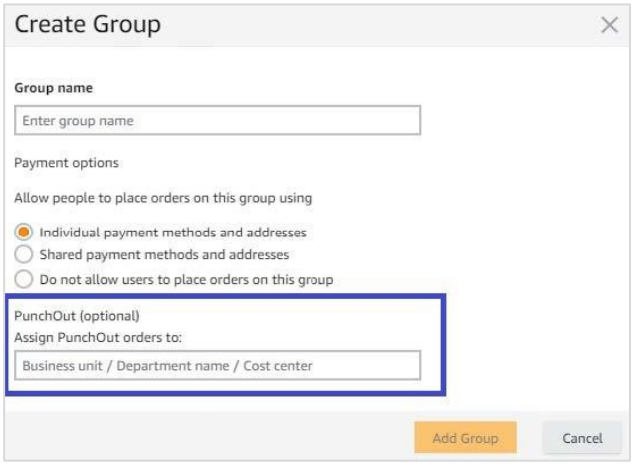
Option 1: Send a Group tag

- Used in scenarios where Amazon Business group structure exactly mirrors customers' directory structure.
- Customer creates a new "Group" attribute in SAML assertion.

- Pass the full group path for a user e.g. \Company\Finance\New York.

Option 2: Send a Group tag

- Used in scenarios where Amazon Business group structure differs from customer's directory structure. For example, a group on customer side is " Finance Cost Center – 001", while the group on Amazon Business is simply "Finance".
- Customer creates a new "GroupTag" attribute in SAML assertion.
- Customer adds a tag to each group on Amazon Business. Your Amazon Business contact can help with this
- Customer simply passes tag in SAML assertion. AB checks if tag in SAML assertion matchers tag on any group, and if match, creates user in that group.
- Group Tag can be setup at the time of group creation as shown below.



FAQ

Which identity providers are supported?

Amazon Business uses the industry standard Security Assertion Markup Language (SAML) 2.0, which means our implementation of SSO integrates easily with any large identity provider that supports SAML. We support service provider initiated SAML with identity providers such as Okta, OneLogin, AWS SSO, TrustLogin, and Azure AD.

Is there any impact to existing users?

There is no impact to existing users when the account switches to SSO.

Do you support SP initiated or IdP-initiated SSO?

We support both.

How can I update my SSO configuration once SSO is switched to Active?

Navigate to the SSO page in your Amazon Business account by going to **Hello, NAME > Business Settings > Single Sign-on (SSO)** in the "System integrations" section. Select **Disable SSO > Restart Testing Mode** and check the confirmation box. Once you make the necessary changes, select **Test again** on the right side of the page and follow the prompts to re-activate. Note that changes to the default settings will only impact new users, not existing users.

Can I bypass SSO and directly access AB by logging in?

An SSO user will be able to access AB directly without a password by navigating to amazon.com/business and still be redirected into an SSO authenticated session.

Does SSO manage users?

No. SSO helps with first time user provisioning and subsequent authentication. SSO will not manage user movement across groups. Once the user is manually moved, SSO will honor the new group.

Appendix

Definitions

- SAML 2.0: The industry-standard SSO communication protocol
- Identity Provider (IdP): A solution that provides SSO capabilities such as authentication, identity of users, groups etc. Common IdPs include Okta, OneLogin, Microsoft ADFS, Azure AD, and AWS SSO (all are supported by AB SSO).
- Service Provider (SP): The application that a user accesses through SSO e.g. Concur, ADP, Salesforce, AWS, or Amazon Business
- SAML Assertion/Attribute/Claim: A SAML Assertion is the request/response passed between user's browser and Amazon Business. It contains Attributes are specific pieces of data that provide information about the user e.g. Email Address, Name, Group, GroupTag. Assertions essentially contain information that verifies who the IdP is, who the user is, and whether the user should have access to Amazon Business.
- Claim is a common term used in Microsoft products (ADFS, Azure) and are interchangeable with assertion/attributes.

Amazon Business Customer Service/Post-Production Support

Contact the Amazon Business customer service team for any transactional questions related to an order, including ordering, quantity availability, shipment speed, delivery tracking, returns, and refunds. This team can also provide administrator support, including feature configuration and system integration support.

Chat with support

Please note that we keep adding new features to Amazon Business and the website. You may see slight differences in terminology and/or layout compared to this document. If you have any questions, please call Amazon Business Customer Support.
Learn more about Amazon Business SSO: https://business.amazon.com/en/solutions/systems-integration/single-sign-on