Data Sheet

Censornet Multi-Factor Authentication (MFA)

Multi-factor authentication from censornet 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 Censornet Platform that also includes Email Security, Web Security and Cloud Application Security. The Censornet 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 Censornet 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.

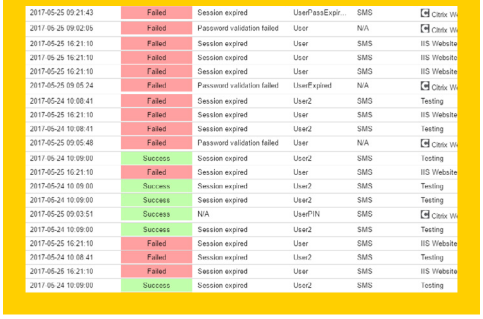
Censornet MFA supports different dispatch policies for the delivery of OTPs via a range of methods including SMS and email as well as via a Censornet mobile app for Android and Apple iOS.

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.

MULTI-FACTOR AUTHENTICATION

- 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
- Censornet 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

Whether audit data is required purely for visibility into authentication activity, or for more formal attestation of compliance with internal policies or external standards, regulations and legislation, Multi-Factor Authentication will provide the evidence needed.



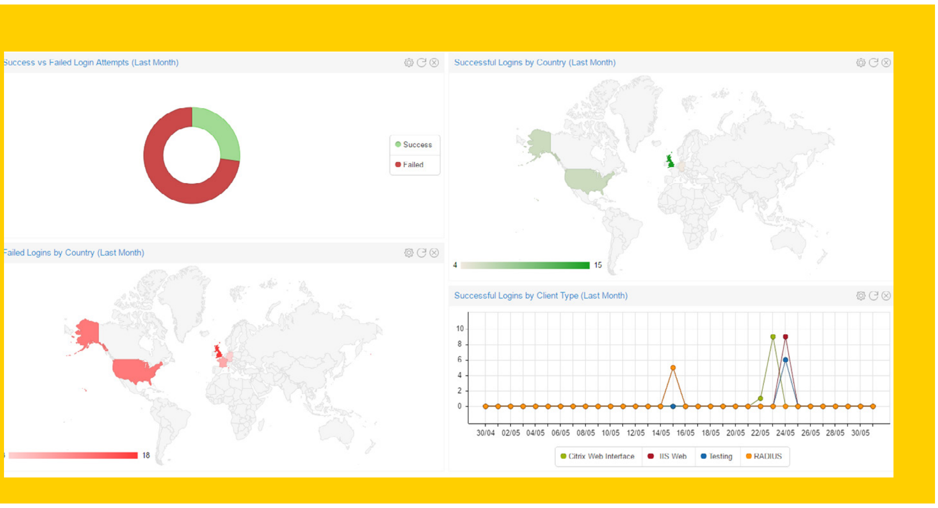
2017-05-25 09:21:43	Failed	Session expired	UserPassExpir...	SMS	Citrix W
2017-05-25 09:02:05	Failed	Password validation failed	User	N/A	Citrix W
2017-05-25 16:21:10	Failed	Session expired	User	SMS	IIS Website
2017-05-25 16:21:10	Failed	Session expired	User	SMS	IIS Website
2017-05-25 16:21:10	Failed	Session expired	User	SMS	IIS Website
2017-05-25 09:05:24	Failed	Password validation failed	UserExpired	N/A	Citrix W
2017-05-24 10:08:41	Failed	Session expired	User2	SMS	Testing
2017-05-25 16:21:10	Failed	Session expired	User	SMS	IIS Website
2017-05-24 10:08:41	Failed	Session expired	User2	SMS	Testing
2017-05-25 09:05:48	Failed	Password validation failed	User	N/A	Citrix W
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing
2017-05-25 16:21:10	Failed	Session expired	User	SMS	IIS Website
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing
2017-05-25 09:03:51	Success	N/A	UserPIN	SMS	Citrix W
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing
2017-05-25 16:21:10	Failed	Session expired	User	SMS	IIS Website
2017-05-24 10:08:41	Failed	Session expired	User2	SMS	Testing
2017-05-25 16:21:10	Failed	Session expired	User	SMS	IIS Website
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing

Censornet's MFA uses memoPasscodes™, a unique way of generating passcodes that makes them very easy to memorize and simple for users to enter when logging in. Passcode randomness – and therefore security – is unaffected.

MFA uses the AD sync engine of the Censornet Platform, allowing full integration with Microsoft® Active Directory with options to use Local Sync or Cloud Sync. Local Sync uses a locally installed AD Connector Service (agent) which pushes all objects, or all objects from a configurable point in the AD tree down, to the Censornet Cloud. Differential updates then occur every 15 seconds. Cloud Sync uses a LDAP or LDAPS connection to pull objects. Local Sync has the additional benefit of not requiring any firewall rule changes. Both methods require a read only service account in AD. Once configured, AD synchronization – and therefore identity – is available across all the Censornet Platform components.

Censornet's MFA uses memoPasscodes™, a unique way of generating passcodes.

Multi-Factor Authentication is fully integrated with the Censornet Platform which provides rich data visualization and reporting across an extensive set of attributes and criteria. Analysis and reporting is available by time, user, IP address, geo-IP data, successful or failed login and client type.


Success vs Failed Login Attempts (Last Month)
Success
Failed
Successful Logins by Country (Last Month)
4
15
Failed Logins by Country (Last Month)
18
Successful Logins by Client Type (Last Month)
10
8
6
4
2
0
30/04
02/05
04/05
06/05
08/05
10/05
12/05
14/05
16/05
18/05
20/05
22/05
24/05
26/05
28/05
30/05
Citrix Web Interface
IIS Web
Testing
RADIUS

KEY FEATURES

Authentication Clients / Protocol Support	• 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 Networks, Microsoft, OpenVPN, Palo Alto Networks, Salesforce, Teldat, VMWare.
OTP Dispatch Polices	• Dispatch policies define OTP delivery method with override for individual users. Delivery methods include: • SMS • Email • Censornet app • SMS with fail-over to email • Censornet app with fail-over to SMS
OTP Random Code Generator	• Based on a FIPS 140-2 approved algorithm.
SMS Type	• Support for both Standard and Flash SMS.

Censornet MFA Mobile App	• Available for Android and iOS for OTP push with end to end encryption.
OTP Transmission	• Costs for OTP transmission are included (subject to fair usage policy).

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 and 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 Trend Reports	• 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.
Log Retention and Autoarchiving	• MFA log data is archived automatically after 1 year and available to download from the Censornet Platform for a period of a further 12 months. Longer retention periods are available.

MANAGEMENT

User Synchronization	• Active Directory synchronization service ensures changes to Active Directory are replicated.
Web Interface	• Fully integrated with the Censornet Platform.

DEPLOYMENT

Backend	• Highly scalable fully redundant and 100% cloud based delivered from multiple data centers located in US, UK and mainland Europe.
Authentication Clients	• Easy to install agents deployed on MFA protected on-premise services in order to connect to the cloud backend.

Autonomous Integrated Cloud Security

E. EMAIL

Secure your entire organization from known, unknown & emerging email security threats - including email fraud.

S. SAT

Defend your organisation against cybercriminals by strengthening your engaging and stimulating automated training.

W. WEB

Protect users from webborne malware, offensive or inappropriate content & improve productivity.

C. CASB

Discover, analyze, secure & manage user interaction with cloud applications - inline & using APIs.

M. MFA

Reduce impact of large scale data breaches by protecting user accounts with more than just passwords.

ID. IDaaS

Control user access with complete identity-threat protection. Automatically authenticate users using rich contextual data.

Our Platform

Our cloud security platform integrates email, web, and cloud application security, seamlessly with identity management and advanced data loss prevention to activate the Autonomous Security Engine (ASE).

This takes you beyond alert driven security and into real-time automated attack prevention.

Advanced DLP

Prevent sensitive data getting into the wrong hands.

Enterprise-grade DLP across email, web and cloud applications for the ultimate real-time protection.

Autonomous Security Engine

Prevent attacks before they enter the kill chain.

Enable traditionally silo'd products to share and react to security events and state data whilst leveraging world class threat intelligence.

CENSORNET LTD

Matrix House, Basing View,
Basingstoke, RG21 4FF, UK

Phone: +44 (0) 845 230 9590

CENSORNET LTD

Park Allé 350D, 2605 Brondby,
Denmark

Phone: +45 61 80 10 13

CENSORNET LTD

700 Lavaca Street Suite 1400-
PMB#100122 Austin, TX 78701

Phone: +1 (877) 302-3323

censornet.com

censornet.