MICHAEL EBY

michaeleby1@gmail.com | GitHub | Blog | LinkedIn

Table of Contents

Universal search

Starburst Galaxy's **universal search** lets you locate your data entities in Galaxy.

Search overview

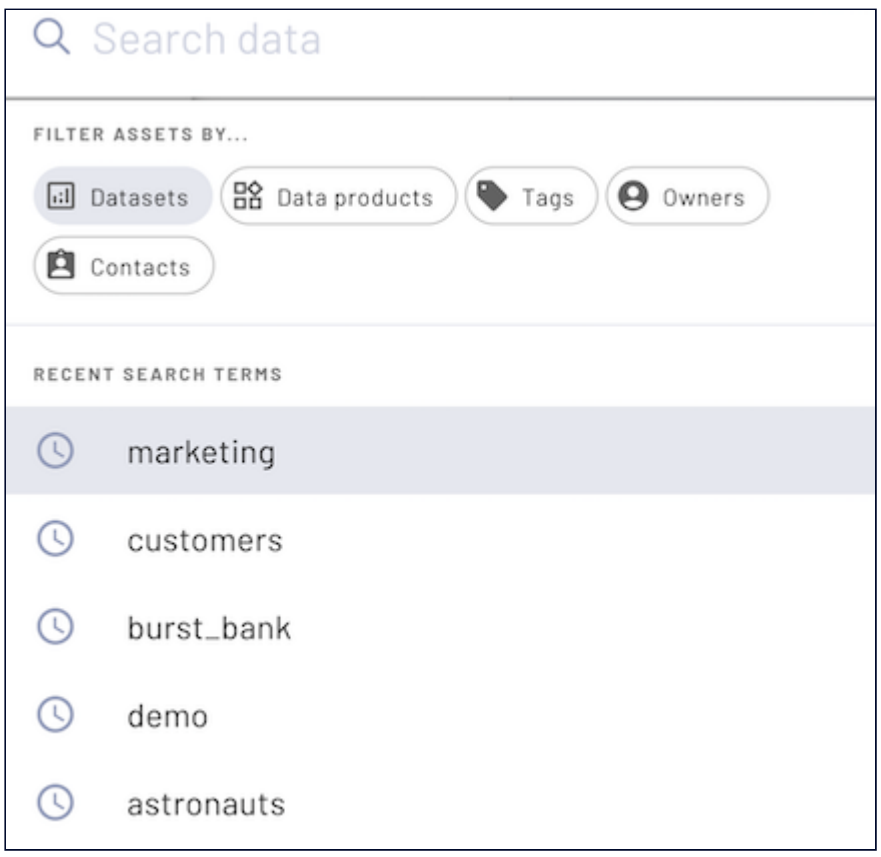
Use universal search to locate any data object by name or metadata name anywhere in your Starburst Galaxy account. You can search for the names of catalogs, schemas, tables, views, columns, data products, tags, owners, or contacts. Universal search parses Galaxy's cached description of your account, which means it does not require any cluster to be enabled or running.

The search type is a case-insensitive anchored search that matches entity names by trying to match the first characters of the search term to the first characters of various target strings. As a result, to locate an entity named `token`, the search string `tok` matches, but search string `ken` does not.

Using universal search

To begin searching:

1. Click the 🔍 magnifying glass icon in the banner of Starburst Galaxy to open the search field. As an alternative, you can open the search field with the key combination `Cmd + K` on MacOS, or `Ctrl + K` on Windows.



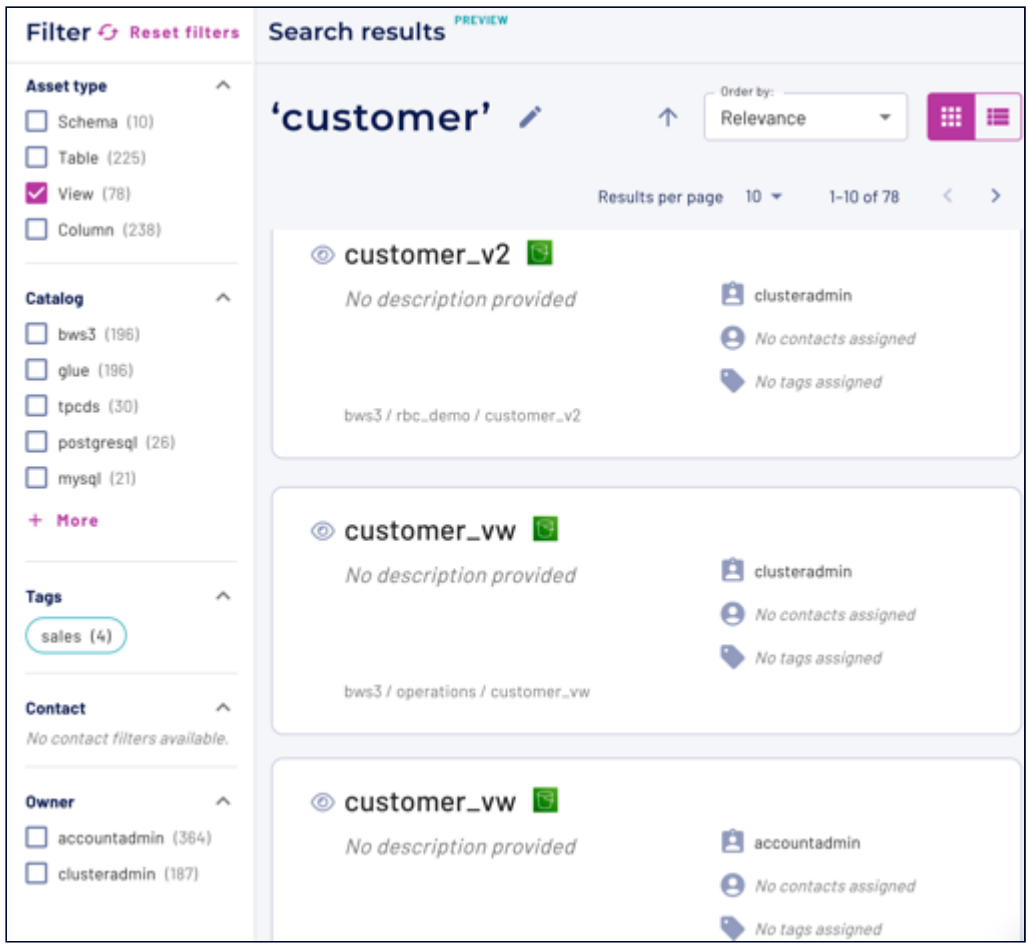
2. In the search field, enter your search term and select a filter category. By default, your search term is matched against any component of dataset names, including catalog, schema, table, view, and column names. You can also restrict the search to the names of data products or tags, as well as the ownership or contact metadata for datasets.
3. Entering a search term shows a truncated preview of the results.
4. Click the matching entity to navigate to that entity in the catalog explorer, or click **View all results** to open the **Search results pane**.

The five most recent search terms are listed in the **Recent search terms** section. Recent terms are saved in browser local storage. Clearing browser data clears recent search terms.

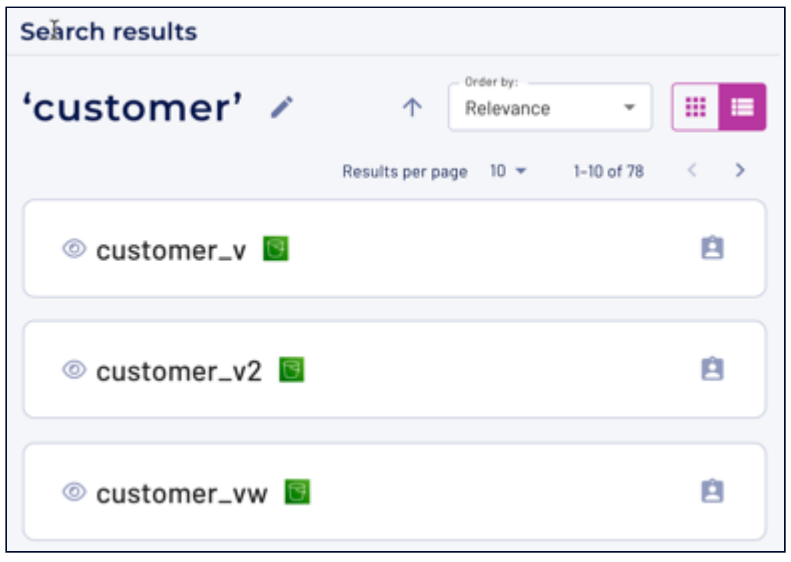
Search results pane

In the search results pane, narrow the scope of the search results using the **Filter** pane. Select one or more filter options to restrict the search results to match selected categories.

For example, to see only views related to your search term, select **View** in the **Asset type** filter category. The results are returned in the default ▦ grid mode:



To use list mode to show only the entity names matching your search term and filters, click the ☰ button:



Available filter categories include:

- **Asset type:** restrict the current search results to match names of catalogs, schemas, tables, views, columns, and/or data products.
- **Catalog:** restrict the current search results to match schema, table, view, or column names in specific catalogs.
- **Tags:** restrict the current search results to match entities that have one or more specified tag names.
- **Contact:** restrict the current search results to match usernames designated as contacts for the entity.
- **Owner:** restrict the current search results to match roles designated as entity owners.

Click the ✎ pencil icon next to the search term to edit the search query or start a new search.

Use the drop-down **Order by** menu to sort results by relevance, name, or description.

Click the **Results per page** drop-down to adjust the number of results you see per page to 5, 10, 25, or more if you have that many results.

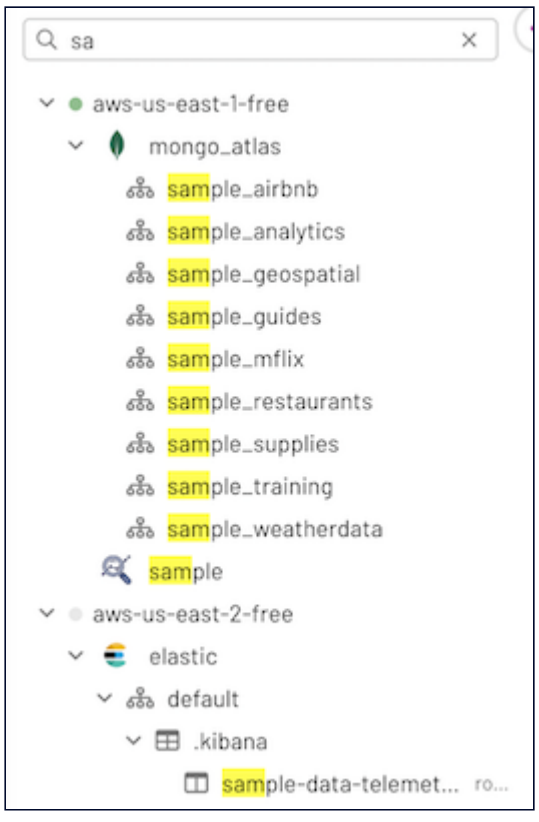
Click a tag in the Starburst Galaxy UI in places such as the catalog explorer and the tags pane to navigate directly to the search results page for that tag.

Search in the query editor

Search for an entity name in the cluster explorer pane of the query editor.

To search your data:

1. If the cluster explorer pane is not visible, click the ⊙ icon to open the pane.
2. Use the **Search data** field denoted by the 🔍 magnifying glass icon at the top of the cluster explorer pane.
3. Type your search term. As you type, entities that match what you are typing are revealed and highlighted in yellow:



In addition to providing search in the cluster explorer, Starburst Galaxy's implementation of universal search provides auto-completion for entity names when typing in the query editor pane.

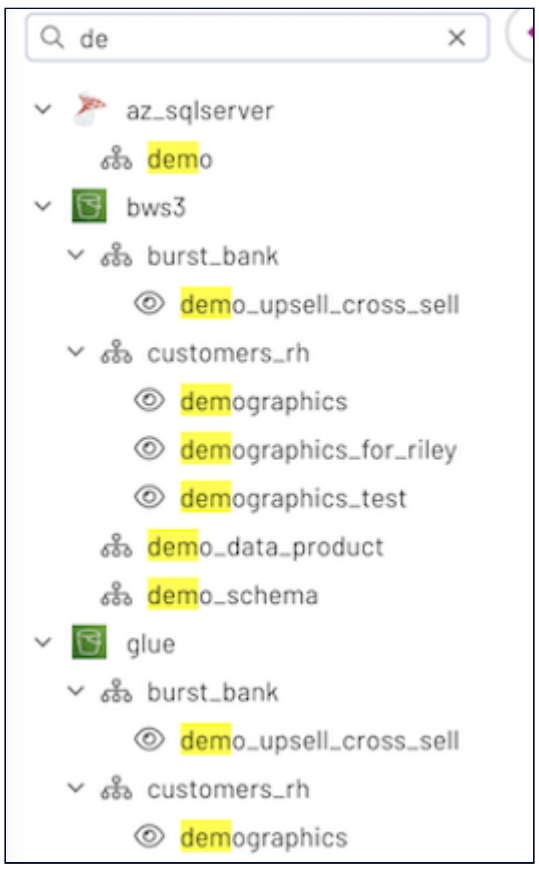
See Query editor > Auto-completion for further information on auto-completion.

Search in the catalog explorer

Search by entity name in the catalog explorer.

To search your data:

1. If the catalog explorer pane is not visible, click the icon to open the pane.
2. Use the **Search data** field denoted by the magnifying glass icon at the top of the catalog explorer pane.
3. Type your search term. As you type, entities that match what you are typing are revealed and highlighted in yellow:



AWS PrivateLink

> **Note:** Starburst Galaxy's support for AWS PrivateLink is a private preview feature. Contact Starburst support with questions or feedback.

General setup phases

To configure a Starburst Galaxy catalog to connect to an AWS data source that is protected with the AWS PrivateLink service, you must configure certain features of the AWS data source to prepare for the connection. There are two phases:

1. **On AWS:** Configure an AWS endpoint service in the AWS Management Console. See the step-by-step instructions for assistance.
2. **In Starburst Galaxy:** Contact your Starburst account team for support.

AWS PrivateLink Overview

Starburst Galaxy supports secure connections to AWS-hosted data sources that are protected with AWS PrivateLink.

AWS data sources can take advantage of the AWS PrivateLink service as one way to secure access without exposing the data source to the public internet. These data sources then operate within a virtual private cloud (VPC) within AWS. Starburst Galaxy also operates securely within its own VPC. Galaxy's support for PrivateLink-secured data sources provides a way to connect VPC to VPC securely within the AWS cloud.

Starburst Galaxy supports AWS PrivateLink for some catalogs. This page provides a general overview of Starburst Galaxy's support for AWS PrivateLink. It is not intended to be a comprehensive guide to creating and administering AWS PrivateLink.

Starburst Galaxy and AWS PrivateLink

With AWS PrivateLink, Starburst Galaxy and your AWS-hosted data service communicate with each other using VPC endpoints. Network traffic between your Galaxy VPC endpoint and your AWS VPC endpoint is secured using private IP addresses. Therefore, you do not need to use an internet gateway or a NAT gateway to connect your cluster to your data source.

> **Note:** You must configure a separate AWS PrivateLink connection for each catalog you would like to connect to Starburst Galaxy.

Contact your Starburst account team to create the VPC endpoint for your Galaxy cluster to use for communication with your AWS VPC endpoint.

AWS endpoint service requirements

Configure your AWS VPC endpoint in the AWS console as an endpoint service. Starburst Galaxy requires that you use a network load balancer to receive the incoming traffic from your Galaxy cluster. You must also create a target group that routes traffic from the cluster to the load balancer.

When you create your Starburst Galaxy cluster and configure a catalog, you must deploy your cluster in the same region as your AWS-hosted data service. Starburst Galaxy does not support cross-region connections with AWS PrivateLink.

Once configured, all traffic from to this data source is routed through AWS PrivateLink. You can federate your queries across multiple data sources in the same cluster that use PrivateLink.

Okta SAML setup

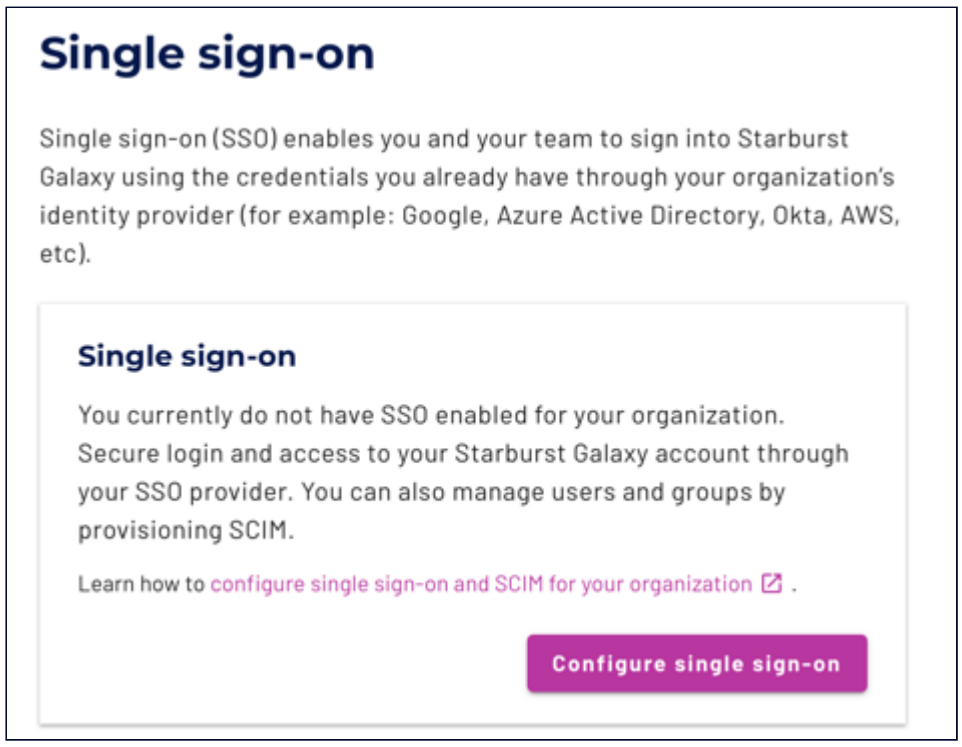
> **Note:** These SSO setup pages are meant for Starburst Galaxy administrators. You must also have admin access to your IdP's configuration site. Familiarity with SSO concepts is presumed.

Starburst Galaxy supports configuring Okta as a single sign-on (SSO) identity provider. There are two parts for full SSO participation, SAML and SCIM.

Follow the steps on this page to configure SAML connectivity between Okta and Galaxy, then go through Okta SCIM setup to complete the process.

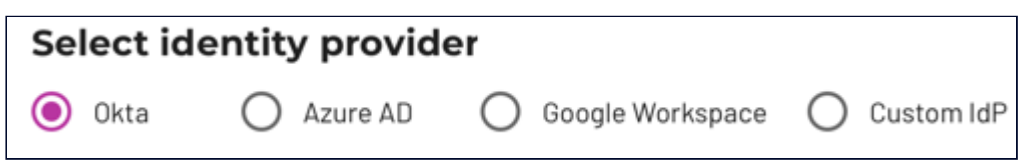
Start on Starburst Galaxy

1. In Starburst Galaxy's navigation menu, open **Access control** > **Single sign-on**.
2. Click `Configure single sign-on`.

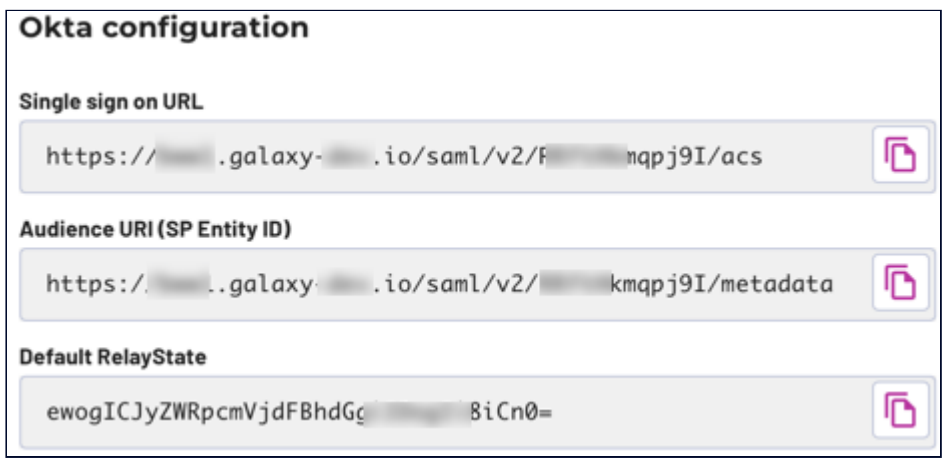


   If Starburst Galaxy is already configured with an SSO provider, you must delete it before you add a new one. However, first see Delete an SSO provider to understand the consequences of SSO deletion.

3. Select **Okta** from the **Select identity provider** options.



4. Take note of the strings in the next three fields, which are ready to copy into Okta. The labels above each field are the same wording as in Okta to help you identify the target location.



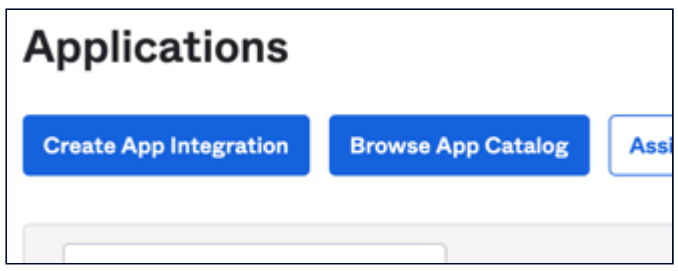
> **Note:** Leave this browser window open to this pane while you open a new browser window.

Copy SAML values to Okta

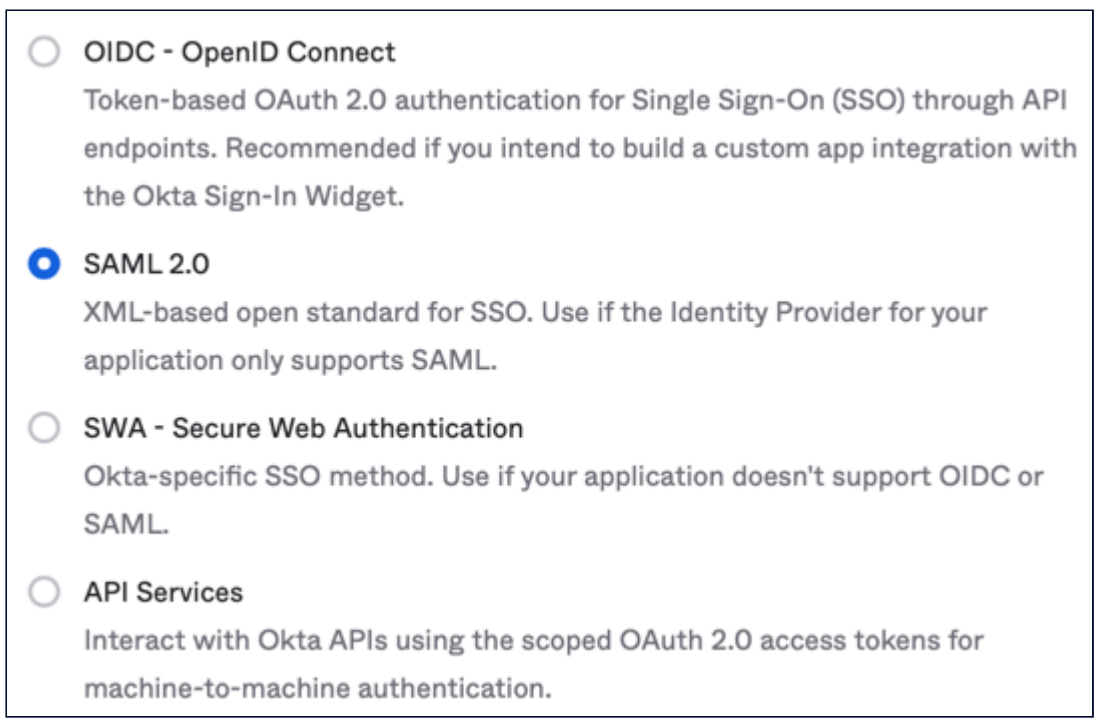
1. In a new browser window, open the admin console for your Okta account or open your normal Okta account and click **Admin** in the top pane.

2. Click the ☰ menu and select **Applications** > **Applications**.

3. In the **Applications** pane, click **Create App Integration**.



4. In the next pane, select **SAML 2.0** and click **Next**.



5. This opens the **Create SAML Integration** pane, which has three tabs.

   In the **General Settings** tab, provide a name for this app integration.

   Remember that the name you choose is visible to specified Okta users in their Okta dashboards. The obvious name to give this app integration is **Starburst Galaxy**.

   You can optionally upload a logo or image file to represent the app in the Okta dashboards of your users.

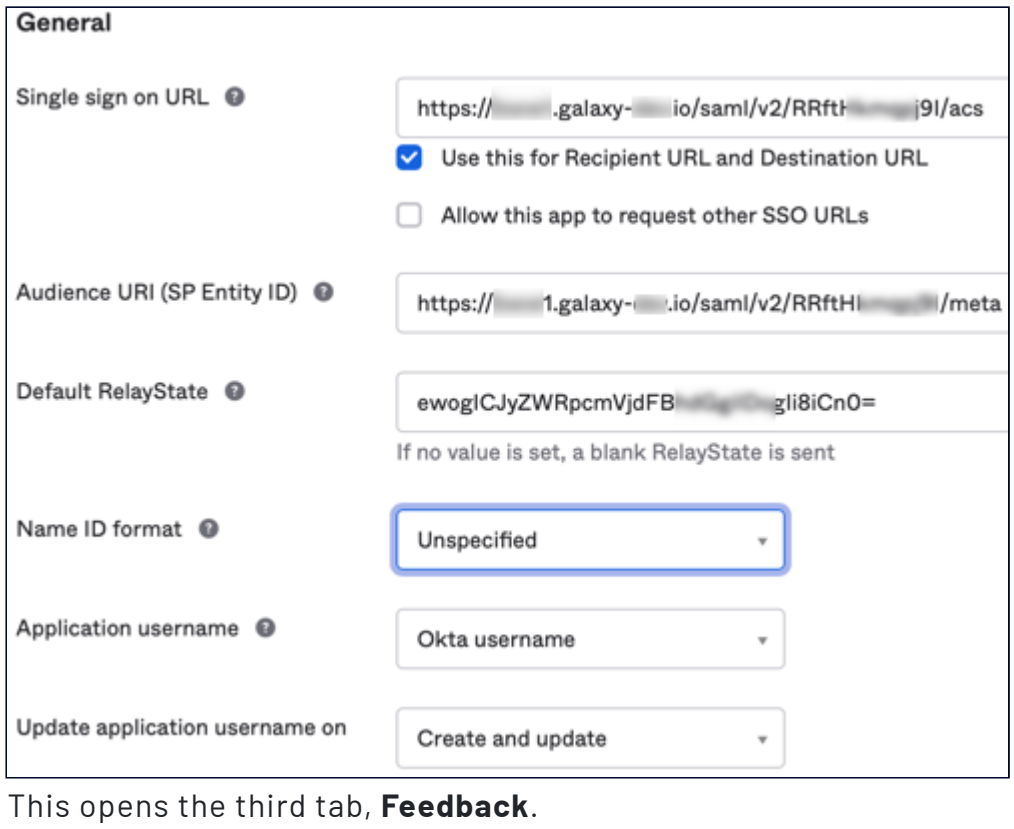
   When done, click **Next**.

6. This opens the second tab, **Configure SAML**.

   In the **SAML Settings > General** section at the top, notice that the first three fields have the same label names as the Starburst Galaxy pane you have open in another window.

   Copy the URIs and token from each field in Starburst Galaxy to its matching field in Okta.

   Leave all other controls on this page in their default settings. Scroll down and click **Next**.



7. This opens the third tab, **Feedback**.

   You must select one of the two options on this tab, but providing feedback is optional. You can leave all fields blank, then click **Finish**.

Copy SAML values to Galaxy

The last **Finish** click in Okta leaves you in the **Sign On** tab, **Settings** pane for your new app integration. The name you assigned is now visible at the top of the page.

Copy information from this Okta pane back to Galaxy. There are two ways to copy the required information:

- With a single metadata URL
- With manual entry of three fields

Metadata URL option

Metadata URL is the easiest option to use because there is a single URL string to copy.

- In Okta's settings page for your app integration, select the **Sign On** tab.
- Scroll down to the **SAML Signing Certificates** section, which shows a table with two rows for **Types** SHA-1 and SHA-2.
- At the end of the SHA-2 row, click to drop down the **Actions** control.

- Select the **View IdP metadata** option.

  This opens a new browser tab showing the contents of an XML file. The XML display varies with browser type, but we are not concerned with the XML content, only with the URL of this web page.

- **In this new tab, go to the address bar and copy the entire URL**.
- In Starburst Galaxy, in the pane you left open, make sure the **Metadata URL** option is selected. Paste the copied URL into the field labeled **Identity Provider metadata URL**
- Proceed to test the configuration.

Manual entry option

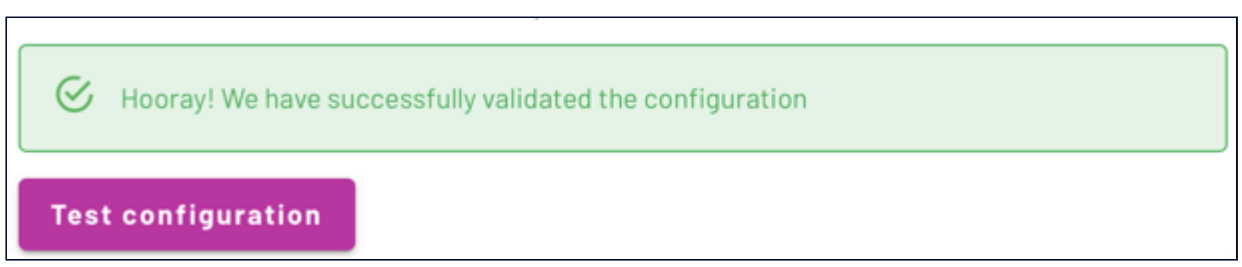
Manual entry requires you to locate and copy three fields of information from Okta to Starburst Galaxy.

- In Starburst Galaxy, in the pane you left open, make sure the **Manual entry** option is selected.

- In the browser window holding Okta, in the settings page for your app integration, scroll down to the **SAML Signing Certificate** section.
- To the right of this section, locate **SAML Setup** with a button labeled **View SAML setup instructions**. Click this button.
- This opens a new browser tab titled **How to Configure SAML 2.0 for your-app-name Application**. This page has three fields. As before, notice that the labels for each field correspond exactly with the labels of the fields on the **Manual entry** pane.
- Copy the three field values from Okta to Starburst Galaxy, field to matching field.
- Proceed to test the configuration.

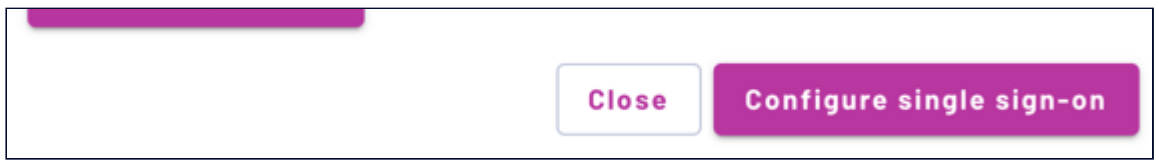
Test configuration

1. In Galaxy, click **Test configuration**.
2. If SAML communication between Okta and Starburst Galaxy is valid, you receive a green success message.



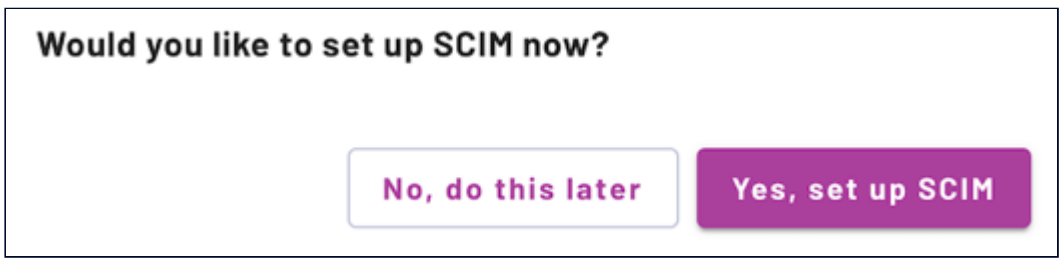
   If you receive a red failure message, go back through these steps to make sure there is not a typo or other error.

3. When the test passes, click **Configure single sign-on** to complete the process.



Proceed to SCIM configuration

Completion of SAML configuration in Starburst Galaxy leaves you at the beginning of the **Provision SCIM** stage where the following dialog appears.



This marks a good stopping point if you need a break, but Okta is not yet configured to provide SSO authentication. You can click the **No, do this later** button or even log off, and your setup position is preserved. When you return, click **Provision SCIM** on this pane.

See Okta SCIM setup for the final configuration steps.

Configure Okta to send user attributes to Galaxy

To use user attributes with policy expressions, you need to configure your IdP to send those attributes to Galaxy:

1. In Okta, navigate to your application, open the **General** tab, and under the **SAML Settings** section, click **Edit**.
2. Click **Next** to navigate to the second tab, entitled **Configure SAML**. In this section, update the attributes statements. For more information, visit the Okta developer guide.

3. Click **Next**, and then **Finish** the configuration change. At this time, new sessions are configured for your SSO provider to send each user's attributes as statements to Galaxy

Existing user sessions do not have updated attributes until the user's session expires and they re-authenticate with your SSO provider. Similarly, if a user's attribute statements are updated while that user has an existing session open, those attributes do not update until the user is re-authenticated via SSO.