ENTRUST IDENTITY

Entrust Identity Device Reputation

Leverage analytics to improve security and reduce user friction

Market Challenge

With digital business on the rise, user and customer demands are quickly evolving to frictionless yet secure experiences. Customer attraction and retention is critical to business success and requires users - such as employees, customers, and consumers - to conduct business anytime, anywhere without the worry of fraudulent activity.

And as mobile and cloud technologies emerge, organizations are changing the way they do business by implementing more efficient internal processes, enhancing user experiences, and offering new products and services.

Solution

Entrust Identity equips you with the tools to meet the demands of digital business transformation with trusted identities and next-generation authentication at its core.

Entrust Identity Device Reputation allows organizations to provide their users a transparent, secure experience by only enabling step-up authentication when a user's registered device is elevated as a risk.

BENEFITS

- Provide a transparent, frictionless user experience
- Stop fraud and abuse in real-time, prior to login
- Find subtle patterns with powerful analytics to fight fraud more effectively
- Make data-driven decisions with detailed fraud evidence
- Deep analytics and machine learning quickly adapt to changing fraud trends
- Prevent previous fraudulent-flagged devices from accessing your network and enterprise application
- Gather risk information about the device before login

Entrust Identity Device Reputation

Entrust Identity Device Reputation at a glance

Recognize, detect, and stop fraud in its tracks

Entrust Identity Device Reputation is part of our next-generation platform and uses best-of-breed device identification, dynamic risk context, and analytics from a global intelligence network to transform static, single-factor authentication processes into adaptive multi-factor solutions. Device Reputation recognizes and detects fraudulent behavior across all types of internet devices including desktop, mobile, and tablets, even prior to login, and integrates with websites and applications.

The power of three – next-generation authentication

Trusted identities and a powerful authentication platform are essential to digital business success. Companies are no longer looking for a single-point solution, and are now searching for a next-generation authentication platform that will empower their users while fighting against fraud.

Breadth, depth, and flexibility

Device reputation and other sources of insight can all be used in our Entrust Identity adaptive risk-based engine, and paired with a wide range of multi-factor solutions. With over 17 authentication methods – including mobile push authentication – extensive scale of use cases, adaptive authentication capabilities, and a comprehensive portfolio of integrations, you can address your immediate needs today and quickly adapt as your digital business evolves. We provide you with the authentication platform of choice for the demands of digital business.

Features

Device ID and registration. Affirm user identity by matching device fingerprints with a high degree of accuracy.

Device change tolerance. Minimizes false negative responses and establishes acceptable risk with built-in intelligence on typical device changes.

Reveal hidden connections. Initiate step-up authentication challenges when bad device activity patterns or actors are recognized.

Evasion detection. Proxy piercing detects fraudulent servers using advanced techniques to unmask anonymizing activity.

Global device intelligence platform. Real-time device feedback from thousands of risk analysts flags suspicious accounts and devices.

“PII-less” precision. Recognition technology instantly identifies without a user’s personally identifiable information.

Entrust Identity Device Reputation

Entrust Identity device analytics

Identify fraud patterns
To help you accurately separate the fraudsters from your trusted users, identify risky device behaviors including:

- Evasion techniques: Identify fraudulent transactions that originate by:
  - Redirecting or concealing the use or location of a device through TOR networks and proxy servers
  - Artificially simulating a mobile device and its operating system through a desktop application
- Device anomalies: Includes location mismatches, time zone and IP address changes, too many devices per account, and exceeded velocity thresholds
- High-risk locations, IPs, and ISPs: Includes high-risk geographic locations or known bad IPs, ISPs, or locations that violate your specific business policy

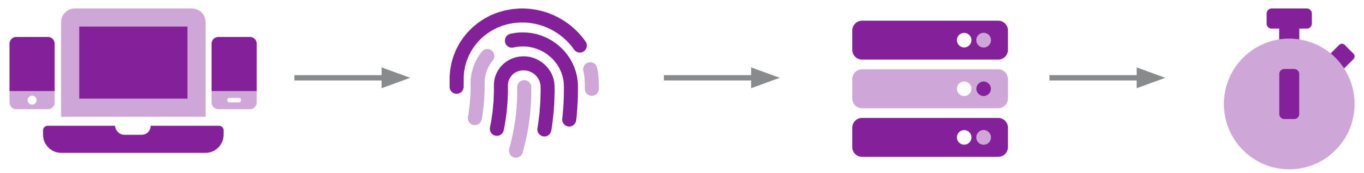
Advanced analytics
Our advanced fraud prevention and detection capabilities extend your protection to fraud patterns that you are most concerned about. For example, Device Reputation can inform you:

- If a particular device has been used to access multiple accounts within a particular time period
- When many devices have been used to access a single account
- If the device has a history of specific types of fraudulent activity
- When the device is linked to other devices or accounts associated with fraud
- Whether the device has violated specific policies that you have defined such as geolocation, chat abuse, spending limits, or cheating

All of this information is gathered and analyzed in the milliseconds before the device logs in to your network.

How Entrust Identity applies Device Reputation

Adding layered security to reduce user involvement provides a seamless and transparent experience, and only relies on multi-factor authentication when needed – giving organizations the right balance between security and usability.



User visits your website or mobile app from any device

Device fingerprint and data attributes are collected via JavaScript or Mobile SDK

Authentication or fraud request is sent to our device intelligence platform for analysis

A customized real-time response is returned about the device and transaction within milliseconds

Entrust Identity Device Reputation

Based on risk-based analysis configuration, our solution provides a recommendation such as the below:

- Allow: Device is trusted and policy says that's all that's required
- Challenge: Device may be under review and policy identifies another factor for authentication is required
- Deny: Device is flagged as untrusted and authentication is refused outright

Use cases for financial institutions and enterprises

Banking

New Account Creation: Securely offer new services by identity-proofing the integrity of your customer's device when they digitally create an account online or through their mobile device.

Online & Mobile Banking: Empower your users to access account information with a seamless and transparent experience and only enable step-up authentication when risk is elevated.

Transaction Verification: Out-of-band transaction verification helps defeat advanced fraud attacks by adding a layer of security and assessing the device integrity.

Employee

BYOD Pre-check: Ensure the integrity of your new employee's device before issuing access to company information, tools, and resources.

Mobile ID Pre-check: Ensure the user's device has not been associated to any fraudulent activity before a trusted identity is provisioned to the device.

Streamline User Access: Reduce the number of times a user needs to authenticate by layering device analytics to identify low-risk situations.

- On-Premises and Cloud Applications
- Partner and Customer Portals

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