



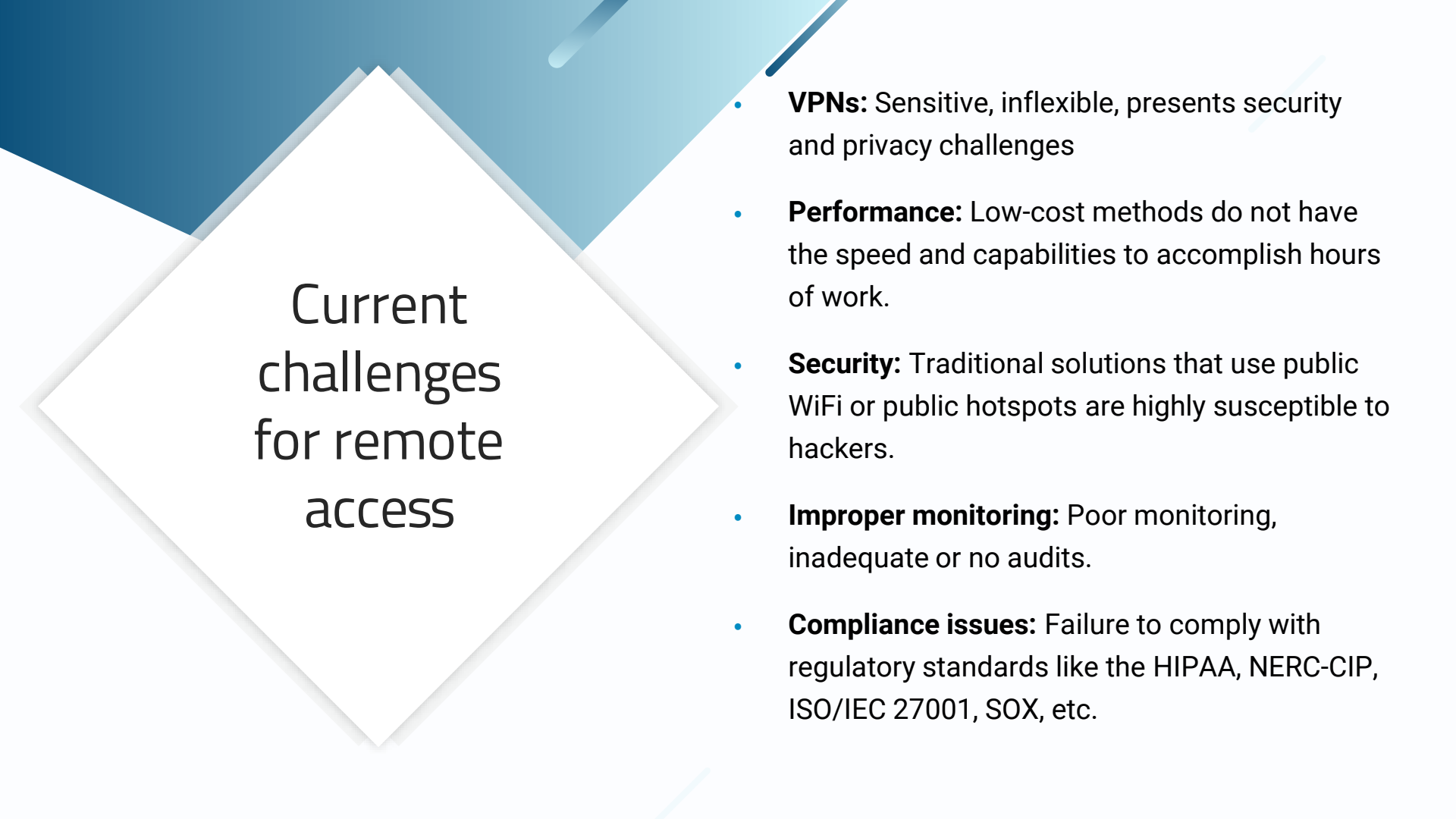
ManageEngine Access Manager Plus

Privileged session management (PSM) solution

- A PRODUCT OVERVIEW

Contents

- [Current challenges for remote access](#)
- [Need for a privileged session management solution](#)
- [Access Manager Plus - Key features](#)
- [Licensing and editions](#)
- [Other resources](#)



Current challenges for remote access

- **VPNs:** Sensitive, inflexible, presents security and privacy challenges
- **Performance:** Low-cost methods do not have the speed and capabilities to accomplish hours of work.
- **Security:** Traditional solutions that use public WiFi or public hotspots are highly susceptible to hackers.
- **Improper monitoring:** Poor monitoring, inadequate or no audits.
- **Compliance issues:** Failure to comply with regulatory standards like the HIPAA, NERC-CIP, ISO/IEC 27001, SOX, etc.

Need for a PSM solution

- To provide secure, authorized connections to remote resources.
- To ensure a reliable and faultless audit trail of every action taken by privileged users.
- To maintain a satisfactory incident response record.
- To prove regulatory compliance with various standards like HIPAA, GDPR, SOX, PCI, and ISO 2700.
- To monitor, audit, and control privileged sessions launched by users across both on-premises and cloud-based applications.
- To respond to an insider attack promptly, or prevent it from happening altogether.
- To protect critical enterprise information when granting access to third-party vendors.

Access Manager Plus

- Key features

1. Effective user management
2. Solid user authentication with TFA
3. Access control workflow
4. Help desk integration
5. Data center remote access
6. One-click remote sessions
7. RemoteApp support
8. Bi-directional remote file transfer
9. Privileged session recording and playback
10. Live monitoring and collaboration
11. In-depth audit trails

1. Effective user management

- Access Manager Plus comes with two predefined user roles – Administrator and Standard User.
- Users in Access Manager Plus can be grouped based on the connection type, or based on the OUs or groups during import from AD.
- User groups allow you to set preferences or assign functions in bulk instead of doing so for each user individually.
- In addition to pre-defined user roles, the administrator can also create **custom roles** for users.
- There are several ways to add users into Access Manager Plus:
 - Add manually
 - Import users from files with CSV or TXT extensions
 - Import from AD/ Azure AD/ LDAP

2. Solid user authentication with TFA

Access Manager Plus provides different types of authentication methods to allow users to rightfully authenticate into the system and prevent unauthorized access.

Primary authentication methods

- Local authentication
- AD/ LDAP/ Azure AD
- RADIUS-based authentication
- Smart card / PKI / certificate
- SAML single sign-on: Okta, Azure AD, ADFS

Two-factor authentication

- PhoneFactor
 - RSA SecurID
 - Google Authenticator
 - Microsoft Authenticator
 - Okta Verify
 - RADIUS-based authentication
 - Duo Security
 - YubiKey
 - Unique password sent through email
-

3. Access control workflow

- Access control mechanism allows users to restrict access to the connections added by them.
- When the access control is in place, no user other than the connection owner will be able to view the passwords or launch a remote connection unless their access request is approved by the owner.
- **Access control workflow:**
- An Administrator or a Standard User enables access control for a connection added by them.
- The user makes a request to access the connection.
- The request is sent to the connection owner for approval. If more users require access to the same connection, all the requests will be queued up for approval.

4. Help desk integration

- Access Manager Plus comes with the facility to integrate with a wide range of ticketing systems to automatically validate service requests related to privileged access.
- The integration ensures only users with a valid ticket ID can access the connections stored in Access Manager Plus.
- The entire process is completely audited - privileged actions and access can be traced using ticket IDs or other attributes.
- The available ticketing systems are:
 1. ManageEngine ServiceDesk Plus On-Demand
 2. ServiceDesk Plus MSP
 3. ServiceDesk Plus
 4. ServiceNow
 5. JIRA

5. Data center remote access via landing servers for RDP and SSH

- Access Manager Plus effectively simplifies the entire process of data center remote access management.
- Configure any number of landing servers to remotely access the IT equipment in your data centers by associating the landing servers with the connections being managed in Access Manager Plus.
- Once the configuration is done, you can launch a direct connection to the remote resources with a single click without worrying about the intermediate hops.
- Access Manager Plus takes care of establishing connection with the landing server(s) and finally with the remote resources, in a fully automated fashion.

6. One-click remote sessions

- You can add RDP, SSH, SQL, and VNC connections manually, or discover Windows and Linux accounts automatically.
- Users can launch highly secure Windows RDP, SSH, VNC, and SQL sessions with a single click, without the need for passwords.
- The sessions require no direct connectivity between the user device and the remote host, and there is no need for installing any plug-in or agent in any of the end-points.
- The only requirement is that the browsers should be HTML 5-compatible such as Google Chrome, Mozilla Firefox, Safari, and Microsoft Edge.
- Customize advanced settings for connections to improve the speed and performance of the remote connections initiated from within the product.
- **Examples:** Keyboard layout, desktop backgrounds, map drives, remote audio support, etc.

7. RemoteApp support for Windows

- Access Manager Plus allows users to connect to particular apps that are configured as RemoteApps in the Windows target systems.
- Configuring RemoteApps for Windows connections limits a user's access to the particular application that is launched, instead of the entire remote desktop.
- **For example**, consider that if you've whitelisted an app, say SQL Studio, for a particular user. Now, when the user launches a session, it will automatically open SQL Studio and the user can only use that application. They cannot see the taskbar or navigate to any other area or perform any other operation other than using SQL Studio.
- Besides allowing manual addition of remote apps, Access Manager Plus also automatically discovers RemoteApps configured in the target Windows systems.

8. Bidirectional file transfer

- Transfer files between a remote system and the local host, or between two remote systems, right from the Access Manager Plus web interface.
- Upload or download files on the remote device.
- This feature is achieved using the SSH file transfer protocol (SFTP).
- There is no size limit imposed for the bi-directional file transfer mechanism.

9. Privileged session recording and playback

- Record and archive the privileged sessions launched from Access Manager Plus web interface as video files.
- Session recording allows enterprises to monitor and control all actions performed by the privileged accounts during privileged sessions, and support forensic audits and compliance requirements.
- Record Windows RDP, SSH, SQL, and VNC sessions launched from the Access Manager Plus web interface.
- Trace sessions using any detail such as the name of the connection, the user who launched the session, or the time at which the session was launched.
- You can also purge recorded sessions that are older than a specified number of days.

10. Live monitoring and session collaboration

- Access Manager Plus lets administrators monitor the privileged sessions on highly sensitive IT assets.
- Shadowing allows admins to join active sessions, observe user activities in parallel, and terminate them in case of suspicious activities.
- Admins can also offer assistance to users while monitoring their activities during troubleshooting sessions.
- Using session collaboration, you will be able to work with session in parallel and perform the same operations as the user who initiated the session.

11. In-depth auditing

- Every single action performed by the user is recorded along with the files they had access to.
- The timestamp and the IP address of all the operations performed by the users are audited within the application.
- Access Manager Plus provides the flexibility of sending notifications to the required recipients whenever a desired event occurs.
- Access Manager Plus allows users to raise SNMP traps and send syslog messages to external log management systems.
- SNMP traps and syslog messages are collected for various audit events, and they help in determining the success or failure of a particular action along with the reason for the same.

Licensing and editions

- Licensing is based on two factors:
 - Number of connections – The maximum number of connections to remote systems via Access Manager Plus at a given point of time.
 - Type of edition – Free or Standard
- **Free Edition** – If your requirement is to have a secure remote access tool to connect to the target systems, the Free Edition would be ideal for you.
- **Standard Edition** – Apart from establishing secure remote connections, if you wish to have enterprise-grade privileged session management features such as access controls, RemoteApp support, session recording and monitoring, session termination, etc., the Standard Edition would be the best choice.
- More extensive edition comparison is available [here](#).

Other resources

- > [System requirements](#)
- > [Product datasheet](#)
- > [Brochure](#)
- > [Online help documentation](#)
- > [Best practices guide](#)

Thank you!

accessmanagerplus-support@manageengine.com

amp-support@manageengine.com