SCIM Provisioning from Okta to VMware Workspace ONE Access

Modified JUN 2020 JAN 2020 VMware Workspace ONE



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

Copyright $^{\odot}$ 2020 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

- 1 SCIM Provisioning from Okta to VMware Workspace ONE Access 4
- Complete Prerequisites in Workspace ONE Access 6
 Create Remote App Access Client 6
 Generate OAuth Bearer Token 7
 Create a Directory of Type Other in Workspace ONE Access 10
- 3 Configure the VMware Workspace ONE Access Application in Okta 11
- 4 Known Issues with the Okta and Workspace ONE Access SCIM Integration 17
- 5 Troubleshooting the Okta and Workspace ONE Access SCIM Integration 19

SCIM Provisioning from Okta to VMware Workspace ONE Access

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

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
- Generate OAuth Bearer Token
- Create a Directory of Type Other in Workspace ONE Access

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.

Create Client				۵
Access Type*	Service Client Toker	T		
Client ID *	OktaSCIM Characters allowed a	e: alphanumeric (A-Z, a-z, 0-9) period (.), underscore (_),	
Scope*	and hyphen (-) and at admin	sign (@).		
Advanced	▼			
Shared Secret	yrGLhxjv5Ssy0c2hl Generate Shared Sec	Jfeooyn2FVFsaaoZy2hUgVo ret	ch5JZzeC7U	
Issue Refresh Token	Refresh Token			
Token Type	Bearer		¥	
Access Token Time-To-Live (TTL)	3 years	(1 year is 365 days)	•	
Refresh Token Time-To-Live (TTL)	90 days	1 day is 24 hours)	T	
Idle Token Time-to-Live (TTL)	4 days	1 day is 24 hours)	T	
* Required				
			Cancel Add	

- 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.

			,		
٦	YPE				
	Inherit auth from parent			4	
	Inherit auth from parent				
	No Auth				
	API Key				
R	Bearer Token				
	Basic Auth				
	Digest Auth				
	OAuth 1.0				
	OAuth 2.0				
	Hawk Authentication				
	AWS Signature				
	NTLM Authentication [Bet	a]			

- 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.

GET NEW ACCESS TOKEN		×
Token Name	WS1 Prod	
Grant Type	Client Credentials	Ŧ
Access Token URL 🕕	https://doi.org/SAAS/auth/oauthtoken	
Client ID 🚺	OktaSCIM	
Client Secret 🕕	PasteYourSecretKeyHere	
Scope 🚺	admin	
Client Authentication	Send as Basic Auth header	*
	Request Token	

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.

POST • https://	com/SAAS/jersey/manager/api/connectormanagement/dire	ctoryconfigs Send T Save T
Params Authorization Headers (11)	Body Pre-request Script Tests Settings	Cookies Code
Headers 🖘 10 hidden	VALUE	DESCRIPTION *** Buik Edit Presets •
The bearer token appear	S.	
POST • https:// co	om/SAAS/jersey/manager/api/connectormanagement/direc	toryconfigs Send T Save T
Params Authorization • Headers (11)	Body Pre-request Script Tests Settings	Cookies Code
Headers 🧭 Hide auto-generated headers		
KEY	VALUE	DESCRIPTION •••• Bulk Edit Presets •
KEY	value Bearer eyJ0eXAlOijKV1QiL	DESCRIPTION •••• Bulk Edit Presets 🕶
KEY Authorization () Cookie ()	value Bearer eyl0eXAIOiJKV1QiL AWSALB=+GxIFUI29u1N9MX49/1cntFkXyB9O1xiN(DESCRIPTION ···· Bulk Edit Presets • [2] Go to cookies
KEY Authorization Cookie Postman-Token	VALUE Bearer eyj0eXAlOIJKV1QiL AWSALB=+GxIFUIZ9u1N9MX49/1cntFkXyB9O1xiN(<calculated is="" request="" sent="" when=""></calculated>	DESCRIPTION •••• Bulk Edit Presets C Go to cookies
KEY Authorization ③ Cookie ③ Postman-Token ③ Content-Type ④	VALUE Bearer eyJ0eXAIOIJKV1QIL AWSALB=+GxIFUIZ9u1N9MX49/1cntFkXyB9O1xINt <calculated is="" request="" sent="" when=""> text/plain</calculated>	DESCRIPTION •••• Bulk Edit Presets C Go to cookies
KEY Authorization ③ Cookie ④ Postman-Token ⑤ Content-Type ③ Content-Length ⑥	VALUE Bearer eyJ0eXAIOJjKV1QiL AWSALB=+GxIFUIZ9u1N9MX49/1cntFkXyB9O1xiNt <calculated is="" request="" sent="" when=""> text/plain <calculated is="" request="" sent="" when=""></calculated></calculated>	DESCRIPTION •••• Bulk Edit Presets
KEY Authorization ③ Cookie ③ Postman-Token ⑤ Ó Content-Type ③ Content-Length ⑥ Host ⑤	VALUE Bearer eyJ0eXAI0IjKV1QiL AWSALB=+GxiFUIZ9u1N9MX49/1cntFkXyB9O1xIN(<calculated is="" request="" sent="" when=""> text/plain <calculated is="" request="" sent="" when=""> <calculated is="" request="" sent="" when=""> <calculated is="" request="" sent="" when=""></calculated></calculated></calculated></calculated>	DESCRIPTION . Bulk Edit Presets ▼
KEY Authorization ③ Cookle ③ Postman-Token ⑤ Gontent-Type ③ Content-Length ③ Host ③ User-Agent ③	vALUE Bearer eyJ0eXAI0IJKV1QiL AWSALB=+GxIFUI29u1N9MX49/1cntFkXyB9O1xINL <calculated is="" request="" sent="" when=""> text/plain <calculated is="" request="" sent="" when=""> PostmanRuntime/7.24.1</calculated></calculated></calculated></calculated></calculated></calculated></calculated>	DESCRIPTION . Bulk Edit Presets
KEY Authorization ③ Cookie ③ Postman-Token ④ Content-Type ④ Content-Length ④ Host ③ User-Agent ③ Accept ⑤	vALUE Bearer eyJDeXAIOIJKV1QiL AWSALB=+GxiFUi29u1N9MX49/1cntFkXyB9O1xiNL <calculated is="" request="" sent="" when=""> text/plain <calculated is="" request="" sent="" when=""> <calculated is="" request="" sent="" when=""></calculated></calculated></calculated></calculated></calculated></calculated></calculated></calculated></calculated></calculated></calculated>	DESCRIPTION . Bulk Edit Presets
KEY Authorization ① Cookie ② Postman-Token ③ Content-Type ③ Content-Length ③ Host ③ User-Agent ③ Accept ③ Accept ③ Accept ⑤	VALUE Bearer eyJOeXAIOIJKV1QiL AWSALB=+GxiFUI29u1N9MX49/1cntFkXyB9O1xINL <calculated is="" request="" sent="" when=""> text/plain <calculated is="" request="" sent="" when=""> PostmanRuntime/7.24.1 */* gzip, deflate, br</calculated></calculated></calculated></calculated></calculated>	DESCRIPTION . Bulk Edit Presets
KEY Authorization © Cookie © Postman-Token © Content-Type © Content-Length © Host © User-Agent © Accept © Accept © Accept © Connection ©	vALUE Bearer eyj0eXAI0ijKV1QiL AWSALB=+GxIFUI29u1N9MX49/1cntFkXyB9O1xINL <calculated is="" request="" sent="" when=""> text2plain <calculated is="" request="" sent="" when=""> PostmanRuntime/7.24.1 */* gzip, deflate, br keep-alive</calculated></calculated></calculated></calculated></calculated>	DESCRIPTION •••• Bulk Edit Presets •
KEY Authorization ③ Cookie ④ Postman-Token ④ Octent-Type ④ Content-Length ④ Host ④ Viser-Agent ① Accept ⑤ Accept ⑥ Accept ⑥ Connection ③ Content-Type	VALUE Bearer eyl0eXAIOJJKV1QiL AWSALB=+GxIFUIZ9u1N9MX49/1cntFkXyB9O1xINt <calculated is="" request="" sent="" when=""> text/plain <calculated is="" request="" sent="" when=""> postmanRuntime/7.24.1 */* gzip, deflate, br keep-allve application/vnd.vmware.horizon.manager.conned</calculated></calculated></calculated></calculated></calculated></calculated>	DESCRIPTION •••• Bulk Edit Presets •

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.

CATEGORIES			
Featured		Q VMware Workspace ONE	6
API Management Apps CASB Directories and HR Systems Security Applications /PN Private Apps	6 5935 3 12 620 21 1	CATEGORIES Virtual Workspaces Workplace Innovation Platforms Workforce Management Workflow Management Workload Automation	
		INTEGRATIONS	in Apps, Productivity
		Workspace	in Apps, ERP
		VMware Partner Network	in Security Applications
		VMware Horizon View VDI	in Security Applications
		workspace.com	in Apps, Project Manag

6 Click Add.

← Back to Add Application

	VMWare Wo	VMWare Workspace ONE		
vm ware ⁻				
Workspace** ONE**	Overview	Overview		
Add	Workspace ONE is a digital worksp single unified workspace and devic Okta-powered authentication to Wo manage login to Workspace ONE c directory and cloud directory users	ace productivity platform combining UEM, Access, and app virtualization services into a e management service. Integrating Okta via SAML with Workspace ONE allows for vrkspace ONE, which maintains consistent policy and SSO for customers who also atalog apps with Okta. By adding SCIM integration with Okta UD in addition, hybrid will now have full access to the Workspace ONE experience for the first time.		
CATEGORIES	Capabilities	Capabilities		
Apps	Access	Provisioning		
LAST UPDATE 2019-10-15T09:26:29	✓ SAML			

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

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

📫 Add VMWare	Workspace" ONE"	
1 General Settings		
General Settings · R	equired	
		General settings
Application label	VMWare Workspace ONE	All fields are required to add this application unless marked optional.
	This label displays under the app on your home page	
Base URL	https://wmareIdentity.com	
	Enter your Base URL. For example, if you log into: https://acme.vmwareidentity.com, enter: https://acme.vmwareidentity.com	
Application Visibility	Do not display application icon to users	
	Do not display application icon in the Okta Mobile App	
Cancel	Done	

8 Click Done.

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



10 Select the Enable API Integration check box.

← Back to Applications wmware workspace" ONE" VMWa	re Workspace ONE TEST2	
General Sign On Provis	Assignments Push Groups	
SETTINGS Integration	Enable API Integration	Cancel
		Save

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



Access Token

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

SETTINGS		
Integration		Cancel
	VMware Workspace ONE was verified s	uccessfully!
	Enable API integration	
	Enter your VMware Workspace ONE credentials	to enable user import and provisioning features.
	API Token	
		Test API Credentials
		Save

- 13 Click Save.
- 14 Click the Edit button.

Арр		okta -	WITWORD Workspace" ONE"	
)kta				
gration	Provisioning to App			Edit
	Create Linera			Enable
	Create Osers			
	Creates or links a user in VMWare W	orkspace ONE when assignin	g the app to a user in Okta.	
	The default username used to creat	e accounts is set to Okta user	name.	

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

General Sign On	Mobile Provisioning Import Assignments Push Groups
SETTINGS	
То Арр	okta
To Okta	
ntegration	Provisioning to App Cancel
	Create Users Zenable
	Creates or links a user in VMware Workspace ONE when assigning the app to a user in Okta.
	The default username used to create accounts is set to Okta username prefix.
	Update User Attributes Enable Okta updates a user's attributes in VMware Workspace ONE when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in VMware Workspace ONE.
	Deactivate Users Zable
	Deactivates a user's VMware Workspace ONE 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.
	Save

16 Scroll down and edit the domain attribute.

domain	Group	"okta.com"	Create	/ ×
domain				

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.

/mware workspa	ce ONE - domain	
Attribute value	Same value for all users v okta.com	"okta.com"
Apply on	Create	
	Create and update	

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.

🕂 Push Groups 🔻 🗮 Refresh Ap	p Groups 📝 Bulk Edit	Q Search	
Group In Okta	Group In VMware Workspace ONE	Last Push	Push Status
1 group has an error. Click Retry All Grou Show Errors	🤱 Retry All Groups		

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.

5

Troubleshooting the Okta and Workspace ONE Access SCIM Integration

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**.