**Part 1: Okta ↔ Microsoft 365 Federation Setup**

Goal: Configure **WS-Fed** federation from Okta to Microsoft 365 and **enable provisioning**.

**Step-by-Step:**

1. **In Okta:**
   * Go to **Applications → Browse App Catalog**
   * Search for **“Office 365”** and add it
   * Use **WS-Federation** (Andy’s preference)
   * Set **Microsoft 365 domain** as:  
     mywiclab114.onmicrosoft.com
2. **Enable Federation:**
   * In Microsoft 365, run **PowerShell** with global admin to federate:

|  |
| --- |
|  |

Here’s how you should configure the \*\*Sign-On Options\*\* for your Okta integration with Microsoft 365, focusing on WS-Federation as Andy recommended:

---

### 1. \*\*Sign-on method\*\*

Select \*\*WS-Federation\*\* since it’s preferred for this integration.

---

### 2. \*\*Application username format\*\*

Choose \*\*Okta username\*\* — this means the user’s Okta login ID will be used as their username in Microsoft 365.

---

### 3. \*\*Update application username on\*\*

Select \*\*Create and update\*\* — so when users are created or updated in Okta, the changes reflect in Microsoft 365.

---

### 4. \*\*Password reveal\*\*

Enable \*\*Allow users to securely see their password\*\* (recommended) to improve user experience during the demo.

---

### 5. \*\*API Credentials / Advanced API Access\*\*

If you have API credentials from Microsoft or Okta to manage provisioning or automation, enable \*\*Allow administrator to consent for Advanced API access\*\*.

Otherwise, you can set this up later after you have the credentials.

---

### Additional:

You will need to configure \*\*Profile Mapping\*\* to sync attributes between Okta and Microsoft 365 user profiles. This is important for provisioning users correctly.

---

If you want, I can help you step-by-step with the WS-Federation setup and profile mapping next?

powershell

CopyEdit

Connect-MsolService

Set-MsolDomainAuthentication -DomainName mywiclab114.onmicrosoft.com -FederationBrandName "Okta" -Authentication Federated -IssuerUri "urn:okta:demo-teal-antlion-29717" -SigningCertificate <cert> -LogOffUri "<logoff url>" -PassiveLogOnUri "<login url>"

* + Okta will give you the exact PowerShell commands in the **Office 365 app integration setup guide** under **Sign On → View Setup Instructions**

1. **Provisioning:**
   * Go to **Provisioning tab** in the app
   * Enter **admin credentials** from Microsoft 365 (the labadmin)
   * Test API connection
   * Set **provisioning rules** (users/groups from Okta to M365)

**✅ Part 2: Automation Script (Demo Reset Setup)**

Goal: Automate creation + cleanup of a **demo environment** in Microsoft 365.

**Recommend doing:**

* Use **Python + MS Graph API** or **PowerShell**
* Script should:
  1. Create users (User1, User2) in Entra ID
  2. Assign to a group / license them if needed
  3. Delete all created users/groups when rerun

We can use something like:

python

CopyEdit

# Python + Microsoft Graph SDK (sample snippet)

from msgraph.core import GraphClient

client = GraphClient(credential=...)

# Create user

user = {

"accountEnabled": True,

"displayName": "Demo User 1",

"mailNickname": "demo1",

"userPrincipalName": "demo1@mywiclab114.onmicrosoft.com",

"passwordProfile": {

"forceChangePasswordNextSignIn": True,

"password": "TempPass123!"

}

}

client.post('/users', data=user)

# Delete users

client.delete('/users/demo1@mywiclab114.onmicrosoft.com')

We can walk through this or use PowerShell if you prefer.