SecureAuth IdP 8.2.x Authentication

SecureAuth IdP Authentication

SecureAuth IdP excels in authentication solutions, ranging from various registration methods to validate a user's identity beyond username and password, to the analysis of a user's login attempt based on IP Address reputation, group memberships, geo-location, and other criteria. By being the middle man between users and protected resources, SecureAuth IdP works to mitigate unauthorized access by placing layers of security throughout the workflow.

Each SecureAuth IdP **realm** can be configured uniquely to ensure that each resource has the right balance of protection and user-friendliness to secure without burdening users. Choose from various workflow options, and combine them with other elements, such as group restrictions, tokens, begin sites, redirect options, and registration methods' enablement to create the best process to access sensitive, corporate data.

Enable 2-Factor Authentication

2-Factor Authentication is enabled in all SecureAuth IdP realms out-of-the-box, so no steps are necessary; however, for reference, to enable 2-Factor Authentication in a realm, utilize the **Workflow** tab in the web admin (see the configuration guide in the list below) and locate the **Authentication Mode** field, which dictates the type of workflow that is employed for login. Select any of the options that include "2nd factor" or "Reg Code" (the **Standard Workflow** is selected by default).

The **Voice**, **SMS / Voice**, and **Email OTP** registration methods are also enabled out-of-the-box. These require profile mapping completion in the **Data** tab (refer to **Identity Management** for more information on directory integrations), but otherwise are ready to be used. Any other registration method(s) can be employed in the **Registration Methods** tab (see the configuration guide in the list below) by selecting "Enabled" in the option's section, and then providing any additional, required configuration.

Adaptive Authentication

SecureAuth's Adaptive Authentication analyzes the user's login attempt and then responds automatically to allow access to authorized users, or to stop or further challenge potentially unauthorized users. Adaptive Authentication analyzes the user's IP Address and any threat data associated to it, the country of origin, the user's group membership information, and geo-location, which compares the time and location of the current login attempt with the last successful access time and location to validate whether it's physically possible for the user to travel to the current location in the time since the last access.

Each Adaptive Authentication criterion can be configured independently from the others (in the **Workflow** tab – see configuration guide(s) in the list below) with distinct **Failure Actions** to hard stop the login process, redirect the user to another realm, step up authentication requirements, continue with the configured authentication requirements, step down authentication requirements, or send them directly to the resource.

Adaptive Authentication is an additional layer placed between the user and the protected resource, occurring before 2-Factor Authentication to allow immediate response to any unauthorized access attempts.

Authentication API

The Authentication API enables customers to leverage SecureAuth IdP's 2-Factor Authentication and Adaptive Authentication abilities into their own, custom applications. By making calls to the API, SecureAuth IdP can validate users and their identities, analyze the login attempt, and respond with suggested actions without requiring the user to leave the application's interface.

Depending on the features being used via API calls, little SecureAuth IdP Web Admin configuration is required. Refer to the configuration guide below for more information and for exact endpoints, parameters, and response examples.

Registration Methods

SecureAuth IdP offers numerous 2-Factor Authentication methods that can be employed in any SecureAuth IdP realm. These include one-time password (OTP) delivery via phone calls, text messages, emails, and PUSH Notifications; time-based one-time passcodes (TOTP) via mobile applications, desktop client applications, browser extensions, and third-party applications; hard token support; certificate-based authentication; social and federated identities; and others.

Registration methods can be enabled and configured in the **Registration Methods** tab (see configuration guide in the list below), and **Device / Browser Fingerprinting**, which is a process in which SecureAuth IdP pulls unique characteristics from a device or browser and creates a score that is then compared to the same characteristics in subsequent logins as authenticates the user upon a successful match, is configured on the **Workflow** tab (see configuration guide in the list below).

Configuration Guides

Workflow Tab Configuration – configure SecureAuth IdP realms with distinct workflow options to increase security or enhance user experience

Refer to **Sample Workflow Configuration Guides** for configuration tips

- **Begin Site Configuration Guides** – enable the use of pre-authentication sites as required by the integration
- **Adaptive Authentication Configuration Guide (version 8.2)** – enhance realm security with SecureAuth's Adaptive Authentication, which utilizes IP Address / Country Restriction, User / Group Restriction, Geo-velocity Restriction, and IP Reputation and Threat Detection services
- **Device / Browser Fingerprinting - Heuristic-based Authentication** – maintain security and improve the user experience with SecureAuth's persistent token method that employs the device / browser recognition as the second factor of authentication
- **SAML Multi-tenant Consumer Configuration Guide** and **SAML Attribute Consumption Configuration Guide** – integrate third-party Identity Providers with SecureAuth IdP to enable SAML consumption and attribute passing to the post-authentication destination

Registration Methods Tab Configuration – configure SecureAuth IdP realms to enable specific registration methods to restrict or increase the user's options to access the post-authentication destination

- **Mobile Login Requests (Push and Push-to-Accept) Configuration Guide** – improve user experience by enabling Push Notification, which sends a notification to the user's pre-enrolled mobile device for instant OTP retrieval; and Push-to-Accept, which sends an Accept or Deny request through the **Authenticate App**
- **Authentication API Guide** – enable 2-Factor Authentication, Adaptive Authentication, and Digital Fingerprinting in a custom application's interface
- **Knowledge-based Authentication (KBA / KBQ) as 2-Factor Authentication Method Configuration Guide** – configure realms to accept knowledge-based answers for 2-Factor Authentication
- **Second Help Desk Registration Method Configuration Guide** – configure the Help Desk 2-Factor Authentication method settings, including utilizing more than one Help Desk option
- **Time-based Passcodes (OATH) Registration Method for 2-Factor Authentication** – enable time-based passcodes for 2-Factor Authentication via **SecureAuth Apps**

PIN OTP Page Configuration Guide – configure the PIN OTP page, which displays a one-time passcode to use for 2-Factor Authentication