Automatic User Provisioning via SCIM

Last Modified on 05/05/2021 12:45 pm EDT

SCIM (v 2.0), or the System for Cross-domain Identity Management specification, is an open standard designed to manage user identity information. The goal of SCIM is to securely automate the exchange of user identity data between your company's cloud applications and service providers, such as UNIFI applications. More information on SCIM can be found here.

Supported SCIM functionality

- Creation, modification, and deletion of users (GET, POST, PUT, PATCH, DELETE methods)
- Creation, modification, and deletion of user groups including the memberships (GET, POST, PUT, PATCH, DELETE methods)
- Querying Schemas, ResourceTypes, ServiceProviderConfig information.
- Querying users by ID, Username (email), ExternalID, and user groups by DisplayName.
- SCIM Requests authentication and authorization via bearer token.

Prerequisites

- A user account in UNIFI with Admin permissions for the organization
- A user account in your Identity Provider with Admin permissions for the organization
- Your Identity provider must support SCIM user & group provisioning.
- Single Sign-On (SSO) for your Identity Provider must be configured.

SCIM configuration tutorials for major Identity Providers

- Microsoft Azure
- Okta
- OneLogin
    - Under the **SCIM Base Url**, put
        - https://licensing.inviewlabs.com/api/scim/ for SCIM v.1.1
        - https://licensing.inviewcloud.com/api/scim/v2/ for SCIM v2.0