

SSO setup OKTA - SCIM integrations

This document is a step-by-step guide to setting up a System for Cross-domain Identity Management (SCIM) integration using Okta and will allow users to fully migrate to using Okta as their identity provider for Vault Platform.



Please note that when connected to an Identity Provider (IDP) you will only be able to control users' access to the resolution hub. All user details and app access will be managed through the IDP.

On this page:

[Features](#)

[Requirements](#)

[Step-by-Step Configuration Instructions:](#)

[In Vault Platform](#)

[In OKTA](#)

[Troubleshooting and Tips](#)

[Need Help?](#)

Features

Vault Platform integration with Okta currently supports the following features.

- Create Users
- Update Users Attributes
- Deactivate Users

We currently don't support the following features:

- Import Users to Okta from Vault Platform
- Create/Update/Deactivate Groups
- Import Groups
- Sync Password

Requirements

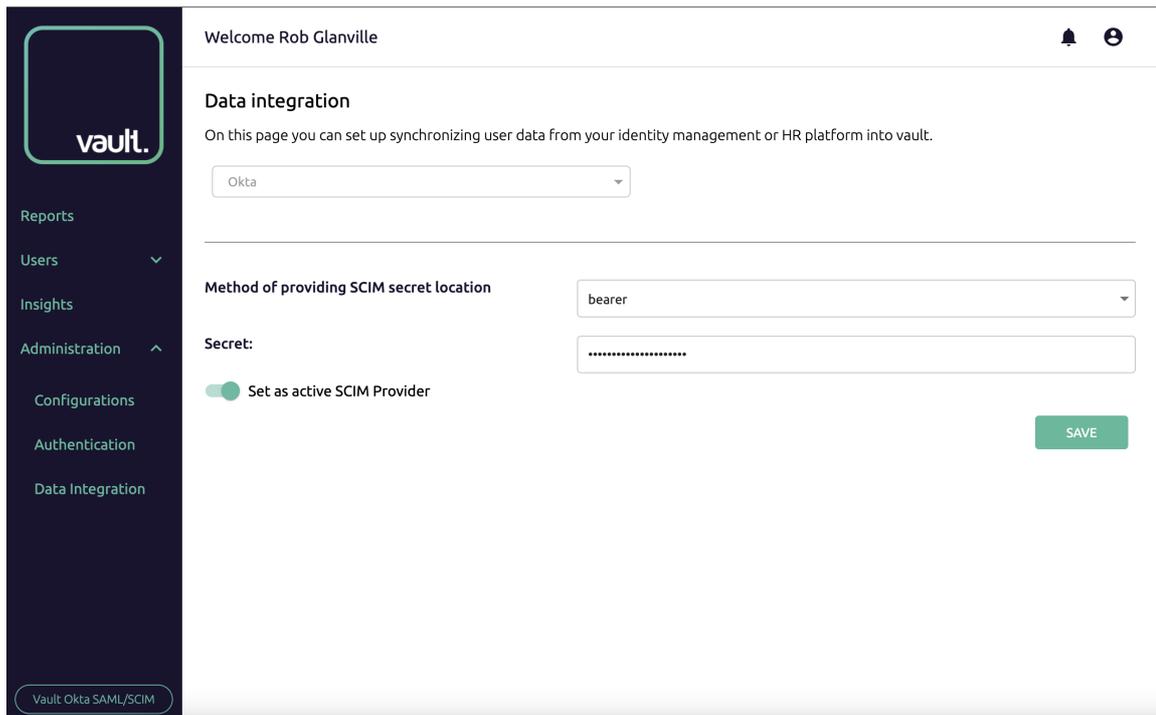
Prerequisites for setting up provisioning for Vault Platform include the following.

- You must have a slug set up with Vault Platform that is used for SSO and SCIM integrations, if you do not have this please contact: support@vaultplatform.com
- You must have data integrations enabled with Vault Platform. If you do not or need to find out if you already have these features enabled please contact: support@vaultplatform.com.

Step-by-Step Configuration Instructions:

In Vault Platform

1. Login to the Resolution Hub at <https://app.vaultplatform.com/login>
2. Navigate to the Data Integrations Tab. Please note you are required to have admin or super admin permissions to view this tab. If you still cannot see the data integrations tab please contact support@vaultplatform.com to enable this feature.
3. Please generate and store a secret password which will be used to validate the SCIM connection. Please ensure this is a hard to guess secret. You can use <https://passwordsgenerator.net/> to create a random password. We suggest 16 or more characters. Please keep a note of this password for later when you need to enter it into the OKTA Integrations page.
4. Set the SCIM secret location to barer, paste the saved secret that generated into the text box, and check that the *Set as active SCIM Provider* is toggled on.



5. Click the save button to save the provisioning settings.

In OKTA

1. Log in to your Okta Admin panel. You must have permission to access that admin panel to add the Vault Platform app to your list of applications.
2. Click on the Provisioning tab, and select integration where you can set up your SCIM integration.

The screenshot shows the Vault Platform configuration page for Okta integration. The page is titled "Vault Platform" and has a navigation bar with tabs: General, Sign On, Mobile, Provisioning (selected), Import, Assignments, and Okta API Scopes. Below the navigation bar, there is a "Settings" sidebar with "Integration" selected. The main content area displays a configuration card for Okta integration. The card includes a link to the configuration guide, a provisioning certification status of "Okta Verified", and contact information for partner support. Below the card, there is a checkbox labeled "Enable API integration" which is checked. Underneath, there is a text input field for the "API Token" and a "Test API Credentials" button. A "Save" button is located at the bottom right of the configuration area.

3. Click Configure API Integration and the click enable API integration.
4. You should enter a secret API Token here in the format of a bearer token. You generated earlier and used in the Vault Platform application.
5. Click Test API Credentials. You should see a Success message: `Vault Platform was verified successfully!`
6. Click save to save the API credentials.
7. You will need to update a profile for mapping OKTA user to SCIM. Please click on GPlease navigate in OKTA to your Directory → Profile editor and click on Mappings next to the Vault Platform app.

The screenshot shows the Okta Profile Editor interface. On the left is a navigation sidebar with categories like Dashboard, Directory, Profile Editor, and Settings. The main content area is titled 'Profile Editor' and includes a 'Learn about Universal Directory' section. Below this, there are tabs for 'Users' and 'Groups', with 'Users' selected. A 'Users' table is displayed with columns for Filters, Profile, and Type. The table lists several user profiles, including 'User (default)', 'Developer Registration SSO User', and 'Vault Platform (SAML & SCIM) User'. A 'Mappings' link is visible for each profile.

Filters	Profile	Type
All	User (default) user	Okta
Okta	Developer Registration SSO User oidc_idp	Identity Provider Mappings
Apps	Rob Vault Provisioning User dev59529444_robvaultprovisioning_1	Application Mappings
Directories	Vault Platform (SAML & SCIM) User dev59529444_vaultplatformsamiscim_1	Application Mappings
Identity Providers	Vault Platform User vaultplatform	Application Mappings

- You must now ensure you have the correct mapping for your application from OKTA to Vault platform. Click on the To App tab and ensure you have mappings for the following parameters:

Display Name	Variable Name	Data type	Attribute Type		
Username	userName	string	Base		
Given name	givenName	string	Custom		
Family name	familyName	string	Custom		
Primary email	email	string	Custom		
Primary email type	emailType	string	Custom		
Title	title	string	Custom		
Display name	displayName	string	Custom		
Address type	addressType	string	Custom		
Street address	streetAddress	string	Custom		
Locality	locality	string	Custom		
Country code	country	string	Custom		
Employee number	employeeNumber	string	Custom		
Department	department	string	Custom		

9. Ensure you have the following mappings enabled for OKTA to app:
Please note: All attributes must be filled in as they are required by Vault Platform.

Vault Platform (SAML & SCIM) User Profile Mappings ✕

Vault Platform (SAML & SCIM) to... **Okta User to Vault Platform (S...**

Okta User User Profile user	Vault Platform (SAML & SCIM) User Profile appuser
Username is set by Vault Platform (SAML & SCIM)	
user.firstName	userName string
user.lastName	givenName string
user.email	familyName string
(user.email != null && user.email != '') ? 'work' :	email email
user.title	emailType email
user.displayName	title string
(user.streetAddress != null && user.streetAddress !=	displayName string
user.streetAddress	addressType string
user.city	streetAddress string
user.countryCode	locality string
user.employeeNumber	country country code
user.department	employeeNumber string
	department string

Enter an Okta user to preview their mappi

- With all of these set you should be complete and you should be able to use provisioning.
- Go to your Assignments tab to add people and groups to be provisioned to your vault platform application.

Troubleshooting and Tips

Please ensure you have the correct authentication methods set and ensure the bearer token you used is the same in the OKTA app as it is on Vault Platform Resolution Hub.

Please ensure you have correctly set up the mapping from OKTA to Vault Platform. Any users which do not have all the required fields will not be added to Vault Platform.

Please ensure you have added users and groups to the app under the assignments tab.

Please check under the assignments tab that there are no errors (red icons) next to user assignments. These errors will look like the following:

General Sign On Mobile Provisioning Import **Assignments**

Assign ▾ **Convert assignments** ▾ Search... **People** ▾

Filters	Person	Type
People	 Rob Glanville rob+oktascim@vaultplatform.com	Individual  
Groups	 Runscope102update Rblycmky346 runscope102rblycmky346@atko.com	Individual  
	  Runscope372update Obnbqfws711 runscope372obnbqfws711@atko.com	Individual  

We currently don't support updating information from Vault Platform to OKTA and we don't yet support groups. If you are trying to provision groups you will get errors.

The features we don't yet support are:

- Import Users to Okta from Vault Platform
- Create/Update/Deactivate Groups
- Import Groups

- Sync Password

Provisioning users will only give them access to the Vault Platform App on iOS/Android. Permissions to access the Resolution Hub (ResHub) must be granted within the ResHub by a manager, admin or super admin. These users will then use SSO to authenticate and log in to the ResHub.



Note: When users are deactivated in Okta, they will be deactivated in Vault Platform. Users will not be able to login to the application, but their data will remain available as an 'inactive user'. To permanently delete user data, contact Vault Platform Support, (support@vaultplatform.com).

Need Help?

If you have problems or issues with Vault Platform and Okta, contact the Vault team techsupport@vaultplatform.com and we'll work with you on it.

Disclaimer

This integration with Okta is currently under development and is not available to customers yet. Please contact to learn more.