SecureAuth User Risk score provider configuration

SecureAuth IdP provides advanced adaptive capability powered by machine learning with its Prevent package to track and analyze the login behavior patterns of authorized users. It tracks the login patterns for a period of time to identify normal patterns, then assigns each user a personal risk score. Since the login behavior pattern and risk score is unique to each user, it prevents bad actor attempts to impersonate authorized users trying to gain access to the targeted login site. For more information about user risk score calculations see Machine learning user risk score calculations.

For each level of user risk (High, Medium, and Low) you can define which action SecureAuth IdP is to take as described in Risk check actions.

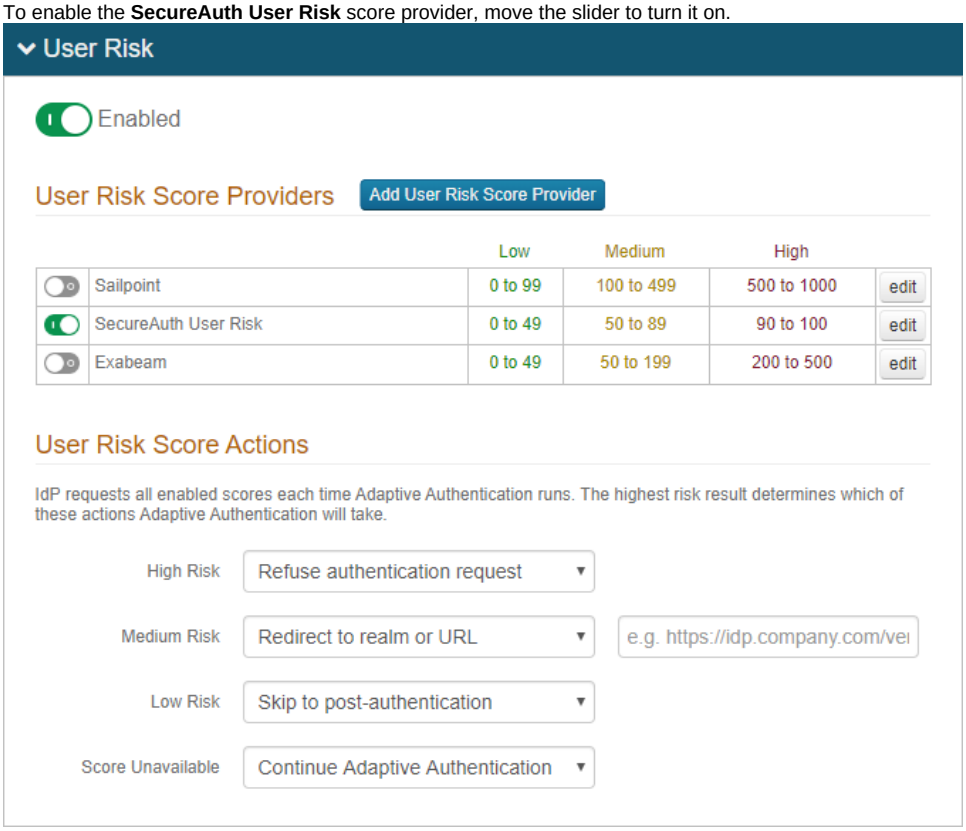
Prerequisites

- SecureAuth IdP realm configured with an application integration
- Prevent package license to use the machine learning user risk score analysis feature – contact SecureAuth Support

---

SecureAuth User Risk score provider configuration

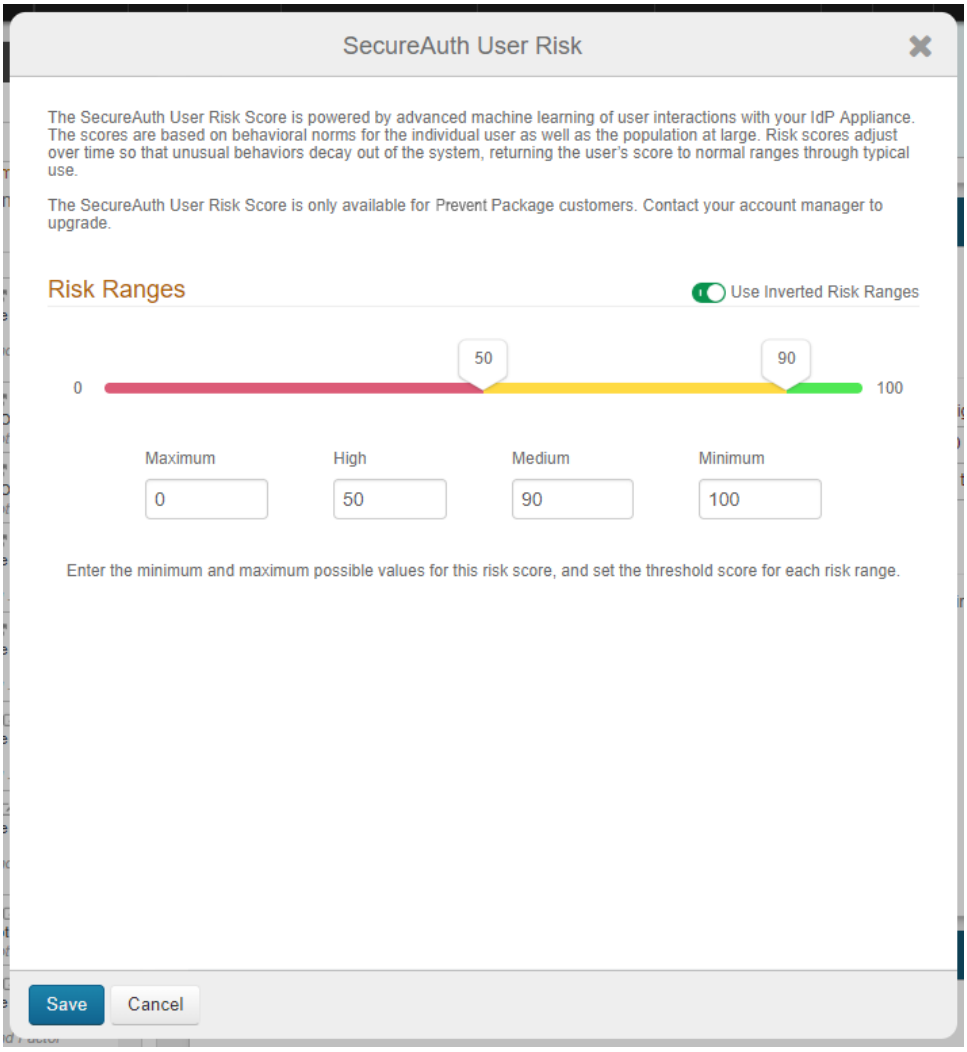
1. Select the **Adaptive Authentication** tab.
2. In the **User Risk** section, move the slider to **Enabled** for the User Risk analysis feature.
3. To enable the **SecureAuth User Risk** score provider, move the slider to turn it on.

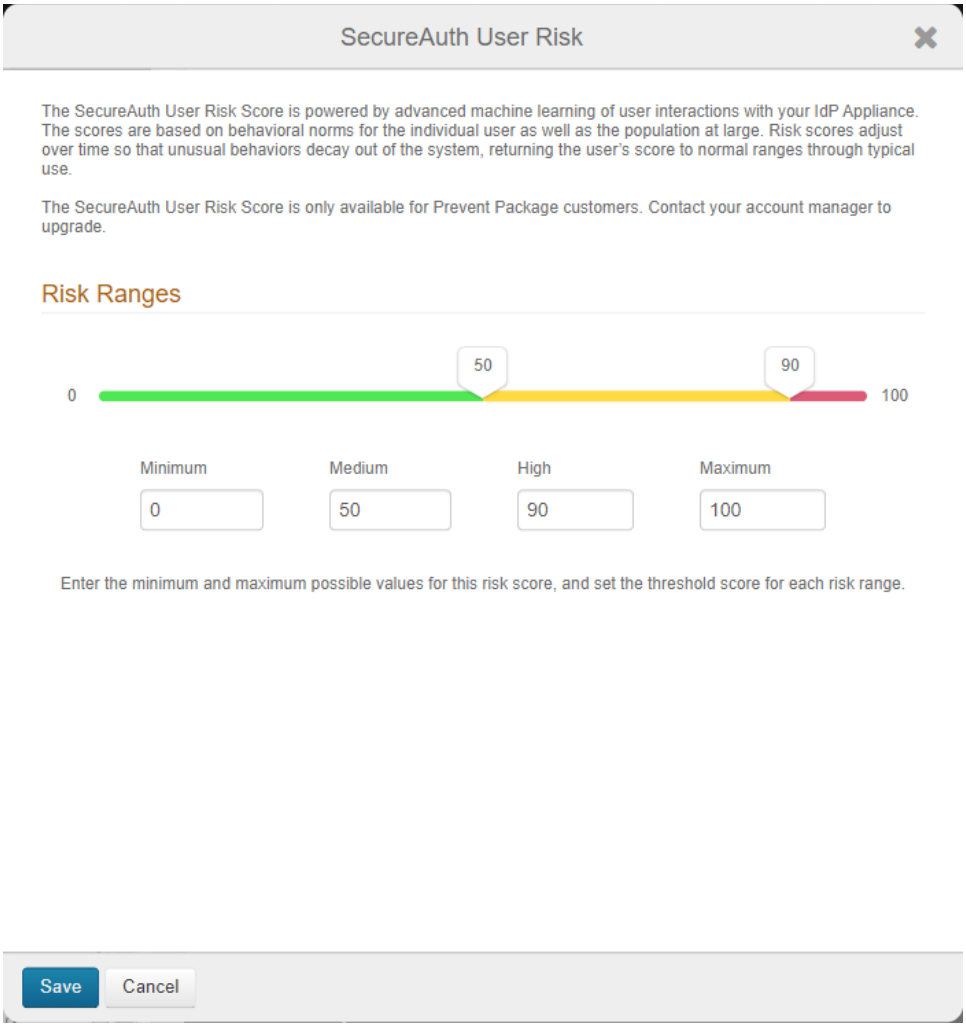


4. To adjust the risk ranges, click **edit** and set the following:

RiskRanges	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.

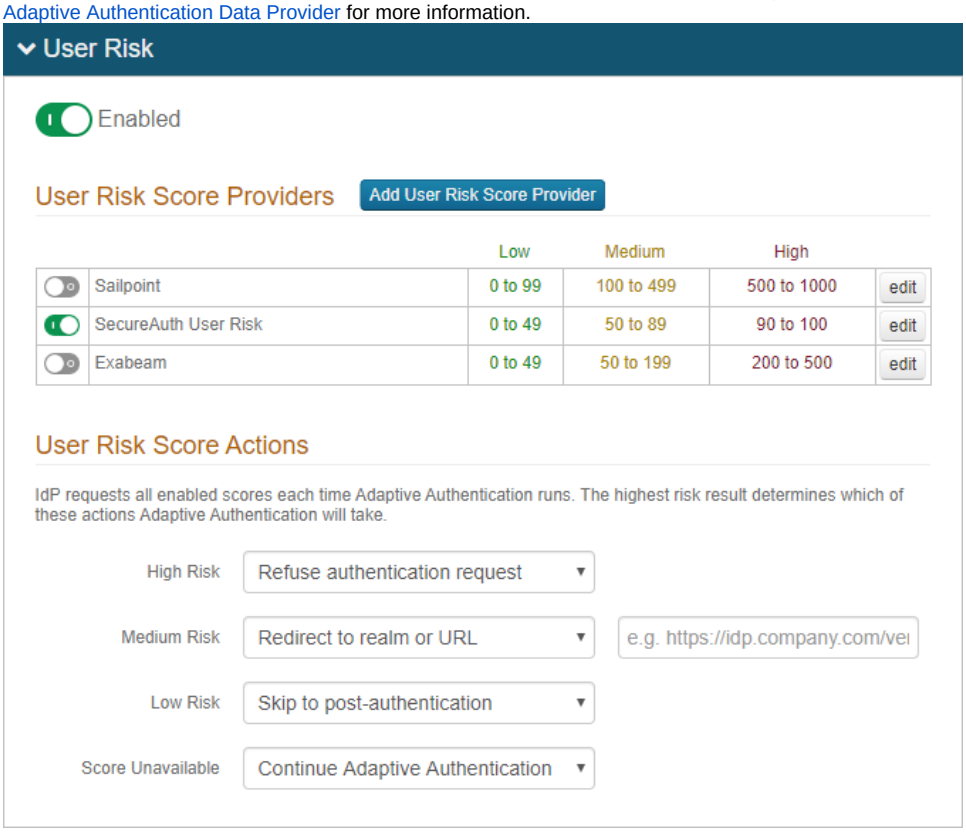
Image example of inverted risk ranges





5. **Save** the configuration.

6. Under **User Risk Score Actions**, for each risk range (**High**, **Medium**, **Low**, and **Score Unavailable**), specify the adaptive authentication action SecureAuth IdP takes when the user risk score falls within the specified range.
   For more information about the actions to take, see 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.



7. **Save** the configuration.