SCIM Provisioning from Okta to VMware Workspace ONE Access

Modified JUN 2020
JAN 2020
VMware Workspace ONE

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

SCIM Provisioning from Okta to VMware Workspace ONE Access 1

You can provision users and groups from Okta to VMware Workspace ONE® Access™ using the VMware Workspace ONE application that is available in the Okta Integration Network (OIN). The VMware Workspace ONE application uses System for Cross-domain Identity Management (SCIM) provisioning, which is an open standard for automating the exchange of user identity information.

To configure SCIM provisioning from Okta to Workspace ONE Access, you perform prerequisite tasks in Workspace ONE Access first and then configure the VMware Workspace ONE application in Okta.

This diagram shows a high-level overview of the provisioning process:

1 Okta is configured to use the VMware Workspace ONE provisioning application.

2 Okta provisions the user to Workspace ONE Access using SCIM.

3 The AirWatch Provisioning adapter in Workspace ONE Access provisions the user to VMware Workspace ONE® UEM, if Workspace ONE UEM is part of your Workspace ONE-Okta integration.

Note This document only covers SCIM user provisioning from Okta to Workspace ONE Access. If you are also using Workspace ONE UEM and want to provision users from Workspace ONE Access to Workspace ONE UEM, see Configuring AirWatch Provisioning App in VMware Workspace ONE Access.

Supported Features

The VMware Workspace ONE application in the Okta Integration Network supports the following features:

- Create users
- Update user attributes
- Deactivate users

- Create groups
- Add or remove group members

Note Using the same Okta group for assignments and for group push is not currently supported. To maintain consistent group membership between Okta and Workspace ONE Access, you must create a separate group that is configured to push groups to Workspace ONE Access.

Requirements

- A Workspace ONE Access SaaS tenant
- An Okta tenant
- (Optional) Workspace ONE UEM SaaS tenant or version 19.09 for dedicated or on premise
- Download and install the Postman app.

About This Document

Follow the procedures in the order in which they are listed in this document. Before you configure the VMware Workspace ONE application in the Okta Admin console, you must perform the following prerequisite tasks in Workspace ONE Access:

- Create a Remote Application Access Client.
- Generate an OAuth bearer token (requires Postman).
- Create a directory of type Other (requires Postman).

Related Documentation

- Integrating VMware Workspace ONE with Okta
- Configuring AirWatch Provisioning App in VMware Workspace ONE Access

Complete Prerequisites in Workspace ONE Access

2

As the first step in configuring SCIM user provisioning from Okta to Workspace ONE Access, complete the required prerequisite tasks in Workspace ONE Access. These tasks include creating a Remote App Access Client, generating an OAuth bearer token, and creating a directory of type Other.

Some of these tasks require you to use the Postman app, so download and install the app from https://www.getpostman.com before you begin.

This chapter includes the following topics:

Create Remote App Access Client

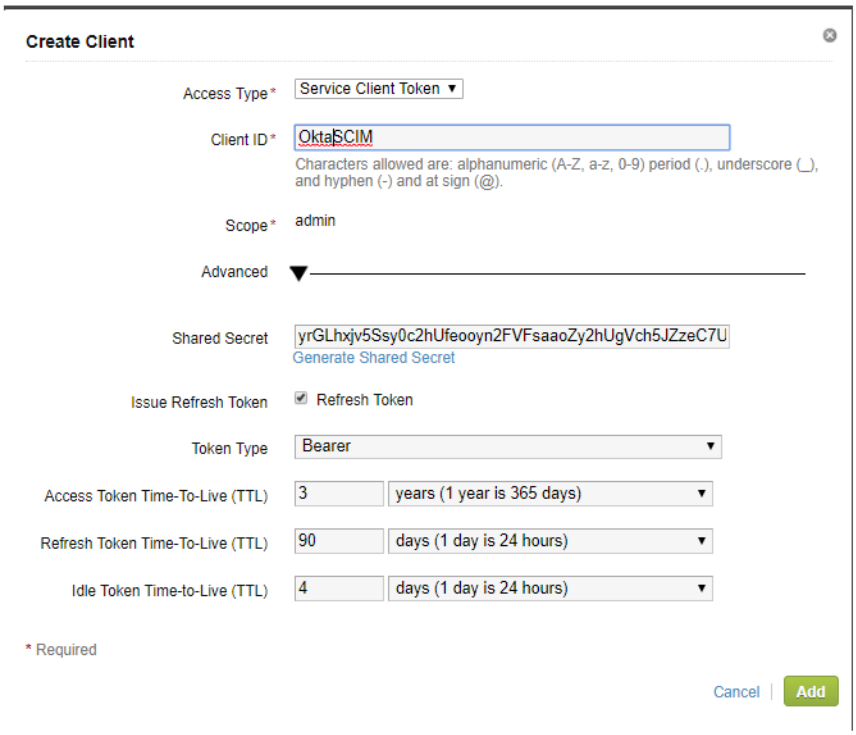
In the Workspace ONE Access console, create a Remote App Access Client.

Procedure

1. Log into the Workspace ONE Access console.
2. Click the arrow on the **Catalog** tab and select **Settings**.
3. Click **Remote App Access** in the left pane.
4. Click **Create Client**.
5. For **Access Type**, select **Service Client Token**.
6. For **Client ID**, enter an ID, for example, `OktaSCIM`.
7. Expand the **Advanced** section.
8. Click **Generate Shared Secret**.

9 Update the **Access Token Time-to-Live** setting to a longer time than the default.

Important Setting the **Access Token Time-to-Live** setting to a longer time is important because you will need to update the Okta configuration with a new bearer token in that time. For example, if you choose one year, you will need to update the Okta configuration every year with a new bearer token.



10 Copy the shared secret. You will need this later in the setup process.

11 Click **Add**.

Generate OAuth Bearer Token

After creating the Remote App Access client, generate an OAuth bearer token.

Prerequisites

Download and install the Postman app. You can download Postman from https://getpostman.com.

Procedure

1 Open a new tab in the Postman app.

2 For the HTTP method, select **POST**.

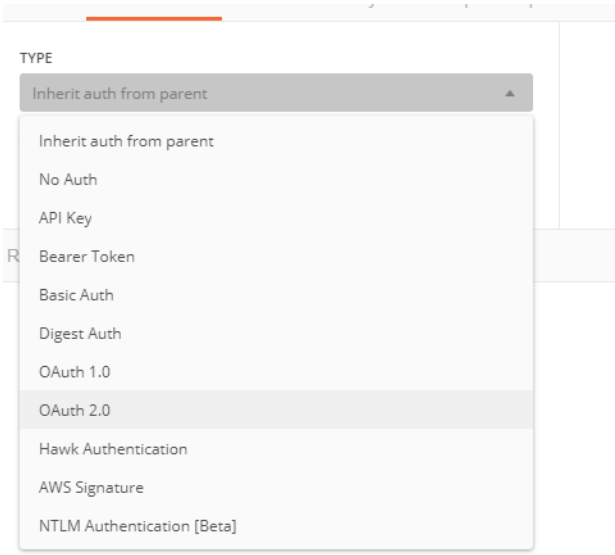
3 For the URL, enter:

```
https://tenanturl/SAAS/jersey/manager/api/connectormanagement/directoryconfigs
```

Replace *tenanturl* with your Workspace ONE Access URL, for example:

```
https://example.vmwareidentity.com/SAAS/jersey/manager/api/connectormanagement/directoryconfigs
```

4 Click the **Authorization** tab and select **OAuth 2.0** as the type.



5 Click **Get New Access Token**.

6 For **Token Name**, enter a name, such as `Workspace ONE`.

7 For **Grant Type**, select **Client Credentials**.

8 For **Access Token URL**, enter https://*tenantURL*/SAAS/auth/oauthtoken, where *tenantURL* is your Workspace ONE Access tenant URL.

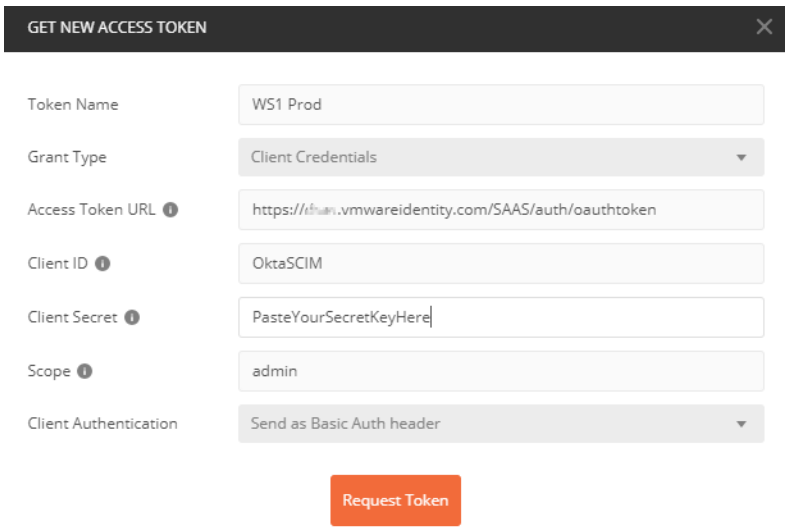
For example: https://example.vmwareidentity.com/SAAS/auth/oauthtoken

Note Workspace ONE Access was formerly called VMware Identity Manager. Old tenants have the domain name vmwareidentity.com while new tenants have the domain name workspaceoneaccess.com.

9 For **Client ID**, enter the Client ID that you set in Create Remote App Access Client.

10 For **Client Secret**, enter the secret that you set in Create Remote App Access Client.

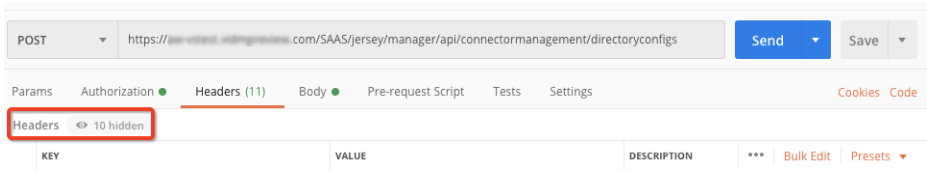
11 For **Scope**, enter **`admin`**.



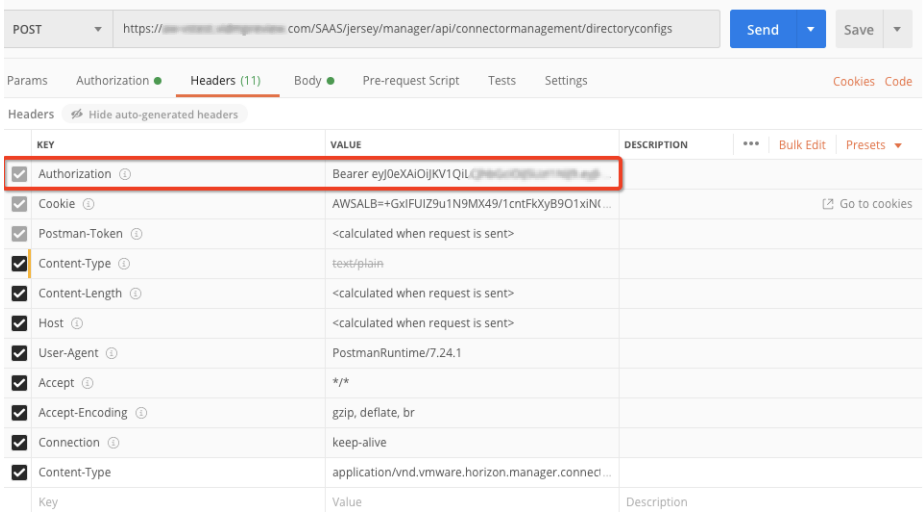
12 Click **Request Token**.

A token is generated and displayed.

13 To verify that the bearer token was added, click the **Headers** tab and click **hidden headers**.



The bearer token appears.



14 If the bearer token was not added, return to the **Authorization** tab and select your token from the available tokens drop-down list and check again.

Create a Directory of Type Other in Workspace ONE Access

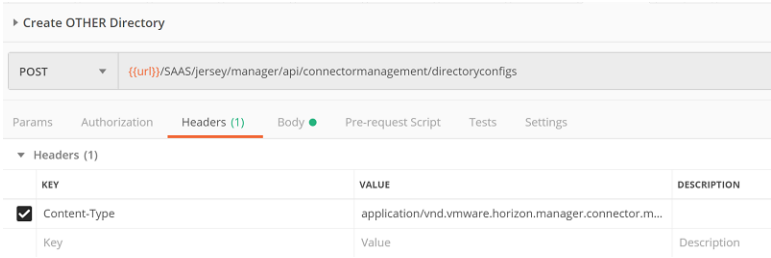
Use the Postman app to create a directory of type Other in Workspace ONE Access for your Okta users.

Procedure

1 Under **Headers**, set the **Content-Type** to:

```
application/vnd.vmware.horizon.manager.connector.management.directory.other+json
```

Tip Start typing in **Content-Type** in the **Key** column to select the Content-Type entry.



2 Click the **Body** tab.

3 Use the following as a sample and click **Send**.

```
{
"type":"OTHER_DIRECTORY",
"domains":["OKTA.COM"],
"name":"Okta Universal Directory"
}
```

Note Make sure that your domain is unique within your tenant.

You should see a result similar to the following:

Configure the VMware Workspace ONE Access Application in Okta

3

In the Okta Admin console, add the VMware Workspace ONE application from the Okta catalog, then configure the application.

Procedure

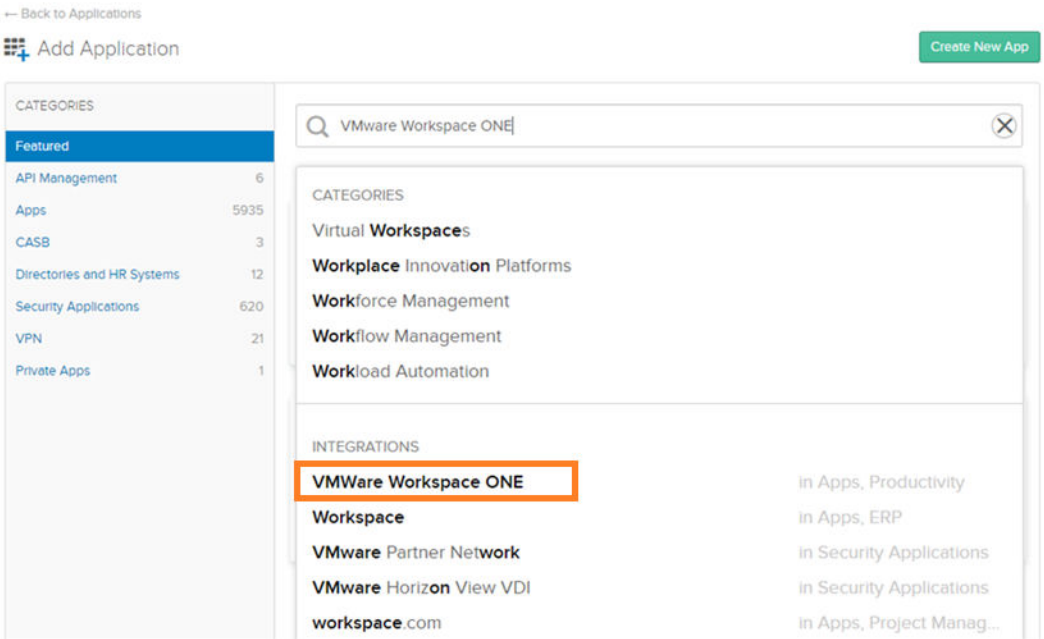
1 Log into the Okta Admin console.

2 Click **Applications > Applications**.

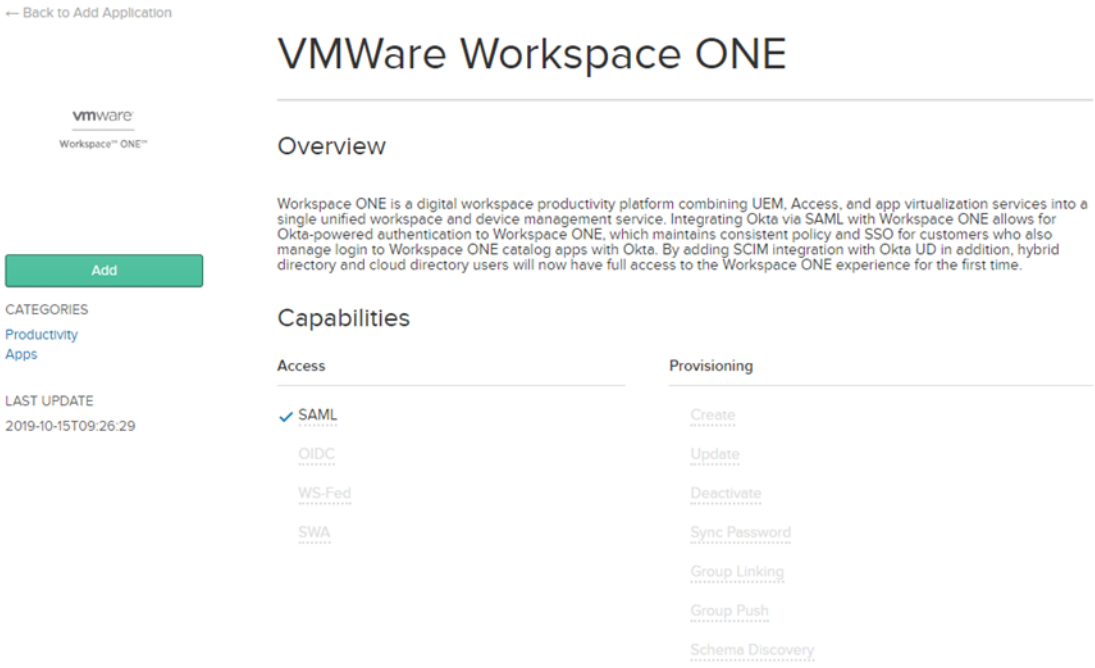
3 Click **Add Application**.

4 Search for the **VMware Workspace ONE** application.

5 Select **VMware Workspace ONE** under **Integrations**.

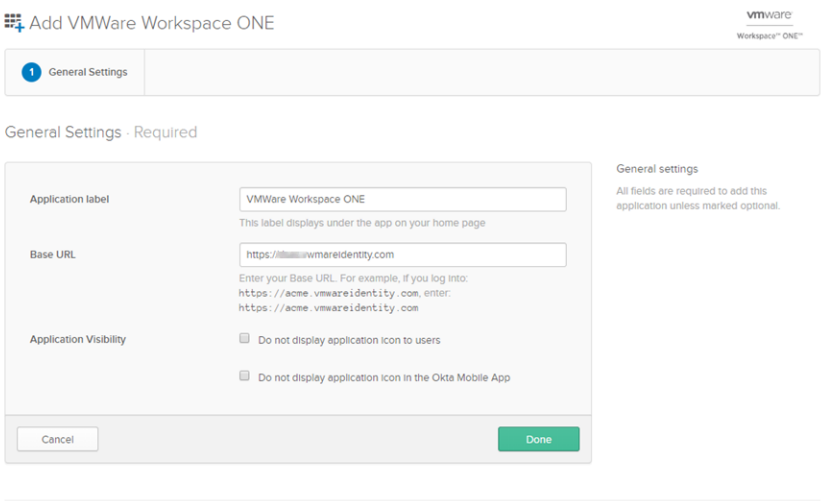


6 Click **Add**.



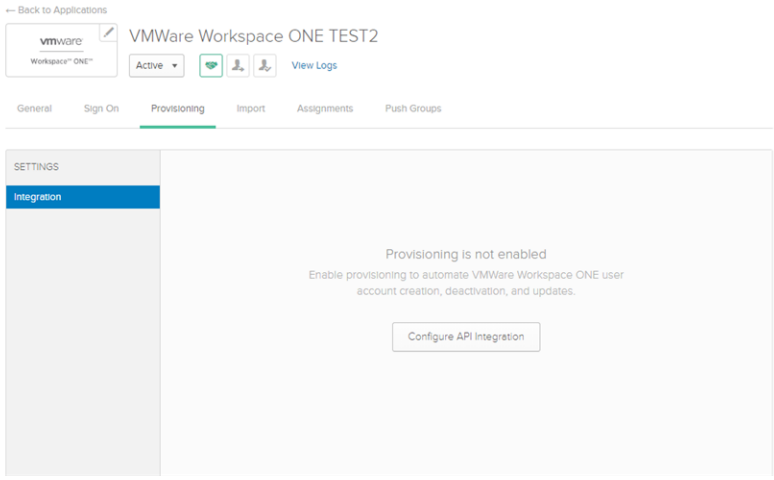
7 In the **Base URL** text box, enter your Workspace ONE Access URL.

For example: **`https://example.vmwareidentity.com`**

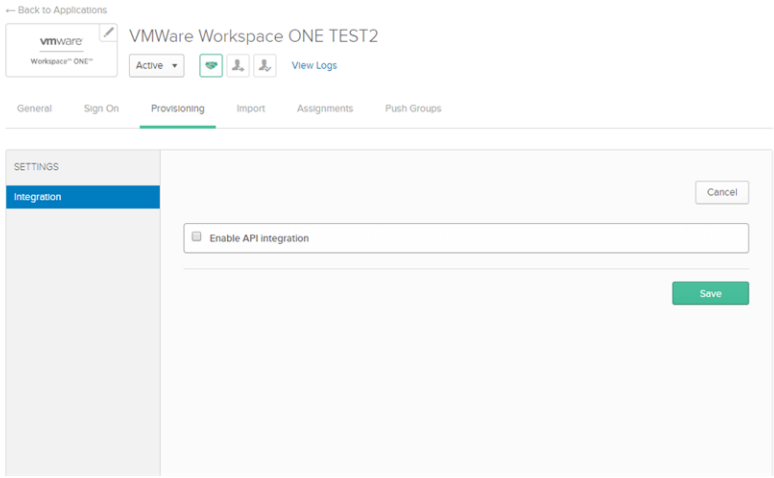


8 Click **Done**.

9 Click the **Provisioning** tab and click **Configure API Integration**.

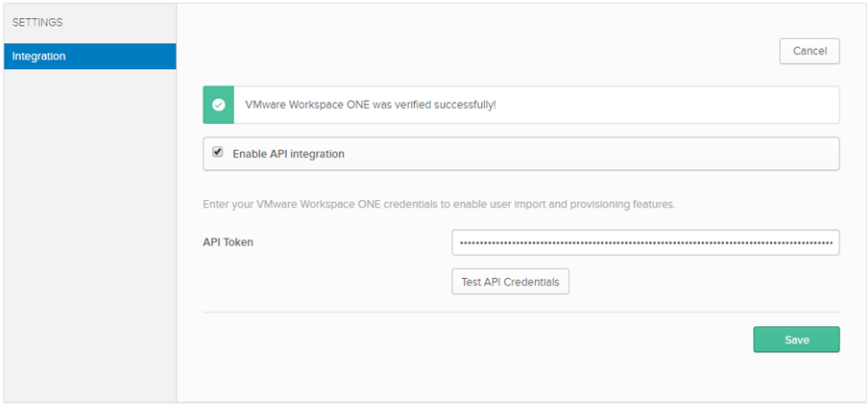


10 Select the **Enable API Integration** check box.



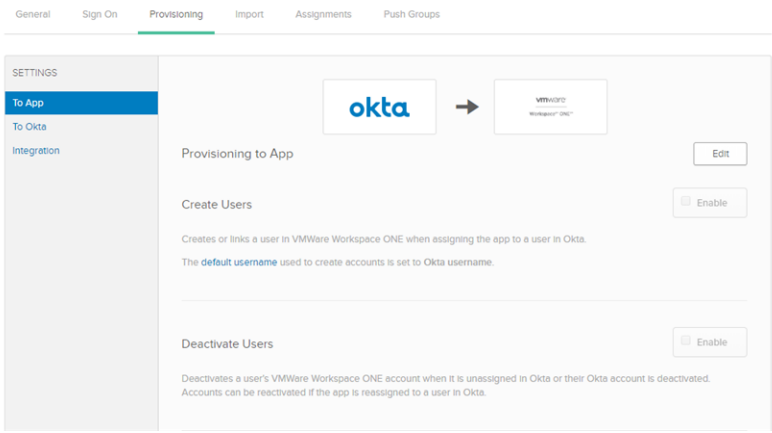
11 In the **API Token** text box, paste the bearer token that you created in Generate OAuth Bearer Token with Postman.

12 Click **Test API Credentials** and ensure that you see a successful message before proceeding.

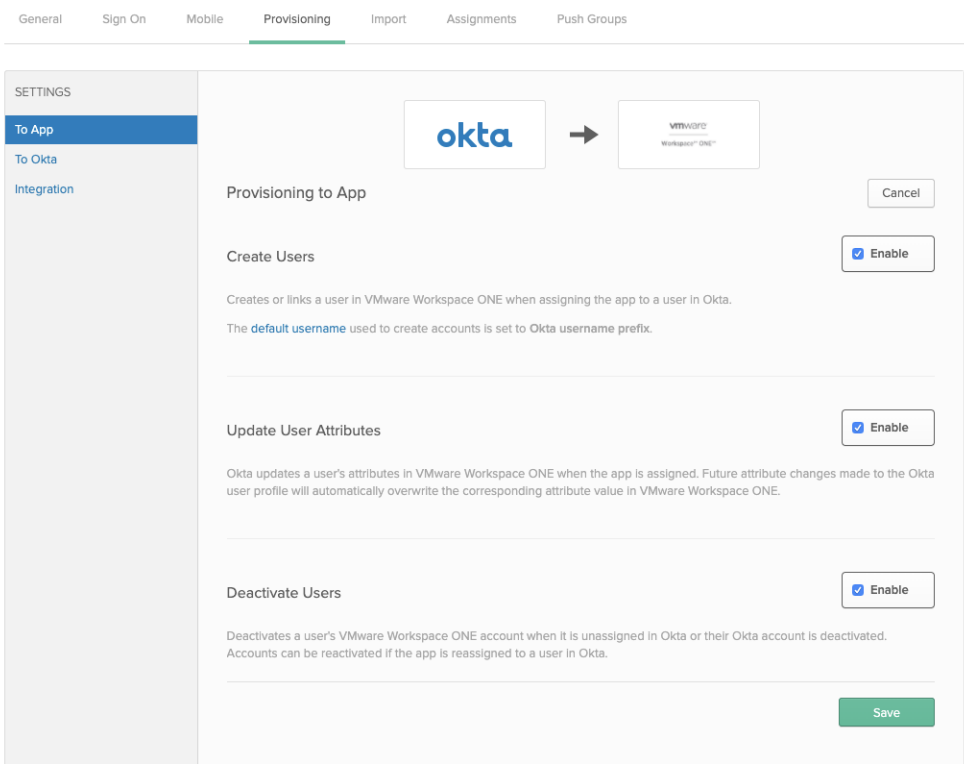


13 Click **Save**.

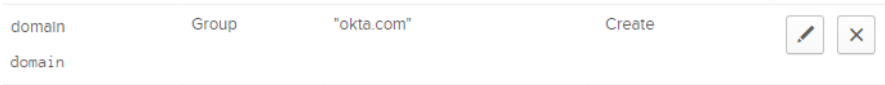
14 Click the **Edit** button.



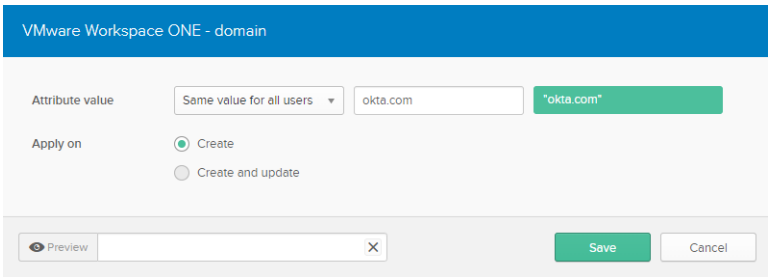
15 Select the **Enable** check boxes for **Create Users**, **Update User Attributes**, and **Deactivate Users**, then click **Save**.



16 Scroll down and edit the **domain** attribute.



17 Edit the domain so that it matches the domain you used when you created the directory in Create a Directory of Type Other in Workspace ONE Access.



18 Click **Save**.

What to do next

SCIM provisioning set up is complete.

Go to the **Assignments** tab in the VMware Workspace ONE application and assign the application to users or groups. When you assign the application to a user, the user is created in Workspace ONE Access. When you remove the application for a user, the user is disabled in Workspace ONE Access.

You can go to the **Push** groups tab in the VMware Workspace ONE application to push groups to Workspace ONE. When you push a group, the group is created in Workspace ONE Access and the group membership is pushed. Members of the group must already be assigned the Workspace ONE Access application.

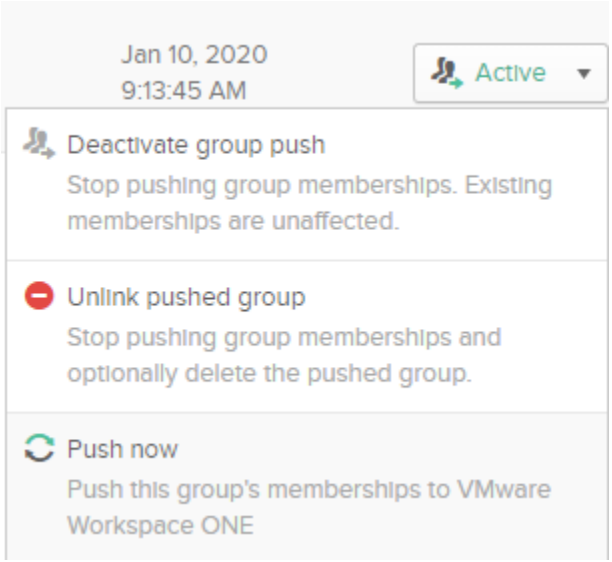
Note Using the same Okta group for assignments and for group push is not currently supported. To maintain consistent group membership between Okta and Workspace ONE Access, you need to create a separate group that is configured to push groups to Workspace ONE Access.

Known Issues with the Okta and Workspace ONE Access SCIM Integration

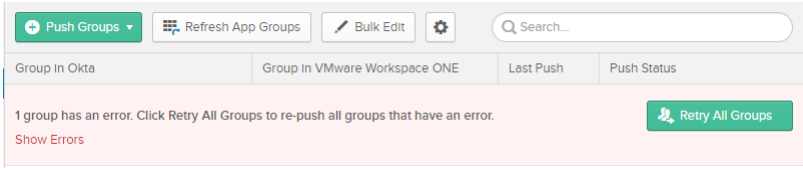
4

The Okta and Workspace ONE Access SCIM integration currently has the following known issues.

Known Issue: When you push groups from Okta to Workspace ONE using the **Push now** command, you might get an error.



Solution: Click the **Retry All Groups** button.



Known Issue: When you delete a user in Okta, the user is disabled in Workspace ONE Access. However, if you recreate the user with the same attributes in Okta again, instead of a new user being created in Workspace ONE Access the old user is updated.

Solution: If you delete a user from Okta, also delete the user from Workspace ONE Access using the SCIM API and from Workspace ONE UEM using the administration console.

To delete the user in Workspace ONE Access, use the following API:

```
DELETE /SAAS/jersey/manager/api/scim/Users/userID
Host: WorkspaceONEAccessTenantFQDN
Authorization: Bearer token
```

WorkspaceONEAccessTenantFQDN is your Workspace ONE Access tenant's fully qualified domain name, such as example.vmwareidentity.com, and *userID* is the user ID that you want to delete.

For example:

```
DELETE https://myaccess.example.com/SAAS/jersey/manager/api/scim/Users/123456
```

Known Issue: User groups created from Okta are associated with the System domain in Workspace ONE Access instead of the actual domain and are not associated with the directory that you created for Okta.

Solution: First, create the group with the correct domain name in Workspace ONE Access manually using the SCIM API, then link the group to the VMware Workspace ONE application in the Okta Admin console.

For detailed information, see the blog post Fixing Group Issues with Okta SCIM for VMware Cloud Services Customers.

Troubleshooting the Okta and Workspace ONE Access SCIM Integration

5

Use this information to troubleshoot some of the common errors that can occur with the Okta and Workspace ONE Access SCIM integration.

- **Error:** "ERRORS REPORTED BY REMOTE SERVER: REQUIRED USER ATTRIBUTES: [DISTINGUISHEDNAME] ARE MISSING."

  Solution: distinguishedName is set as a required attribute in Workspace ONE Access. Deselect the Required check box in the Workspace ONE Access **Identity & Access Management > Setup > User Attributes** page.

- **Error:** "ERRORS REPORTED BY REMOTE SERVER: USER CREATION IS NOT SUPPORTED FOR SPECIFIED DIRECTORY ID."

  Solution: You are attempting to create a user in a directory that is not of type Other. Verify that when you completed the prerequisites you did not use a domain that is used by another directory. It is possible that the domain was used for Just-in-Time (JIT) users. If so, you must create another directory of type Other with a unique domain.

- **Error:** "ERRORS REPORTED BY REMOTE SERVER: USER DOMAIN NAME SPECIFIED FOR THE USER RESOURCE DOESN'T BELONG TO THE DIRECTORY."

  Solution: The domain you configured in the attribute mapping in Okta does not match the domain for the directory created in Workspace ONE Access. Ensure that they match.

- **Error:** AUTOMATIC PROVISIONING OF USER <USERNAME> TO APP VMWARE WORKSPACE ONE FAILED: MATCHING USER NOT FOUND.

  Solution: The **Create Users** and **Deactivate Users** settings are not enabled in the **Provisioning** tab of the VMware Workspace ONE app. Go to the **Provisioning** tab, click **Edit**, and select the **Enable** check box for **Create Users** and **Deactivate Users**.