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 Securtiy. 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 authentiation 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 fo a wide range of systems, services and applications including all major VPN vendors (including Critix 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

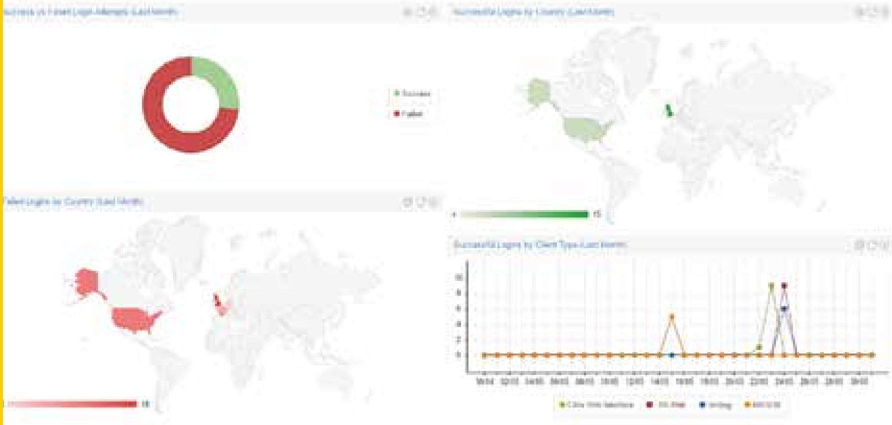
Whether audit data is required purely for visibility into authentication activity, or for more formal attestation of compliance with internal policies or external standards, regulations and legislation, Multi-Factor Authentication will provide the evidence needed.

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 andomness - and therefore security - 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 visualzation 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)
Failed Logins by Country (Last Month)
Successful Logins by Client Type (Last Month)

## KEY FEATURES

| | |
|---|---|
| **Authentication Clients / Protocol Support** | • Support for protecting an unlimited number of authentication clients:<br>• RADIUS (protects VPN access e.g. Citrix Access Gateway or Cisco VPN)<br>• Windows Logon (protects RDP access to servers)<br>• ADFS (protects cloud applications such as Salesforce or Google Apps)<br>• Citrix Web Interface (pre-dates Citrix Access Gateway with RADIUS)<br>• 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:<br>• SMS<br>• Email<br>• Censornet app<br>• SMS with fail-over to email<br>• 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.<br>• 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.cr |
| **Scheduling and Alerting** | • Link reports to schedules and optionally only receive a report when there is content (alert mode).<br>• Alert on failed logins, specific users, etc. |
| **Top Trend Reports** | • A selection of pre-defined trend reports with chart and table data. Trend reports ca 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 futher 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. |