Directory Sync Okta support
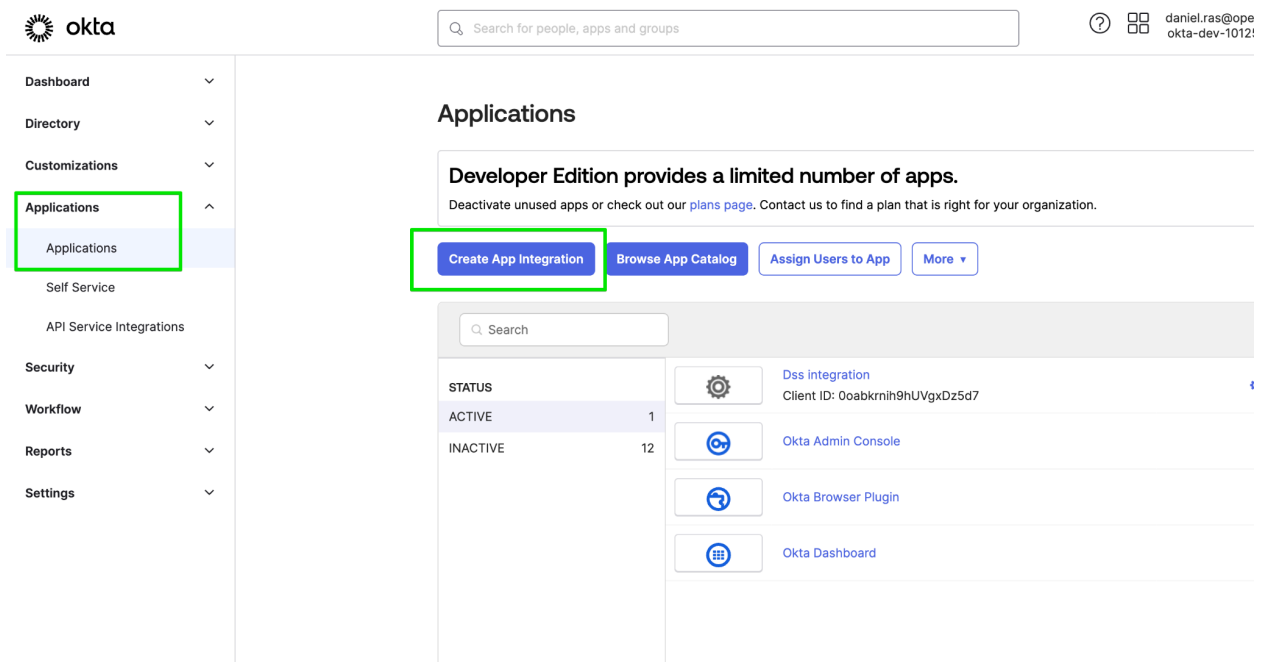
This document outlines the configuration process for integrating Directory Sync with Okta.

Okta portal configuration

Create an API app

1. Log in to your Okta account and navigate to **Applications** → **Create App Integration**.

2. Select **API Services** and choose a name for your app.

⊞ New API Services App Integration

General Settings

App integration name

My API Services App 1

Save   Cancel

3. To enable integration with Directory Sync, go to **Edit** and activate **Public/Private Key Authentication**

← Back to Applications

⚙️

DSS TEST 2

Active ▾   🔒   View Logs

General   Okta API Scopes   Application Rate Limits

Client Credentials   Edit

Client ID

0oactok8tsq8ZBkRz5d7   📋

Public identifier for the client that is required for all OAuth flows.

Client authentication

🔵 Client secret

⚪ Public key / Private key

CLIENT SECRETS

Client Credentials

Cancel

Client ID	0oactok8tsq8ZBkRz5d7

Public identifier for the client that is required for all OAuth flows.

Client authentication
- ○ Client secret
- ● Public key / Private key

PUBLIC KEYS

Configuration
- ● Save keys in Okta
- ○ Use a URL to fetch keys dynamically

KID	Status	Created

No public keys are configured. Click **Add key** to get started.

Add key

Save Cancel

Add a public key

Paste your own public key or automatically generate a new key pair.

Clear   Generate new key

Done Cancel

---

4. Copy the generated private key and store it securely for future reference.

Add a public key

Paste your own public key or automatically generate a new key pair.

Clear   Generate new key

{
    "kty": "RSA",
    "e": "AQAB",
    "kid": "WVhoMHh79OPEghItAypuXEa_j_m10DAzqhuWgE7bWi4",
    "n": "ng5-9jDcCeBYLvrO2DjAeeIYLL7Z99q-awI2wr9sHVkYDLGoLwkJrKeJP62425ZT4isv_7hbSiYaN9ZZxEZY_Iy9
}

Private key - Copy this!

The private key appears only once for enhanced security. Copy this key and store it somewhere safe for use later.

JSON   PEM   Copy to clipboard

{
    "d": "I25d9SveQ6OEOSHVqQBN23S81RkCbS6exYe1RWJaZtjQTJYtvL-CqO7UlE8J88Wm77odNC68Xiqc8XvuWxKnA5QB
    "p": "y3g5oQOFOwzAWB_1wW4ykIL-t09yYo-d--at-XWhRuT9efNUzXWRAwQVD5ud7Hs5SoIgx4m0qQibq-dZRjDgyX1K
    "q": "xtzSNDn3Ho5o5-wemMLdBdXnpwEdtACHReTH2pHj2DgNaF3kwSS5Kp0L4Hh8amVj3HCD9wRsmMVNHMU3sB6e436r
    "dp": "FCvCAs1XiugTtWjNszRafOsP11qf61dzgQJ4Ys-fgmi3HDzcPlYWXycrc1WpDUWWA2XtG_rx1wQMcrlHp2a3Eil
    "dq": "bgmypwOMInRayDp3k7__3ULHtDmB3iCMubgmfmNL2FDr2lxaQCW58EKGV-dTsOv5nfkEjKL-FGrYiJr4fZP0B54
    "qi": "vix-hRZsiPNRJBGKVT0zV_w5K2rhFqPikOCXellmMze_j-cjwomwMGTbU0_XkVD_iF2fYKv1f-9iUSK6BTYfVy_
    "kty": "RSA",
    "e": "AQAB",
    "kid": "WVhoMHh79OPEghItAypuXEa_j_m10DAzqhuWgE7bWi4",
    "n": "ng5-9jDcCeBYLvrO2DjAeeIYLL7Z99q-awI2wr9sHVkYDLGoLwkJrKeJP62425ZT4isv_7hbSiYaN9ZZxEZY_Iy9
}

Done   Cancel

5. Grant the following permissions:
   Okta.users.read
   Okta.groups.read

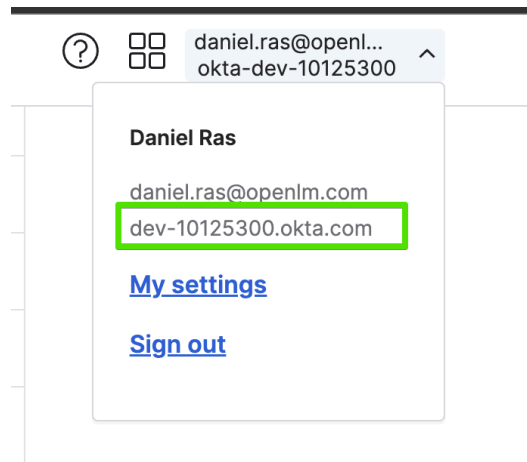← Back to Applications

DSS TEST 2

Active ▾   🔒   View Logs

General   **Okta API Scopes**   Application Rate Limits

Consent	Scope	Consent	Actions
Any			
Granted	okta.agentPools.manage❓	Not granted	✓ Grant
Not Granted	okta.agentPools.read❓	Not granted	✓ Grant
	okta.apiTokens.manage❓	Not granted	✓ Grant

OpenID Connect clients can access Okta APIs on behalf of a user. Scopes control which API endpoints and operations the client user can be allowed.

"Self" scopes allow a resource to only read or manage itself. Other scopes

6. Save your Okta domain (e.g., yourcompany.okta.com) and the Client ID of the created app for use in Directory Sync configuration.

DSS configuration

Domain settings (connection to Okta)

1. Log in to your Directory Sync account and navigate to the **Domain Manager** tab.
2. Click **Add Domain** and select **Okta Directory** from the **Directory Type** dropdown list.
3. Input the Okta domain details nto the **Okta Domain** field.
4. Enter the Client ID into the **Client ID** field.
5. Paste the **Client Private Key** from step 3 above into the Client Private Key field.
6. Click **Save.**
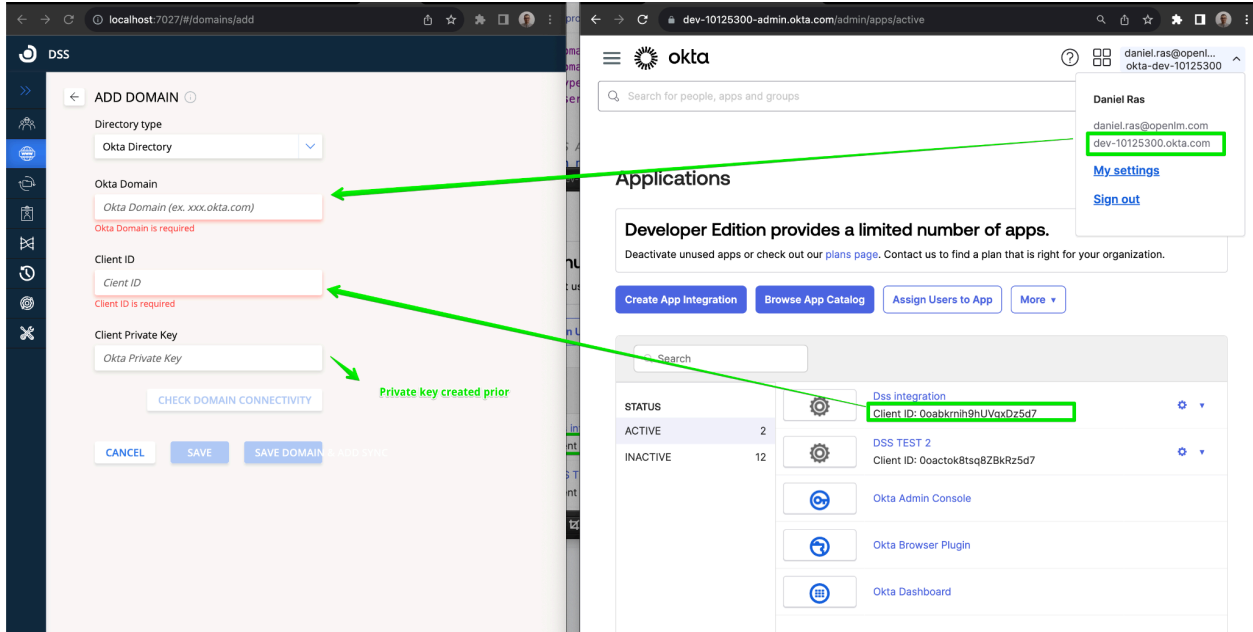
Start node options:

Choose from the following options:

- Empty: Sync all users and groups.
- Users/useremail@mail.com: Sync only the specified user.
- Groups/groupname: Sync groups starting from the specified group.
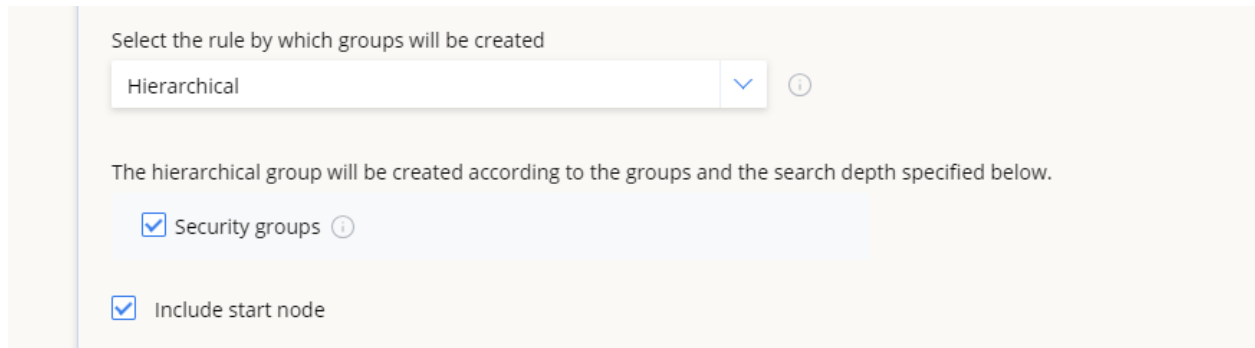
Sync Attribute

Select login as the sync attribute.

Hierarchical Group Rules

Only groups are supported, as Okta does not have organization units or administrative units. The structure consists of users in groups, with a maximum search depth of 1.

Select the rule by which groups will be created

Hierarchical

The hierarchical group will be created according to the groups and the search depth specified below.

☑ Security groups ⓘ

☑ Include start node

Entity Attributes

Entity Attributes, according to which we can create virtual groups:

The highest search depth of objects is 1, because Okta doesn't allow groups inside groups. So structure is only users in groups (1 level, if taking in account root node):

By following these steps, you should successfully integrate Directory Sync with Okta for seamless user and group synchronization.