How to configure Okta as a Chronicle IdP

How-to guide

Requirements

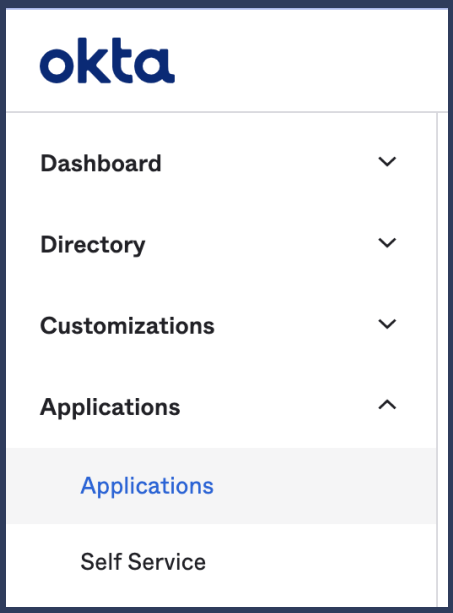
- You will need an account with access to the Okta admin portal, and the rights to create an app integration
- You will need an account to login to Chronicle

Overview

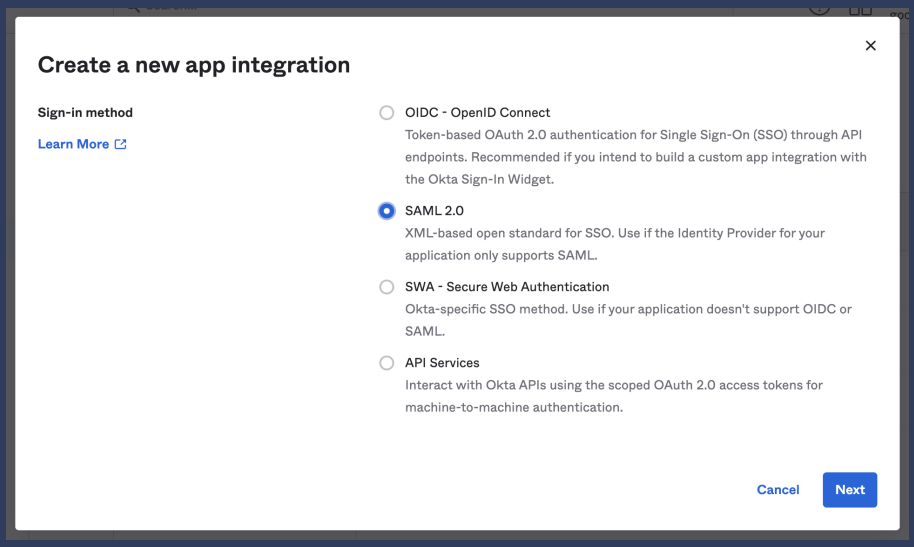
This document describes the process for integrating Okta into Chronicle to provide single sign-on (SSO) capabilities for you and your organization.

Creating the SAML Application

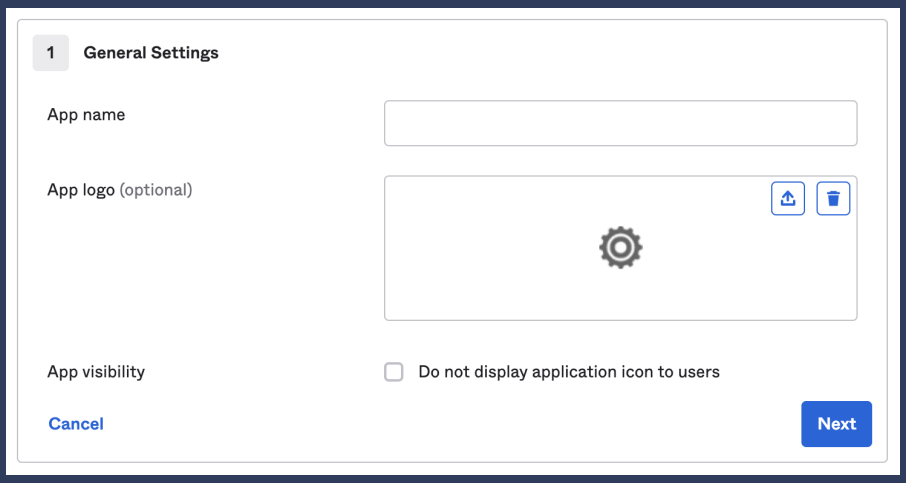
1. Login to the Okta admin portal, select **Applications** > **Applications** from the sidebar.



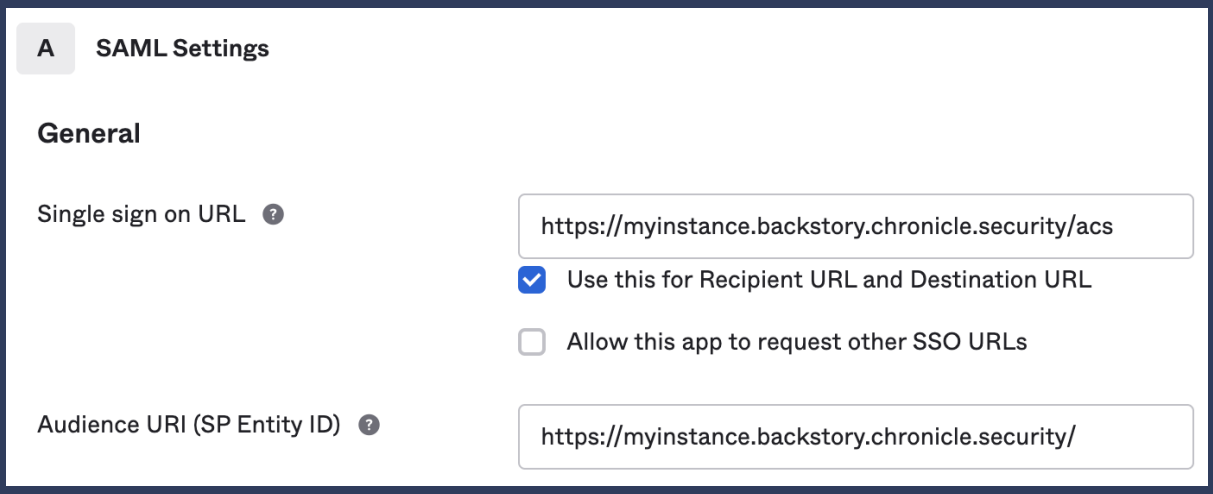
2. Click **Create App Integration**
3. Select **SAML 2.0** and click **Next**



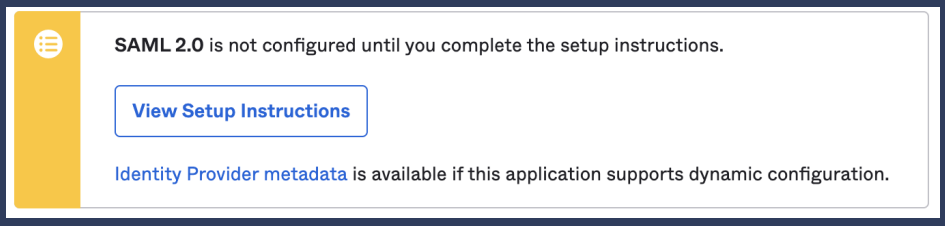
4. Complete the **App name**, add an icon if you like, and use the **App visibility** checkbox to show or hide the application as required. When done click **Next**.



5. On the **SAML Settings** page, under **Single sign on URL** enter the ACS callback URL provided by Google on setting up your instance, this will be in the format: *https://myinstance.backstory.chronicle.security/acs*, and under **Audience URI**, enter the URL for your instance in this format: *https://myinstance.backstory.chronicle.security/*. Click **Next**. On the final screen select either option and click **Finish**.



6. Now we can download the application metadata XML file by going to your application, selecting the **Sign On** tab, and clicking the **Identity Provider metadata** link, and saving the resultant page to your computer.



Integrating Okta groups with RBAC (Optional)

RBAC in Chronicle provides a number of possible roles, you can create Google groups for each of these roles, or just a subset. For the sake of this document, we are just going to use **Admin**, **Editor**, and **Viewer** groups and roles.

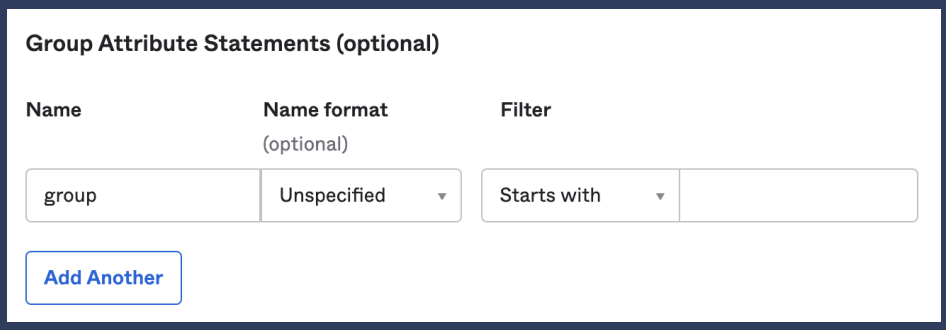
If the groups you wish to use for mapping don't already exist, then go to **Azure Active Directory** > **Groups** and create them.

Go to your Enterprise application, and click on the **Single sign-on** section. Click **Edit** under **Attributes & Claims**, click **Add a group claim**. Select **Security Groups**, leave **Source attribute** as **Group ID.** You can add a filter here if required, and ensure you check the **Customize the name of the group claim** and enter the name as **group**. Click **Save**.

If the groups you wish to use for mapping don't already exist, then go to **Directory** > **Groups** and create them.

Go to your SAML application, and click on the **General** tab. Click **Edit** under **SAML Settings**. Click **Next** and under **Group Attribute Statements (optional)** enter **group** under the Name field, leaving **Name format** as

Unspecified, and adding a **Filter** as needed (to minimise the number of group names sent). When done click **Next** and **Finish**.



Configuring Chronicle

After providing the metadata XML file generated earlier, you will be able to login to your Chronicle instance using your Google identity, via the URL provided by Google. You can now configure RBAC using either groups or users as follows:

1. Login to Chronicle
2. Click the menu icon in the top right corner of the UI

3. Select **Settings**, you will see your Profile appear. If you added group claims to your SAML application then you should see the passed groups here (if you did add group claims but don't see the groups listed then double check your SAML application configuration and raise a ticket with Chronicle support if you still cannot see the groups).
4. Click **Users & Groups** in the left hand menu, this will display any users or groups configured with explicit permissions in your system.
5. Follow the instructions here to add/remove users or groups and map them to the relevant permissions.
6. If you want to, and once you have completed the above steps, you can change the default permission through the dropdown in the top right hand corner of this window: