# Entrust Identity - Adaptive Risk-Based Access and Authentication

## Market Challenge

Increased security and improved user experience may seem at odds, but they don't have to be.

## Solution

Entrust Identity's adaptive risk-based engine provides an added level of security when conditions warrant, like a user logging in for the first time from a new device, at an abnormal time of day, or from a different geolocation. Requiring additional authentication like a mobile push notification only for these situations minimizes user friction while also reducing fraud and protecting corporate resources.

## BENEFITS

- Identify and address suspicious behavior before a breach happens

- Keep user friction to a minimum

- Minimize help desk calls with intelligent step-up authentication

- Integrate risk-based authentication directly into your own applications

- Flexibility to layer additional authentication as needed

## At a glance

Entrust Identity's adaptive risk-based authentication evaluates a broad range of contextual attributes, including the identity of mobile devices or PCs, geo-location, geo-velocity, user behavior, and user credentials. It also considers inputs from external fraud and analytics sources. All these factors quickly result in one of three outcomes:

- Allow user access
- Present user with a step-up challenge
- Deny user access

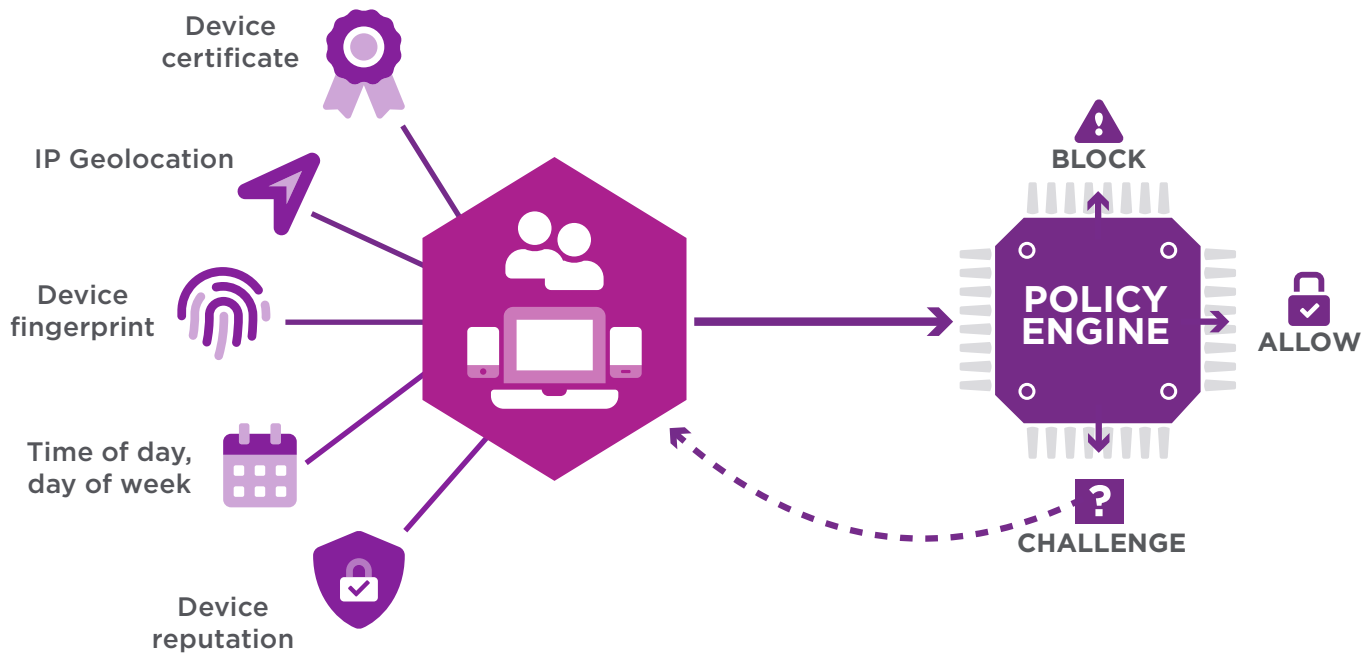# Entrust Identity - Adaptive Risk-Based Access and Authentication



**Figure 1** Adaptive Authentication can assess a range of information including external risk scores to affirm the user identity. Once all attributes are assessed, the user will be allowed, blocked, or issued an authentication challenge.

## HOW IT WORKS

With criminal attacks becoming increasingly sophisticated, traditional device fingerprinting is no longer sufficient. Entrust Identity offers easy-to-deploy toolkits that provide extensive device attribute collection, analysis, and access context for both browser-based and mobile application-based access.

Our toolkits allow you to customize which identity variables are collected, so you can create an authentication solution that fits your specific needs. As well, our solution goes a step further in selecting the right authenticators based on user risk profile and tendencies. Device reputation is an essential element of our adaptive authentication strategy. You can apply weightings to the different factors to holistically understand the risk through the policy engine. This is all done pre-authentication to ensure that the request is coming from a legitimate user.

With deep insight, Entrust Identity adaptive risk-based authentication leads to fewer step-up challenges, fewer help desk calls, and a measurable reduction in fraudulent transactions. From mobile push authentication and user self-service to out-of-band transaction verification and extension of user identities across multiple channels and domains, Entrust Identity is adaptable to your evolving business needs.

# Entrust Identity - Adaptive Risk-Based Access and Authentication

## Features
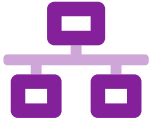
### Policy engine

Rich policy controls define which device parameters are collected and give you the option to assign specific weightings to each parameter.

### Device certificate

Can be used to transparently validate the authenticity of a user's computer or mobile device.

### IP geolocation

Parameters can be assessed and balanced against a number of checks including:

- IP address – is the IP address black-listed?
- Expected location – is the user expected to authenticate from this location?
- Location history – has the user authenticated from this location previously?
- Velocity – has the user authenticated from previous locations in a time frame that is inconsistent with the distance between the locations?

### Device fingerprint

When a user accesses the website or application, the device and access context is assessed in real time – weighing aspects of the device's digital fingerprint.

### Time of day, day of week

Configures security policy to access specific resources and applications between specific times and days of the week to different groups within the organization.

### Device reputation

Recognizes and detects fraudulent behavior across all types of web-enabled devices – including desktop, mobile, and tablets, even prior to login – and integrates with websites and applications.

# Entrust Identity - Adaptive Risk-Based Access and Authentication

## About Entrust Identity

With 25+ years of digital identity expertise and 50+ years of security innovation, Entrust is an identity and access management leader. Our high assurance solutions are proven with Fortune 500s and governments and are deployed by 10K+ customers around the globe. Entrust Identity secures digital identities and corporate assets, while also improving workforce productivity and removing friction for consumers and citizens.

## ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

**Learn more at**
**entrust.com**

**ENTRUST**

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
**info@entrust.com**    **entrust.com/contact**