DATASHEET

TrustLayer Multi-Factor Authentication

Multi-factor authentication from TrustLayer provides protection from account compromise through the use of weak or stolen passwords – whether they were obtained through phishing, social engineering, brute force attacks or purchased online.

MFA is fully integrated with the TrustLayer Platform that also includes Email Security, Web Security and Cloud Application Security. The TrustLayer Platform provides a single web portal for central policy configuration and management, as well as data visualization and reporting.

MFA is primarily cloud-based, simplifying implementation and accelerating time to value for organizations of all sizes. No complex infrastructure is required, and easy to install authentication clients are available for all major vendors.

The Cloud MFA service is available in addition to the TrustLayer on premise MFA product that is specifically for organizations that want core components running within their own environments.

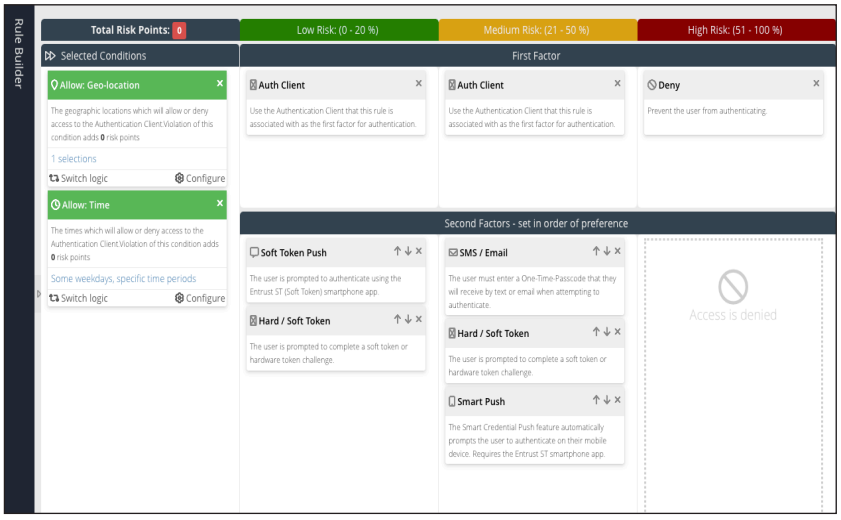
Cloud Multi-Factor Authentication provides a single pane of glass to analyze and manage user authentication activity across multiple systems, services and applications regardless of whether users are on the corporate network or working remotely.

TrustLayer MFA supports different dispatch policies for the delivery of OTPs via a range of methods including email as well as via a TrustLayer mobile app for Android and Apple iOS.

Automatic fail-over across multiple delivery methods critically provides higher assurance that users will receive OTPs – even when they have no mobile signal, for example. Fail-over is provided on the backend and provides a frictionless user experience compared to other offerings where users have to select their authentication method manually.

MFA

- 100% cloud-based backend simplifies implementation and management
- Designed to deliver an unrivalled user experience, architected for superior security
- Multi-tenant and multi-tiered – ideally suited to organizations of any size as well as MSPs
- Session specific one-time passcodes (OTPs) locked to individual sessions to prevent phishing
- Real-time generated OTPs provide improved security over predetermined time-based sequences
- Dispatch policies offer a choice of OTP delivery methods with automatic fail-over for delivery assurance regardless of user situation or location
- One-click lockout of individual users to immediately revoke access to all MFA protected services
- TrustLayer app for Android and Apple iOS devices for end-to-end encrypted OTP push notifications
- Out-of-the-box support for a wide range of systems, services and applications including all major VPN vendors (including Citrix and Cisco), Microsoft (including OWA) and major cloud applications (including O365 and Salesforce)
- Fully integrated with Microsoft® Active Directory
- Multi-layered highly scalable and resilient backend with intelligent load balancing



KEY FEATURES

Auth Clients/Protocols	Support for protecting an unlimited number of authentication clients: • RADIUS (protects VPN access e.g. Citrix Access Gateway or Cisco VPN) • Windows Logon (protects RDP access to servers) • ADFS (protects cloud applications such as Salesforce or Google Apps) • Citrix Web Interface (pre-dates Citrix Access Gateway with RADIUS) • IIS Website (protects Outlook Web Access or RD Web Access)
Vendor Support	Vendors supported include Barracuda, Check Point, Cisco, Citrix, F5, Google, Juniper
OTP Random Code Gen	Based on a FIPS 140-2 approved algorithm
TrustLayer MFA App	Available for Android and IOS for OTP push with end-to-end-encryption

REPORTING

Real-time Visibility	Productivity charts display instant visibility on compliance with defined policies. Query authentication activity in real-time by user, IP address, geo-IP data, login outcome, authentication client type. See exactly which users are authenticating to which systems, services and applications.
Report Builder	• Administrators can define their own reports based on available field names and criteria. • Reports can be saved and then exported to CSV or PDF. Audit reports can be searched using criteria including time, user, IP address, geo-IP data, successful or failed login and client type.
Scheduling & Alerting	Link reports to schedules and optionally only receive a report when there is content (alert mode). Alert on failed logins, specific users, etc.
Top Trends	A selection of pre-defined trend reports with chart and table data. Trend reports can be exported to PDF and emailed to recipients.
Multiple Views	Analyze and report by user, IP address, geo-IP data, login outcome, authentication client type.