

Adaptive Authentication API endpoints

Introduction

This guide explains how to configure the SecureAuth IdP Adaptive Authentication API endpoints for Adaptive Authentication workflows which analyze end-user login activity and effectively mitigate attacks from unauthorized users attempting to gain access to protected resources.

Adaptive Authentication definitions

What's new in SecureAuth IdP version 9.3

- [Advanced adaptive capability powered by machine learning](#), available with the Prevent Threat Service license, enables machine learning for user risk score analysis.
- Risk Ranges can be inverted to have a high score indicate a good user, and a low score indicate a risky user.

Previous Adaptive Authentication API guide

See [Adaptive Authentication API Guide](#) for the SecureAuth IdP v9.1 and v9.2 guide.

POST endpoints

The two Adaptive Authentication API endpoints are /adaptauth and /accesshistory which use the POST method.

/adaptauth

This endpoint uses the POST method to enable SecureAuth IdP Adaptive Authentication to analyze an end-user's profile, group, IP address, country, geo-velocity, and any risks detected by threat intelligence data.

HTTP Method	URI	Example	SecureAuth IdP version support
POST	/api/v1/adaptauth	https://secureauth.company.com/secureauth2/api/v1/adaptauth	v9.1+

Definitions

The API utilizes the information configured in the **Adaptive Authentication / Workflow** section of the SecureAuth IdP Web Admin.

Functions

SecureAuth IdP returns a response that contains these functions:

Function	Description
Status	Configured Failure Action
Realm Workflow	Workflow configured in the Web Admin
Suggested Action	Suggested next step to take based on the configurations

Status function and failure action

<pre>{ "user_id": "<USERNAME>", "parameters": { "ip_address": "<IP ADDRESS>" } }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_2ndfactor_password": "username_2ndfactor_password", "suggested_action": "suggested_action", "2ndfactor_password": "2ndfactor_password", "status": "Continue", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_2ndfactor_password": "username_2ndfactor_password", "suggested_action": "password", "2ndfactor_password": "password", "status": "SkipTwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_2ndfactor_password": "password", "suggested_action": "password", "2ndfactor_password": "password", "status": "TwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_2ndfactor_password": "password", "suggested_action": "none", "2ndfactor_password": "password", "status": "Authenticate", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_2ndfactor_password": "password", "suggested_action": "stop", "2ndfactor_password": "password", "status": "HardStop", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_2ndfactor_password": "password", "suggested_action": "redirect", "2ndfactor_password": "password", "status": "IPRedirect", "message": "" }</pre>	<pre>{ "status": "disabled", "message": "Please enable the Analyze Engine within your SecureAuth realm." }</pre>
<p>Example:</p> <pre>{ "user_id": "jsmith", "parameters": { "ip_address": "111.222.33.44" } }</pre>							

The IP Address is not required if only performing **user / group restriction**; otherwise, it is required for all other functionality

<pre>{ "realm_workflow": "realm_workflow", "username_password": "username_password", "suggested_action": "suggested_action", "password": "password", "status": "Continue", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_password": "username_password", "suggested_action": "suggested_action", "password": "password", "status": "SkipTwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_password": "username_password", "suggested_action": "suggested_action", "password": "password", "status": "TwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_password": "username_password", "suggested_action": "suggested_action", "password": "password", "status": "Authenticate", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_password": "username_password", "suggested_action": "suggested_action", "password": "password", "status": "HardStop", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username_password": "username_password", "suggested_action": "suggested_action", "password": "password", "status": "Redirect", "message": "" }</pre>
--	---	---	--	--	--

<pre>{ "realm_workflow": "2ndfactor", "2ndfactor": "2ndfactor", "suggested_action": "2ndfactor", "2ndfactor": "SkipTwoFactor", "status": "Continue", "message": "" }</pre>	<pre>{ "realm_workflow": "2ndfactor", "suggested_action": "none", "status": "SkipTwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "2ndfactor", "suggested_action": "2ndfactor", "status": "TwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "2ndfactor", "suggested_action": "none", "status": "Authenticate", "message": "" }</pre>	<pre>{ "realm_workflow": "2ndfactor", "suggested_action": "stop", "status": "HardStop", "message": "" }</pre>	<pre>{ "realm_workflow": "2ndfactor", "suggested_action": "redirect", "status": "IPRedirect", "message": "" }</pre>
--	--	---	---	---	---

<pre>{ "realm_workflow": "realm_workflow", "usernamepassword_2ndfactor": "usernamepassword_2ndfactor", "suggested_action": "none", "2ndfactor": "SkipTwoFactor", "status": "Continue", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "usernamepassword_2ndfactor": "usernamepassword_2ndfactor", "suggested_action": "none", "2ndfactor": "SkipTwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "usernamepassword_2ndfactor": "usernamepassword_2ndfactor", "suggested_action": "2ndfactor", "status": "TwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "usernamepassword_2ndfactor": "usernamepassword_2ndfactor", "suggested_action": "none", "status": "Authenticate", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "usernamepassword_2ndfactor": "usernamepassword_2ndfactor", "suggested_action": "stop", "status": "HardStop", "message": "https://example.com", "status": "IPRedirect", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "usernamepassword_2ndfactor": "usernamepassword_2ndfactor", "suggested_action": "suggested_action", "status": "redirect", "message": "https://example.com", "status": "IPRedirect", "message": "" }</pre>
--	--	--	--	--	--

<pre>{ "realm_workflow": "realm_workflow", "username": "username", "suggested_action": "none", "status": "Continue", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username": "username", "suggested_action": "none", "status": "SkipTwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username": "username", "suggested_action": "2ndfactor", "status": "TwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username": "username", "suggested_action": "none", "status": "Authenticate", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username": "username", "suggested_action": "stop", "status": "HardStop", "message": "https://example.com", "status": "IPRedirect", "message": "" }</pre>	<pre>{ "realm_workflow": "realm_workflow", "username": "username", "suggested_action": "stop", "status": "HardStop", "message": "https://example.com", "status": "IPRedirect", "message": "" }</pre>
--	---	--	--	--	--

<pre>{ "realm_workflow": "persistent_token", "suggested_action": "none", "status": "Continue", "message": "" }</pre>	<pre>{ "realm_workflow": "persistent_token", "suggested_action": "none", "status": "Continue", "message": "" }</pre>	<pre>{ "realm_workflow": "persistent_token", "suggested_action": "2ndfactor", "status": "TwoFactor", "message": "" }</pre>	<pre>{ "realm_workflow": "persistent_token", "suggested_action": "none", "status": "Authenticate", "message": "" }</pre>	<pre>{ "realm_workflow": "persistent_token", "suggested_action": "stop", "status": "HardStop", "message": "" }</pre>	<pre>{ "realm_workflow": "persistent_token", "suggested_action": "redirect", "status": "IPRedirect", "message": "" }</pre>
--	--	--	--	--	--

/accesshistory

This endpoint uses the POST method to create an end-user access history for geo-velocity calculations. Once the end-user is authenticated, the information is posted to the endpoint, and a new entry is created and stored in the end-user profile. On the next login attempt, SecureAuth IdP uses the stored information to validate whether the distance traveled from the previous login to the current attempt is feasible.

HTTP Method	URI	Example	SecureAuth IdP version support
POST	/api/v1/accesshistory	https://secureauth.company.com/secureauth2/api/v1/accesshistory	v9.1+

POST endpoint JSON parameters and response examples

JSON Parameters	Success Response	Failure / Error Response
------------------------	-------------------------	---------------------------------

```
{
  "user_id":
"<USERNAME>",
  "ip_address": "<IP
ADDRESS>"
}
```

Example:

```
{
  "user_id": "jsmith",
  "ip_address":
"111.222.33.44"
}
```

```
{
  "status": "valid",
  "message": "Access History request has
been processed."
}
```

```
{
  "status": "invalid",
  "message": "Access History was
not saved."
}
```

Resources

[Adaptive Authentication configuration](#)

[API configuration](#)

[Authentication API configuration](#)