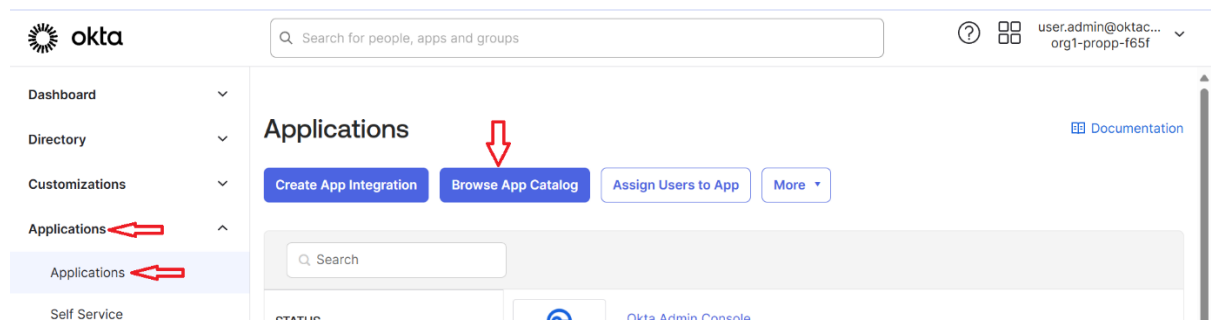


EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

In this guide you will learn how to successfully establish a SAML 2.0-based integration and API provisioning between two Okta instances, allowing for user identity federation and automatic provisioning between Org1 and Org2.

In this exercise you will access the Okta Application Catalog to configure the Org2Org integration in Org1, followed by setting up SAML 2.0 for authentication. Afterward, the Identity Provider is configured in Org2 with the required SAML details such as the IdP Issuer URI, Single Sign-On URL, and certificate. Org1's SAML settings are then configured by copying the Assertion Consumer Service URL and Audience URI from Org2. API integration for provisioning is enabled by entering and verifying the Org2 API key. User management features, including creating, updating, and deactivating users, are then activated. Users and groups, such as the Contractors group, are assigned, and their status is set to active. Finally, the user is verified in Org2 by ensuring they are created and have access to the Okta Org2Org app, confirming successful provisioning. Steps below:

- Log in as Super admin in Org1



- From dashboard
- Click **Applications**, click **Applications**, then click **Browse App Catalog**
- Type in **Okta Org2Org**, click on **Org2Org** , then click **Add Integration**

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

Scheduled Maintenance: Okta will be performing planned maintenance on our Org Creator Manager Database infrastructure. More info [here](#).

Okta

Search for people, apps and groups

user.admin@oktac...
org1-propp-f65f

Dashboard

Directory

Customizations

Applications

Applications

Self Service

API Service Integrations

Security

Workflow

Reports

Settings

Applications > Catalog > All Integrations

Browse App Integration Catalog

Create New App

Use Case

All Integrations	7925
Apps for Good	12
Automation	204
Centralized Logging	49
Directory and HR Sync	85
Bot or Fraud Detection	10
Identity Proofing	49
Identity Governance and Administration (IGA)	76
Lifecycle Management	723
Multi-factor Authentication (MFA)	67

Search for "Okta Org2Org"

Sort by: Default

Okta Org2Org

Single Sign-On

Authenticate and provision users from a source org into another Okta org

SWA SAML SCIM

Okta Advanced Server Access

Single Sign-On

Automate IAM across dynamic server fleets at any scale

Workflows Connectors SAML SCIM

Okta

Search for people, apps and groups

user.admin@oktac...
org1-propp-f65f

Dashboard

Directory

Customizations

Applications

Applications

Applications > Catalog > Single Sign-On > Okta Org2Org

Last updated: July 11, 2024

Add Integration

- Populate **Base Url** with **Org2 Url**, check **Automatically log in when use land on login page**, then click **Next**

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

Okta Search for people, apps and groups user.admin@oktac... org1-propp-f65f

Add Okta Org2Org

1 General Settings 2 Sign-On Options

General settings- Required

Application label: Okta Org2Org
This label displays under the app on your home page

Base Url: <https://org2-propp-f65f.oktapreview.com>
Required field for SSO and Provisioning: Please enter the login URL of the target Okta Org

Application Visibility: ☐ Do not display application icon to users

Browser plugin auto-submit: ☒ Automatically log in when user lands on login page

Cancel Next

General settings
All fields are required to add this application unless marked optional.

- Check **SAML 2.0**, click **View Setup Instructions**

Scheduled Maintenance: Okta will be performing planned maintenance on our Org Creator Manager Database infrastructure. More info [here](#).

Okta Search for people, apps and groups user.admin@oktac... org1-propp-f65f

SAML 2.0

Default Relay State:
All IDP-initiated requests will include this RelayState.

Attributes (Optional) [Learn More](#)

Disable Force Authentication: ☐ Never prompt user to re-authenticate.

with Okta.
You can sync passwords to this app
If you enable provisioning and password push, you can automatically synchronize Okta passwords to Okta Org2Org.
Application Username
Choose a format to use as the default username value when assigning the application to users.

Okta Search for people, apps and groups user.admin@oktac... org1-propp-f65f

SAML 2.0 is not configured until you complete the setup instructions.
[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

Advanced Sign-on Settings
These fields may be required for a Okta Org2Org proprietary sign-on option or general setting.

Hub ACS URL:
Enter your Source org Assertion Consumer Service URL

Audience URI:

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

- Use SAML 2.0 setup instructions
- From org2 dashboard
- Click **Security**, click **Identity Providers**, then click **Add identity provider**
- Select **SAML 2.0**, click **Next**

The screenshot shows the Okta admin console interface. On the left sidebar, the 'Security' menu item is highlighted with a red arrow. The main content area is titled 'Identity Providers' and has a sub-tab 'Identity providers' selected, also indicated by a red arrow. Below the sub-tab, there is a button 'Add identity provider' with a plus icon, which is pointed to by a red arrow. Below this button, a table lists available identity providers. The first row, 'SAML 2.0 IdP', is highlighted with a blue border and a checkmark, and is pointed to by a red arrow. Below the table, the 'Next' button is highlighted with a red arrow. The table has columns: Name, Type, Account mode, and Profile source. The providers listed are SAML 2.0 IdP, Salesforce IdP, Xero IdP, and Yahoo IdP. There is also a 'Yahoo Japan IdP' entry below the main table.

Customizations ▾

Applications ▾

Security ← ▴

General

HealthInsight

Authenticators

Authentication Policies

Global Session Policy

okta

user.admin@oktac...
org2-propp-f65f ▾

Search for people, apps and groups

Identity Providers

[Documentation](#)

Identity providers Routing rules

+ Add identity provider ⚙

Search...

Name	Type	Account mode	Profile source
SAML SAML 2.0 IdP	Salesforce Salesforce IdP	Xero Xero IdP	Yahoo Yahoo IdP
YAHOO! JAPAN Yahoo Japan IdP			

Previous Cancel

Next

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

- Name **IDPro**, select **idpuser.subjectNameId**, Account Link Policy select **Automatic**, If no match is found check **Create new user(JIT)**

The screenshot displays the Okta Admin Console interface for configuring an Identity Provider (IDP). The top navigation bar includes the Okta logo, a search bar, and user information. The main content area is divided into two columns: General settings and Authentication Settings.

General settings

- Name:** IDPro (indicated by a red arrow)

Authentication Settings

- IdP Usage:** SSO only
- Account matching with Persistent Name ID:** ☒ Use Persistent Name ID (Higher Security). Determine the associated user account by matching the Name ID with the External ID. If no match is found, account matching with IdP Username will be used. [Read more](#)
- Account matching with IdP Username:**
 - IdP username:** idpuser.subjectNameId (indicated by a red arrow). [Expression Language Reference](#)
 - Filter:** ☐ Only allow usernames that match defined RegEx Pattern
 - Match against:** Okta Username. Choose the user attribute to match against the IdP username.
 - Account Link Policy:** Automatic (indicated by a red arrow)
 - Auto-Link Restrictions:** None
 - If no match is found:** ☒ Create new user (JIT) (indicated by a red arrow). ☐ Redirect to Okta sign-in page

General settings

All fields are required to add this identity provider unless marked optional.

Authentication Settings

Expressions allow you to reference, transform, and combine attributes before you store them on a user profile or before passing them to an application for authentication or provisioning.

IdP Usage

Specifies how users from this IdP will be evaluated.

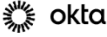
SSO only: Okta evaluates requests coming from the IdP as a password (knowledge factor).

Factor only: Okta evaluates requests coming from this IdP as a possession factor.

- Profile Source check **Update attributes for existing user**


EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

- Populate **IdP Issuer URI**, **IdP Single Sign-On URL**, then click **Browse files**
- Upload certificate downloaded from **SAML 2.0** setup instructions page, click **Finish**



Search for people, apps and groups

?

 user.admin@oktac...
org2-propp-f65f

Dashboard

Directory

Customizations

Applications

Security

General

HealthInsight

Authenticators

Authentication Policies

Global Session Policy

Profile Enrollment

Identity Providers

Delegated Authentication

Networks

Request Binding

Request Signature

Request Signature Algorithm

Response Signature Verification



Response Signature Algorithm


Destination

Okta Assertion Consumer Service URL


Max Clock Skew

JIT Settings optional



Profile Source   ☒ Update attributes for existing users



Reactivation Settings  ☐ Reactivate users who are deactivated in Okta



☐ Unsuspend users who are suspended in Okta

Group Assignments  None


SAML Protocol Settings


IdP Issuer URI   http://www.okta.com/exk8reff4u1hLcTj0x7


IdP Single Sign-On URL   https://org1-propp-f65f.oktapreview.com/app/

IdP Signature Certificate  

Browse files...

Request Binding  HTTP POST

Request Signature  ☒ Sign SAML Authentication Requests

Request Signature Algorithm  SHA-256

HTTP POST

☒ Sign SAML Authentication Requests

SHA-256

Response or Assertion

SHA-256


☒ Trust-specific

☐ Organization (shared)

2 Minutes

Previous

Cancel

 Finish

© 2024 Okta, Inc. Privacy Status site OP2 Preview Cell (EMEA) Version 2024.08.3 E Download Okta Plugin Feedback

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

- Copy **Assertion Consumer Service URL** and paste in **Hub ACS URL** in **Org1**
- Copy **Audience URI** and paste in **Audience URI** in **Org1**
- Click **Done**

Scheduled Maintenance: Okta will be performing planned maintenance on our Org Creator Manager Database infrastructure. More info [here](#).

okta Search for people, apps and groups user.admin@oktac... org2-propp-f65f

Identity providers / Edit IdP [Okta help](#)

SAML IDPro

Active Edit profile and mappings

Summary

IdP ID	00a8ff730lmDzpeX0×7
SAML metadata	Download metadata
Assertion Consumer Service URL	https://org2-propp-f65f.oktapreview.com/sso/saml2/00a8ff730lmDzpeX0×7
	Copy
Audience URI	https://www.okta.com/saml2/service-provider/spnidwtjnfioimvnwzxc
	Copy

Advanced Sign-on Settings

These fields may be required for a Okta Org2Org proprietary sign-on option or general setting.

Hub ACS URL [https://org2-propp-f65f.oktapreview.com/sso/saml2/0](#)
Enter your Source org Assertion Consumer Service URL

Audience URI [https://www.okta.com/saml2/service-provider/spnidw](#)

Credentials Details

Application username format [Okta username](#)

Update application username on [Create and update](#)

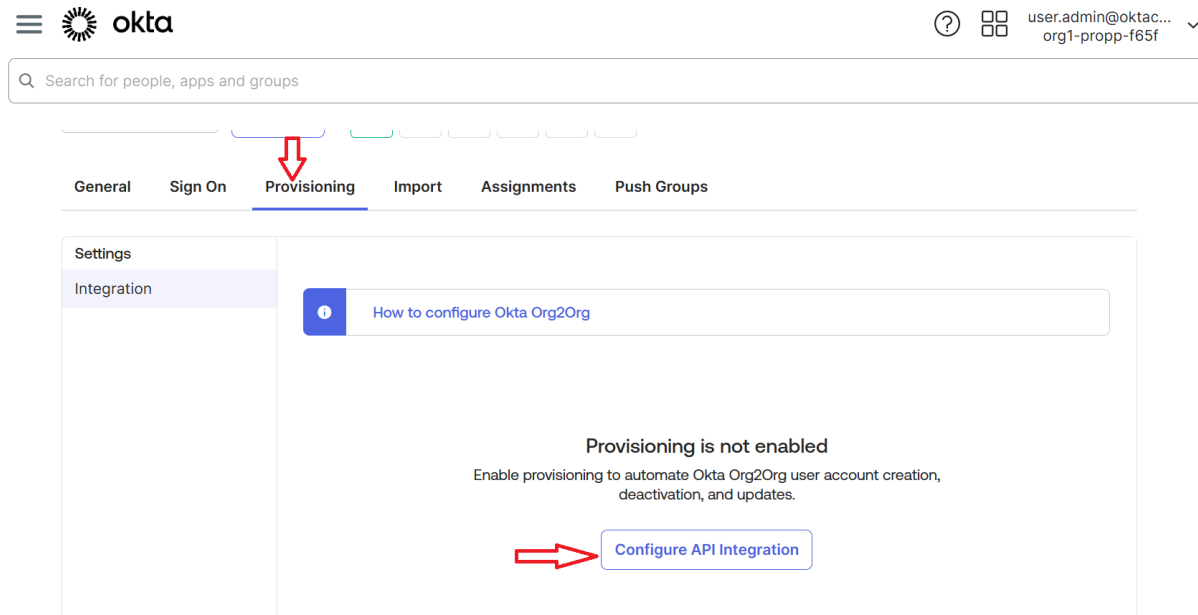
Password reveal ☒ Allow users to securely see their password (Recommended)

[Previous](#) [Cancel](#) [Done](#)

prompted to enter the username manually when assigning an application with password or profile push provisioning features.

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

- Click **Provisioning**, click **Configure API Integration**



- Check **Enable API Integration**
- Populate **Security token with Org2 API Key**, click **Test API Credentials**
- Make sure Okta Org2Org verified successfully, then click **Save**

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

The screenshot shows the 'Settings' page with the 'Integration' tab selected. A red arrow points to the 'Enable API integration' checkbox, which is checked. Below this, there is a text input field for the 'Security token' with a red arrow pointing to it. The 'Prefer Username Over Email' checkbox is unchecked, and the 'Import Groups' checkbox is checked. A red arrow points to the 'Test API Credentials' button. At the bottom right, a red arrow points to the 'Save' button.

Settings
Integration

How to configure Okta Org2Org

Cancel

☒ Enable API integration

Enter your Okta Org2Org credentials to enable user import and provisioning features.

Security token

Prefer Username Over Email ☐

Import Groups ☒

Test API Credentials

Save

Scheduled Maintenance: Okta will be performing planned maintenance on our Org Creator Manager Database infrastructure. More info [here](#).

okta

user.admin@oktac...
org1-propp-f65f

Search for people, apps and groups

Settings
Integration

How to configure Okta Org2Org

Cancel

☒ Okta Org2Org was verified successfully!

☒ Enable API integration

Enter your Okta Org2Org credentials to enable user import and provisioning features.

Security token

Prefer Username Over Email ☐

Import Groups ☒

Test API Credentials

Save

- Click **Edit**, Enable **Create users**, Enable **Update User Attributes**, Enable **Deactivate Users**, then click **Save**

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

The screenshot displays the Okta Admin console interface. At the top, the 'Integration' tab is selected. Below it, a diagram shows the 'okta' logo pointing to an application icon, with the text 'Provisioning to App' underneath. To the right of this diagram is a red arrow pointing to an 'Edit' link. Below the diagram, the 'Create Users' section is visible, with a red arrow pointing to an 'Enable' checkbox. The 'Update User Attributes' section is also visible, with a red arrow pointing to an 'Enable' checkbox. The 'Deactivate Users' section is visible, with a red arrow pointing to an 'Enable' checkbox. The 'Sync Password' section is visible, with a red arrow pointing to an 'Enable' checkbox. At the bottom right, there is a red arrow pointing to a 'Save' button. The top navigation bar includes the Okta logo, a search bar, and a user profile dropdown menu.

Integration

okta → [App Icon]

Provisioning to App

Edit

okta

Search for people, apps and groups

Create Users ☒ Enable

Creates or links a user in Okta Org2Org when assigning the app to a user in Okta.

The [default username](#) used to create accounts is set to **Okta username**.

Update User Attributes ☒ Enable

Okta updates a user's attributes in Okta Org2Org when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Okta Org2Org.

Deactivate Users ☒ Enable

Deactivates a user's Okta Org2Org account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

Sync Password ☐ Enable

Creates a Okta Org2Org password for each assigned user and pushes it to Okta Org2Org.

Save

- Click **Assignment**, click **Assign**, click **Groups**, then click **Assign** on Contractors

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

Okta

Search for people, apps and groups

← Back to Applications

Okta Org2Org (3)

Active

General Sign On Provisioning Import Assignments Push Groups

Assign

Convert assignments

Search...

People

Assign to People

Assign to Groups

Groups

Type

01101110

01101111

01101100

01101100

01101101

01101110

01101111

No users found

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app.

Go to self service settings

Requests Disabled

Edit

Scheduled Maintenance: Okta will be performing planned maintenance on our Org Creator Manager Database infrastructure. More info [here](#).

Okta

Search for people, apps and groups

← Back to Applications

Okta Org2Org (3)

Assign Okta Org2Org (3) to Groups

Search...

Contractors

All Contractors

Assign

Everyone

All users in your organization

Assign

- Initial Status select **active_with_pass**, then click **Save and Go Back**
- Click **Done**

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

The image shows two overlapping screenshots from the Okta user management interface. The top screenshot displays the 'Initial status' dropdown menu, which is set to 'active_with_pass'. A red arrow points to this dropdown. Below it, another red arrow points to the 'Save and Go Back' button. The bottom screenshot shows a modal titled 'Assign Okta Org2Org (3) to Groups'. This modal lists two groups: 'Contractors' (All Contractors) and 'Everyone' (All users in your organization). A red arrow points to the 'Done' button at the bottom right of the modal.

user.manager
This is the default value [Override](#)

user.manager
This is the default value [Override](#)

Security question

Security answer

Initial status [active_with_pass](#)
Overrides default value [Reset](#)

[Save and Go Back](#) [Cancel and Go Back](#)

Assign Okta Org2Org (3) to Groups

Search...

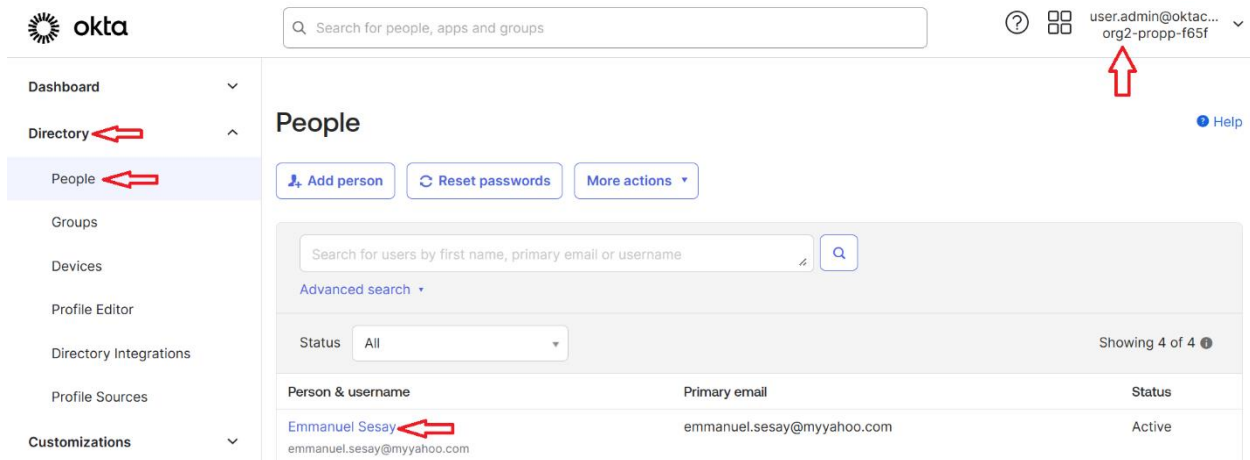
[Contractors](#)
All Contractors [Assigned](#)

[Everyone](#)
All users in your organization [Assign](#)

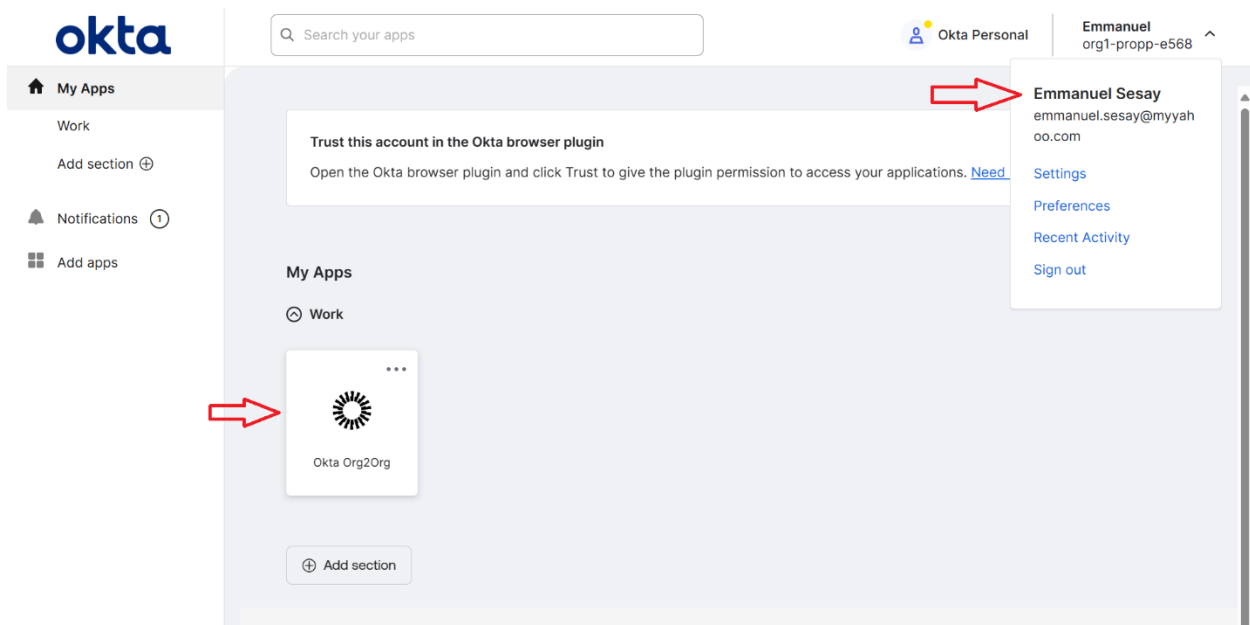
[Done](#)

- Make sure user account is in **Org2**
- From **Org2** dashboard
- Click **Directory**, click **People**

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2



- Log in as user
- Make sure user have access to **Okta Org2Org** App from user's dashboard



- Click on **Okta Org2Org** App
- Make sure user is push through to **Org2**

EMMANUEL SESAY's OKTA JR. ENGINEER GUIDE P2

