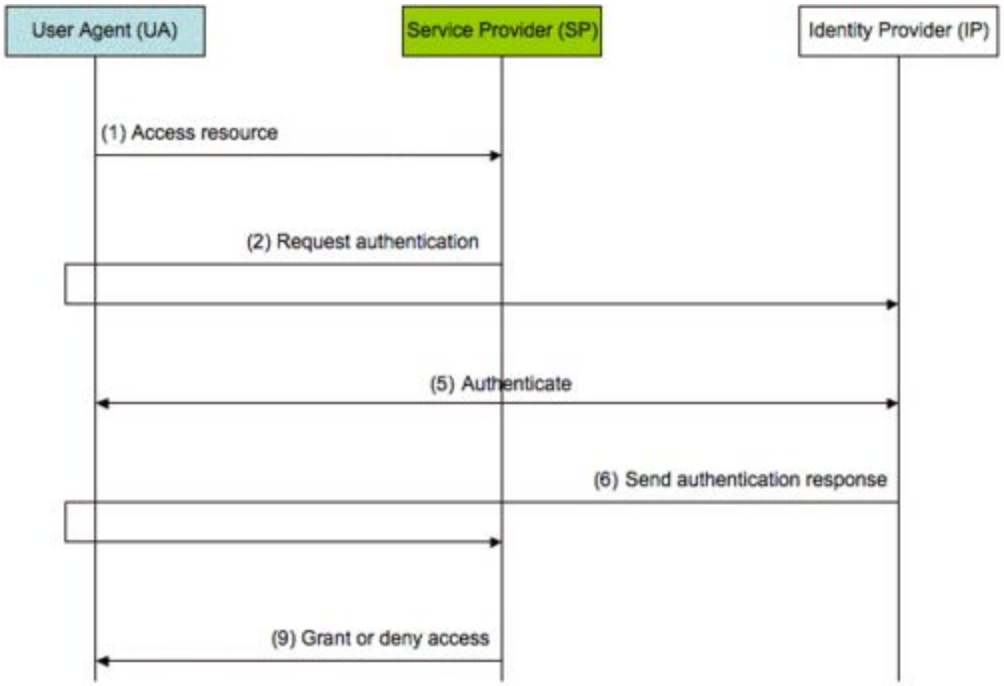
Via TRM SSO Setup Guide

Overview

Via TRM supports SAML 2.0 for single sign-on (SSO). When a user visits *Via* TRM's website and attempts to sign in using SSO, they will be transferred to the University's website (identity provider) and be asked for their credentials. Upon successful authentication, they will be redirected back to *Via* TRM's website (service provider) as a traveler or admin.

The communication between the identity provider and service provider is done through an exchange of digitally signed XML documents.



Requirements

Via Metadata

The *Via* metadata is available at:

https://<your-via-subdomain>.via-trm.com/sso/metadata

Client Metadata

Please provide your metadata to your *Via* account manager.

NOTE: When provided a URL endpoint based metadata, *Via* TRM will cache this for about a half a day. *Via* will automatically fetch a new version once the cache expires. For file-based metadata, please send *Via* the updated metadata file whenever there are changes.

SAML Response Attributes

Please include the following in the attributes in the SSO assertions:

- Email address
- Unique identifier for the person (this is used for SIS synchronization - student ID or other unique identifier)
- Role (i.e. Faculty, Admin, Student, Staff, Graduate, etc.)

Role Mapping

Roles in Via are mapped to the role returned in the SSO assertions in coordination with your Via integration project manager. A typical mapping is below to use as a starting point. Your mappings may vary.

SAML Role Attribute Value	Account exists in Via?	Role in Via	Notes
student	Yes or No	Traveler	Traveler is automatically created in Via when the account does not exist
faculty	Yes	Assigned admin role in Via	
staff	Yes	Assigned admin role in Via	
faculty	No	Access Denied	
staff	No	Access Denied	
<anything else>	n/a	Access Denied	

Test Users

Please provide *Via* TRM with 5 test users for testing the SSO integrations (1 admin, 4 students)

These should be fake user accounts with fake data. They should not contain real user data.

The test accounts must authenticate properly with the client staging SSO service and ideally also exist in the client SIS. *Via* TRM will use the ID provided during SSO authentication to request data from the SIS (if available).

Setup SSO Checklist

- ❑ (Via) Provide client with metadata
- ❑ (Via) Setup SSO on the Via side
- ❑ (Client) Setup SSO and and authorize Via using the Via metadata
- ❑ (Client) Provide Via with 5 test users (1 admin, 4 students)
- ❑ (Via) Test SSO