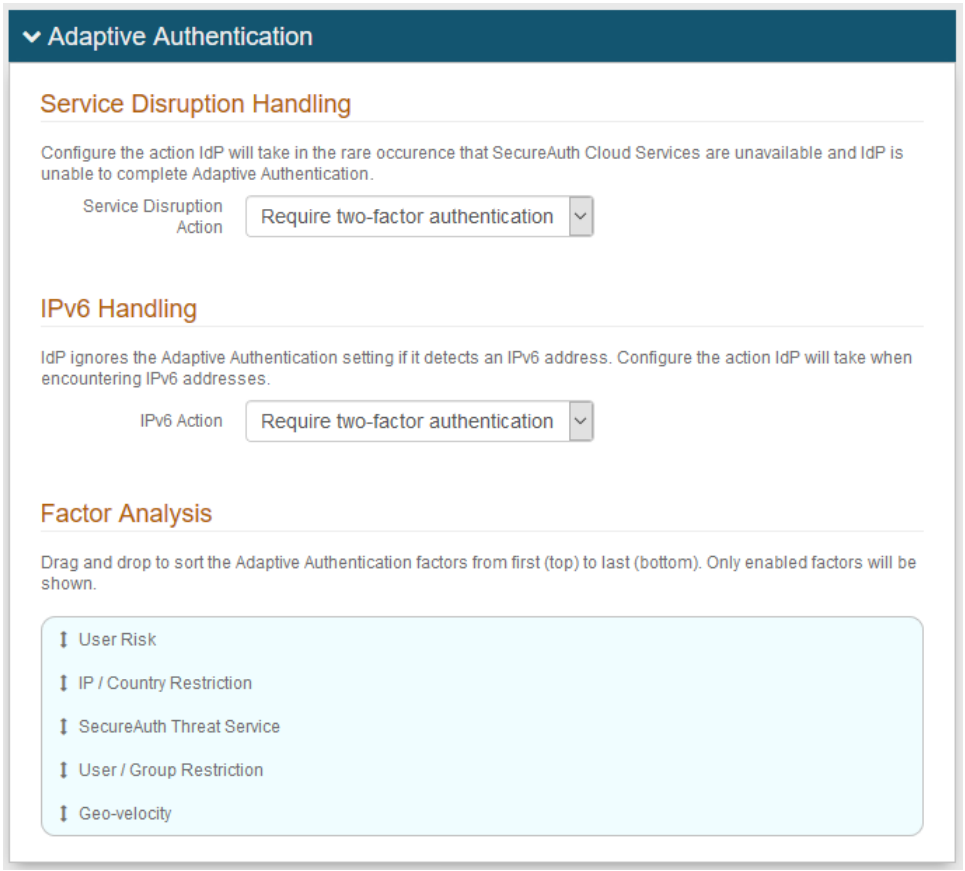
Adaptive Authentication tab configuration

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

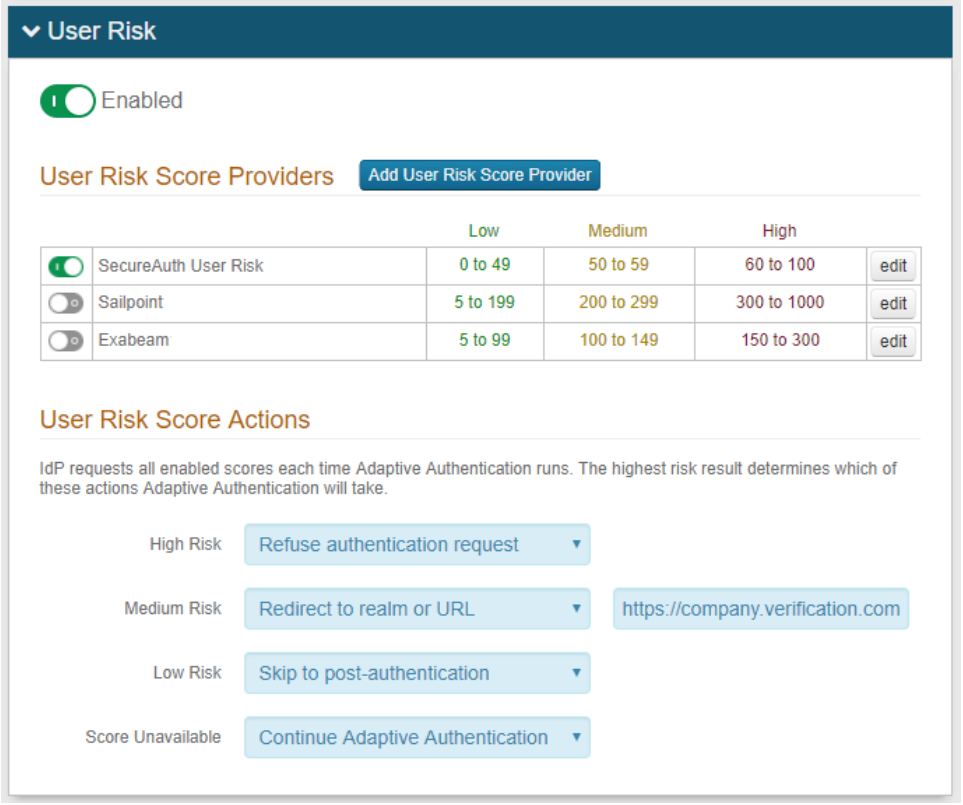
1. Go to the **Adaptive Authentication** tab.
2. In the **Adaptive Authentication** section, set the following:

Service Disruption Handling	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. Select the risk check action to authenticate the end user. For more information about the actions to take, see the risk check action definitions.
IPv6 Handling	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. Select the risk check action to authenticate the end user. For more information about the actions to take, see the risk check action definitions.
The default selection (**Require two-factor authentication**) 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.	
Factor Analysis	List includes all enabled adaptive authentication risk checks factors. The list is in order by processing sequence; you can **drag and drop** selections to reorder the processing sequence.



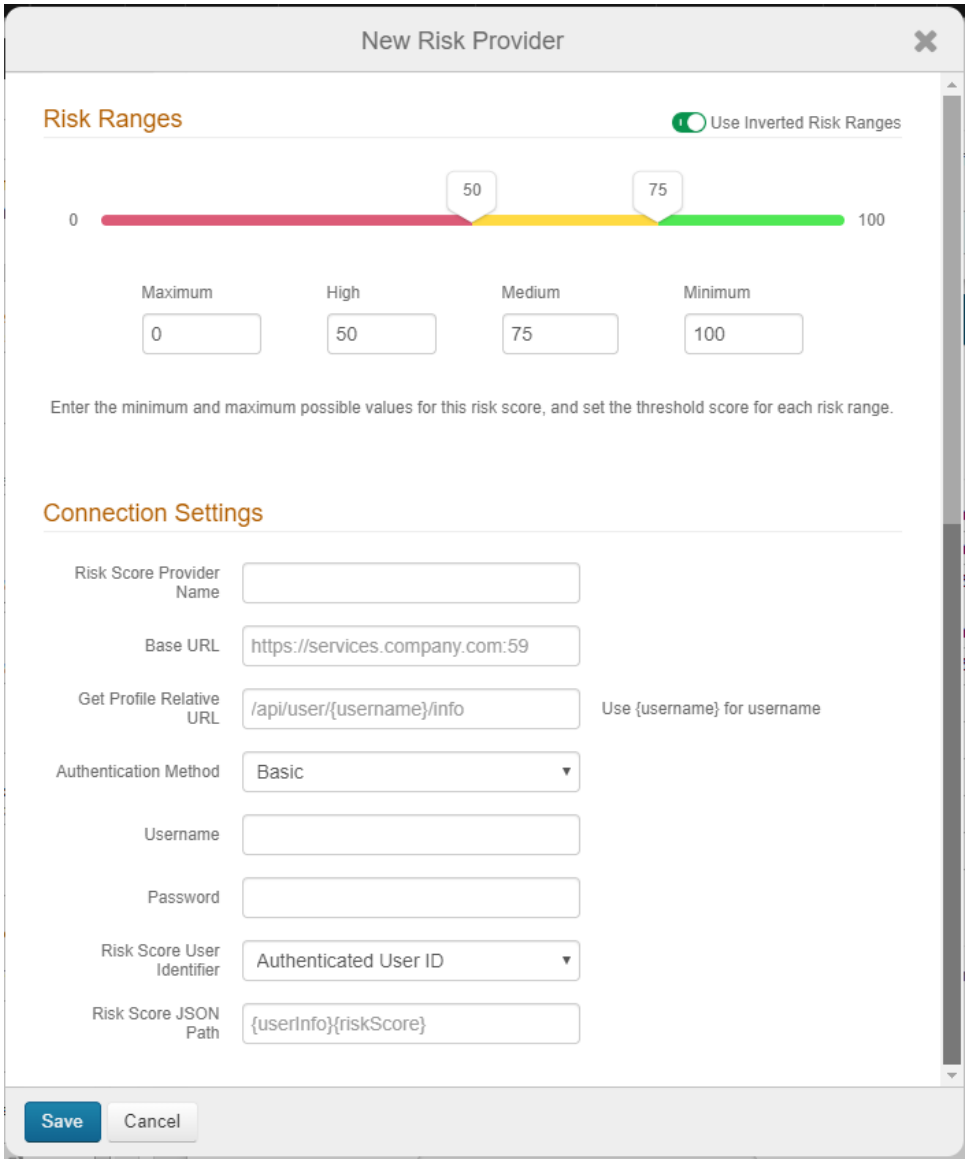
3. In the **User Risk** section, move the slider to **Enabled** for the User Risk analysis feature.
4. Click **Add User Risk Score Provider** or **edit** an existing user risk score provider.
    - To use and configure the SecureAuth User Risk solution, see SecureAuth User Risk score provider configuration
    - 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



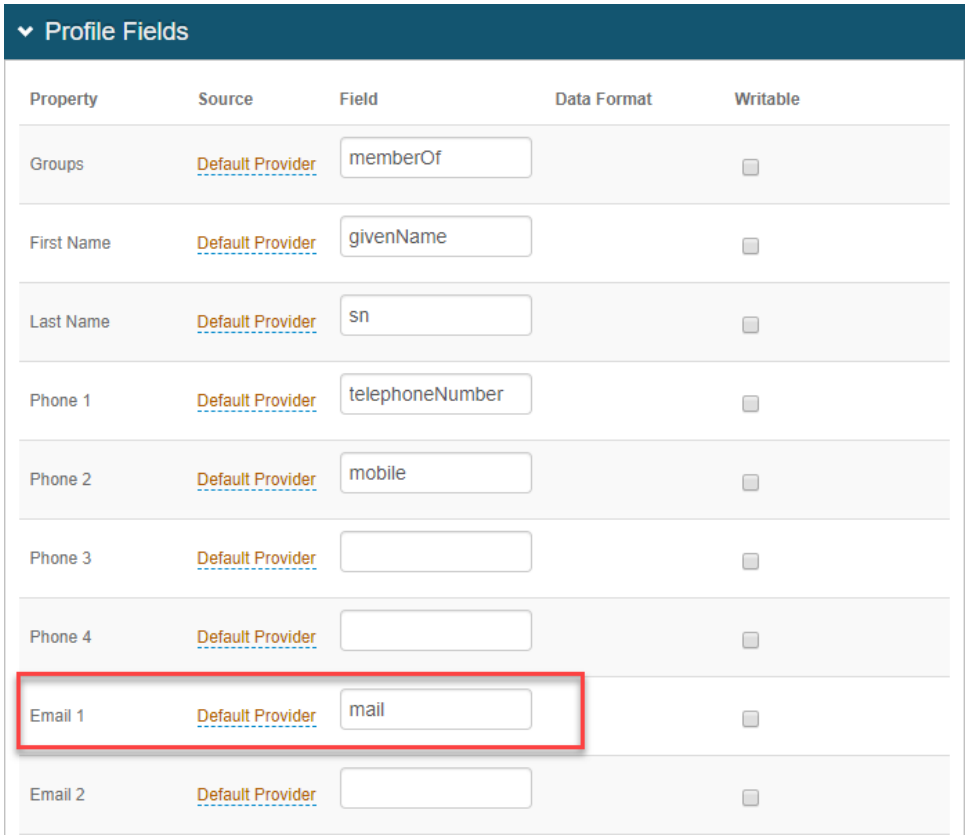
5. On the risk ranges configuration page, set the following:

Risk Ranges	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



RiskScoreProviderName	Set the descriptive name for the risk provider.
BaseURL	Set the base URL of the risk provider instance in this format: https://services.company.com:59.

GetProfileRelativeURL	Set the endpoint of the REST API provider in this format: /api/user/{username}/info. Insert the {username} variable in the position the endoint expects the userID to be in the string.
AuthenticationMethod	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.
RiskScoreUserIdentifier	Set the target user ID in the format to which the user risk provider expects to identify end users. It most cases, it is the same value as the defa **Authenticated ID**. In other cases, the user risk provider might use a different user ID; for example, the end user logs in with a sAMAccount n 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, f **Score User Identifier** field, you would select **Email 1**. ## Data tab mapping example



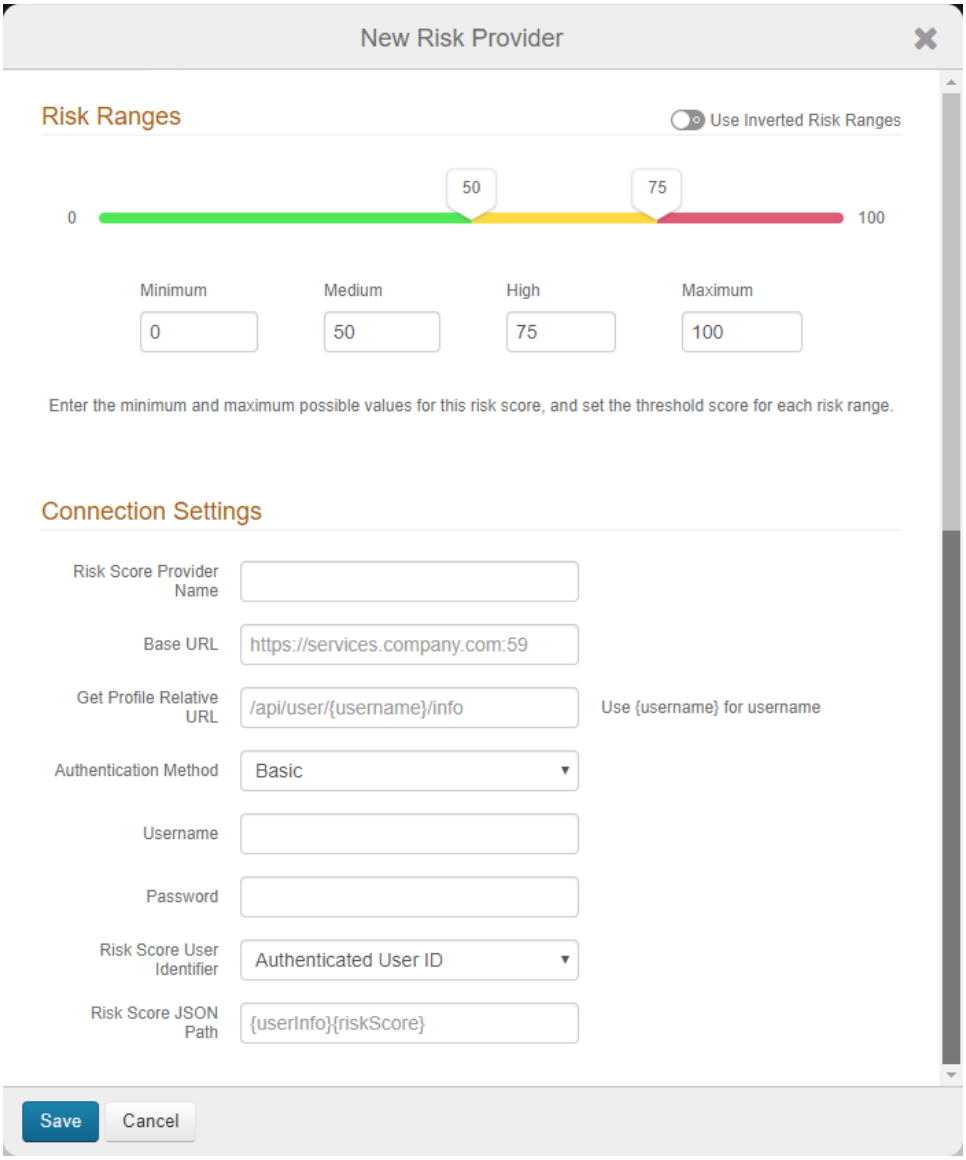
RiskScoreJSONPath

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

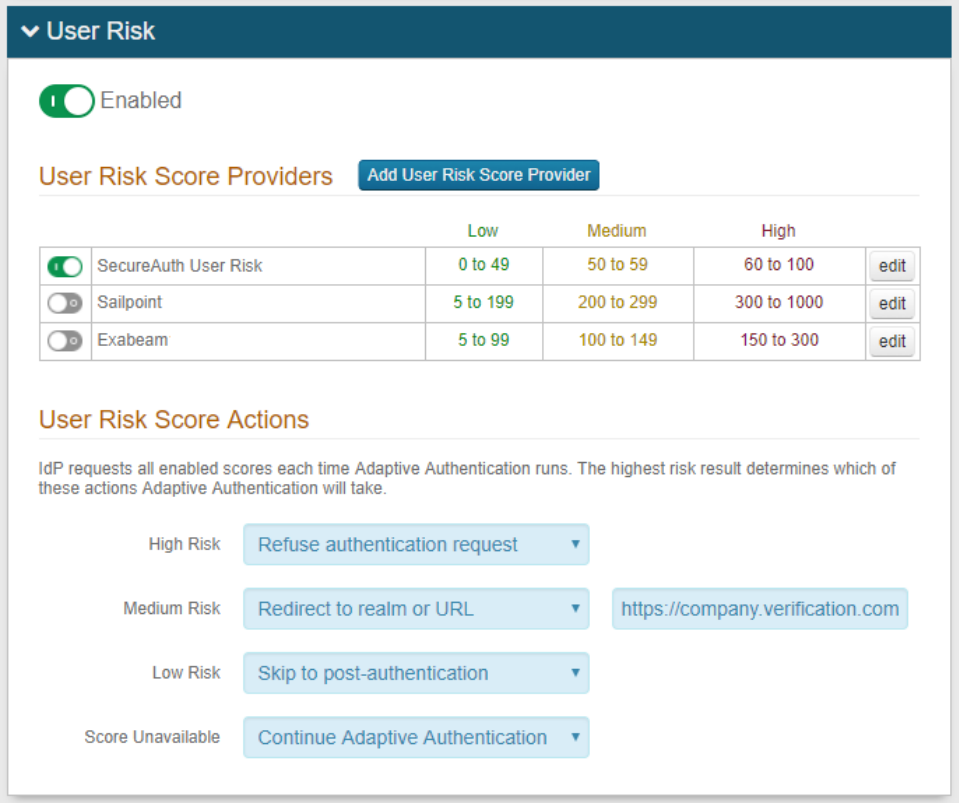
{userInfo}{riskScore}	{
	"status": true,
	"user": "rfobber",
	"userInfo": {
	"riskScore": 90,
	},
	}

{risk_score}	{
	"status": found,
	"userID": "rfobber",
	"risk_score": 0
	}



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.



8. **Save** your changes.