Office 365 with Okta- PBC

Lab Guide

Printed January 2017

Contact Okta, Inc @ training@okta.com

Table of Contents

Lab 10-1: Deploy Directory-mastered Accounts with O365 Using Microsoft Provisioning

Objectives	Configure Windows Directory Sync server for provisioning of users between Active Directory and O365.
Scenario	You are using Microsoft Directory Sync server and need the employee information in Active Directory to be automatically be updated in O365. **Note: To complete this lab, work with your 1st O365 tenant.**
Duration	30-35 minutes

Explore Your 1nd O365 Tenant

1. Open a new browser tab.
2. In the address bar, type the following:
   https://portal.office.com
3. Log in using the second set of provided O365 administrator credentials.
4. On the Office 365 welcome screen, click **Admin**.
5. In the left pane, expand **Settings** and click **Domains**.
6. In the right pane, note the subdomain for your O365 tenant.
   For example, okta014.oktaice.com
7. Verify that the .onmicrosoft.com subdomain is set to default.
   a. If it is not, in the top-right corner, click the **Okta Training (Edit)** link.
   b. Scroll to the bottom of the **Company Profile** page and in the **Default domain** list, select the **.onmicrosoft.com** domain.

Add an Alternate UPN Suffix

1. In the VM, in Windows **Server Manager**, click the **Tools** menu and then click **Active Directory Domains and Trusts**.
2. In the **Active Directory Domains and Trusts** window, click the **Actions** menu and then click **Properties**.
3. In the **Alternative UPN suffixes** field, type your domain name (okta###.oktaice.com) and then click **Add**.
4. Click **OK**.

Enable AAD Sync

1. Return to your web browser and **sign in to your 3rd Microsoft tenant** at portal.office.com.
2. In the left pane, expand **Users** and click **Active users**.
3. In the **Active users** pane, click **More** and then click **Directory Synchronization**.
4. Click **Go to the DirSync Management**.

5. Verify that **Dirsync is enabled** is set to **true**.

Run the IdFix Tool

1. On your VM desktop, open the **Microsoft** folder.
2. Right-click the **IdFix.zip** file and then click **Extract All**.
3. Click **Extract**.
4. In the extracted folder, double-click the **IdFix** file.
5. Click **Run** and then click **Ok**.
6. In the top bar, click **Query**.
7. In each row, click the **UPDATE** field value and change the domain from @oktaice.local to the following:
   @ okta###.oktaice.com
   For example, change awillems@oktaice.local to awillems@okta001.oktaice.com
8. Under the **ACTION** column, select **EDIT**.
9. When all changes have been made, in the top bar, click **Apply**.
10. When the warning appears, click **Yes**.

Install Windows AAD Sync Tool

1. On your VM desktop, open the **Microsoft** folder.
2. Double-click the **AzureADConnect.msi** file.
3. If a Security Warning appears, click **Run**.
4. Follow the instructions in the **Microsoft Azure Active Directory Connect** setup wizard as follows:
   Note: This might take over 10 minutes. If the wizard fails to complete, log out of the VM and then log back in, uninstall the application, and try to run it again.
   a. On the **Welcome** page, select **I agree to the license terms and privacy notice** and then click **Continue**.
   b. On the **Express Settings** page, click **Use express settings**.
   c. On the **Connect to Azure AD** page, enter the credentials for your O365 tenant.
      For example, admin@okta###.onmicrosoft.com
   d. Click **Next**.
   e. On the **Connect to AD DS** page, enter your Okta admin credentials.
      For example, administrator@oktaice.local
   f. Click **Next**.
   g. On the **Azure AD sign-in** page, click **Next**.
   h. On the **Configure** page, click **Install**.
   i. When the installation completes, click **Exit**.

Verify Users in Your Microsoft Tenant

1. Return to your web browser and **sign into your 1st Microsoft tenant at portal.office.com**.
2. In the left pane, expand **Users** and click **Active users**.
   You should now see users with the correct domain name @okta###.oktaice.com
   Note: If you do not see any users, wait a few minutes to let the sync complete.

Run an AD Agent Import

1. Return to the Okta Admin app.
2. Point to **Directory** and click **Directory Integrations**.
3. In the table, click the **Active Directory** instance.
4. Click the **Import** tab.
5. Click **Import Now** and then click **Import**.

Create a New O365 App

1. Point to **Applications** and click **Applications**.
2. Click **Add Application**.
3. In the **Search for an application** field, type the following:
   office 365
4. Next to the **Microsoft Office 365** entry, click **Add**.
5. In the **Enter basic info** dialog box, perform the following:
   a. In the **Microsoft Tenant Name** field, type the subdomain of your 1st Microsoft tenant name.
      For example, if your tenant name is okta021.onmicrosoft.com, enter only okta021. Get your Microsoft tenant name from the O365 Domains section.
   b. In the **Your Office 365 company domain** field, type the following:
      okta###.oktaice.com
      Note: This is NOT your Okta org.
   c. Click **Next**.
6. In the **Configure sign on settings** dialog box, select **SWA** and then click **Save and Assign**.
7. Click the **Sign On** tab and then perform the following:
   a. Click **Edit**.
   b. Under **Sign On Methods** select **WS-Federation**.
   c. Leave the default selection of **Let Oka configure WS-Federation automatically for me**.

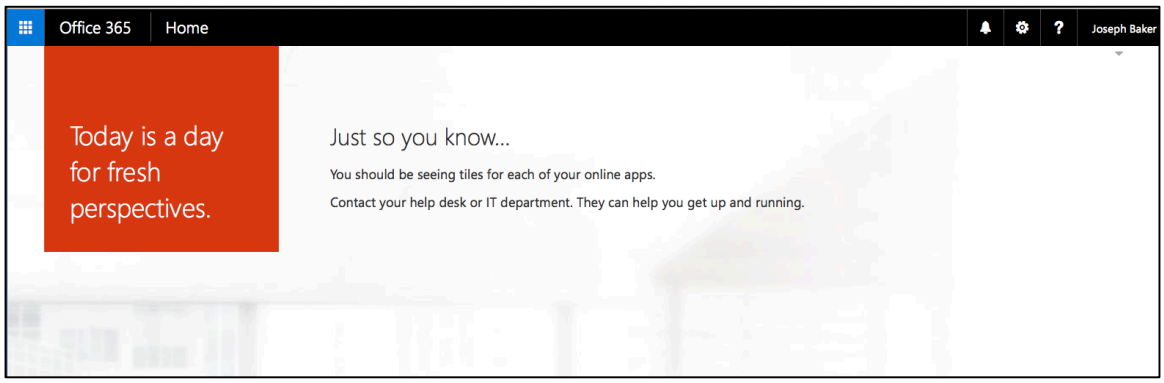
d. Under **Credentials Details**, in the **Application username format** list, select **AD user principal name**.
e. Click **Save**.

Assign a User in Okta

1. Click the **Assignments** tab.
2. Click the **Assign** list and then click **Assign to People**.
3. In the **Assign Microsoft Office 365 to People** dialog box, perform the following:
   a. In the **Search** field, type the following:
      Joseph
   b. In the resulting matches, next to the **Joseph Baker** account, click **Assign**.
   c. Verify his username is joseph.baker@okta###.oktaice.com
   d. Click **Save and Go Back**.
   e. Click **Done**.

Test with a User

1. Sign in to your Okta org with the **joseph.baker** credentials.
2. Select a security image.
3. Click **Create My Account**.
4. On the Okta app page, click the **Office 365** app.
5. Verify that you can sign in successfully.
   Joseph will not see any Microsoft applications because you did not assign him a license.



6. Sign out of Okta.

Optional Step:

Provision to O365: Licenses/Roles

1. Sign back into Okta with the Okta Admin credentials.
2. Click **Admin**.
3. Point to **Applications** and click **Applications**.

4. In the **Applications** table, locate and click the **Microsoft Office 365** application you configured in Lab 5-1.
5. Click the **Provisioning** tab and perform the following:
    a. Click **Enable Provisioning**.
    b. Select **Enable provisioning features**.
    c. Under **API Credentials**, perform the following:
        i. Leave the credential information in the **Admin Username** and **Admin Password** fields.
        ii. Click **Test API Credentials**.
    d. Under **Provisioning Style**, next to **Office 365 Provisioning Type**, select **Licenses/Roles Management Only**.
    e. Scroll down the tab and click **Save**.

Test with Your Active Directory User

1. Sign out of your Okta org and sign back in using your Active Directory account.
2. On the Okta app page, click the **Office 365** app.
3. Verify you can authenticate into Office 365.

Lab 10-2: Deploy Directory-mastered Accounts with O365 Using Okta Provisioning

Objectives	Set up Office 365 with Active Directory using Okta Provisioning
Scenario	You need the employee information in Active Directory to be automatically be updated in O365. **Note: To complete this lab, work with your 2nd O365 tenant.**
Duration	10 minutes

Explore Your 2nd O365 Tenant

8. Open a new browser tab.
9. In the address bar, type the following:
   https://portal.office.com
10. Log in using the second set of provided O365 administrator credentials.
11. On the Office 365 welcome screen, click **Admin**.
12. In the left pane, expand **Settings** and click **Domains**.
13. In the right pane, note the subdomain for your O365 tenant.
    For example, okta014.oktaice.com
14. Verify that the .onmicrosoft.com subdomain is set to default.
    a. If it is not, in the top-right corner, click the **Okta Training (Edit)** link.
    b. Scroll to the bottom of the **Company Profile** page and in the **Default domain** list, select the **.onmicrosoft.com** domain.

Create a New O365 App

1. Point to **Applications** and click **Applications**.
2. Click **Add Application**.
3. In the **Search for an application** field, type the following:
   office 365
4. Next to the **Microsoft Office 365** entry, click **Add**.
5. In the **Enter basic info** dialog box, perform the following:
   a. In the **Microsoft Tenant Name** field, type the subdomain of your Microsoft tenant name.
   For example, if your tenant name is okta014.onmicrosoft.com, enter only okta014. Get your Microsoft tenant name from the O365 Domains section.

b. In the **Your Office 365 company domain** field, type the following:
okta###.oktaice.com
Note: This is NOT your Okta org.
c. Click **Next**.

6. In the **Configure sign on settings** dialog box, perform the following:
   a. Select **SWA**.
   b. Leave **Okta username** as the **Default username**.
   c. Click **Save and Assign**.
   The dialog boxes closes and the app appears on the Assignments tab.
7. Click the **Sign On** tab and perform the following:
   a. Click **Edit**.
   b. Under **Credentials Details**, in the **Application username format** list, select **Custom**.
   c. Click the **custom expression** link.
   The Custom Field Mapping Expressions dialog box opens.
      i. Under Examples, select and copy the **Use the part of the email address that comes before the "@" symbol** syntax.
      ii. Paste the syntax in the **Type an expression here** field.
      iii. Append the syntax to include the oktaice domain with your specific Okta org number, as follows:
      ${f:substringBefore(user.email, "@")}@okta###.oktaice.com
      iv. Click **Preview**.
      v. Click **Use This**.
   d. On the **Sign On** tab, click **Save**.
8. Click the **Provisioning** tab and then perform the following:
   a. Click **Enable Provisioning** and then select **Enable provisioning features**.
   b. Under **API Credentials**, perform the following:
      i. In the **Admin Username** field, type the following:
      admin@okta###.onmicrosoft.com
      ii. In the **Admin Password** field, type the instructor-provided password.
      iii. Click **Test API Credentials**.
      iv. Under **Provisioning Style**, next to **Office 365 Provisioning Type**, select **User Sync**.
      v. Under **Provisioning Features**, enable **Create Users**, **Update User Attributes**, **Deactivate Users**.
      vi. Click **Save**.
      vii. Scroll up the page.

Transform Attributes from Okta to O365

1. Point to **Directory** and click **Profile Editor**.
2. Next to the new **office365** profile, click **Mappings**.
3. Click the **Okta to Microsoft Office 365** tab.
4. Locate the **Mail** attribute for **Microsoft Office 365 User Profile**.
5. In the **Okta User Profile** field, change the **source.email** syntax to the following:
   substringBefore(source.email,"@") + "@okta###.oktaice.com"
   Where ### is your 2nd Office 365 tenant number.
6. At the bottom of the window, in the **Preview** field, type and select the following account:
   okta.admin
7. Verify the new string syntax shows as follows:
   okta.admin@okta###.oktaice.com
8. Click **Exit Preview**.
9. Click **Save Mappings**.
10. Click **Apply updates now**.

Assign O365

1. Point to **Applications** and click **Applications**.
2. Click **Microsoft Office 365**.
3. On the **Assignments** tab, perform the following:
   a. Click the **Assign** list and then click **Assign to People**.
   b. Next to the **Jack Bailey** account click **Assign**.
   c. Verify the **User Name** is **jack.bailey@okta###.oktaice.com** and click **Save and Go Back**.
   d. Click **Done**.

Verify Accounts Have Provisioned to O365

1. Return to **your 2nd Microsoft tenant** at portal.office.com.
2. In the left pane, expand **Users** and click **Active users**.
3. Verify the Jack Bailey account is active.

Enable Federation

1. In the Okta Admin app, perform the following:
   a. Click the **Sign On** tab and next to **Settings**, click **Edit**.
   b. Select **WS-Federation**.
   c. Leave the default selection of **Let Oka configure WS-Federation automatically for me**.
   d. Click **Save**.
2. Sign out of Okta.

Test with a User

1. Sign into your Okta org with the **Jack Bailey** credentials.
2. Click the **Office 365** app.
3. Verify O365 authenticates Jack Bailey.