Google SAML SSO Configuration for SSD (Spinnaker Software Delivery)

1. Purpose

This document provides a **step-by-step technical guide** to configure **Google SAML Single Sign-On (SSO)** for an **SSD instance**. It covers Google-side prerequisites, Kubernetes configuration, SSD Gate changes, and post-configuration validation.

---

2. Prerequisites

2.1 Google Workspace

- Google Workspace (Admin) access
- Ability to create and manage **SAML applications**
- User email IDs must exist in Google Workspace
- Relevant Google Groups (example: `ssd-sandbox-admin`)

2.2 SSD Environment

- SSD deployed on Kubernetes
- Access to the SSD namespace
- `kubectl` access with permissions to:
- Create secrets
- Edit ConfigMaps
- Update deployments
- Restart pods

---

3. Google SAML Application Setup (High-Level)

1. Log in to **Google Admin Console**
2. Navigate to:
3. **Apps → Web and mobile apps → Add App → Add custom SAML app**
4. Configure the application using SSD SAML values (Entity ID, ACS URL)
5. Download the **IdP Metadata XML** file
6. Default filename: `GoogleIDPMetadata.xml`

   This metadata file is required for SSD Gate configuration.

---

4. Create Kubernetes Secret for SAML Metadata

4.1 Rename Metadata File

Rename the downloaded file:

```
GoogleIDPMetadata.xml → metadata.xml
```

4.2 Create Secret

Create a Kubernetes secret named `saml-files` in the SSD namespace:

```
kubectl create secret generic saml-files
  --from-file=metadata.xml
  -n <NAMESPACE>
```

5. Update SSD Gate ConfigMap

5.1 Edit ConfigMap

Edit the `ssd-gate-config` ConfigMap:

```
kubectl edit configmap ssd-gate-config -n <NAMESPACE>
```

5.2 Add Metadata Configuration

Add the following entry under SAML configuration:

```
metadata_File: /app/saml/metadata.xml
```

Save and exit.

6. Update SSD Gate Deployment

6.1 Edit Deployment

```
kubectl edit deploy ssd-gate -n <NAMESPACE>
```

6.2 Add Volume Mount

Add the following under `volumeMounts` :

```
- mountPath: /app/saml
  name: saml-files
```

6.3 Add Volume Definition

Add the following under `volumes` :

```
- name: saml-files
  secret:
    secretName: saml-files
    optional: true
    defaultMode: 420
    items:
      - key: metadata.xml
        path: metadata.xml
```

Save the deployment.

---

7. Restart SSD Gate Pod

Restart the Gate deployment to apply changes:

```
kubectl rollout restart deploy ssd-gate -n <NAMESPACE>
```

Wait until the pod is fully running.

---

8. Configure Organisation & Role Mapping (Mandatory)

When using **Basic Authentication + SAML**, group names differ (example: `admin` vs `ssd-sandbox-admin`).

Without this mapping, users may encounter: - **Organisation not found** - **Team details not found**

8.1 SupplyChain API Call

URL:

```
http://localhost:8099/ssdservice/v1/setup
```

Method: POST

Payload:

```
{
  "organisationName": "opsmx",
  "organisationRoles": [
    {
      "group": "ssd-sandbox-admin",
      "permission": "admin"
    }
  ]
}
```

Use Postman or curl (via port-forward if required).

---

9. Restart Gate Service (Recommended)

After role mapping, restart the Gate service once more:

```
kubectl rollout restart deploy ssd-gate -n <NAMESPACE>
```

---

10. Validation

1. Access the SSD UI URL
2. Select **Login with Google / SAML**
3. Authenticate using an **OpsMx Google Workspace email ID**
4. Verify:
5. Successful login
6. Organisation and teams are visible
7. Data is accessible

---

11. Post-Login Access Management

If users need additional permissions:

1. Navigate to:
2. **Setup → Access Management**
3. Assign appropriate roles to:
4. Users
5. Teams
6. Groups

---

12. Common Issues & Troubleshooting

Issue	Possible Cause	Resolution
Login successful but no data	Org-role mapping missing	Run setup API call
SAML error on login	Metadata not mounted	Verify secret & volume mount
Gate pod crash	Incorrect config path	Recheck `metadata_File` value

---

13. Summary

- Google SAML metadata must be mounted as a Kubernetes secret
- SSD Gate requires explicit metadata file configuration
- Organisation-role mapping is mandatory for SAML users
- Gate restart is required after every configuration change

Document Version: 1.0
Applies To: SSD with Google SAML SSO