AmZetta

zMFA
Enterprise Authentication Software

IRONCLAD AUTHENTICATION
Authenticate users with One Time Passwords (OTP), digital certificates, and even biometrics

SIMPLIFIED AUDITS
Log access history to corporate data and trace device locations accessing the network to resolve identified threats

COMPLETELY COMPATIBLE
Rest based API's allow for protection of virtually any application

PRODUCT
OVERVIEW

AmZetta zMFA is multi-factor authentication (MFA) software that enables the configuration of user access and permissions and is available as a supplementary license to the AmZetta zGateway software. zMFA supports multiple standardized user authentication methods, such as One Time Password (OTP), digital certificates, and even biometrics in order to meet the security requirements of virtually any organization. AmZetta zMFA can be integrated with the zGateway software, as well as all third-party devices accessing the network via RADIUS or TACACS, Microsoft Windows desktop login, Microsoft Windows server login, and Linux server login. With zMFA, one-time passwords can be sent to users via SMS or Email, or users can elect to generate an OTP using the zMFA token feature available for mobile phones and PC. The zMFA plugin for biometric access enables reliable login to user desktops with unparalleled security. AmZetta

zMFA's robust feature set ensures it can meet the security requirements of nearly all organizations, while its versatile compatibility enables it to seamlessly integrate with most existing infrastructures to provide user friendly authentication services. Also, with the zMFA REST-based API, any application can be protected with ironclad multi-factor authentication methods.

Do you know who's accessing your data?

2,244 Cyber Attacks per Day

Cyber attacks and data breaches can cost corporations millions of dollars.

As cyber attacks become more formidable, the lack of rigorous authentication increases the likelihood of data becoming compromised.

zMFA - Offers Protection for:

- **Microsoft Windows Desktop Login**
- **Remote Access Gateways**
- **Microsoft Windows Server Login**
- **SSL VPN, Firewalls, and Managed Switches**

- **RDP into Windows Desktops & Servers**
- **Any corporate application via REST API**
- **Linux Server Console & Remote Shell Access**

Protect corporate data with multi-factor authentication	Configure, Monitor and Audit User Permissions	Prevent Identity Theft, and Phishing scams, and Spyware from Internet Online Applications	Completely secure the entire corporate network with authentication for both local and remote devices and remote devices
SMS Token	Email Token	Mobile App Token	Desktop Software Token

FEATURES

Multi-Factor Authentication

zMFA protects company data with multiple factor authentication methods. zMFA supports One-Time-Password (OTP) based security on standard credential-based authentication. zMFA also supports biometric authentication via the a desktop plugin to adhere to high-security protocols. zMFA can even calculate the potential threat of access incidences and adapt to require users to further authenticate via stronger or alternative methods. Access risk is calculated based on various factors, such as users' location, the device attempting to gain access, browser used, access time, and more. AmZetta zMFA also guarantees a user-friendly experience with a simple yet secure software framework. Administrators have the ability to fully customize the level, type, and rigor of security to be enforced on the end users.

Protect Desktop Logins

AmZetta zMFA can require authentication for Microsoft Windows login, Linux Console login, and Shell login using multi-factor authentication. Once installed, the zMFA client for Windows secures the entire Windows desktop OS, as well as Windows Server OS with strong authentication options. If a user is using RDP to remotely log into a Windows Desktop or Server, the user must navigate two-factor authentication. The Linux desktop and server consoles, as well as shell access, also can be protected using zMFA.

Flexible Token Support

zMFA supports various OTP approaches, including via multiple tokens such as SMS, Email, PC software and mobile application. zMFA can also integrate with any OATH-compliant hardware token for increased adaptability.

Availability

AmZetta zMFA is offered as an optional add-on to zGateway licenses, but can also be utilized as a standalone product. zMFA natively supports High Availability and Automatic Failover to ensure corporate security cannot be compromised by hardware malfunctions.

Privilege Access Audit & Control

By deploying zMFA, companies can monitor, configure and audit users' access at the department level for an overview perspective of access history. While many organizations cannot track user access at the individual level – exposing them to untraceable security breaches – zMFA requires that power users must provide their personal domain accounts to access the privileged user accounts. Additionally, users can be required to enter additional authentication methods like OTP and biometric data based on configurable, dynamic risk-based policies.

Protect Network Logins

By default, AmZetta zMFA includes built-in RADIUS- and TACACS-based interfaces to natively integrate with any managed devices that support two-factor authentication via the respective protocols. Since nearly all firewalls, NAC devices, managed routers and switches require two factor authentication for administrator user access, zMFA can be configured to require strong authentication for privileged user access to integral network devices.

Integrate with Any Application

zMFA can be integrated with any application using the provided REST-based API. The REST-based APIs are intuitive and include a workflow, allowing any developer to integrate with any application that requires protection via multi-factor authentication.

Detailed Auditing & Monitoring

With AmZetta zMFA, businesses can trace and audit which users have accessed specific corporate data, when the data was accessed, and from where the access took place to discern potential associated risks. zMFA logs and reports pertinent endpoint information which can be leveraged to track the location of access.