GRONIVA

Okta SSO Configuration Guide

OpenID Connect (OIDC) Integration · Version 1.0

Protocol: OpenID Connect (OIDC)	**Application:** Groniva
Grant Type: Authorization Code	**Support:** shriram@groniva.com

Overview

This guide explains how to configure Single Sign-On (SSO) between Okta and Groniva using OpenID Connect (OIDC). Once configured, your users will be able to log in to Groniva using their existing Okta credentials — no separate password required.

Who is this guide for?
This guide is intended for IT Administrators who manage their organization's Okta tenant and wish to enable SSO access to Groniva for their users.

Supported Features

- **SP-Initiated SSO:** Supported

SP-Initiated SSO
Groniva supports SP-Initiated SSO only. The login flow must always start from the Groniva login page — users click "Sign in with Okta", are redirected to Okta to authenticate, and returned to Groniva automatically upon success.

Prerequisites

Before you begin, ensure the following are available:

✓	An active Okta administrator account with permission to manage applications.
✓	Access to the Groniva Administrator Dashboard.
✓	**Groniva application base URL** (e.g., `https://gcpl.groniva.com`)

1 Add Groniva in Okta and Obtain Client Credentials

1. Log in to your Okta Administrator Dashboard.
2. Go to **Applications > Applications**, then click **Browse App Catalog**.
3. Search for **Groniva** and click **Add Integration**.
4. Review the **General Settings** and click **Done**.
5. Navigate to the **Sign On** tab of the newly created Groniva application in Okta.
6. Scroll down to the **OpenID Connect ID Token** section. Here you will find your **Client ID** and **Client Secret**. Keep this page open or copy these values securely — you will need them in Step 2.
7. Take note of your **Okta Domain** (e.g., `https://yourcompany.okta.com`). You will use this as your Issuer URL.

Security Tip
Treat your Client Secret like a password. Never share it publicly, commit it to version control, or expose it in client-side code. Store it securely in a secrets vault or environment variable.

2 Configure OIDC Settings in Groniva

8. Open a new browser tab and log in to your **Groniva Administrator Dashboard**.
9. Navigate to **Search Menu** › search for **SSO Configuration** › open **SSO Configuration**.
10. Select **Okta** as your Identity Provider.
11. Fill in the following fields using the values collected from Okta in Step 1:
    a. **Client ID:** Paste the Client ID from Okta.
    b. **Client Secret:** Paste the Client Secret from Okta.
    c. **Okta Domain / Issuer URL:** Enter your Okta domain (e.g., `yourcompany.okta.com`).
12. Click **Save Configuration** in Groniva.

What happens next?
Once saved, Groniva will use these credentials to communicate with Okta during every login. Users will be redirected to Okta to authenticate and returned to Groniva automatically upon success.

3 Assign Users to Groniva in Okta

13. In Okta, go to the **Assignments** tab of the Groniva integration.
14. Click **Assign** and choose one of:
- **Assign to People** — to grant access to individual users.
- **Assign to Groups** — recommended for organizations with many users.
15. Select the users or groups you want to grant access to Groniva.
16. Click **Assign**, then click **Save and Go Back**.
17. Click **Done**.

Tip
Assigning by Group is recommended for production environments. Any new employee added to the group will automatically gain access to Groniva without additional configuration.

4 Test the Integration

SP-Initiated SSO Test

Navigate to your Groniva login page (e.g., `https://[your-subdomain].groniva.com`) and click the **Sign in with Okta** (or SSO) button.

1	You are redirected to the **Okta login page**.
2	Enter your Okta credentials and complete authentication (including MFA if enabled).
3	You are redirected back to **Groniva** and logged in successfully.
4	Verify that your **name, email, and role** are populated correctly from Okta.

Success!
If you are redirected back to Groniva and see your dashboard, the SSO integration is working correctly. You can now communicate the SSO login URL to your end users.

Troubleshooting

If you encounter issues during setup or testing, refer to the table below:

Error / Issue	Solution
`"Invalid Client"` or `"Unauthorized Client"`	Double-check that the **Client ID** and **Client Secret** pasted into Groniva exactly match the values in Okta, with no extra spaces or characters.
User not redirected to Okta	Ensure SSO is enabled in Groniva's SSO Configuration and that the **Issuer URL** matches your Okta domain exactly.
User assigned but cannot access	Verify the user is assigned in the **Assignments** tab of the Groniva app in Okta (Step 3).
Redirect URI mismatch error	Contact Groniva support — this may indicate a configuration issue on the integration side.

✉ **Need more help?**
Contact the Groniva support team at **shriram@groniva.com** and include your Okta domain and a description of the issue.

