

# Adaptive Authentication tab configuration

To implement adaptive authentication risk checks in SecureAuth IdP, make the following configuration settings on the Adaptive Authentication tab.

1. Go to the **Adaptive Authentication** tab.
2. In the **Adaptive Authentication** section, set the following:

<b>Service Disruption Handling</b>	<p>When there is a service disruption to the SecureAuth Cloud Services, this impacts the ability of SecureAuth IdP to process adaptive authentication risk checks and provide secure authentication login methods to end users.</p> <p>Select the risk check action to authenticate the end user.</p> <p>For more information about the actions to take, see the <a href="#">risk check action</a> definitions.</p>
<b>IPv6 Handling</b>	<p>When an IPv6 address is detected, to which SecureAuth IdP cannot process, this impacts the ability of SecureAuth IdP to process adaptive authentication risk checks and provide secure authentication login methods to end users.</p> <p>Select the risk check action to authenticate the end user.</p> <p>For more information about the actions to take, see the <a href="#">risk check action</a> definitions.</p>
<p>The default selection (<b>Require two-factor authentication</b>) requires end users to use a two-factor authentication method which does not involve SecureAuth Cloud Services such as: email, knowledge-based answers, HID hard tokens (including YubiKey devices), or timed passcodes from a desktop or mobile app. These two-factor authentication methods must be configured on this realm.</p>	
<b>Factor Analysis</b>	<p>List includes all enabled adaptive authentication risk checks factors.</p> <p>The list is in order by processing sequence; you can <b>drag and drop</b> selections to reorder the processing sequence.</p>

Adaptive Authentication

### Service Disruption Handling

Configure the action IdP will take in the rare occurrence that SecureAuth Cloud Services are unavailable and IdP is unable to complete Adaptive Authentication.

Service Disruption Action:

### IPv6 Handling

IdP ignores the Adaptive Authentication setting if it detects an IPv6 address. Configure the action IdP will take when encountering IPv6 addresses.

IPv6 Action:

### Factor Analysis

Drag and drop to sort the Adaptive Authentication factors from first (top) to last (bottom). Only enabled factors will be shown.

- ↑ User Risk
- ↑ IP / Country Restriction
- ↑ SecureAuth Threat Service
- ↑ User / Group Restriction
- ↑ Geo-velocity

3. In the **User Risk** section, move the slider to **Enabled** for the User Risk analysis feature.
4. Click **Add User Risk Score Provider** or **edit** an existing user risk score provider.
  - To use and configure the SecureAuth User Risk solution, see [SecureAuth User Risk score provider configuration](#)
  - To add and configure the Exabeam third-party user risk solution, see [Connect Exabeam UEBA to SecureAuth IdP](#)

- To add and configure the SailPoint third-party user risk solution, see [Connect SailPoint IdentityIQ to SecureAuth IdP](#)

**▼ User Risk**

Enabled

**User Risk Score Providers** Add User Risk Score Provider

	Low	Medium	High	
<input checked="" type="checkbox"/> SecureAuth User Risk	0 to 49	50 to 59	60 to 100	<a href="#">edit</a>
<input type="checkbox"/> Sailpoint	5 to 199	200 to 299	300 to 1000	<a href="#">edit</a>
<input type="checkbox"/> Exabeam	5 to 99	100 to 149	150 to 300	<a href="#">edit</a>

**User Risk Score Actions**

IdP requests all enabled scores each time Adaptive Authentication runs. The highest risk result determines which of these actions Adaptive Authentication will take.

High Risk	Refuse authentication request	▼	
Medium Risk	Redirect to realm or URL	▼	https://company.verification.com
Low Risk	Skip to post-authentication	▼	
Score Unavailable	Continue Adaptive Authentication	▼	

5. On the risk ranges configuration page, set the following:

**R  
i  
s  
k  
R  
a  
n  
g  
e  
s**

Configure the risk ranges for **Minimum**, **Medium**, **High**, and **Maximum** risk scores.

By default, a low score indicates a good user, and a high score indicates a risky user.

Alternatively, you can set the risk ranges in reverse order by moving the slider to enable **Use Inverted Risk Ranges**.

With inverted risk ranges, a low score indicates a risky user, and a high score indicates a good user.

Image example of inverted risk ranges

### New Risk Provider ✕

#### Risk Ranges Use Inverted Risk Ranges

Maximum

High

Medium

Minimum

Enter the minimum and maximum possible values for this risk score, and set the threshold score for each risk range.

#### Connection Settings

Risk Score Provider Name

Base URL

Get Profile Relative URL  Use {username} for username

Authentication Method  ▼

Username

Password

Risk Score User Identifier  ▼

Risk Score JSON Path

Risk Score Provider Name

Set the descriptive name for the risk provider.

Base URL

Set the base URL of the risk provider instance in this format: https://services.company.com:59.

Get Profile Relative URL

Set the endpoint of the REST API provider in this format: /api/user/{username}/info.  
Insert the {username} variable in the position the endpoint expects the userID to be in the string.

Authentication Method

Set the authentication method supported by the REST service. Options are:

- Basic
- OAuth
- Cookie

Username

Set the username of the risk provider service account to which it has access to retrieve user profile information.

Password

Provide the password associated with the Username.

Risk Score User Identifier

Set the target user ID in the format to which the user risk provider expects to identify end users. In most cases, it is the same value as the default **Authenticated ID**. In other cases, the user risk provider might use a different user ID; for example, the end user logs in with a sAMAccountName and the user risk provider uses an email address as the user identifier.

To use another user identifier, you must map that field to a property in the Data tab. Then, from the **Risk Score User Identifier** list, select the Property.

For example, on the **Data** tab, in the Profile fields section, Email 1 field is mapped as a Default Provider source with a field entry of mail. So, for the **Risk Score User Identifier** field, you would select **Email 1**.

Data tab mapping example

▼ Profile Fields

Property	Source	Field	Data Format	Writable
Groups	<a href="#">Default Provider</a>	memberOf		<input type="checkbox"/>
First Name	<a href="#">Default Provider</a>	givenName		<input type="checkbox"/>
Last Name	<a href="#">Default Provider</a>	sn		<input type="checkbox"/>
Phone 1	<a href="#">Default Provider</a>	telephoneNumber		<input type="checkbox"/>
Phone 2	<a href="#">Default Provider</a>	mobile		<input type="checkbox"/>
Phone 3	<a href="#">Default Provider</a>			<input type="checkbox"/>
Phone 4	<a href="#">Default Provider</a>			<input type="checkbox"/>
Email 1	<a href="#">Default Provider</a>	mail		<input type="checkbox"/>
Email 2	<a href="#">Default Provider</a>			<input type="checkbox"/>

**Risk Score JSON Path** Set the risk score JSON path values used to parse the JSON string returned to SecureAuth IdP and to extract the numeric score value from it following table for example JSON path values.

Risk Score JSON path	Example JSON response
{userInfo}{riskScore}	<pre>{   "status": true,   "user": "rfobber",   "userInfo": {     "riskScore": 90,   }, }</pre>
{risk_score}	<pre>{   "status": found,   "userID": "rfobber",   "risk_score": 0 }</pre>

New Risk Provider ✕

### Risk Ranges

Use Inverted Risk Ranges

Enter the minimum and maximum possible values for this risk score, and set the threshold score for each risk range.

### Connection Settings

Risk Score Provider Name

Base URL

Get Profile Relative URL 
Use {username} for username

Authentication Method

Username

Password

Risk Score User Identifier

Risk Score JSON Path

6. **Save** the user risk configuration.
7. Under **User Risk Score Actions**, for each risk range (**High**, **Medium**, **Low**, and **Score Unavailable**), select the adaptive authentication action SecureAuth IdP takes when the user risk score falls within the specified range. For more information about the actions and its descriptions, see the [risk check action](#) definitions. The **Score Unavailable** risk score can occur when the user is not found in the data source or does not have an assigned risk score in the data source.

If the SecureAuth IdP is unable to communicate with the data source, see the Knowledge base article [Unable to Communicate with the User Risk Adaptive Authentication Data Provider](#) for more information.

### ▼ User Risk

Enabled

#### User Risk Score Providers [Add User Risk Score Provider](#)

	Low	Medium	High	
<input checked="" type="checkbox"/> SecureAuth User Risk	0 to 49	50 to 59	60 to 100	<a href="#">edit</a>
<input type="checkbox"/> Sailpoint	5 to 199	200 to 299	300 to 1000	<a href="#">edit</a>
<input type="checkbox"/> Exabeam	5 to 99	100 to 149	150 to 300	<a href="#">edit</a>

#### User Risk Score Actions

IdP requests all enabled scores each time Adaptive Authentication runs. The highest risk result determines which of these actions Adaptive Authentication will take.

High Risk: [Refuse authentication request](#)

Medium Risk: [Redirect to realm or URL](#)

Low Risk: [Skip to post-authentication](#)

Score Unavailable: [Continue Adaptive Authentication](#)

8. **Save** your changes.