API Tab Configuration

Introduction

Use this guide to configure the API tab in the Web Admin for each SecureAuth IdP realm. This tab includes options for generating API credentials and e nabling / disabling specific API functionality.

SecureAuth APIs use GET and POST / PUT HTTP requests in adherence with RESTful programming best practices. These endpoints enable secure end-user Authentication and Identity Management (IdM) operations within the context of custom software applications. The Login for Endpoints API lets end-users log on Windows / Mac workstations on the network using a valid Multi-Factor Authentication method.

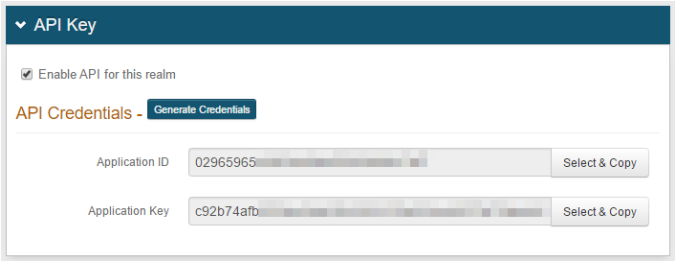
See the following guides for more information and to configure pertinent API endpoints:

- Authentication API Guide
- Identity Management API Guide
- Login for Endpoints Configuration Guide

Prerequisites

Create a **New Realm** for the target resource on which the configuration settings apply

API



1. Check **Enable API for this realm** to enable the use of SecureAuth IdP APIs on this realm

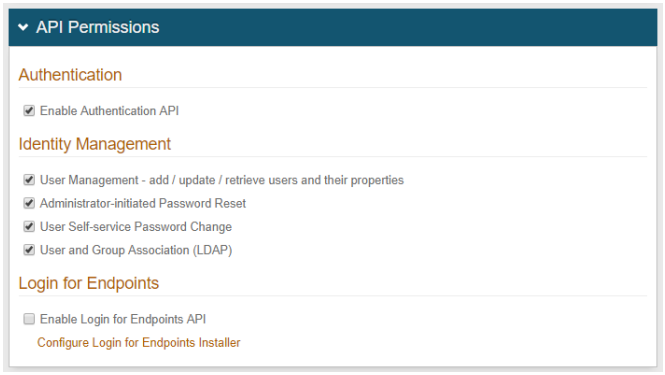
    This option acts as a global on / off switch for APIs on the realm, but the specific options in the **API Permissions** section below must also be checked in order to use Authentication, IdM, and Login for Endpoints APIs

If the **Enable API for this realm** option is selected but none of the **API Permissions** options below are checked, then the end-user can only access the **dfp** and **js** endpoints (see **Authentication API Guide**)

2. Under **API Credentials** click **Generate Credentials** to generate a unique Application ID and Application Key for the realm

    These values are used as a means of communication to the SecureAuth API endpoints and are included in the application headers to make calls to the endpoints

API Permissions



Authentication

3. Check **Enable Authentication API** to enable the **Authentication API** endpoints

4. Enable either **Identity Management** or **Login for Endpoints** API configuration options defined below

Identity Management

To configure the Identity Management (IdM) API, enable the option(s) to be used:

- Check **User Management - add / update / retrieve users and their properties** to enable to following user management capabilities:
  - Retrieve User Profile
  - Update User Profile
  - Create User
- Check **Administrator-initiated Password Reset** to enable admins to send an end-user a new password requested via an application
- Check **User Self-service Password Change** to enable end-users to change their own password, which requires the current password before a password change is allowed
- Check **User and Group Association (LDAP)** to enable userID and groupID associations to be made within an LDAP directory

  Four association methods are available with this option:

  - Single user to single group
  - Single user to multiple groups
  - Single group to single user
  - Single group to multiple users

See the **Identity Management API Guide** for more information on configuring Identity Management APIs

Login for Endpoints

To configure the Login for Endpoints API, check **Enable Login for Endpoints API** and then click **Configure Login for Endpoints Installer**

Use the **Login for Endpoints Installer Configuration** page to configure the API endpoint for Windows or Mac workstations on the network which end-users can access via a valid Multi-Factor Authentication method

See **Login for Endpoints Configuration Guide** for more information on configuring the Login for Endpoints API