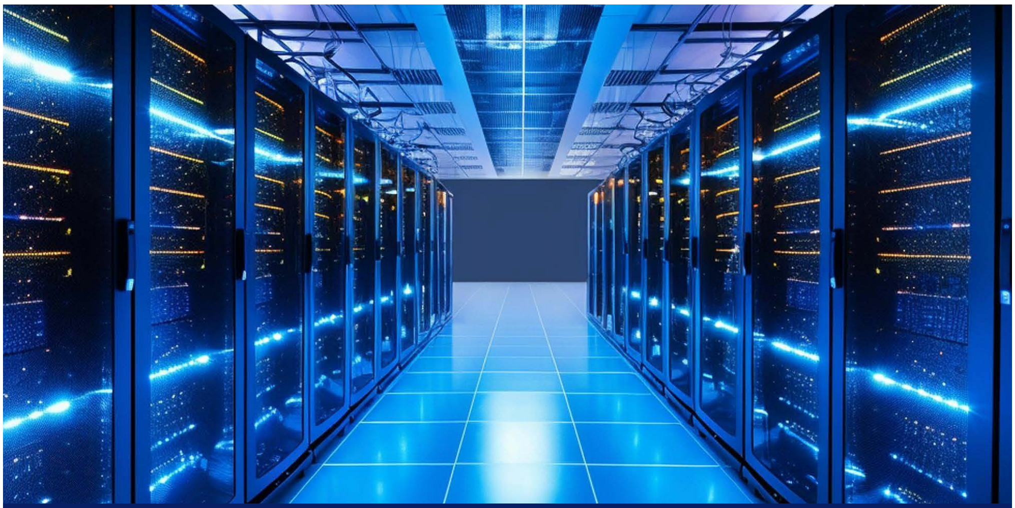
ManageEngine
ADManager Plus

Data protection techniques and security measures adopted by ADManager Plus

www.admanagerplus.com

Table Of Contents



How do we secure the ADManager Plus installation directory?

Safeguarding the product installation directory is vital, as this is the storehouse of all the program data which can be manipulated if it falls into wrong hands. The installation must be well-secured to guarantee that ADManager Plus is tamper proof against manipulation.To secure the directory, an elaborate set of steps must be taken which are outlined in this guide.

How do we secure the data in transit?

The web communication between the ADManager Plus client and the server happens using HTTPS. Admins can set HTTPS as the default protocol through the Admin settings in the product. For more security, we can set up an LDAP over SSL connection to secure the information exchange between ADManager Plus and the LDAP servers. Along with this, all the .ppm files used to update the product are digitally signed to verify that they come from a trusted source. This ensures that data in the .ppm file has not been tampered with, validating the authenticity of software updates.

How do we secure ADManager Plus' database?

In today's data-driven world, many companies search for an IT solution to ensure that their database security remains intact. Here is how ADManager Plus' database is secured:

Database passwords

Database passwords, which are random for each ADManager Plus installation, are encrypted using CryptTag with the AES-256 algorithm.

Database encryption key

The randomly generated database encryption key is encrypted using CryptTag with the AES-256 algorithm.

Database access

Server admins, users with access to installation folder, or users with access to server machines can access the built-in database from a local host.

Built-in technician password

Built-in technician passwords are stored in the database as a hashed value using the BCrypt algorithm with salt.

Database backup

The database back-ups are always protected with passwords. We use the unique CryptTag value as a password available in the conf or customer-config.xml file in the ADManager Plus installation folder. We can also manually set the password for the zip files in the admin settings

How do we ensure the security and privacy of data handled by ADManager Plus?

The Security Hardening and Privacy settings available under the Admin tab in ADManager Plus assists in securing the product. These settings enable you to protect ADManager Plus during logins, data transit, and redirections.

The Privacy Settings tab is where you can enable password protection for exported reports and enable data anonymization for added privacy.

The Security Hardening tab, on the other hand, helps fortify the security of the product which includes different options like,

Enforce HTTPS

Establish a secure connection between web browsers and the ADManager Plus web server. Click here to learn how to enable HTTPS in ADManager Plus.

Change default admins password

Change the default password and use a strong one to strengthen the security of the Admin account and, to ensure it is not compromised, change it periodically. Click here to learn how to change the default admin account's password.

Enforce two-factor authentication

Add an additional layer of security while logging in to ADManager Plus. For more information on 2FA services available in ADManager Plus, refer to this help document.

Enable CAPTCHA

Configure CAPTCHA settings after a specific number of invalid login attempts to mitigate bot-based attacks. Click here to learn how to enable CAPTCHA in ADManager Plus.

Allow/restrict IPs

As an added security measure, list the IP addresses to block or provide access to ADManager Plus by referring to the steps mentioned here.

Block invalid login attempts

Block a particular technician's account once a specific number of consecutive unsuccessful login attempts have been made. Click here to learn how to block invalid technician login attempts in ADManager Plus.

Enforce secure TLS

Ensure older TLS versions are disabled. ADManager Plus supports TLS versions 1.0, 1.1, and 1.2. Click here to learn how to enforce secure TLS in ADManager Plus.

Secure installation directory

As noted above, ensure that the installation directory is either C:\Program Files or C:\Program Files(x86) to limit access to run or alter the product to admins only.

Hide password in the product GUI

We can hide the password from being displayed in the product UI while executing password specific tasks using this option.

Other security measures

Role-based access control: ADManager Plus enables you to compartmentalize your data among the product's technicians. For delegation of actions, we provide nine default roles that can be assigned to users and three built-in users such as administrator, help desk technician, and HR associate. These roles are used to limit user access, and to control specific features and device information. In addition to these built-in roles, you can create customized roles too. This way, you can ensure that data is accessed only by authorized personnel.

ADManager Plus admin audit report: ADManager Plus provides a built-in option to generate an audit trail of all the actions performed on users with different help desk roles and technicians. This enables you to ensure accountability within the solution itself.

Session termination after idle time: WithADManager Plus, you can set up a session expiry time and if the session is idle for more than 10 minutes (which is the minimum time), then the session will be terminated.

Export report with passwords: ADManager Plus provides a built-in option to export reports in the required format that are protected with a strong passwords set in Admin Settings.This way, you can ensure that the report data is only seen by an authorized personnel.

Email server communication: The JavaMail API used for email communication is encrypted using SSL and TLS algorithms.

Active Directory authentication: Active Directory logins are performed using the Kerberos/NTLM authentication mechanism.

External app communication: Secured data such as Authtokens that support REST API communication and passwords are encrypted in the database and hidden within the product.The audits for data received from external applications through webhooks are available and can be accessed in the webhook history within the product. Moreover, for in-bound and out-bound data flow, we support external application's authorization standards.

Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus

M365 Manager Plus | RecoveryManager Plus

About ManageEngine ADManager Plus

ADManager Plus is an identity governance and administration (IGA) solution that simplifies identity management, ensures security, and improves compliance. With ADManager Plus, manage the user life cycle from provisioning to deprovisioning, run access certification campaigns, orchestrate identity management across enterprise applications, and protect data on your enterprise platforms with regular backups. Use over 200 reports to gain valuable insights into identities and their access rights. Improve the efficiency of your IGA operations with workflows, automations, and role-based access control policies. ADManager Plus' Android and iOS applications help with on-the-go AD and Azure AD management.
For more information about ADManager Plus, visit manageengine.com/products/ad-manager/.

$ Get Quote

⤓ Download