ManageEngine
Access Manager Plus

Security specifications

Overview

ManageEngine Access Manager Plus is a web-based privileged session management software that regulates access to remote systems through secure channels from a unified console.

Access Manager Plus deals with administrative access to critical enterprise systems, and any compromise on its security framework will expose organizations to serious risks. Therefore, Access Manager Plus architectural design comes with a range of security and privacy checks, that cover various stages of the product workflow—installation, user authentication, access control, data transmission, and storage. This document provides an overview of the security and privacy specifications in Access Manager Plus.

Note: This document outlines the security and privacy settings specific to Access Manager Plus only. To read about ManageEngine's overall security policy, click here .

Access Manager Plus protects data at various levels and is classified into the following categories:

Security specifications	
1. Vaulting and encryption mechanism	• AES-256 encryption • Dual encryption—first at the application and then at the database level • Encryption key and encrypted data cannot reside together • FIPS 140-2 compliant mode • SafeNet Luna PCIe HSM

2. Identification and authentication	**Application-level authentication** • Integration with identity stores like Microsoft AD, Azure AD, any LDAP-compliant directory service, Azure AD, and RADIUS • Local authentication mechanism using the SHA2 (SHA512) algorithm • Smart card authentication • SAML 2.0 single sign-on **Two-factor authentication** • PhoneFactor • RSA SecurID • One-time unique password sent by email • Google Authenticator • RADIUS Authenticator • Microsoft Authenticator • Okta Verify • Duo Security • YubiKey
3. Data security and integrity	**Data transmission** • Encrypted and over HTTPS • SSL mode for client connections **Data storage and management** • Dual AES-256 encryption **Web GUI input validation** • Protection against SQL injections, cross-site scripting, buffer overflow, and other attacks **IP restrictions** • Web-based IP restrictions

	Privacy settings • Masking of sensitive data
4. Access control measures	**Data access control** • Granular access control mechanism • Request-release workflow for password access • Ticketing system integration
5. Secure remote access	**One-click remote connections** • Windows Remote Desktop Protocol (RDP), SSH, SQL, and VNC sessions from any HTML5-compatible browser • No need for additional plug-in or agent software • Remote connections are tunneled through the Access Manager Plus server • RemoteApp support for Windows • Passwords needed to establish remote sessions do not need to be available on the user's browser • No direct connectivity between user device and remote host • Bidirectional remote file transfer
6. Privileged session management	• Privileged session recording and playback • Real-time monitoring • Session collaboration and termination

7. Audit, accountability control, and real-time alerts	**Detection capabilities and non-repudiation measures** • Real-time alerts for password, user, and access events • In-depth audit trails • SIEM support • SNMP traps and syslog messages
8. Backup and disaster recovery	**Provision for backup** • Live and periodic database backup • Encrypted storage of backup files **System failure recovery** • Disaster recovery with MS SQL server and PostgreSQL server
9. Build and patching process	• Mandatory vulnerability scans and penetration tests • Hotfix builds and bug fixes

1. Vaulting and encryption mechanism: Secure by design

1.1 Installation of master key

- Access Manager Plus uses AES-256 encryption (the strongest known encryption that the US government has approved). The key used for encryption is auto-generated and is unique for every installation. This serves as the first-level encryption key.

- The first-level encryption key is not allowed to be kept with the Access Manager Plus installation. This is done to ensure that the encryption key and the encrypted data, in both live and backed-up databases, do not reside together.

- The recommended setup is to store the key in a physically separate server or device and ensure that it is available to the server during application start-up. Subsequently, the key is held only in the server memory and never written anywhere.

- Access Manager Plus also supports periodic rotation of the encryption key, where a new key is generated and applied to the existing data and then the old key is discarded. More info

1.2 Database key

- The Access Manager Plus database is secured through a separate key, which is auto-generated and unique for every installation.

- The key for the database can be stored securely within Access Manager Plus.

- Access Manager Plus also allows users to store the database key in any secured location, leaving the key accessible to only the server.

- The RDBMS is always configured to accept only secure connections (forces SSL mode for client connections) and clients can connect only from the same local host. In cases where

the web server and the RDBMS have to reside in separate servers, the configuration enforces connections only from configured IP addresses.

1.3 FIPS-compliant mode

- Access Manager Plus can be set up to run in the FIPS 140-2-compliant mode (using a SQL server as the backend database) where all encryption is done through FIPS 140-2-certified systems and libraries.

1.4 SafeNet Luna PCIe HSM

- Access Manager Plus also provides support for SafeNet Luna PCIe HSM to give administrators the option to enable hardware data encryption.
- SafeNet HSM handles all the encryption and decryption methods, and stores the encrypted key and data directly in its hardware module, which is fitted to a computer or a network server.

2. Identification and authentication

2.1. Strong application-level authentication: Various options

Access Manager Plus provides various options for uniquely identifying the users who will be accessing the application. All the options are complemented by various two-factor authentication provisions, which provide an extra layer of security.

- **Integration with identity stores:** Access Manager Plus readily integrates with external identity stores like Microsoft Active Directory, any LDAP-compliant directory service (Novell eDirectory and Oracle OID), and RADIUS. Users can be imported from identity stores and the respective authentication mechanism can be leveraged. Users will be uniquely identified through their respective accounts in the identity store. More info.

- **Unique accounts and strong local authentication:** Access Manager Plus comes with a local authentication mechanism in which unique accounts are created for users. Users will be able to access the application with their credentials. Access Manager Plus employs the SHA2 algorithm to generate passwords, which ensures that each login password is unique and irreversibly secured.

- **Common access card:** supports smart card authentication. The user must possess the smart card and know the personal identification number (PIN) as well. For more details, click here.

- **SAML compliant service:** Access Manager Plus offers support for SAML 2.0, which facilitates integration with federated identity management solutions for single sign-on. Access Manager Plus acts as the service provider (SP) and it integrates with the identity provider (IdP) by using SAML 2.0. The integration basically involves supplying details about the SP to the IdP and vice versa. After you integrate Access Manager Plus with an IdP, the logged-in users can log on from the respective identity provider's GUI without providing the credentials again. For more details, click here.

2.2. Assurance mechanism: Two-factor authentication (2FA)

To introduce an additional level of security, Access Manager Plus provides two-factor authentication. Users will be required to authenticate through two successive stages to access the web interface. The second level of authentication can be done using one of the following:

- **PhoneFactor:** This leading global provider of phone-based 2FA enables simple and effective security by placing a confirmation call to your phone during the login process.

- **RSA SecurID:** Integrate RSA SecurID with Access Manager Plus to generate a one-time validation token that changes every 60 seconds.

- **Unique password through email:** Authenticate by emailing users unique passwords. The passwords validate the user for one login session and then expire.

- **Google Authenticator:** Time-based numeric tokens can be received by installing the Google Authenticator app on your smart phone or tablet.

- **RADIUS Authenticator:** Leverage the authentication mechanisms of any RADIUS-compliant system, such as Vasco Digipass, to create one-time passwords.

- **Microsoft Authenticator:** Provide the six-digit token on the Microsoft Authenticator app.

- **Okta Verify:** Use the six-digit token on the Okta Verify app.

- **Duo Security:** Leverage Duo security authentication.

- **YubiKey:** Generate one-time passwords with YubiKey.

- Apart from these, Access Manager Plus supports any TOTP-based authenticator.

For more details, click here.

3. Data security and integrity

3.1 Data transmission

- All data transmissions between the Access Manager Plus user interface and the server are encrypted and take place through HTTPS.

- All data transmission between the Access Manager Plus server and database occurs over SSL.

- Communication between the primary and secondary servers is encrypted over HTTPS.

3.2 Data storage and management

- Access Manager Plus is designed as a web application with a web server for business logic and RDBMS for data store.

- Upon applying appropriate initialization vectors and other standard good practices around encryption, the first-level encryption key with AES-256 algorithm is generated in the web server.

- The encrypted data is pushed to the RDBMS for storage by using SQL queries. Next, Access Manager Plus encrypts the data with built-in AES functions of RDBMS for dual layers of encryption.

- The recorded data of privileged sessions is also encrypted before storage and can be played only through the proprietary player because data is stored in the proprietary format.

3.3 Web GUI input validation

- Access Manager Plus thoroughly validates all inputs in the GUI. Use of special characters and HTML code are filtered, and the application is guarded against common attacks like SQL injections, cross-site scripting, buffer overflows, and other attacks.

3.4 IP restrictions

- Access Manager Plus allows administrators to limit inbound connections to the Access Manager Plus server by enforcing IP-based restrictions to minimize unwanted traffic. It provides an added layer of security by letting the administrator choose exactly which systems should be allowed to or blocked from accessing and sending requests to the Access Manager Plus server.

3.5 Privacy settings

- Access Manager Plus provides privacy settings to enhance privacy within the product. Privacy settings helps admins mask or control the inclusion of personally identifiable information (PII) in the product. This information can be a user's name, phone number, or location, or a resource's DNS name, department, URL, or secondary domain controller name.

4. Access control measures

4.1 Data access control

- All data access in Access Manager Plus is subjected to the granular access control mechanism. Resource ownership and sharing practices are well-defined, and users get access only to authorized passwords.

- For highly sensitive assets, an extra layer of security could be enforced by forcing the authorized users to go through a request-release mechanism. Whenever a sensitive IT resource needs to be accessed, a request must be made, which goes to the administrator (persons who are designated to authorize access) for approval and is released for a limited time period. More info.

- All access to resources (who accessed what resource and when) and all operations performed by users on any resource are captured in audit trails, ensuring accountability for all users and actions.

- **Ticketing system integration:** Access Manager Plus also integrates with a wide range of ticketing systems to automatically validate service requests related to privileged access. The integration ensures that only users with a valid ticket ID can access the resources. This integration also extends to the Access Manager Plus workflow, which helps in granting approvals to password access requests upon automatic validation of corresponding service requests in the ticketing system.

5. Secure remote access

5.1 One-click remote connections

- Access Manager Plus allows users to launch highly secure, reliable, and completely emulated Windows RDP, SSH, SQL, and VNC sessions from any HTML5-compatible browser without the need for additional plug-in or agent software. More info.

- Remote connections to end points are tunneled through the Access Manager Plus server, requiring no direct connectivity between the user device and remote host.

- In addition to superior reliability, tunneled connectivity provides extreme security, as passwords needed to establish remote sessions do not need to be available on the user's browser.

- **RemoteApp support:** Access Manager Plus allows users to connect to particular apps that are configured as RemoteApps in the target systems. Adding RemoteApps to RDP connections increases accessibility and ease of use when connecting to remote machines, and makes privileged sessions easier to control for IT admins, as it limits a user's access to the particular application that is launched. More info.

- **Bidirectional remote file transfer:** Access Manager Plus allows users to upload and download files to and from any remote system. Access Manager Plus is capable of bi-directional file transfer i.e., you can transfer files between different paths in two systems. Bi-directional file transfer is achieved using the Secure File Transfer Protocol (SFTP). More info.

6. Privileged session management

- All actions performed by the users during the privileged session are video recorded and stored securely for future forensic analysis. More info.

- In addition to session recording, Access Manager Plus allows administrators to monitor privileged sessions in real time. If any suspicious activity is found, the administrator can snap the connection immediately.

7. Audit, accountability control, and real-time alerts

7.1 Detection capabilities

- Access Manager Plus provides real-time alerts and notifications on various events, including access, modification, deletion, changes in share permissions, and other specific events. More info.

- The audit module, which records every user and system action, also lets administrators configure what events need to be sent to security information and event management (SIEM) systems. The event alerts can either be sent as standard syslog messages or SNMP traps. More info.

7.2 Non-repudiation measures

- Every action and scheduled task executed by users in the user interface is audited.

- The audit information, which contains details such as who did what operation, when, and from where is stored in the same database. The audit logs are tamper-proof, ensuring non-repudiation.

- The RDBMS is always configured to accept only secure connections (forces SSL mode for client connections), and clients can connect only from the same local host. In cases where the web server and the RDBMS have to reside in separate servers, the configuration allows connections only from specific IP addresses.

8. Backup and disaster recovery

8.1 Provision for backup

- Access Manager Plus offers provisions for both live backup of the database and periodic backup through scheduled tasks.

- All sensitive data in the backup file is stored in the encrypted form in a ZIP file under the default backup directory or under the destination directory configured by the admin.

- The backup copy will not have the encryption master key because Access Manager Plus does not allow both the encryption key and the encrypted data in both live and backed-up database to reside together. Unless one presents the encryption key, sensitive data cannot be deciphered from the backup copy.

- While a database backup operation is in progress, no configuration change can be performed in Access Manager Plus. More info.

8.2 System failure and recovery

- In the event of a disaster or data loss, users can quickly make a fresh install of the same version of Access Manager Plus and restore the backed-up data to the database.

- Disaster recovery for Access Manager Plus with MS SQL server or PostgreSQL server as the backend database can be performed only with the master key initially used for encryption upon installation. More info.

9. Build and patching process

- The Access Manager Plus team works closely with the MESRC to run mandatory vulnerability scans and penetration tests before every major release to ensure that the latest builds are completely foolproof. In addition, the team also runs continuous vulnerability assessments on these builds to ensure that they are free from any new vulnerabilities.

- Users are notified immediately to upgrade to the latest version as and when there is a new security patch or update.

- In the event of a security concern or escalation, users are requested to submit a detailed report on the vulnerability or security bug. Meanwhile, the product team evaluates the validity and risks associated with the bug and prioritizes the release based on the severity.

- Hotfix builds are released within 24 to 72 hours of reporting of an issue depending on the severity of the issue, and the team will approve the builds for release only after they have been tested for further vulnerabilities or bugs.

manageengine.com/amp

Technical support

Telephone: +1 408 454 4014

Email: amp-support@manageengine.com

ManageEngine

Access Manager Plus