ManageEngine
AD360

Learn how to harden your MFA against brute-force attacks

Introduction:
Are your digital doors locked tight enough?

Think of your digital accounts as the front doors to your most valuable assets. Your password? That's just a single lock—useful, but easily picked by a savvy criminal equipped with the right tools. Imagine securing your doors with multiple robust locks, each requiring a different key, or even your fingerprint, to open. This is exactly what multi-factor authentication (MFA) does—strengthening your digital security by adding extra layers of verification.

But here's the catch: Just as thieves can up their lock-picking skills, cyberattackers are getting smarter, increasingly using brute-force tactics to bypass even sophisticated MFA setups. It's no longer enough just to have MFA—you need MFA that’s hardened against these relentless attacks.

In this e-book, you'll discover practical, actionable strategies to reinforce your MFA defenses. From understanding the subtle differences between MFA methods to identifying vulnerabilities you didn't even know existed, you'll learn how to fortify your digital doors so they're practically impenetrable. Ready to ensure that your digital fortress can withstand even the most determined intruders? Let’s dive in.

Understanding MFA

What exactly is MFA? (Definition and key advantages)

MFA is an advanced security process that requires users to verify their identity using two or more methods before gaining access to resources such as apps or online accounts. Unlike simply entering a username and password, MFA will prompt users to enter a code sent via email or text message, answer a security question, provide a fingerprint scan, or insert a hardware token. Common MFA methods include sending a time-based one-time password (TOTP), push notifications, and biometric verification like facial recognition or fingerprint scans.

The primary advantage of MFA is its ability to significantly reduce the risk of cyberattacks. Even if attackers steal a password, the additional security layers present a formidable challenge to unauthorized access. MFA is different from two-factor authentication (2FA) or two-step verification; 2FA generally implies exactly two verification steps, whereas MFA involves two or more. As cloud environments grow and users increasingly access sensitive data from varied locations and devices, identity has become the cornerstone of digital security, making MFA a critical measure.

Exploring different types of MFA factors (Knowledge, possession, inherence, and location)

Typically, MFA employs four main types of authentication factors:

- **Knowledge factors:** Information known only to the user, such as passwords, PINs, security questions, or a TOTP from an authenticator app.
- **Possession factors:** Items physically held by the user, like smartphones receiving SMS codes or push notifications, hardware tokens, security keys, or smart cards.
- **Inherence factors:** Unique biological or behavioral characteristics of the user, including fingerprints, facial scans, voice patterns, or typing behavior.
- **Location factors:** Verification based on the user's physical or network location. Trusted locations might ease access, while unusual locations trigger additional verification steps, highlighting the growing sophistication of context-aware security.

Popular MFA methods and their considerations

Different MFA methods come with unique strengths and potential vulnerabilities:

- **TOTP:** Authenticator apps (e.g., Google Authenticator or Authy) generate temporary codes that refresh approximately every 30 seconds. While user-friendly, TOTPs can become vulnerable if poorly implemented—for instance, without rate limits, attackers might exploit codes using brute force.
- **Push notifications:** Convenient for users, this method sends login requests directly to smartphones, requiring users to simply tap approve or deny. However, push notifications face MFA fatigue attacks, where attackers flood users with repeated requests, hoping they'll eventually approve one.
- **Biometrics:** Leveraging unique physical traits like fingerprints or facial scans, biometrics offer strong security due to the difficulty of replication. Yet, biometric methods require specialized hardware, and concerns persist about the secure storage of biometric data and potential spoofing by advanced attackers.
- **SMS and email OTPs:** Widely accessible, these methods send temporary verification codes via text messages or emails. Although easy and convenient, SMS OTPs face threats like SIM-swapping attacks, while email OTPs become risky if an email account is compromised.
- **Hardware tokens:** Physical devices resembling key fobs or USB sticks generate secure codes directly. Hardware tokens provide robust protection against phishing, but users may find them inconvenient due to portability issues or device compatibility requirements.

Common MFA methods: Security and usability considerations

MFA method	Security strength	Usability	Key considerations
TOTP	Generally strong, especially with short validity periods	Convenient for users with smartphones	Requires secure secret key management and rate limiting
Push notifications	User friendly	Very convenient	Highly susceptible to MFA fatigue attacks
Biometrics	Strong due to unique characteristics	Convenient on devices with biometric scanners	Privacy concerns, potential for spoofing, and hardware dependency
SMS OTP	Widely accessible	Simple to use	Vulnerable to SIM swapping and interception
Email OTP	Accessible to most users	Relatively simple to use	Security depends on the security of the email account
Hardware tokens	Strong, phishing-resistant	Can be inconvenient to carry and may require specific readers	Secure storage and management of tokens are crucial

The growing threat of brute-force attacks against MFA

Brute-force attacks, in the context of MFA, involve attackers attempting to guess the second or subsequent authentication factors after they have potentially compromised the first factor, such as the user's password. These attacks are not limited to any single MFA method and can target various forms of secondary authentication, including OTPs, push notifications, and even biometric verification in certain scenarios. The objective remains the same as traditional brute-force attacks on passwords: to gain unauthorized access by systematically trying different combinations until the correct one is found.

The growing threat of brute-force attacks against MFA

Several common techniques are employed by attackers to target MFA implementations:

Password spraying:

This type of brute-force attack focuses on attempting a small number of commonly used passwords against a large number of accounts. The goal is to exploit the reality that many users choose weak or easily guessable passwords, and by trying only a few passwords per account, attackers aim to avoid triggering account lockout mechanisms that are typically activated after multiple failed login attempts on a single account. This is often described as a "low-and-slow" technique, designed to evade detection over extended periods.

Attackers typically obtain lists of usernames through various means, such as publicly available information or data breaches, and then use databases of common passwords to attempt logins. The success of password spraying is heavily reliant on users employing weak or default passwords across multiple accounts, highlighting the critical need for organizations to enforce strong and unique password policies.

Credential stuffing:

This attack technique involves using stolen username and password combinations, often obtained from previous data breaches, to attempt logins on numerous other platforms and services. The underlying assumption is that many users reuse the same credentials across multiple online accounts. Attackers acquire massive databases of compromised credentials from sources like the dark web and utilize automated tools, such as bots, to perform large-scale login attempts across various websites and applications.

In contrast to password spraying, credential stuffing is often a "high-and-fast" approach. The effectiveness of this technique underscores the importance of users adopting unique passwords for every online account and remaining vigilant about the risks associated with data breaches.

MFA fatigue, MFA bombing:

This social engineering attack exploits the user's potential to become overwhelmed by repeated MFA requests. Attackers, having likely already obtained the user's primary credentials through a tactic like phishing, initiate a barrage of MFA push notifications or other authentication prompts to the user's registered devices. The aim is to fatigue the user into eventually approving one of the requests, either accidentally—or intentionally, to stop the constant stream of notifications—thereby granting the attacker unauthorized access.

This technique capitalizes on the human tendency to prioritize convenience over security when faced with persistent and annoying prompts. Notable real-world examples of successful MFA fatigue attacks include breaches against Uber, Cisco, and Twilio, demonstrating the vulnerability of even seemingly strong MFA methods to social engineering tactics that target user behavior.

Exploiting weaknesses in specific MFA implementations (e.g., AuthQuake):

Attackers often look for vulnerabilities in the design or configuration of specific MFA methods or platforms. A prime example is the AuthQuake vulnerability discovered in Microsoft's MFA implementation. This flaw allowed attackers to bypass the protection by exploiting a lack of rate limiting on failed login attempts and an extended time interval during which TOTP codes remained valid. The extended validity window, intended to accommodate potential time discrepancies and delays, inadvertently provided attackers with a larger timeframe to rapidly generate and test numerous OTP combinations.

This incident highlights that the security of MFA is not solely determined by the inherent strength of the authentication method itself but is also critically dependent on its correct and secure implementation, including the implementation of appropriate rate limiting and timeouts.

Essential best practices for hardening MFA

To effectively defend against brute-force attacks targeting MFA, organizations should implement a range of best practices:

1. Adopt rate limiting for login and MFA attempts

A critical measure to prevent automated brute-force attacks is to limit the number of failed login attempts and MFA challenges that can be initiated within a specific time period. This involves configuring thresholds for both the initial username and password login attempts and the subsequent MFA verification steps. Setting appropriate time windows for these limits, such as allowing only a certain number of attempts per minute or hour, can significantly hinder attackers trying to rapidly guess credentials or MFA codes.

Implementing rate limiting is crucial for mitigating both password spraying attacks, which rely on trying common passwords against many accounts, and direct brute-force attacks against the MFA factor itself, such as attempts to guess OTP codes.

2. Establishing effective account lockout policies

Temporarily locking user accounts after a defined number of consecutive failed authentication attempts is another essential security measure. This prevents attackers from continuously trying different password combinations or MFA codes. Organizations need to define a clear lockout threshold, specifying the number of failed attempts that will trigger the lockout. Additionally, the lockout duration, which determines how long the account remains inaccessible, should be carefully considered. Some systems also incorporate an observation window, which is the timeframe within which the failed attempts are counted.

It is important to strike a balance between setting a sufficiently low threshold and duration to deter attackers while avoiding accidental lockouts of legitimate users who might mistype their credentials.

3. Comprehensive monitoring and alerting for suspicious MFA activity

Implementing robust monitoring systems is vital for detecting and responding to unusual patterns in MFA usage that could indicate an ongoing attack. Security teams should monitor for various indicators, such as a high volume of failed login attempts, particularly if they are spread across multiple user accounts, which could be a sign of password spraying. Unusual login locations or times that deviate from a user's normal behavior should also trigger alerts. Repeated MFA rejections by a user might indicate an MFA fatigue attack or a compromised account. Tracking MFA enrollment and usage rates can help identify gaps in implementation.

Utilizing a security information and event management (SIEM) system can greatly enhance these capabilities by providing real-time monitoring, correlation of events from various sources, and automated alerting on suspicious activity. Proactive monitoring is crucial for the early detection of brute-force attacks targeting MFA, allowing for timely intervention and mitigation of potential damage.

4. Educating users on MFA security and attack vectors

A critical layer of defense against attacks targeting MFA is a well-informed user base. Organizations should conduct regular training sessions to raise awareness among employees about the importance of MFA and the different types of attacks they might encounter, such as MFA fatigue. Users should be trained to recognize and report any suspicious MFA prompts, especially those they did not initiate.

It is crucial to emphasize the dangers of approving unexpected push notifications without verifying their legitimacy. Users should also be educated on the importance of not sharing OTPs or other MFA codes with anyone. User awareness plays a vital role in preventing social engineering attacks that aim to bypass even strong technical security controls.

5. Avoiding less secure MFA methods (e.g., SMS-based OTPs)

The security of the chosen MFA method directly impacts an organization's overall resilience against brute-force attacks. They should prioritize the use of stronger and more resilient MFA factors over those known to have significant vulnerabilities. For instance, SMS-based OTPs, while widely accessible, are susceptible to SIM-swapping attacks and are generally considered a less secure option.

Organizations should consider phasing out or supplementing SMS-based OTPs with more secure alternatives, such as authenticator applications, biometric authentication, or hardware security tokens.

6. Combining MFA with strong and unique password policies

While MFA adds a robust second layer of security, it should not be seen as a replacement for good password hygiene. The first line of defense remains strong and unique passwords. Organizations should enforce password complexity requirements, including minimum length and the use of a mix of uppercase and lowercase letters, numbers, and special characters. The use of common or easily guessable passwords should be prohibited. Encouraging or even enforcing the use of passphrases, which are longer and easier to remember but harder to crack, can also improve security.

Moreover, password reuse should be strictly prevented. Organizations should also consider integrating with services like Have I Been Pwned to automatically block users from using passwords that have been previously compromised in data breaches. A weak password, even with MFA enabled, still represents a potential vulnerability that attackers might attempt to exploit.

Advanced MFA security measures to enhance protection

Contextual authentication (Device, location, time)

This approach leverages information about the user's login attempt to assess the associated risk and dynamically adjust authentication requirements. For example, if a login attempt originates from a device or location that the user has never used before, or if the login occurs at an unusual time, the system might require a stronger form of MFA or additional verification steps. Implementing geo-fencing to restrict access from specific geographic locations can also be an effective way to mitigate risk. Contextual authentication adds a layer of intelligence to the MFA process, making it more adaptive and responsive to potential threats.

Risk-based authentication (Adaptive MFA)

This advanced technique takes contextual authentication a step further by dynamically adjusting the level of authentication required based on a calculated risk score assigned to each login attempt. The risk score is typically determined by analyzing various factors, including the user's location, the device being used, their historical behavior, and the sensitivity of the resource being accessed. Logins deemed to be high-risk might trigger additional authentication factors or even be blocked outright, while low-risk logins might proceed with standard MFA or even a reduced number of factors. Risk-based authentication provides a balance between security and user experience by only increasing authentication friction when the risk warrants it.

Behavioral biometrics

This sophisticated authentication method analyzes a user's unique patterns of interaction with their device, such as their typing speed, mouse movements, and scrolling patterns, to verify their identity. Behavioral biometrics can be used as an additional authentication factor alongside traditional MFA methods or even as a form of continuous authentication, passively monitoring user behavior throughout a session. This approach offers a potentially more secure form of authentication as it is difficult for attackers to replicate the genuine behavioral patterns of a legitimate user.

Phishing-resistant MFA (FIDO2/WebAuthn)

These are authentication methods specifically designed to withstand phishing attacks, a common tactic used to steal credentials. FIDO2 and the underlying WebAuthn standard utilize cryptographic protocols and hardware-backed security keys to ensure that the authentication process is securely bound to the legitimate website or application being accessed. This prevents attackers from intercepting or replaying authentication factors, even if they manage to trick a user into visiting a fake login page. Phishing-resistant MFA is widely considered the gold standard in the industry for protecting against credential theft and should be prioritized for high-risk users and sensitive resources.

How security teams can strengthen their identity security with ManageEngine AD360

The increasing sophistication of cyberattacks necessitates a robust approach to securing access to sensitive resources. MFA is a critical security layer, demanding users provide multiple verification factors to gain access. However, even MFA is susceptible to brute-force attacks, where malicious actors attempt to gain unauthorized access by systematically trying various authentication possibilities.

Security teams can leverage ManageEngine AD360, a comprehensive identity and access management (IAM) solution, to implement a range of best practices aimed at hardening their MFA deployments against such persistent threats. By providing features encompassing rate limiting, account lockout policies, comprehensive monitoring, support for strong authentication methods, and integration with robust password policies, AD360 offers a strong foundation for building a resilient MFA framework.

Leveraging rate limiting in AD360

Rate limiting is a fundamental security technique employed to mitigate automated brute-force attacks by imposing restrictions on the number of login and MFA attempts permitted within a specific timeframe. This approach introduces a significant hurdle for attackers who rely on the speed and volume of automated tools to try numerous authentication combinations rapidly. By limiting the rate at which attempts can be made, organizations can effectively increase the time and resources required for a successful brute-force attack, making it less practical and more likely to be detected.

AD360 provides mechanisms to implement rate limiting for login attempts. The platform allows administrators to configure account lockout policies that automatically block user accounts after a predefined number of consecutive invalid login attempts. This functionality prevents attackers from making unlimited login guesses in a short period. For instance, setting a policy to lock an account after five failed attempts within a 15-minute window inherently limits the rate of unsuccessful logins.

For offline MFA, AD360 allows administrators to set the number of times a user can perform offline authentication based on the number of attempts or the number of days, after which they must connect online for re-authentication. This prevents the potential abuse of offline MFA in scenarios where an attacker might have gained access to a device. Similarly, administrators can enable the configuration of limits for self-service password reset and account unlock actions, which often involve MFA as a verification step. By restricting the number of times these actions can be performed within a given timeframe, the platform indirectly limits the rate at which MFA can be triggered for these sensitive operations.

AD360 rate limiting configuration:

Feature	Description	Configuration options
Login attempt limits	Restricts failed login attempts before account lockout	Number of attempts, lockout duration, reset timer
Offline MFA attempt limits	Limits offline MFA attempts allowed	Number of attempts or days before online re-authentication
Self-service password reset/unlock limits	Restricts password reset/unlock actions within a timeframe	Number of actions, time period
MFA session timeouts	Limits the duration of an active MFA session	Timeout duration

Implementing account lockout policies with AD360

Account lockout policies serve as a critical defense mechanism against brute-force attacks by temporarily disabling user accounts after a specified number of failed authentication attempts. This measure significantly hinders attackers by forcing delays between their attempts, making exhaustive guessing attacks impractical and increasing the likelihood of detection.

Key parameters of an effective account lockout policy include the lockout threshold, which defines the number of failed attempts that trigger the lockout; the lockout duration, which specifies how long the account remains disabled; and the reset account lockout counter, which determines the time after which the failed attempt counter is reset.

AD360 provides robust capabilities for establishing and managing account lockout policies, particularly relevant in the context of MFA. The platform recognizes the importance of account lockout as a primary defense against brute-force attacks. AD360 offers a Block User feature that functions similarly to the account lockout policy in Active Directory. Administrators can configure the maximum number of invalid identity verification attempts allowed within a given time frame and specify the duration for which users should be blocked upon exceeding this threshold. This functionality extends to scenarios where users fail MFA challenges during login or self-service password reset attempts.

With AD360, policies can be applied based on organizational units (OUs) and groups, allowing for tailored lockout settings for different user populations based on their security sensitivity. For instance, more stringent lockout policies with lower thresholds and longer durations might be applied to privileged accounts compared to standard user accounts.

When configuring account lockout policies for MFA, it is crucial to strike a balance between security and user convenience. Setting the lockout threshold too low can lead to frequent accidental lockouts, increasing help desk workload, while setting it too high might provide attackers with too many opportunities to guess credentials. Recommended best practices suggest a lockout duration between 30 and 60 minutes and a lockout threshold between 15 and 50 attempts. Furthermore, considering different security levels for various user groups and implementing fine-grained password policies can further enhance the effectiveness of account lockout in an MFA environment.

AD360 account lockout policy settings for MFA

Setting	Description	Configuration options
Maximum invalid attempts	Number of failed login/verification attempts before lockout	Configurable number of attempts
Lock user	Duration for which the user account is locked after exceeding attempts	Preset period of time (minutes)
Self-service policy	Enforce self-service policies for specific users and groups.	OU- and group-based policies
Integration with AD lockout	Enforce account lockout policies to prevent unauthorized access after multiple failed login attempts	Lockout threshold and lockout duration

Comprehensive monitoring and alerting of suspicious MFA activity

Effective security against brute-force attacks on MFA requires not only preventative measures but also the ability to detect and respond to malicious activity in real time through comprehensive monitoring and alerting. Monitoring login and MFA events can help identify patterns indicative of an attack, such as a high volume of failed MFA attempts, login attempts originating from unusual geographical locations or unfamiliar devices, or atypical patterns in MFA usage.

AD360 provides a range of capabilities for monitoring and alerting on suspicious MFA activity. The platform can track login attempts and identify instances of high volumes of failed logins originating from a single IP address, location, or targeting a specific account within a short timeframe.

Leveraging its user behavior analytics (UBA) features, AD360 can establish baselines of normal user activity and detect anomalies, including unusual logon failures that might signal a brute-force attempt. Administrators can configure alert profiles within AD360 to receive instant notifications via email and SMS when suspicious activities are detected, enabling a timely response to potential threats.

The adaptive MFA capabilities of AD360 further enhance monitoring by evaluating risk factors such as the number of consecutive logon failures, the geolocation of the user requesting access, the type of device being used, and the IP address, allowing for the identification of potentially compromised accounts or malicious actors attempting to gain access. Furthermore, AD360 offers real-time access monitoring and alerting functionalities, providing administrators with immediate visibility into user activities and access attempts.

Security teams can also leverage AD360's reporting and auditing features to investigate suspicious MFA events and identify potential security breaches. They can generate various MFA-related reports, including the MFA Failures Report and MFA Usage Audit Report, which can offer valuable insights into the success and failure rates of MFA attempts. These reports can help identify users experiencing issues with MFA, as well as potential targets of brute-force attacks. Additionally, AD360's auditing capabilities allow for the examination of event logs to trace the source of account lockouts and other suspicious activities. The availability of detailed audit logs and reports specific to MFA events is crucial for post-incident analysis, allowing security teams to understand the attack vector, identify compromised accounts, and refine their security measures to prevent future incidents.

Secure MFA methods supported by AD360

AD360 supports a diverse array of MFA methods, providing organizations with flexibility in choosing options that align with their security requirements and user convenience. These methods include biometric authentication such as fingerprint and facial recognition; TOTPs generated by authenticator applications like Google Authenticator, Microsoft Authenticator, and Zoho OneAuth; FIDO passkeys; YubiKey hardware tokens; smart cards; push notifications sent to trusted devices; email verification codes; SMS verification codes; and more. This wide selection allows organizations to implement MFA across various access points, including machine logins, VPN connections, web applications, and self-service portals.

When hardening MFA against brute-force attacks, it is crucial to prioritize the deployment of more secure MFA methods and avoid less secure options like SMS-based OTPs. While AD360 does support SMS verification, security teams should be aware of the inherent vulnerabilities associated with this method, such as the risk of SIM swapping and interception.

Instead, stronger MFA methods like FIDO passkeys and biometric authentication offer enhanced security and phishing resistance. FIDO passkeys, utilizing public key cryptography, provide a passwordless authentication experience that is highly resistant to phishing attacks and manipulator-in-the-middle attacks. Biometric authentication, leveraging fingerprint or facial recognition, offers a convenient and secure method that ties authentication to the user's unique biological traits. TOTP authenticators, while requiring a separate application, provide a good balance of security and usability by generating time-sensitive codes that are difficult for attackers to intercept or reuse. AD360's support for these stronger authentication methods empowers organizations to move beyond less secure options and build a more resilient MFA infrastructure.

AD360-supported MFA methods and security considerations

MFA method	Security strength	Phishing resistance	Ease of use
Maximum invalid attempts	High	Excellent	High
Biometric authentication (fingerprint/facial recognition)	High	Good	High
TOTP authenticator apps (Google/ Microsoft/Zoho OneAuth)	Medium to high	Good	Medium to high
YubiKey	High	Excellent	Medium
Push notification	Medium	Moderate	High
Email verification	Low to medium	Low	High
SMS verification	Low	Low	High

Enforcing strong password policies with AD360 for enhanced MFA security

While MFA adds a crucial layer of security, the strength of this layer is significantly enhanced when coupled with robust and unique password policies. Even with MFA in place, weak or compromised passwords can still be exploited by attackers. A strong password acts as the initial barrier, increasing the difficulty for attackers in their initial attempts to gain access. By making it harder to guess or crack the primary password, organizations reduce the likelihood of attackers even reaching the MFA stage of the authentication process.

AD360's Password Policy Enforcer provides comprehensive capabilities for establishing and enforcing strong password policies. This feature allows administrators to define custom password complexity rules, including a minimum password length and the requirement for a mix of uppercase and lowercase letters, numbers, and special characters. Furthermore, it enables the banning of weak or leaked passwords, including common dictionary words, keyboard sequences, palindromes, and passwords found in known data breaches through integration with services like Have I Been Pwned.

Administrators can also restrict the consecutive repetition of characters and enforce password history to prevent users from reusing recently used passwords. A key strength of AD360's Password Policy Enforcer is its granularity, allowing for the creation and application of different password rules to specific OUs and groups based on their unique security requirements. This ensures that high-risk users, such as administrators, can be subject to more stringent password policies while maintaining a balance of usability for other users.

By enforcing these robust password policies, AD360 significantly reduces the attack surface for brute-force attempts, making it considerably more challenging for attackers to compromise the initial password and subsequently attempt to bypass MFA.

AD360 password policy features that enhance MFA

Feature	Description	Configuration options
Custom password complexity rules	Define password length and character requirements	Makes initial password guessing harder
Password history enforcement	Prevents the reuse of recent passwords	Reduces risk of exploiting previously compromised passwords
Banning weak and leaked passwords	Blocks common and compromised passwords	Eliminates easily guessable passwords
Custom blocklisted password dictionaries	Allows defining organization-specific banned passwords	Addresses context-dependent weak passwords
Have I Been Pwned integration	Allows admins to identify compromised accounts and take steps to change passwords and strengthen security	Reduces risk of using globally compromised passwords
Granular policy application	Applies different policies to specific OUs and groups	Enables stronger policies for high-risk users

Strengthening your security posture with a resilient MFA strategy

The increasing sophistication of brute-force attacks targeting MFA necessitates a proactive and comprehensive approach to hardening these implementations. Key best practices include implementing robust rate limiting for both login and MFA attempts, establishing effective account lockout policies, ensuring comprehensive monitoring and alerting for suspicious MFA activity, and educating users on MFA security and potential attack vectors. Organizations should also prioritize the use of stronger MFA methods and combine them with stringent password policies.

Furthermore, advanced MFA security measures such as contextual authentication, risk-based authentication, behavioral biometrics, and phishing-resistant MFA offer enhanced protection against evolving threats.

AD360 provides a comprehensive suite of features to implement and manage a resilient MFA strategy. Its support for a wide range of authentication methods, adaptive MFA capabilities, robust password policy enforcement, and comprehensive reporting and auditing tools empower security teams to effectively prevent brute-force attacks and strengthen their overall security posture. By diligently implementing these strategies and leveraging available technologies, your organization can significantly enhance its resilience against credential-based attacks and safeguard their valuable data and resources.

ManageEngine
AD360

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

About AD360

ManageEngine AD360 is a unified identity platform that seamlessly connects people, technology and experiences while giving enterprises full visibility and control over their identity infrastructure. It offers automated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing, compliance and identity analytics—all from a single, intuitive console. With extensive out-of-the-box integrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems to enhance security and streamline identity operations. Trusted by leading enterprises across healthcare, finance, education, and government, AD360 simplifies identity management, fortifies security and ensures compliance with evolving regulatory standards.

For more information, please visit www.manageengine.com/active-directory-360/.

$ Get Quote Download