ManageEngine
Access Manager Plus

Privileged session management

Establish a strong foothold in the fight against privileged access misuse by controlling, monitoring, and recording privileged sessions of high-risk accounts.

What is a privileged session?

A privileged session is an internet session launched by a user with administrative privileges while accessing a system, device, or application in the IT infrastructure—either locally or remotely—and comprises all the activities carried out during that session.

A privileged session can be a database or security administrator accessing confidential corporate information at the data center via an RDP or SSH session; a third-party vendor remotely accessing specific enterprise applications via a remote access tool; or a maintenance engineer accessing critical servers located in various industrial plants and automation systems, like PLCs and SCADA, for troubleshooting or software patching.

The security risks associated with privileged sessions

If you're an IT administrator, you know initiating a privileged session today is a risky yet inevitable task. Although a mix of both modern and traditional tools and technologies can help enterprises facilitate remote access and boost operational efficiency, unchecked privileged access also introduces a host of new challenges in terms of security and compliance.

1. Organizations often play down privileged accounts

Privileged accounts and the credentials that secure them are tapped into an organization's most critical systems, because they have the highest permission levels. Not surprisingly, privileged accounts remain a ripe target for cybercriminals. If an attacker were to gain access to just one mismanaged privileged account, they could easily escalate their access to the most sensitive systems inside the

network. Such malicious privileged sessions enjoy the benefit of the doubt since they're launched via legitimate privileged accounts by attackers impersonating privileged users.

2. The results of Internet of Threats

Sensitive business data, like privileged accounts, certificates, tokens, keys, and passwords, are prime targets for cybercriminals, because they offer unrestricted privileged access to every nook and cranny of the IT infrastructure. To minimize risks and balance IT security against productivity, organizations must provide appropriate, controlled access for privileged users to secure critical systems. If privileged sessions are not managed with tight controls, they can be compromised by malicious actors—both external and internal—causing irreversible damage to corporate data.

3. Risks from third-party collaborations

One of the biggest challenges organizations face today is the failure to understand their third-party relationships and their associated risks. According to a 2020 Ponemon Institute report (via Security Boulevard), 53% of organizations have experienced at least one data breach caused by a third party in the last two years. Attackers also leverage third-party remote access points to gain a foot in the door and launch attacks in due course. With the increasing reliance on remote vendors and the threat landscape constantly changing, it's difficult to identify third-party threats and vulnerabilities without proper monitoring tools in place.

4. Failure to limit access to sensitive systems

In most organizations, employees often have a surplus of high-level privileges and access permissions that are actually unnecessary for their roles, paving the way

for privilege abuse. These privileges generally go unnoticed and unmanaged, inviting several security risks and jeopardizing businesses. IT teams often fail to handle the consequences of too much access, especially when it comes to former employees. Failure to nullify a former employee's identity and access permissions allows disgruntled employees to have access to sensitive data even if they're no longer with the organization.

5. Decentralized remote access provisioning and management

Many organizations today still rely on multiple tools and manual, piecemeal strategies to provision remote access to employees due to budgetary constraints or sheer ignorance of the risks of insecure access methods. Such a decentralized system can cause huge disparities in remote access policies and workflows across the organization, leaving several security gaps behind and making it complicated for IT teams to manage all of an organization's privileged sessions.

How to secure privileged access to confidential systems

How do you, as an IT administrator, overpower this modern landscape of threats and securely establish a strategy to provide privileged access to employees, third-party vendors, applications, and devices? How do you manage and monitor every privileged activity happening in your on-premises, hybrid, and cloud infrastructure, and ensure no malicious activity goes unnoticed? And how do you lock all of the backdoors fabricated by bad actors to stay secure without ebbing productivity?

The ordeal of dealing with such questions can seem like a daunting challenge for many IT teams today. This is where privileged session management comes in.

Privileged session management: An IT security process to control and supervise privileged access

Privileged session management (PSM) is a fundamental IT security component of an identity and access management program that regulates privileged access to critical systems while strictly governing the sessions through session recording and auditing.

A PSM tool helps increase oversight and accountability, and mitigates the risk of privileged access misuse by continually managing, monitoring, and auditing the activities carried out by privileged users, including trusted insiders, third-party contractors, applications, and systems. It's also an inseparable part of the emerging Zero Trust model that encourages organizations to not automatically trust that users are always using their elevated access for the right things and ensure that the best security practices are being followed religiously.

Benefits of using an effective PSM tool

A PSM tool monitors and records the activities of every privileged user from the time they launch a privileged session to when that session ends, enabling security administrators to proactively identify and terminate suspicious or unauthorized activities in real time. It provides an unimpeachable audit trail of all privileged activities that enables compliance and eases forensic investigations. Implementing a PSM solution as part of their cybersecurity program helps enterprises mitigate security risks, reduce operational complexity, improve visibility into privileged access, and adhere to compliance standards.

1. Provides centralized access to geographically sequestered assets

A privileged session manager allows IT and security heads to have a central point of control to manage access to critical resources from anywhere across the globe, have granular controls on access pathways, and define how other privileged remote users connect to critical systems.

2. Enables granular access to stakeholders and third parties

A robust PSM tool provides an easy-to-utilize workflow that enables easy provisioning and de-provisioning of privileged access while creating complete accountability for privileged users. It enables temporary, role-based access for third parties—like contractors, vendors, and outsourced employees—to access specific enterprise systems or applications without the need for privileged account credentials.

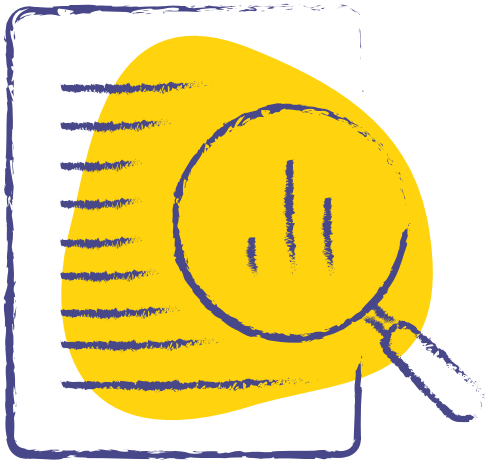
3. Increases productivity and simplifies administration

Implementing a PSM solution facilitates centralized administration of distributed remote IT assets through a single point of control. Privileged users can update, troubleshoot, and manage data center systems centrally, facilitating quick, efficient administration. It also ensures improved quality of work and better accountability through standardized policies and efficient supervision.

4. Tightens overall access governance

Besides providing granular access, PSM solutions also provide admins with the right controlstomonitorandmanagegeographically distributed assets. Real-time monitoring of privileged remote sessions promotes organizational transparency and provides IT admins with the ability to proactively mitigate insider attacks through session recording and shadowing.

5. Helps comply with various remote access compliance standards



A PSM tool helps organizations meet industry compliance standards, like SOX, HIPAA, ICS CERT, GLBA, PCI DSS, FDCC, and FISMA, and allows them to secure all their data. Implementing PSM as part of a comprehensive cybersecurity strategy enables organizations to record all activities related to critical IT infrastructure and privileged access, helping them effortlessly adhere to audit and compliance requirements.

6. Improves security and reduces risk

A privileged session manager helps secure critical systems by eliminating direct access to them. It serves as a proxy gateway server to tunnel privileged connections from the user device to the target system. This prevents unexpected access from unauthorized systems, limits all access pathways to corporate systems to this tool, and allows for more secure communications without the need for providing confidential passwords.

Access Manager Plus: ManageEngine's privileged session management solution

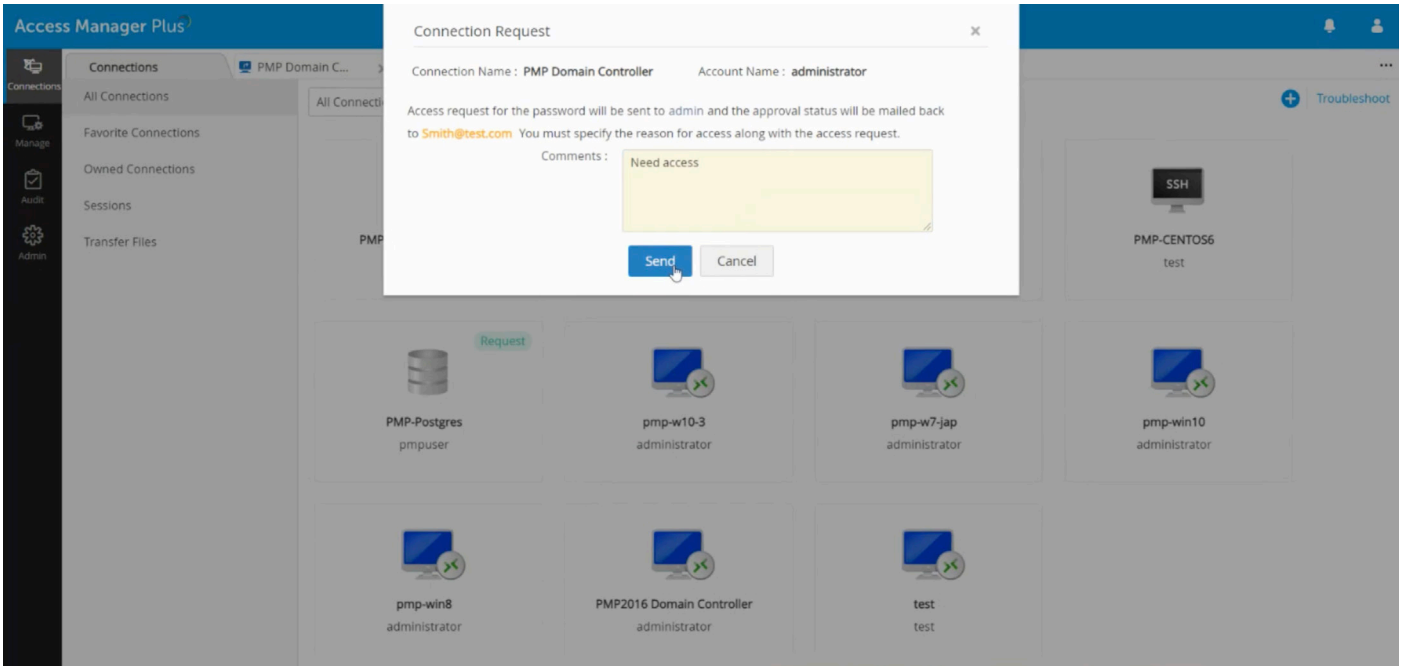
Access Manager Plus is a secure remote access and privileged session management tool from ManageEngine that helps you regulate and monitor all remote privileged access in your organization. It serves as a proxy server between end-user devices and target systems while simultaneously preventing credential exposure and direct access to critical systems via insecure and unauthorized pathways.

Access Manager Plus helps improve oversight and accountability of privileged user activities via session shadowing, recording, and auditing.

Privileged access control workflows

On a daily basis, an IT team typically handles many permanent and temporary access requests raised by users and third-party vendors to access various corporate systems. To ensure effective management of these privileged access requests and uninterrupted functioning of business routines, IT teams must maintain a streamlined workflow as part of their PSM strategy.

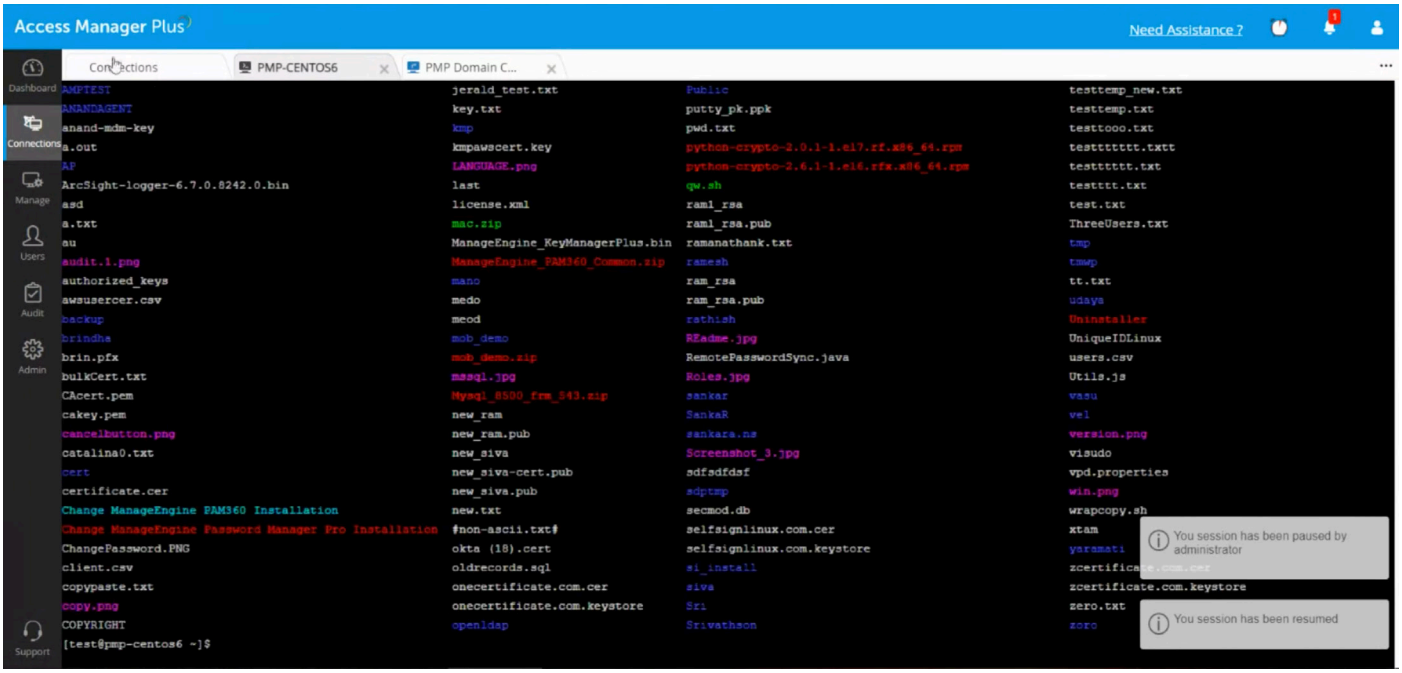
Configure access controls in Access Manager Plus by setting up approval requirements for privileged sessions, mandating users to provide a reason and/or the corresponding ticket ID that can be integrated with an existing ticketing system. You can also associate certain resources or applications to a user that they're entitled to request access to, and ensure only the minimum access required is granted for the minimal amount of time.



Secure remote access provisioning

Access Manager Plus serves as a proxy through which a privileged session is initiated and relayed to the target systems. Since there's no direct connectivity between the user device and target systems, the enterprise network is protected against unauthorized access and any virus or malware that may exist on the user's system.

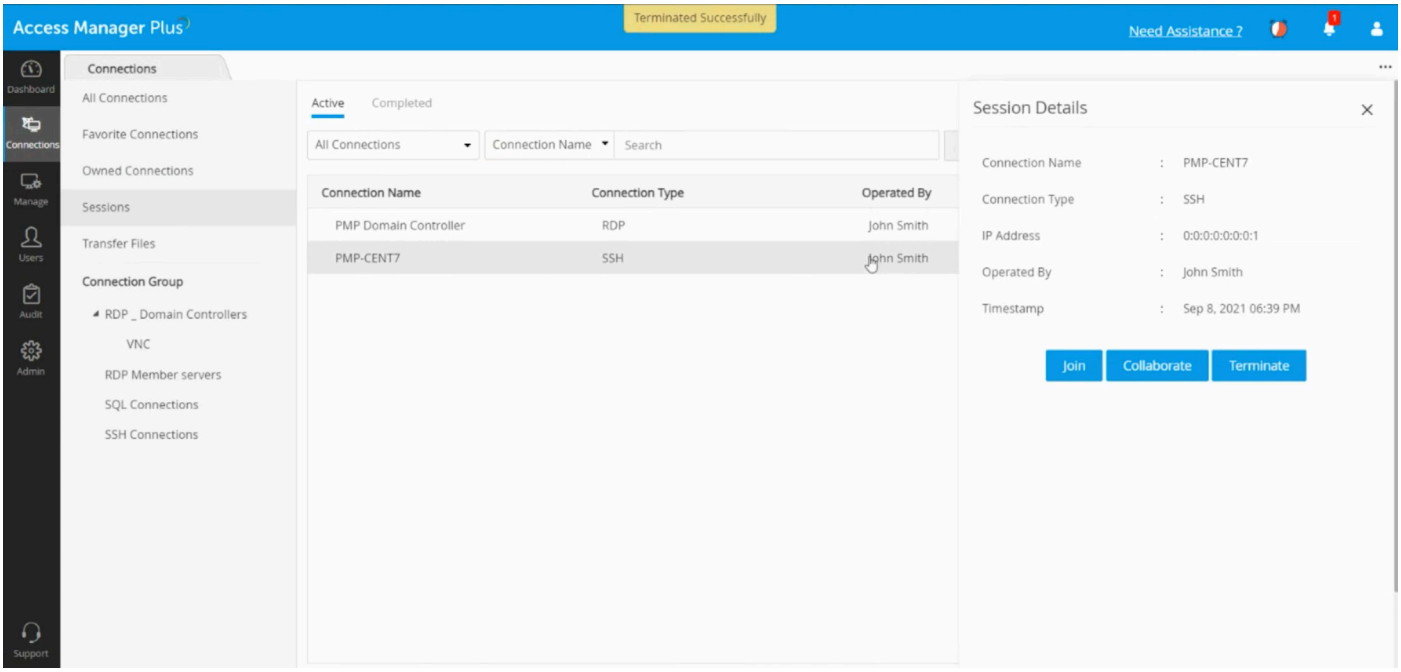
Provision employees and external stakeholders secure and controlled RDP, SSH, SQL, or VNC access to sensitive systems across your on-premises, cloud, and hybrid infrastructure without exposing privileged credentials. Allow users to launch multiple remote sessions simultaneously to improve productivity.



Session collaboration, shadowing, and termination

Access Manager Plus lets you collaborate with users on an active remote session to share knowledge, monitor user activity for compliance with the established security policies, or assist with troubleshooting.

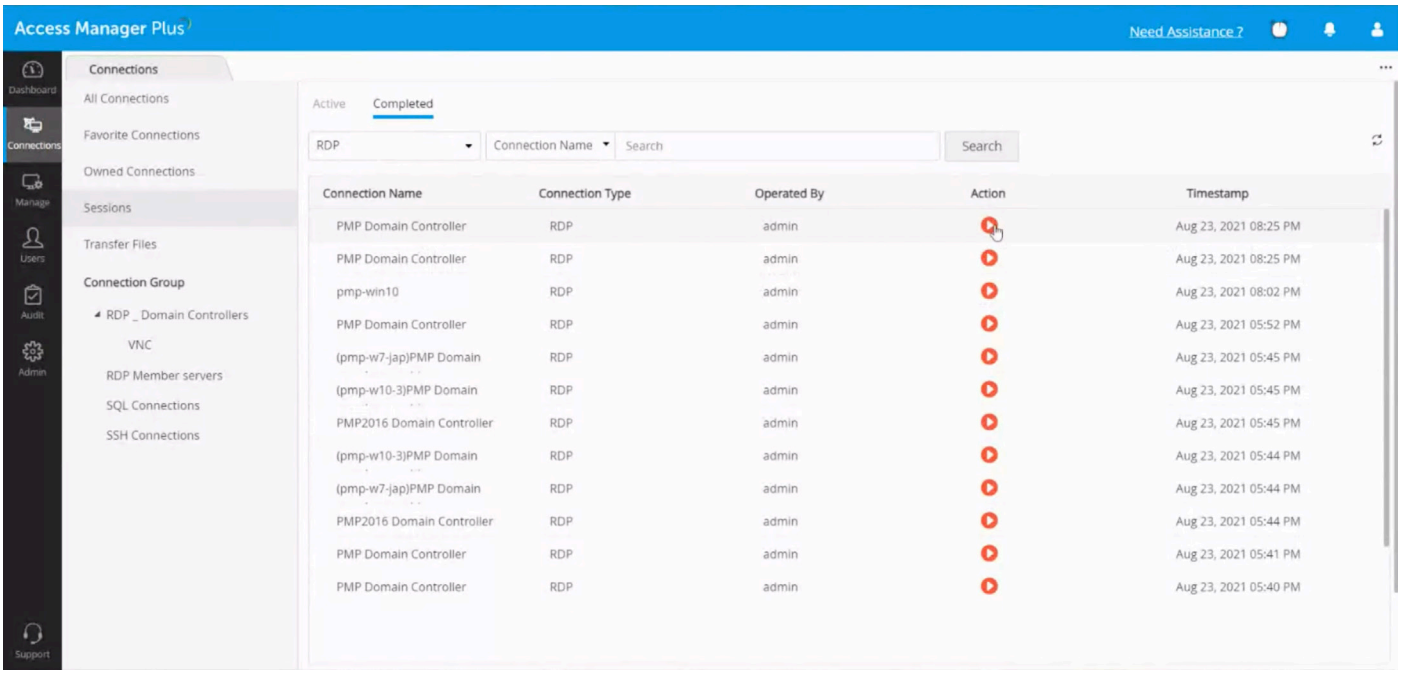
Shadow privileged sessions that involve critical systems and third-party vendors to proactively uncover fraudulent activities and ensure only authorized users access confidential systems in accordance with the scope of activities they're allowed to perform. If you catch a suspicious or unauthorized activity during a privileged session, you can terminate the session immediately and alert the concerned security teams.



Session recording and playback

Privileged session recordings offer tamper-proof evidence of a user's privileged access. Should an attacker break through your defenses and access your systems, you can easily filter and review past session recordings to uncover the source and adjust policies to prevent another attack.

By default, Access Manager Plus records all RDP, VNC, SSH, and SQL sessions launched from the application. The recorded sessions can be traced using any details, such as the name of the connection, the user who launched the session, or the time at which the session was launched.

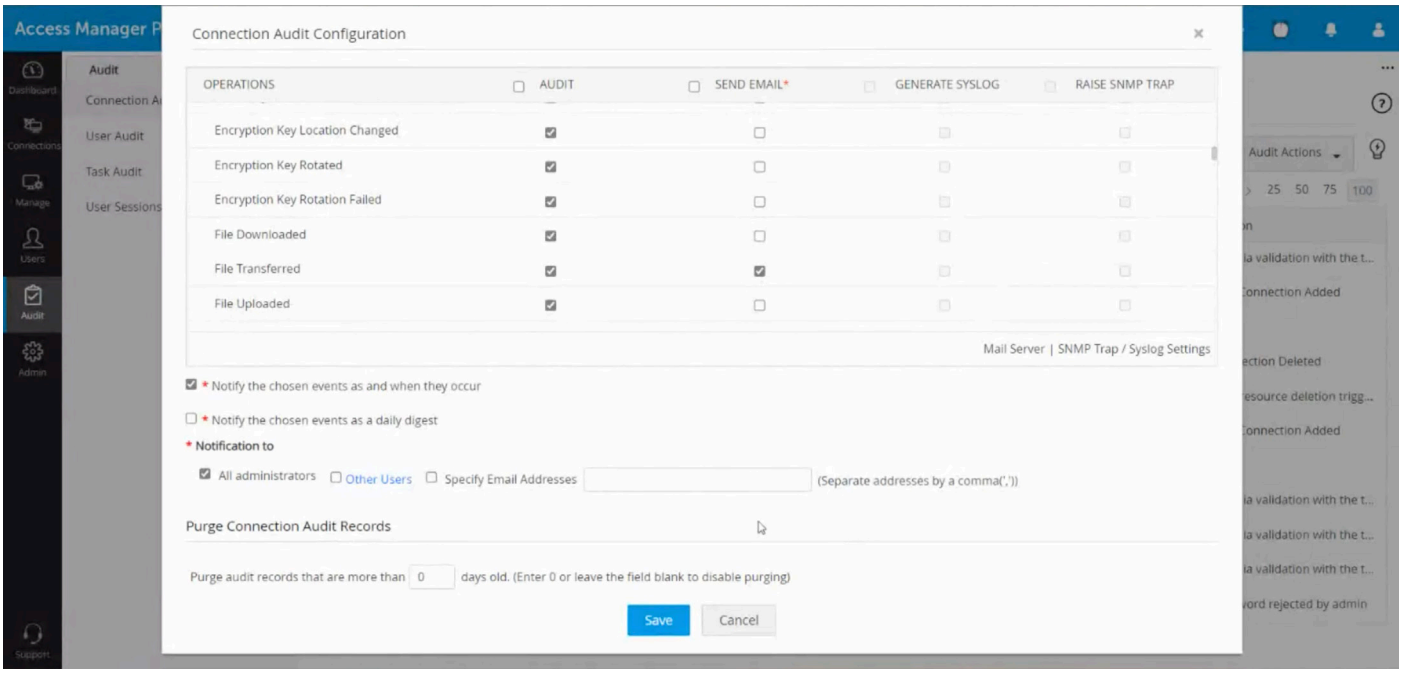


Comprehensive auditing

Audit trails help in identifying suspicious behavior. Automated audit logs enable administrators to identify system implementation issues, operational issues, unusual or suspicious activities, and other system errors. Various compliance standards, like HIPAA, SOX, and PCI DSS, expect organizations to monitor and capture all actions performed by privileged accounts, and session management provides an immutable audit log that can be shared with auditors to demonstrate compliance.

Access Manager Plus' immutable audit logs contain the record of all events around privileged account activities, scheduled and completed tasks, and remote accesses. This data helps in complying with regular internal audits and forensic investigations and demonstrating who accessed what resource or files, where, when, and why.

You can also integrate Access Manager Plus with your existing security information and event management tool to export privileged access data via syslog messages or with your network management tool to receive access-related logs via SNMP traps. Doing so lets you notify the concerned teams of potential breaches and prioritize and execute remedial actions accordingly.



Learn more about privileged session management

With cyberattacks getting increasingly sophisticated and dangerous by the minute, it's high time IT security administrators get smart about protecting their organization's critical information. Implementing security best practices and highly recommended PSM practices will help your organization achieve a strong defense mechanism against unauthorized access threats.

If you want to see privileged session management in action, sign up for a free trial of Access Manager Plus where you can test out all the features of the tool. You can also try the demo version where you can get hands-on knowledge of how the tool works.

manageengine.com/amp

Technical support

Telephone: +1 408 454 4014

Email: amp-support@manageengine.com

ManageEngine

Access Manager Plus