SAFEGUARD CYBER

OKTA CONFIGURATION GUIDE

CONFIGURE USER PROVISIONING WITH OKTA

Supported Features

- Create Users
- Update User Attributes
- Deactivate Users
- Group Push

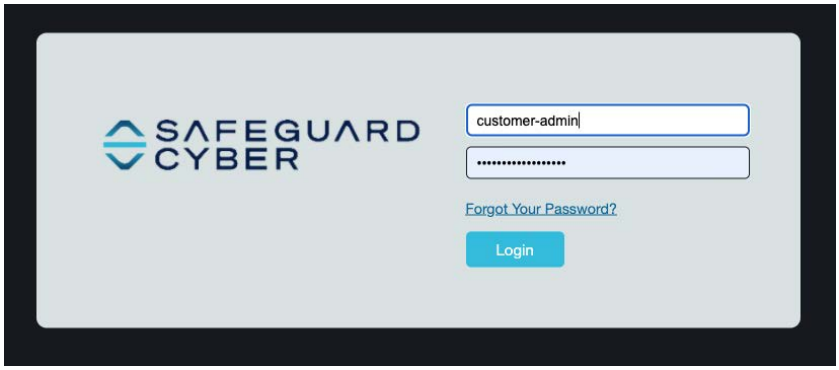
REQUIREMENTS

There are two things that are required in order to provision Authors into Safeguard Cyber:

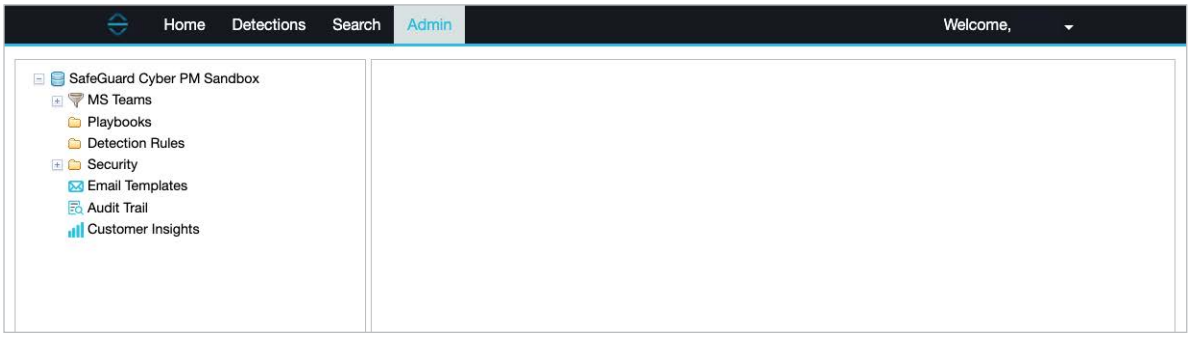
- You must have a SafeGuard Cyber account with Admin privileges
- You must have an Okta account with Administrator privileges

Step 1.
In SafeGuard Cyber, enable the Okta SCIM integration

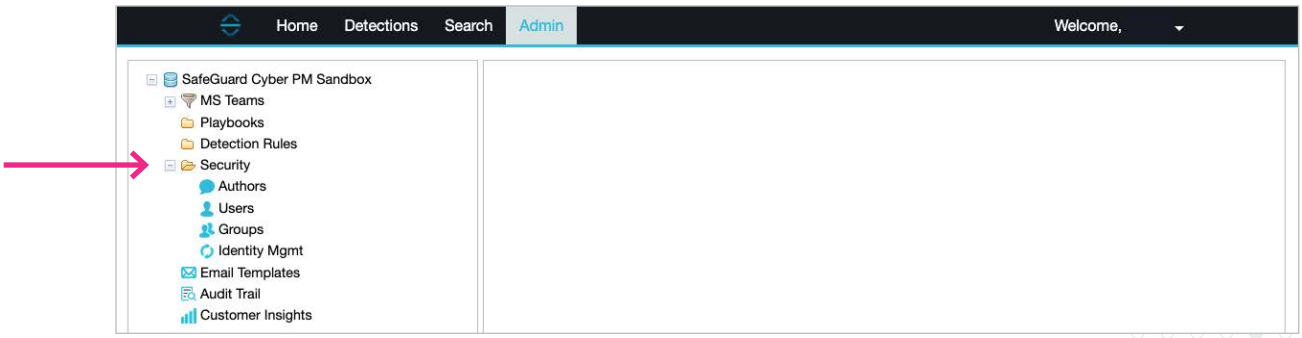
A. Log in to SafeGuard Cyber with Admin privileges



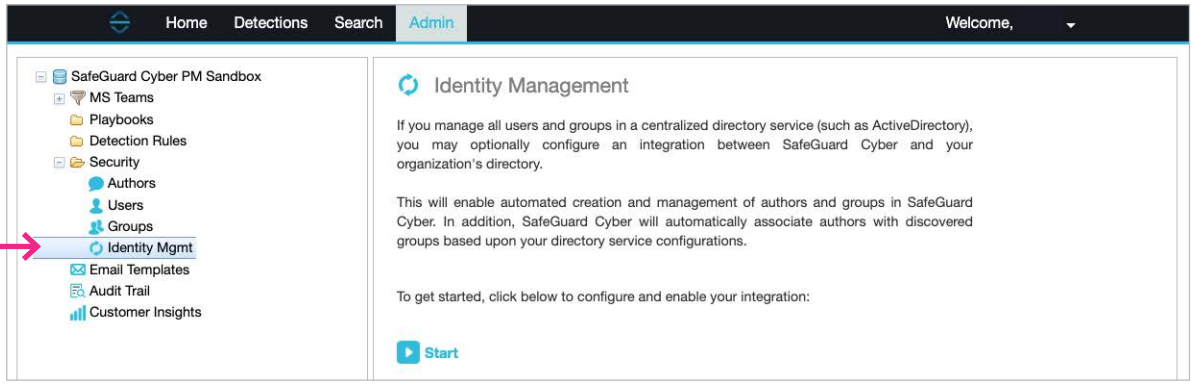
B. Navigate to the Admin tab



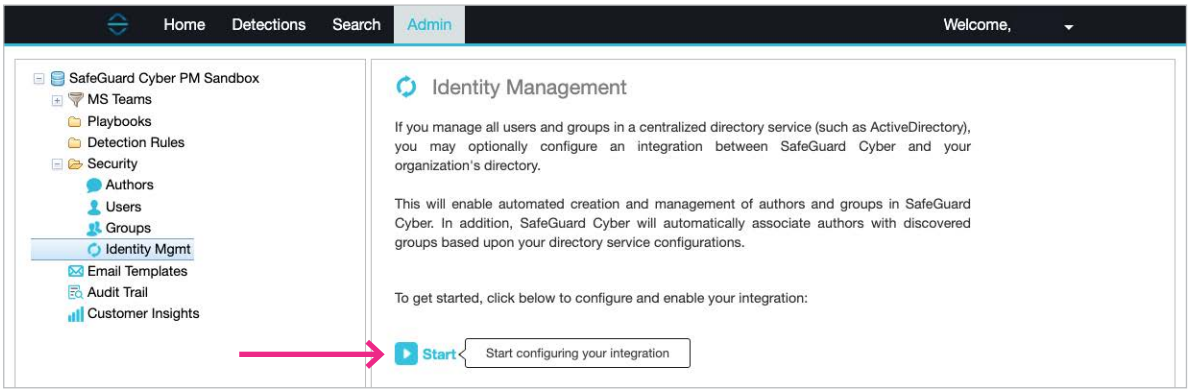
C. Click on the “Security” folder on the left-side navigation bar to expand the folder



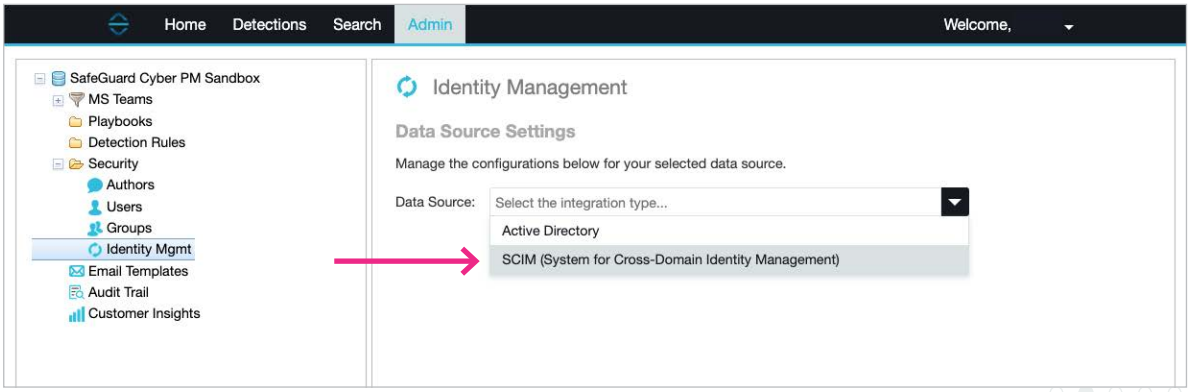
D. Click on “Identity Mgmt”



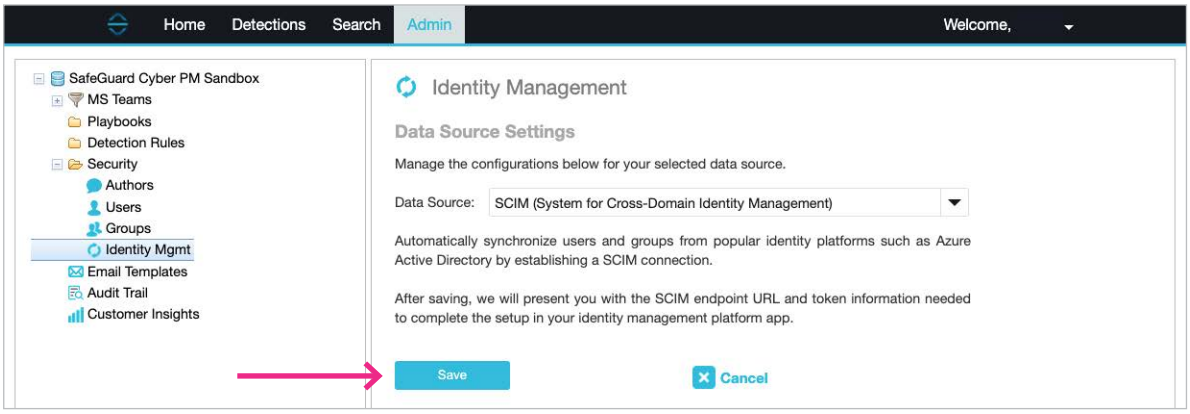
E. Click on the “Start” button to begin the configuration



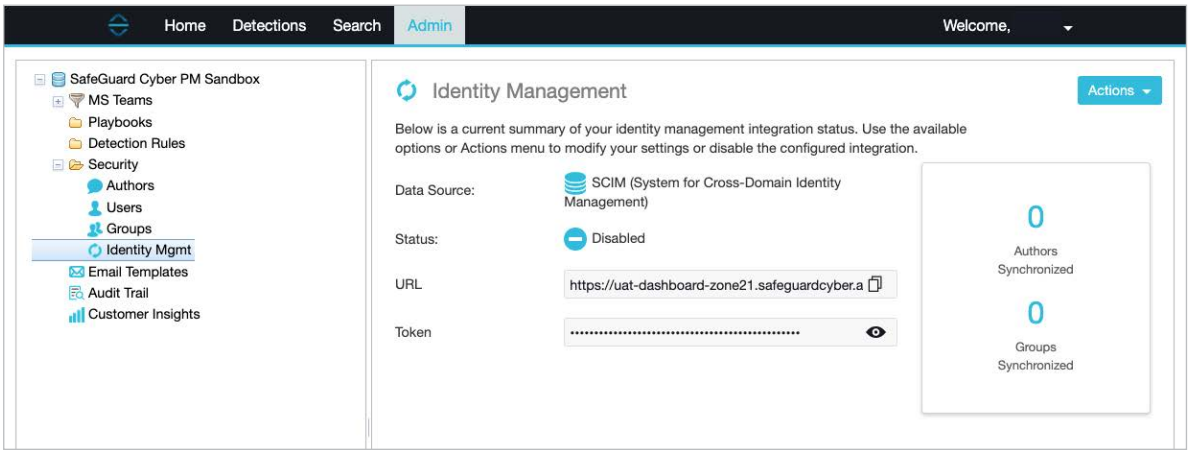
F. Select the “SCIM (System for Cross-Domain Identity Management)” option from the menu



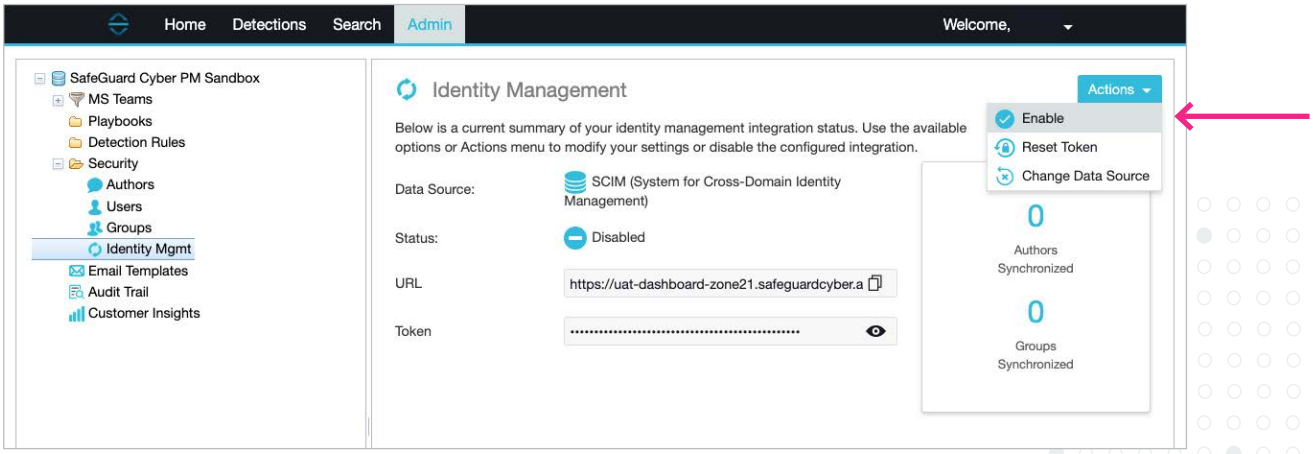
G. Save the configuration



H. Once the configuration is saved, you will be shown the SCIM URL and Token for your SafeGuard Cyber account. **NOTE:** This information will be used in Step 3-A when configuring provisioning for the SafeGuard Cyber app integration within Okta.



I. Click on the “Action” drop-down and select “Enable”. This is REQUIRED for the Okta SCIM integration to function.



Step 2.
In Okta, Create a Group Admin account, and Assign Groups

A. Sign in to Okta as an Administrator. Add a new user that will be the Group Administrator for Groups you wish to sync into SafeGuard Cyber.

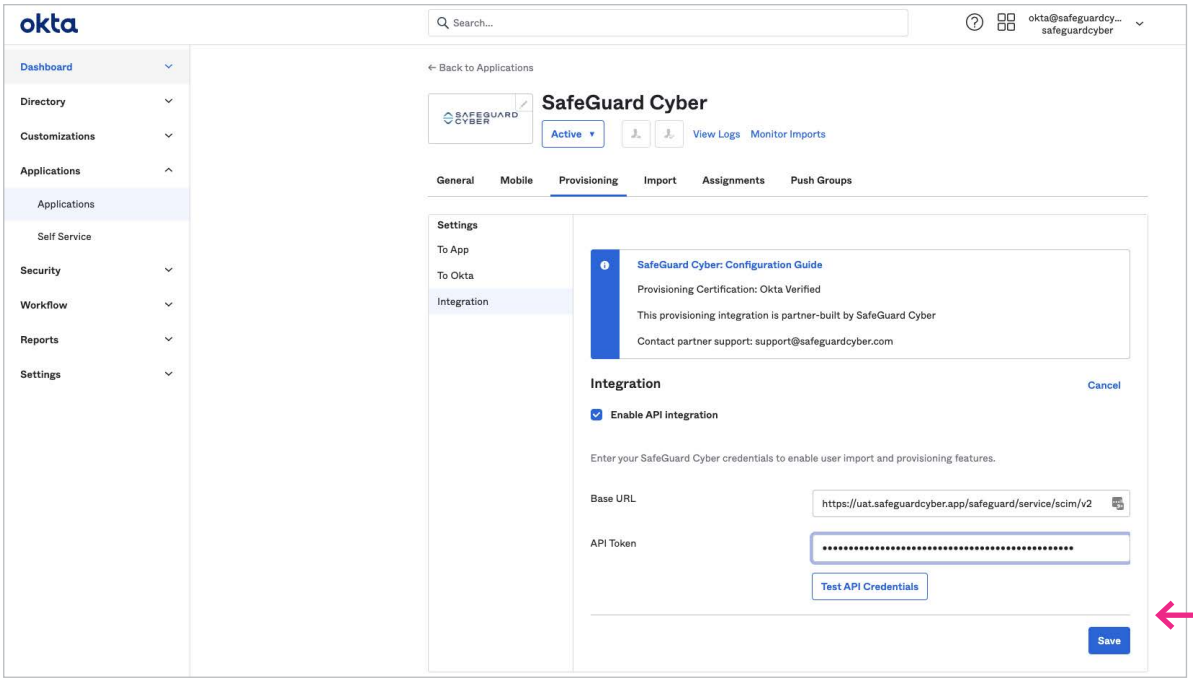
B. Create one or more Groups that will contain users you wish to sync into SafeGuard Cyber. These users will be synced into SafeGuard Cyber as Authors.

C. Assign the "Group Administrator" role to the user you created in Step 2-A. Within Group Admin Permissions, select "Can administer users in specific groups" and assign the group(s) created in Step 2-B.

Step 3.
In Okta, configure provisioning for the SafeGuard Cyber app integration

A. Sign in to Okta as an Administrator, and follow instructions for configuring provisioning for an app integration.

1. The app integration is called "SafeGuard Cyber," which you can find by searching within "Browse App Catalog."
2. Within the "SafeGuard Cyber" app integration, navigate to the "Provisioning" Tab.
3. Click on "Configure API Integration" and select "Enable API Integration."
4. Using the values from Step 1-H, above, enter the SafeGuard Cyber "URL" as the Okta "Base URL" and the SafeGuard Cyber "Token" as the Okta "API Token".

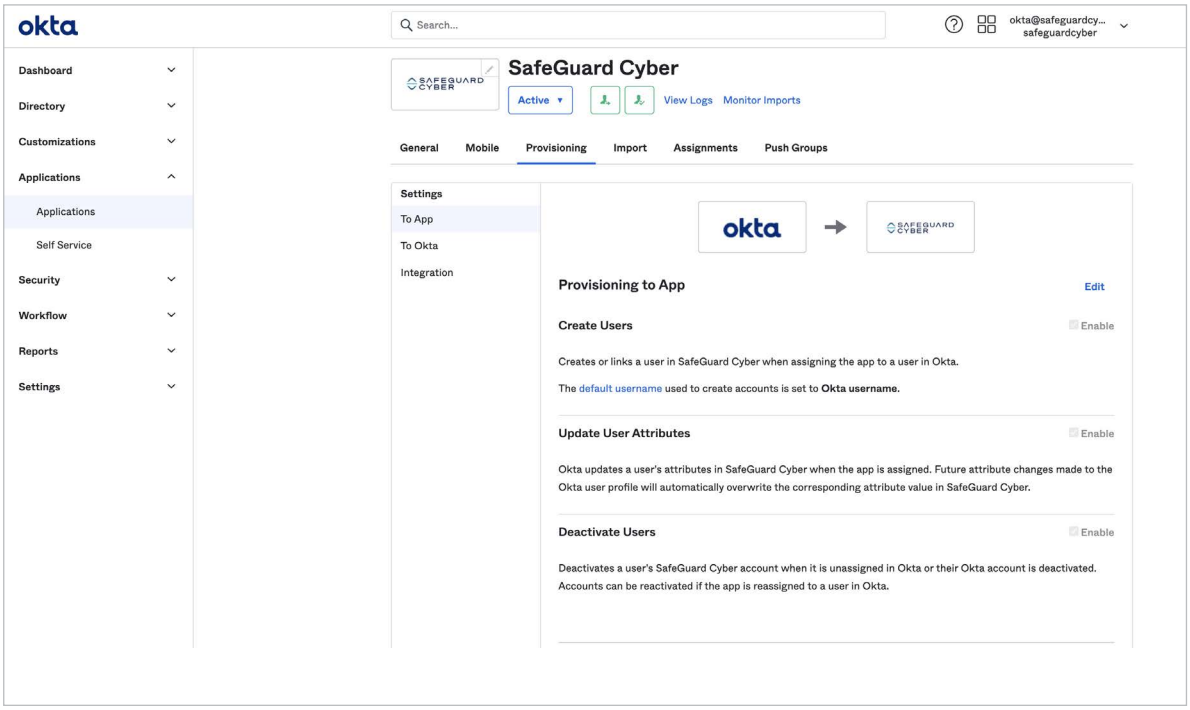


B. Click “Test API Credentials” to test your API credentials. If you receive an error, verify and retry your credentials.

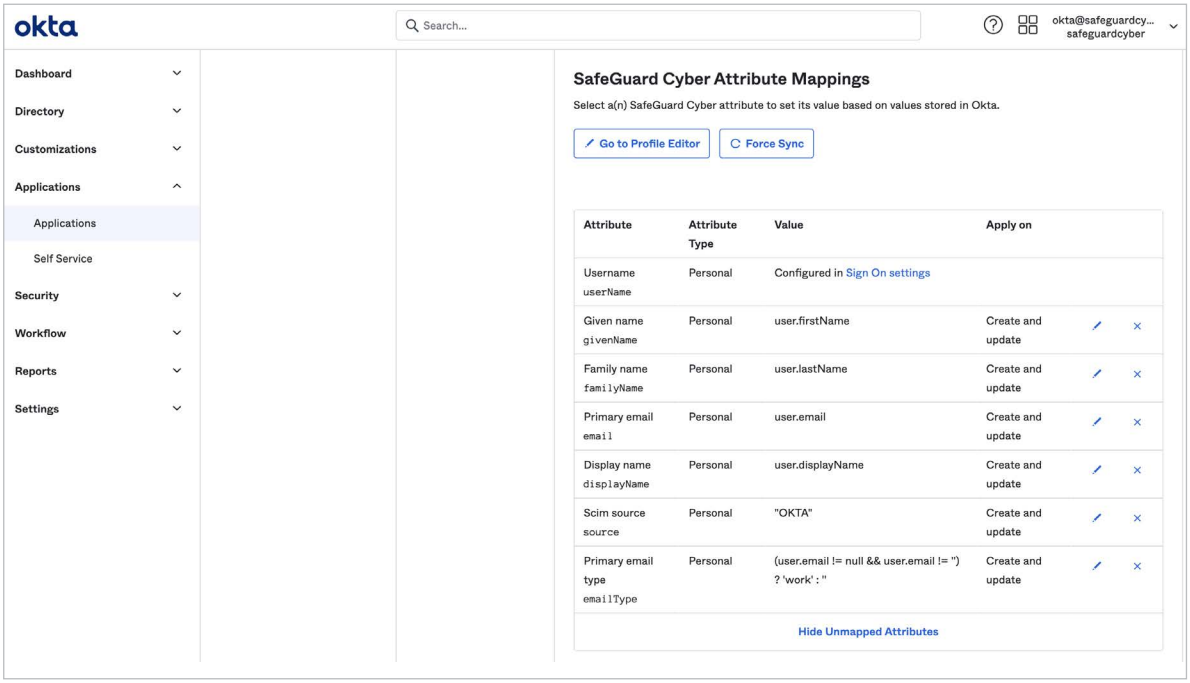
C. Click “Save”.

D. Within “Settings”, click “To App”, and then “Edit” to select the provisioning options you’d like to enable.

   1. SafeGuard Cyber recommends that you enable Create Users, Update User Attributes, and Deactivate Users.



2. In Attribute Mappings at the bottom of the “To App” page, configure the following mappings:

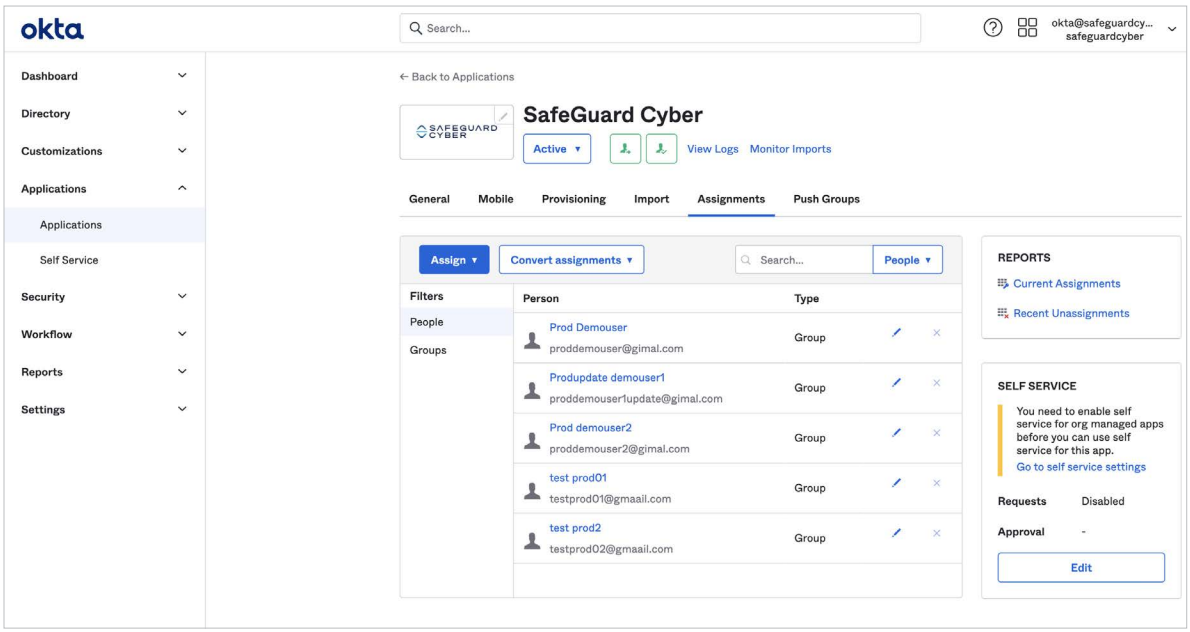


ATTRIBUTE MAPPINGS			
Attribute	**Attribute Type**	**Value**	**Apply on**
UserName userName	Personal	Configured in Sign On Settings	
Given name givenName	Personal	user.firstName	Create and update
Family name familyName	Personal	user.lastName	Create and update
Primary email email	Personal	user.email	Create and update
Primary email type emailType	Personal	user.email != null && user.email != ‘’) ? ‘work’ : ‘’	Create and update
Display name displayName	Personal	user.displayName	Create and update
Scim source source	Personal	“OKTA”	Create and Update

Note: User provisioning uses an email address to identify a user in the SafeGuard Cyber app and then create a new SafeGuard Cyber Author account or link to an existing SafeGuard Cyber Author account.

Step 4.
In Okta, assign Users to the SafeGuard Cyber app

A. In Okta, click the “Assignments” tab of the SafeGuard Cyber app integration, as shown below:



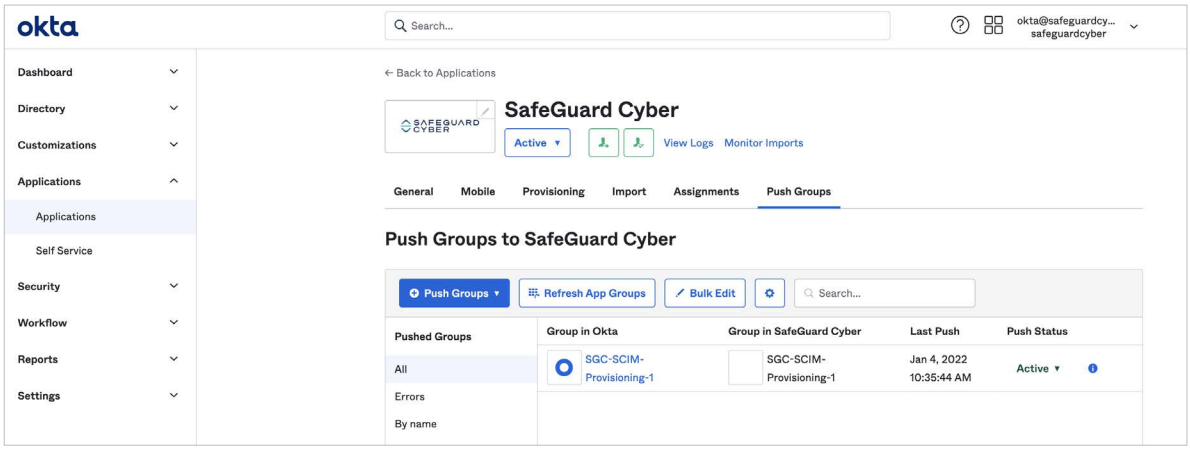
B. Click “Assign,” then “Groups.” Select the Group(s) you’d like to assign.

Step 5.
Push groups to SafeGuard Cyber

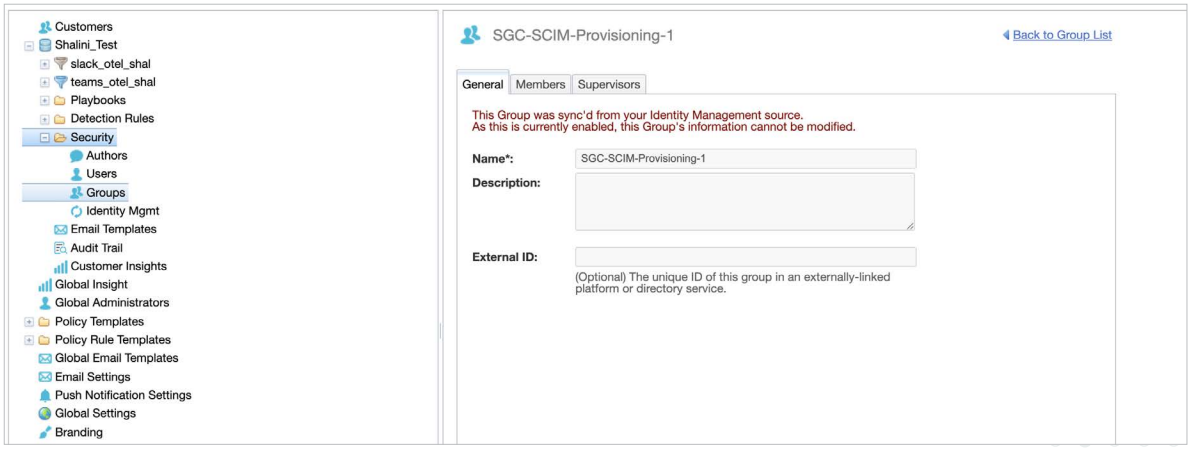
SafeGuard Cyber recommends using the group synchronization feature to automatically manage user synchronization, instead of manually managing them. This section describes how to configure group-based management.

A. In Okta, click the “Push Groups” tab and then click the “Push Groups” menu. Within the “Push Groups” menu, select “Find groups by name”. Type to find the Group you created in Step 2-B, select this Group, and then click “Save.”

B. Review to make sure all desired groups have been pushed (Push Status should show as “Active”). See screenshot, below:



C. Within SafeGuard Cyber, you should see a Group that was created by an external source. See screenshot, below:



TROUBLESHOOTING AND TIPS

- SafeGuard Cyber recommends that you do not assign individual Okta users to the SafeGuard Cyber app integration, as this prevents several useful features within SafeGuard Cyber from functioning for those users (e.g. reporting, group-based policy enforcement, and group-based reviewer assignment). Instead, we recommend that you assign Okta users to Groups, and then add these Groups as Push Groups within the SafeGuard Cyber app integration.
- Safeguard Cyber does not support changes to the username or email address of users directly assigned to the SafeGuard Cyber app integration in Okta. However, the username and email address for users can be updated from the Directory in Okta.
- If an Okta Group assigned as a Push Group within the SafeGuard Cyber app integration is Unlinked, re-linking the Group with the "Link Group" functionality in Okta can create unexpected behavior. Instead, SafeGuard Cyber recommends you remove the Group from Push Groups, and then re-add it.
- If a user is removed from a Group within Okta, but this change is not reflected within SafeGuard Cyber, manually re-pushing Groups within Okta should result in correct Group Memberships within SafeGuard Cyber.
- The SafeGuard Cyber API call to GET User details (/Users) will return an extra emailType attribute "username". This is due to our internal handling of user information, and is expected behavior.

Contact support@safeguardcyber.com
if you have any questions or issues.

SAFEGUARD CYBER

SafeGuard Cyber protects the human connections organizations need to thrive in a digital world. The cloud-based SafeGuard platform empowers the secure and compliant adoption of social, mobile, and cloud-based communication channels at the scale of global business. Built on innovative agentless architecture and award-winning risk analytics, the SafeGuard platform secures business critical communications, detects and stops cyber threats, and ensures compliance in real-time without disruption to natural workflows.

410A East Main Street, Charlottesville VA 22902 | 1-800-974-3515 | www.safeguardcyber.com