**VAST Online / Okta Configuration**

**Prerequisites**

SSO integration is available within VAST Online version 4.0.12 onwards.

**Supported Features**

The following provisioning features are supported by VAST Online currently:

* SMAL SSO
  + Flows
    - IdP-initiated
    - SP-initiated

**Configuration Steps**

Step 1: Add VAST Online from the OIN

* Sign in to your Okta admin dashboard
* Navigate to Applications -> Applications -> Browse App Catalog C. Search for “VASTOnline” using the search bar and click on the “VASTOnline” app.
* Click “Add Integration”
* Two additional values are required. The authentication service URL is the same as the login URL that you would have been provided for your tenancy. I.e. if its <https://dealers.vol.mamscloud.com/auth>, then enter the value dealers.vol.mamscloud.com/auth.
* The tenant id is provided as part of single sign on configuration page. See Stage 2 (table) on how to access it.

Step 2: VAST Online Configuration

SSO config screen accessed via -

[{baseurl}/vastweb#/security/singlesignon](#/security/singlesignon)



1. Enable SSO.
2. Enter the callback URL.
3. Enter the issuer.
4. Enter Single Sign-on URL.
5. Enter Single Sign-on Entity ID.
6. Enter the X.509 certificate.
7. Enter the administrator who is still able to access VAST Online directly (without being redirected to Okta).
8. Click save.

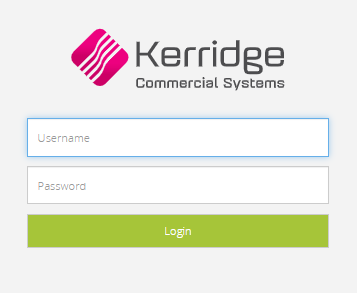
|  |  |  |
| --- | --- | --- |
| Field Name | Value | Source |
| Callback URL | {base url}/authservice/saml/acs | VOL |
| Issuer | See generated Metadata | Okta |
| Single Sign-on URL | See generated Metadata | Okta |
| Single Sign-on Entity ID | Value is pre-generated on the single sign configuration page. This is known as the tenant Id and should be provided as the tenant id variable into OKTA. | VOL |
| X.509 | See generated Metadata | Okta |
| Sign Sign On Bypass User |  | VOL |

**Generated Metadata:**

The values listed above can be found at the VASTOnline Okta integration under the Sign-On tab inside SMAL 2.0 section, under the Metadata details section.

**SP-Initiated SSO**

With SSO enabled within Vast Online it is still possible for a user to instigate the login process via the VAST Online login:



The user should enter their username.

Note users will not have a valid password with VAST Online so the password has no relevance and can be ignored.

Once the user has entered their username then clicked login they will be redirected to Okta where they will be instructed to enter their Okta credentials.

**Troubleshoot**

If you have any questions or experience any problems with your VASTOnline Okta integration, please contact support via support@kerridgecs.com