

VAST Online – SCIM Configuration Guide

Features

The following SCIM provisioning features are supported:

- Create users
- Update user attributes
- Deactivate users

The only support flow is from OKTA to VAST Online.

Requirements

Before enabling SCIM provisioning please ensure that your tenancy has been configured for use with Single Sign On.

Follow this guide for further information:

https://vastonlinereleases.blob.core.windows.net/production/OKTA/VASTOnline_OKTA_Configuration.docx

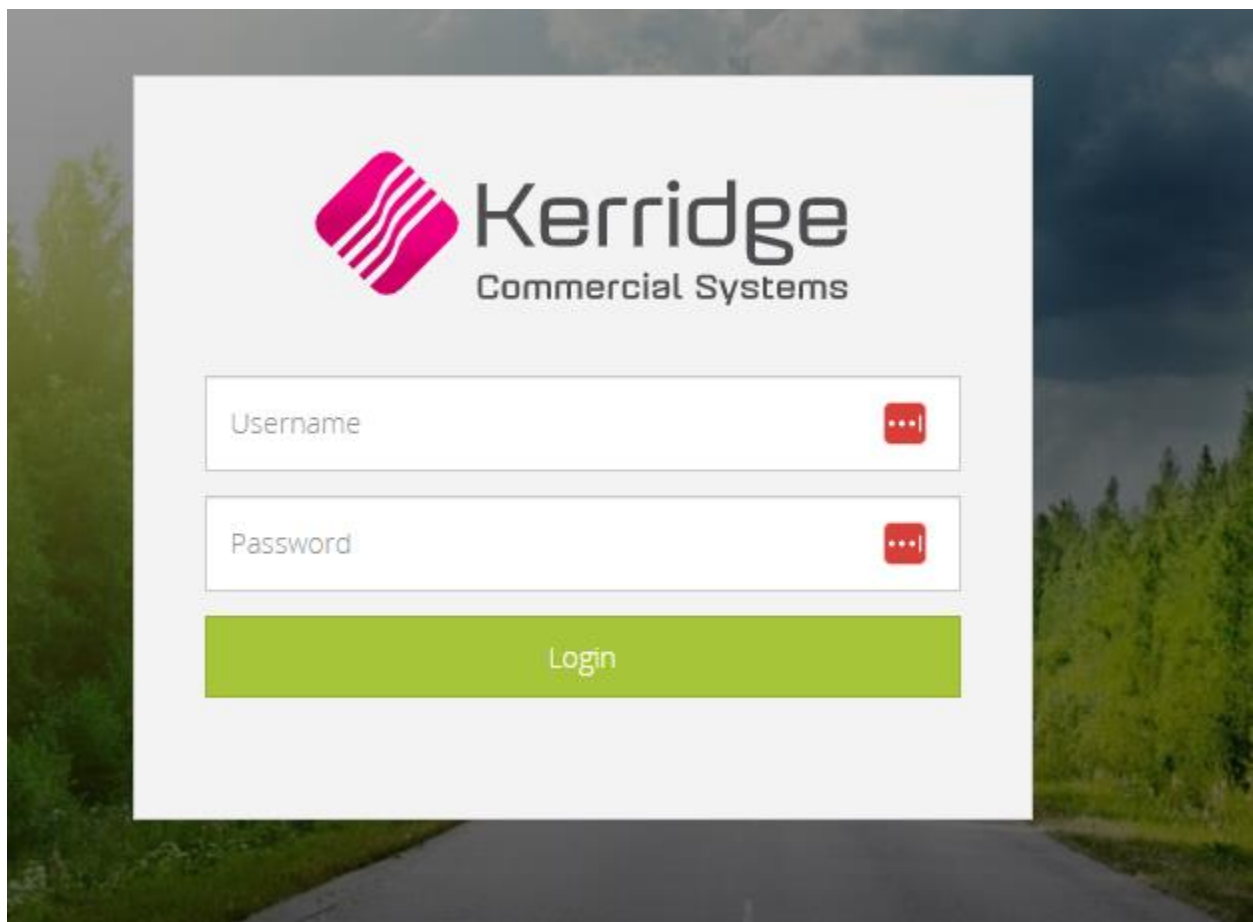
Step-by-Step Configuration Instructions

The VAST Online OKTA integration supports provisioning via SCIM. When enabled the integration supports the provision and status activation of users.

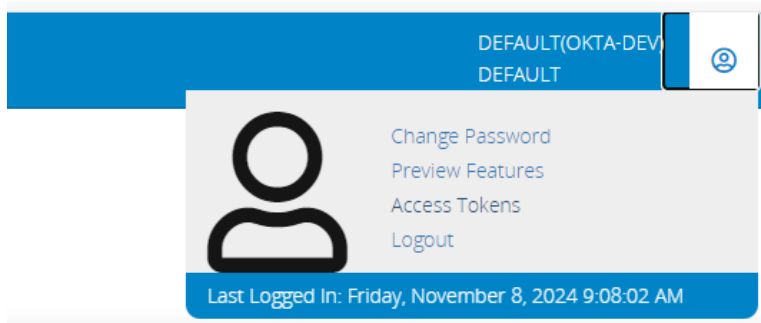
Step1: Generating a SCIM service public access key

To allow OKTA to access SCIM provisioning services within VAST Online a public access token key must be generated first.

From the login screen, login to VAST Online:



When logged in, click on the profile jump menu, and then click “Access Tokens”.



Click “New Token”

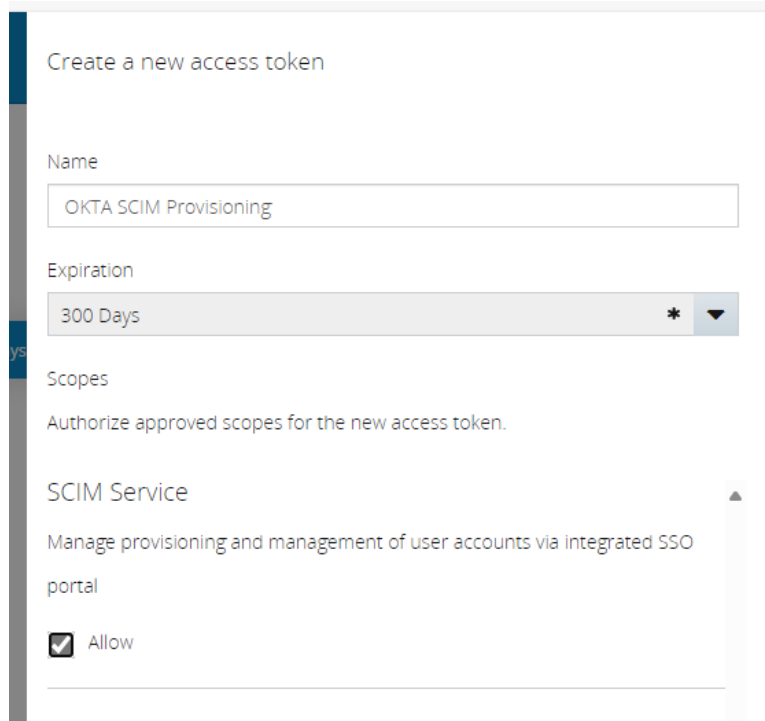
Personal Access Tokens

Security tokens provide access to public api services behind Vast Online.



On the “Create a new access token” slider, enter a useful identifier for the token. Select how long the token should be valid for, and then select the scopes which should be applied.

You should only ever select the minimum scope that is needed. For SCIM just select “Allow” under the SCIM service heading.



The screenshot shows a web interface for creating a new access token. The title is "Create a new access token". There are three main sections: "Name", "Expiration", and "Scopes".

- Name:** A text input field containing "OKTA SCIM Provisioning".
- Expiration:** A dropdown menu showing "300 Days" with a "*" icon and a downward arrow.
- Scopes:** A section titled "SCIM Service" with a description: "Manage provisioning and management of user accounts via integrated SSO portal". Below this, there is a checkbox labeled "Allow" which is checked.

Please note, granting SCIM service services generates an access token that grants the following permissions:

- Read/Write to SCIM
- Read/Write to Users
- Read/Write to Employees

At the time of writing, you must remember to re-generate the access token prior to the token expiring.

Clicking “Create” will create the token. You must copy the token and keep it safe at this point. You should never share this token with anyone else other than for the purpose of configuring OKTA.

Token Created

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJtYW0vbWljcm9zZXJ2aWNlcy5jb2



Warning

The security token must be copied and stored safely now. You will be unable to see this token again, unless you create another token. To store security tokens safely, it's recommended to use a hardware security module (HSM) or an operating system-specific key-store. This can help ensure that sensitive data is protected and secure.

Days

Step 2: Configure SCIM Services in OKTA

Navigate to the VAST Online application integration from within OKTA.

Go to the “Provisioning” tab to configure the integration.

VASTOnline: Configuration Guide

Provisioning Certification: Okta Verified

This provisioning integration is partner-built by VASTOnline

Contact partner support: support@kerridgecs.com, <https://support.kerridgecs.com>

Integration Cancel

Enable API integration

Enter your VASTOnline credentials to enable user import and provisioning features.

API Token

- API Token: Enter the API token generated for the SCIM service.
- Run ‘Test API Credentials’ to ensure successful test.

If the test is successful, you will see the following confirmation.

Integration Cancel

VASTOnline was verified successfully!

Click the ‘Save’ button to ensure any changes are saved.

The 'To App' configuration should be setup like so.

The screenshot displays the 'To App' configuration page in Okta. On the left, a sidebar contains 'Settings', 'To App' (selected), 'To Okta', and 'Integration'. The main content area features a warning message: 'One or more required attributes are not mapped. To prevent provisioning failures, scroll down to VASTOnline Attribute Mappings and set mappings for the attributes that are marked with a warning icon.' Below this is a diagram showing the 'Okta' logo pointing to a box with a red warning icon. The 'Provisioning to App' section includes a 'Cancel' link and three enabled options: 'Create Users', 'Update User Attributes', and 'Deactivate Users'. Each option has a description and an 'Enable' checkbox. A 'Save' button is located at the bottom right.

- Enable provision features you wish to use, suggested options are Create users, Update User Attributes & Deactivate users.

Step 3: Profile Mappings

The standard mappings are used, so in most cases no changes should be needed unless you wish to map them differently from the OKTA side.

The additional fields should be configured like so:

Display Name	Variable Name	External Name	External Namespace	Type
Username	userName	Defaults		
Given name	givenName			
Family name	familyName			
Email	email			
Employee number	employeeNumber			
BranchId	branchId	branchId	urn:ietf:params:scim:schemas:core:2.0:User	string
RoleName	roleName	roleName	urn:ietf:params:scim:schemas:core:2.0:User	string

The “BranchId” points to the default store the user will be provisioned too.

The “RoleName” points to the VAST Online role that the user will be provisioned with. The role should point to its descriptive name.

For example, a user who is a System Administrator will be assigned to a role with the name of “System Administrator Role”.

Step 4: Verify 'Sign-On' configuration

Ensure that the "default username" used to create accounts in Okta is set to "Email":

Credentials Details

Application username format

Email

Update application username on

Create and update

[C Update Now](#)

Password reveal

Allow users to securely see their password
(Recommended)

Troubleshooting and Tips

N/A.