ManageEngine
AD360

Security measures available in AD360 to ensure data confidentiality

www.manageengine.com/active-directory-360/

Table of Contents

Document summary

AD360 and its components require Domain Admin privileges to carry out all the desired operations. If you do not wish to use a domain admin account, you can use a user account that has been granted sufficient privileges to carry out the desired operations. This guide elaborates all the necessary roles and permissions required for the various features of each component integrated with AD360.

Note: For some components, such as RecoveryManager Plus, you still need an account with admin privilege to use all the features.

HTTPS for secure connection between the web client and server

SSL is a cryptographic technique that provides end-to-end encryption for web requests. By applying a valid SSL certificate in AD360, you can enable HTTPS connection between the client (web browser) and the server (AD360) so that all the information transferred between the two are encrypted and remain safe from security attacks.

AD360 also allows you to centrally apply a SSL certificate and enable HTTPS for the components integrated with it.

Refer to this guide to learn how to enable HTTPS in AD360.

LDAPS for secure connection between AD360 and Active Directory

By default, LDAP communication between a client and the Active Directory server is not encrypted. LDAP over SSL (LDAPS) secures the LDAP connection between the client (in this case, AD360) and the LDAP server (Active Directory server). Once you've applied a SSL certificate in AD, you can configure AD360 to use LDAPS connection for improved security.

Refer to this guide to learn how to enable LDAPS in AD360.

Securing AD360 installation folder from tampering

The AD360 installation directory contains important files required for it to function properly, including files that are used to start and stop the product and the license file. By default, AD360 will be installed in the C:\ManageEngine folder. This will grant even non-admin users belonging to the Authenticated Users group Full Control permission over the files and folders in the product's installation directory, meaning any domain user can access the folder and modify its contents, potentially making the product unusable.

To overcome this issue, you need to manually disable inheritance and remove the Authenticated Users from certain AD360 home folder's ACL.

Refer to this guide for detailed steps.

2FA for login security

To ensure that only authorized users can access AD360, it supports two-factor authentication (2FA). Once enabled, AD360 will require users to authenticate using one of the authentication mechanisms listed below in addition to AD credentials whenever they log in.

- Email Verification
- SMS Verification
- Google Authenticator
- RSA SecurID
- Duo Security
- RADIUS Authentication

Refer to this guide for setting up 2FA in AD360.

Smart card authentication

If you have a smart card authentication system enabled in your environment, you can configure AD360 to authenticate users through it, bypassing other first factor authentication methods. This feature provides an additional authentication option for AD360 login by enabling the use of smart cards/PKI/certificates to grant access to the product. Smart card authentication strengthens the security further because getting access to AD360 shall then require the user to possess the smart card and know the personal identification number (PIN) as well.

When a user attempts to access AD360's web-interface, they would be allowed to proceed further only after completing smart card authentication in the machine, i.e., by presenting the smart card and subsequently entering the PIN.

Refer to this guide for configuring smart card authentication.

Integration with SSO providers for access controls

While 2FA and smart card authentication can safeguard access to AD360, you can take security up a notch by enabling single sign-on (SSO). AD360 supports any SAML-based identity provider, including Okta, OneLogin, Ping Identity, and AD FS, to easily manage secure access to its web console. By enabling SSO, you can use the access policies, adaptive multi-factor authentication (MFA), session management, and other access management techniques available in identity provider to control access to AD360.

Refer to this guide to learn how to enable SAML SSO in AD360.

IP-based access restriction

To further control who can access AD360, you can configure IP-based rules to allow or deny access to the web console. You can allow or deny inbound connections to specific IPs or IP ranges. This adds an extra layer of security by allowing connection from only trusted sources and blocking unwanted and malicious traffic.

Refer to this guide for more information.

API/Product URLs access restriction

You can also control which user can access which feature or API of AD360 by configuring IP-based rules. Similar to IP-based access restriction, which allows or denies access to the entire product, API/Product URLs restriction allows or denies access to a specific product URL (feature, say, the Admin tab) or API call.

Refer to this guide to learn how to restrict API or product URL access in AD360.

Block users after invalid login attempts

Attackers often use brute-force attempts to hack a user account and gain access to applications and resources. To thwart such attempts, AD360 can be configured to block user accounts after a certain number of consecutive invalid login attempts.

AD360 also supports CAPTCHA to prevent bot-based attacks. CAPTCHA serves as a security measure against bot-based brute force attacks. Enabling this setting will display a CAPTCHA image on the login page. End-users must enter the characters shown in the CAPTCHA image to log into the AD360 web portal.
You can configure whether to always show CAPTCHA or only after a certain number of invalid login attempts. Apart from the CAPTCHA image, you can also enable Audio CAPTCHA to assist visually impaired users.

Refer to this guide to configure CAPTCHA and Block User settings.

Role-based Access Control

All the AD360 components come built-in with user roles which define who can access the components and what features of the component that they can access. You can securely grant access to help desk technicians or non-Admin users by assigning them roles. For example, users who have been assigned the Admin role can access and configure all the features of the product, which users with Technician or Operator role can only access the Dashboard and Reports tab, and they cannot make any changes that affect the working of the product.

Steps to configure the roles and assigning them to users vary from component to component. Refer the Admin Guide of each component for more information.

Safety measures against common security threats

AD360 comes built-in with safety measures against some of the common security attacks employed by cyber attackers. These include:

- **Bypassing client-side validations:** By exploiting this vulnerability, an attacker bypasses the client-side input validation for targeted content, say, password fields. Attackers usually bypass a web application's input validations by either removing JavaScript using a web developer tool or by handling the HTTP request (using a proxy tool) in a way that it does not go through the browser. AD360 practices both client-side and server-side validation to defend against this type of attack.

- **Bypassing client-side validations:** By exploiting this vulnerability, an attacker bypasses the client-side input validation for targeted content, say, password fields. Attackers usually bypass a web application's input validations by either removing JavaScript using a web developer tool or by handling the HTTP request (using a proxy tool) in a way that it does not go through the browser. AD360 practices both client-side and server-side validation to defend against this type of attack.

- **Information leakage through comments:** Information leakage occurs when an application unintentionally discloses sensitive data, such as the technical details of a network or application, or user-specific data. Depending on what data is leaked, it could be used by an attacker to exploit the target web application, its hosting network, or the application's users.

  The AD360 team has made sure that no sensitive information is disclosed through comments in the source code.

- **Cross-site request forgery (CSRF) vulnerability:** CSRF is an attack that tricks a web browser into executing an unwanted command in an application that a user is logged in to. This is accomplished by a user inadvertently clicking a malicious link on a legitimate website. This sends a HTTP request the user did not intend to raise, which includes a cookie header that contains the user's session ID. Also, because the application authenticates the user at the time of the attack, it's impossible for the application to distinguish between legitimate and forged requests.

  AD360 sends out every request with a token. This prevents the execution of actions that do not provide necessary authentication tokens.

- **Weak SSL cipher:** An application relying on SSL/TLS for data transmissions with weak ciphers leaves the application unprotected and allows an attacker to steal or manipulate sensitive data.

  AD360 allows you to replace the cipher technique used by default to another method that is stronger based on your requirement.

- **SQL injection through framework build:** SQL injection occurs when an attacker adds or injects malicious code into a SQL statement executed by the web application. A successful SQL injection allows attackers to spoof a user's identity, tamper with existing data, and even gain complete control over the web application's server.

  Database operations for AD360 are handled through our internal framework to prevent SQL injections and other similar attacks.

DES and AES-256 encryption methods for data storage

All the product-related data, such as domain details, details of accounts that use AD360 authentication, etc., are stored in the product using strong encryption methods for maximum security. Different components employ different encryption methods for various purposes, such as DES, AES-256, and SHA-512. All the encryption methods used in AD360 are some of the most secure encryption technique and are considered to be logically unbreakable.

Session expiration to terminate idle sessions

AD360 supports Session Expiration, which terminates the inactive session of users based on a predefined period. If a user walks away from their computers without logging out of AD360 or locking their computer, anyone can access the product and make unauthorized changes. The Session Expiration feature reduces the possibility of someone accessing the inactive session of an authorized user. When the inactive time limit is reached, the user will be locked out automatically. The user must log back in to continue with the session.

Refer to the General section in this guide for steps to configure Session Expiration.

Reverse proxy support to conceal server identity

A reverse proxy is a server that's used as a strategic point in the network. It enforces web application security by hiding the location and identity of a server when remote users access an application over the internet. The reverse proxy server receives requests from external clients and forwards them to the target web application servers, which are usually located inside the LAN and are not directly accessible from outside. It also receives the response from the servers and forwards it to the client. Throughout this whole process, the client assumes that the reverse proxy is the web application server.

AD360 comes built-in with a reverse proxy server. You can use AD360 to act a reverse proxy for itself and the products that you've integrated with it. AD360 lets you enable a context-based reverse proxy, a port-based reverse proxy, or both.

Refer to this guide for configuration steps.

Audit report for monitoring admin and user activities

All the actions performed by the admins, technicians, and other users are recorded in audit reports in each component. These reports provide information on who made which change, when, and from where. You can define how often these report must be generated, export these reports in various file formats, and configure it to be delivered through email to various stakeholders.

SIEM integration for advanced security analytics and threat detection

For in-depth analysis and threat analysis, you can forward the logs generated by its components to a syslog server or SIEM solution. This help you gain even better understanding of how users use AD360 and its components, detect threats, and more.

Refer to this guide for more information.

High availability for uninterrupted service

High availability describes a family of practices aimed at delivering a specific level of availability by eliminating or mitigating failure modes. AD360 supports high availability in case of system and application failures. High availability is achieved through automatic failover: when the AD360 service running on one machine fails, another instance of the AD360 service running on a different machine will automatically take over. You can set up and manage high availability for AD360 and its integrated components directly from the AD360 console.

Refer to this guide for more information.

About AD360

AD360 is an identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. AD360 provides all these functionalities for Windows Active Directory, Exchange Server, and Office 365. With AD360, you can choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments—all from a single console.

For more information about AD360, please visit www.manageengine.com/ad360

$ Get Quote Download