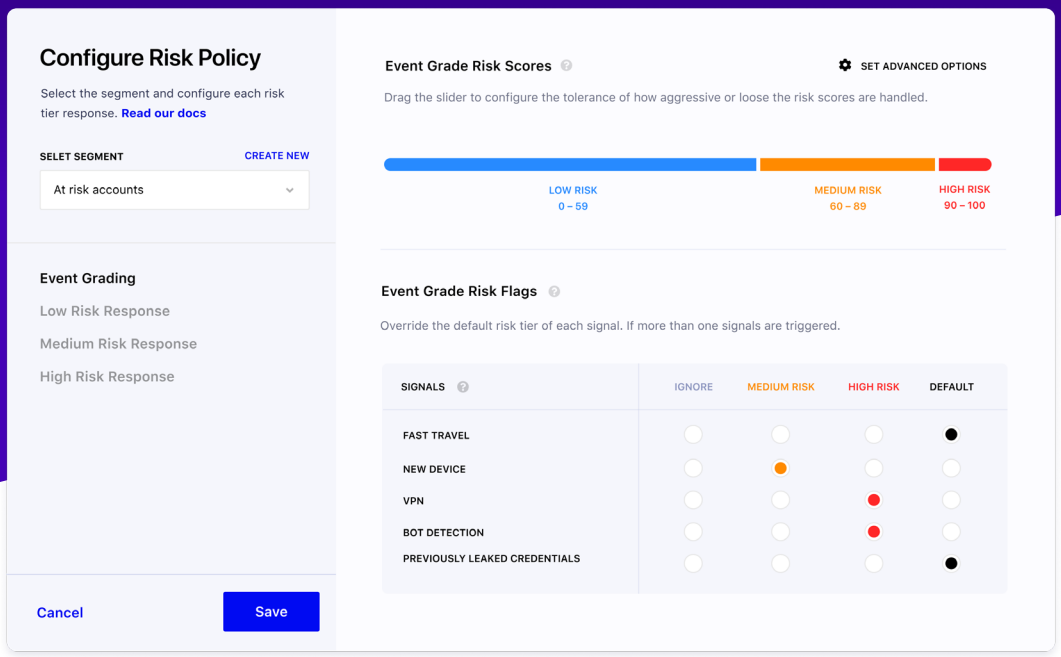
Castle

# Risk Policies

Create custom policies tailored to your business objectives and risk tolerance




## Gain Control with Risk Policies

Managing risk and delivering strong security to protect user accounts from critical events can feel like a balancing act, especially when countered with providing a good user experience that won't impact customer retention or conversion rates. On top of this, many organizations are challenged with the fact that not all of their end-users segments are the same and they may want to treat certain groups or scenarios differently based on their exposure to risk.

With Castle Risk Policies, you gain more flexibility in how you manage risk. Whether it's building a policy around user traits, critical events, or device context, you can easily create granular risk policies with customized logic, risk scores, and responses. This allows you to continue to optimize the user experience but also align with the needs of your business and risk tolerance.

## Key Features

- ✓ DEFINE SEGMENTS FOR USERS, DEVICES, AND EVENTS
- ✓ CONFIGURE CUSTOM POLICIES
- ✓ DEFINE CUSTOM RISK TIERS
- ✓ CUSTOMIZE INLINE AND OUT-OF-BAND RESPONSES
- ✓ BUILD GRANULAR RISK LOGIC
- ✓ CONFIGURE CUSTOM WHITELISTS AND BLACKLISTS

### Creating Segments for a Custom Risk Policy

To create a custom risk policy, a customer first needs to define what segments they want to develop a policy around. Segments can be defined as a combination of user, device, and event traits that are important to your business and that you want to treat with greater or lesser sensitivity. Here are some examples of the different types of traits.

#### User Focused Traits

- ✓ HIGH-VALUE USERS
- ✓ NEW USERS
- ✓ BUYERS VS SELLERS
- ✓ DORMANT ACCOUNTS

#### Device Focused Traits

- ✓ DEVICE OR OS TYPE
- ✓ MOBILE VS WEB ACCESS
- ✓ IP, ISP, OR LOCATION
- ✓ USER-AGENT SUBSTRING

#### Event Focused Traits

- ✓ HIGH-VALUE PURCHASES
- ✓ ACCESSING SENSITIVE DATA
- ✓ PROFILE UPDATES
- ✓ BANKING OR CARD DETAILS CHANGED

---

### Customizing the Risk Engine with Risk Policies

Next you can define a custom risk engine to increase or decrease friction for the segment. This can be done by defining Low, Medium, and High risk tiers. For each tier, you can set risk score thresholds. You can also associate specific threat signals to a given tier, such as:

- ✓ **New location**
- ✓ **New device**
- ✓ **Datacenter, VPN, or tor access**
- ✓ **Missing device fingerprint**

Finally, define how you want to respond to each scenario by establishing custom inline and out-of-band response rules for each tier of your new risk policy.

As an example, you may have users or scenarios that you want to treat with more caution based on the risk tolerance of your business. With Risk Policies, you can create a segment that targets power users at the time of a high value purchase, and apply a policy that blocks all attempts from a datacenter and enforces MFA on all attempts from a new device or new location.