Privileged Account Manager Overview

With the use of NetIQ Privileged Account Manager (PAM), IT managers can manage and monitor who has administrative access to servers, networks, and databases. Without revealing their access credentials to these systems, administrators are permitted to manage delegated access to those systems. A consolidated activity log for several platforms is also provided. Privileged Account Manager provides highly trusted security solution. Privileged Account Manager also facilitates to record keystrokes and capture screens of privileged session. In this way, suspicious activities are detected at the earliest and helps in reducing such risky actions in future.

Privileged Account Manager offers Super User Privilege Management (SUPM) and Shared Account Password Management (SAPM) to secure the privileged accounts in the company.

For more information about these features, see “Key Features” on page 2.

How Privileged Account Manager Solves Business Challenges

Privileged Access Management is an essential component in protecting organizations against cyber-attacks, ransomware, malware, phishing, and data leaks.

Users with a privileged identity can be employees, consultants, partners, and customers, but can also be applications, services, things, and devices.

The following are the common use cases of Privileged Account Manager:

- **Credential Management**
  Discover, store, and manage privileged credentials for users, applications, and databases from a single console.

- **Session Monitoring**
  Implement credential checkout, session recording, and keystroke logging to verify privileged accounts and users.

- **Seamless Integration**
  Manage and monitor privileged access to accounts, applications, data, and systems from a single console.

- **Risk-based Intelligence**
  Integrate policy-based risk analysis or assessment of privileged credential activity to streamline enforcement and reporting.
Privileged Account Manager is a one-stop solution if your business requires any of the following access control capabilities:

- Providing Active Directory (AD) authentication and authorization policies to non-Windows and cloud resources.
- Helping discern between identities granted with domain level access to Active Directory or Microsoft Exchange when only a subset of access rights are required to be productive.
- Protecting resources from attacks directed at elevated access.
- Identifying, managing, and reporting on access for those who post utmost risk to an organization.
- Securing privileged credentials and providing flexible controls to balance cybersecurity and compliance requirements with operational and end-user requirements.
- Managing access of users who might harm your organization, maliciously or accidentally.
- Determining and providing access depending on the context: who, what, when, where, history.

**Key Features**

The following is an illustration of some of the capabilities which the key features of Privileged Account Manager solve.
Active Directory Bridging

Using the Active Directory Bridging (AD Bridging) method, you can log in to non-Windows systems using the AD credentials.

Least Privilege Delegation

Privileged Account Manager grants only the minimal access rights or permissions necessary to carry out a function. Least privilege delegation is a significant step in guarding privileged access to sensitive and valuable data and assets.

Credential Vault

A Credential vault is an encrypted safe protecting privileged credentials that permit access to high-tier systems. Due to the fact that users are shielded from important system passwords, there is no longer a chance that a hacker may obtain them through Cyber attacks.

Multi-factor Authentication

Used together with NetIQ Advanced Authentication, Privileged Account Manager supports multi-factor authentication to provide secure access from any device with minimal administration. Advanced Authentication delivers various authentication mechanisms that enable identity assurance and proofing apart from traditional username and password based authentication. You can authenticate on diverse platforms by using various authenticators such as Fingerprint, OTP, and Smartphone.

Adaptive Attribute Provisioning

Privileged Account Manager provides a method for adaptive resource provisioning to dynamically distribute resources for applications in response to workload variation.

Privileged Session Management

Privileged Account Manager monitors, manages, and records sessions started by privileged accounts. Session recording makes it possible to see how users interact with sensitive data, which helps in the investigation of data hacks and compliance mandates.

Group Policy Management

The users, groups, and roles are provided with only necessary permissions which help in easy resource management.

Linux and UNIX Root Delegation

Privilege Account Manager allows administrators to increase security as it protects sensitive data from network monitoring by encrypting root commands or sessions it controls in both Linux and UNIX machines.

Risk Based Authentication

Using the OAuth2 framework, you can integrate NetIQ Advanced Authentication with Privileged Account Manager to use multi-factor authentication and utilize Risk Service capabilities. Based on the risk score the user can either successfully log into Privileged Account Manager or get rejected at the log in screen.
Agent and Agentless Based Monitoring

Agentless enables you to secure, manage and monitor privileged access to remote machines through Privileged Account Manager. The ability to capture session audits and create video recordings of the privileged sessions varies from one agentless module to another. This approach is easy to manage as new updates to the agent need not be applied.

The Agent is an installable component that resides on a machine and helps to manage and monitor privileged access to the machine. It creates comprehensive session audits and video recordings of the privileged sessions of the machine beyond the limits of the Agentless approach. This approach requires regular maintenance and is not suitable for a sophisticated environment.

Choose the Agent or Agentless approach based on the requirement.

Architecture

The following diagram depicts a basic architecture of Privileged Account Manager:

Primary Components

Privileged Account Manager contains two primary components:

- “Privileged Account Manager” on page 5
- “Privileged Account Manager - Agent” on page 5
Privileged Account Manager

Manager is the server component of the product. It provides a centralized registry, enabling services and administration of the entire product from any single point on the enterprise network. The Manager component can be administered through the Privileged Account Manager administration console.

The default capabilities are:

- **Administration Manager**: Provides the functionality for the web-based user interface. Framework consoles can be installed on the Administration Manager and are used to control product features.
- **Access Manager**: Maintains a list of user accounts and provides authentication services for the Framework. It needs to be installed with a local Registry Manager to create a secure user authentication token.
- **Audit Manager**: Maintains the repository for all auditing information that the Framework collects.

NOTE: We recommend you to deploy only two Audit Managers, even in large environments.

- **Command Control Manager**: Maintains the rule configurations and is responsible for validating user command requests.
- **Compliance Auditor**: Collects, filters, and generates reports of audit data for analysis and signoff by authorized personnel.
- **Messaging Component**: Provides the transport mechanism and communicates with the e-mail servers to provide reporting functionality.
- **Package Manager**: Manages a repository for Framework packages.
- **Registry Manager**: Maintains a database of all Framework hosts and modules. Provides certificate-based registration features for the hosts.
- **Syslog Emitter**: Forwards the audit logs to a Syslog server.
- **User Request Dashboard**: Facilitates you to view and update emergency access and credential checkout requests.
- **Auditing**: Facilitates you to control access to Reports console.
- **Credential Vault**: Facilitates you to control the access to Credential Vault console.
- **Distribution**: Facilitates you to restrict installation and deployment of certain packages.
- **User Info**: Facilitates you to control access to Hosts console.

Privileged Account Manager - Agent

Privileged Account Manager - Agent is the client component of the product. It receives and implements instructions from the Manager on all hosts. The following Agent packages are installed on all the hosts:

- **Registry Agent**: Provides a local cached lookup for module locations. The Registry Agent queries the Registry Manager when local cached information is not available or is not updated.
- **Distribution Agent**: Provides the interface to control the installation and removal of packages in the Framework. It has methods to install, remove, and list the available and updatable packages. The Distribution Agent retrieves packages from the local Package Managers.
- **Store and Forward Agent**: Provides a store and forward mechanism for guaranteed delivery of messages. It is used for replication of the manager databases.
- **Command Control Agent**: Enables the Framework to control and audit user commands.
Managing Privileges in Various Endpoints

Privileged Account Manager provides the capability to connect to a remote host using SSH (UNIX/Linux), RDP Relay (Windows), direct RDP and credential provider (Windows) without knowing the privileged account credentials, such as passwords or identity certificate of the user. There is also an option for you to connect to target machines without any agent installed in those machines. This feature is possible with RDP Web Relay and SSH Web Relay. You can also configure Privileged Account Manager to connect to any database, or application server with secure and controlled access. The use of shared keys allows Privileged Account Manager to provide any type of shared credentials to privileged users. You can capture users’ activity in different formats, such as keystroke, screenshots, session, and video.

Before trying to connect to remote hosts, you must configure Roles and Policies in Privileged Account Manager. You must create User Roles, Resource Pools, and Assignments in the component called Access Control with administrator privileges. For more information about Access Control, see Access Control.

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>A Windows Server user can get privileged access on the target Windows machine (server and desktop), using RDP Relay, direct RDP, Web RDP Relay, and credential provider. For information about privileged access to Windows machines, see Privileged Access to Windows.</td>
</tr>
<tr>
<td>UNIX/Linux</td>
<td>A UNIX/Linux Server user can get privileged access on the target UNIX/Linux machine, using SSH Relay, Web SSH Relay, usrun command, pcksh, and cpcksh. For information about privileged access to UNIX/Linux machines, see Privileged Access to UNIX and Linux.</td>
</tr>
<tr>
<td>Database and Applications</td>
<td>A Privileged Account Manager user can access databases like Oracle database, and any application server such as, LDAP. All the actions that the user performs on the database or any application can be monitored by configuring the settings on the Manager for Privileged Account Manager. The shared credentials are also managed by using Credential Vault. For more information about shared account credentials refer Privileged Access to Applications and Cloud Services. A user who has an account in the database server can also be monitored through Privileged Account Manager. For more information about database monitoring, see Privileged Access to Databases.</td>
</tr>
<tr>
<td>Shared Keys</td>
<td>Privileged Account Manager provides shared key functionality to share any type of value or key with privileged users. For more information about shared keys refer, Working with Credentials.</td>
</tr>
</tbody>
</table>

Support for Double Byte Characters

Privileged Account Manager adds support for double byte characters. Many diverse characters are used in the writing systems of some languages, such as Chinese, Japanese, and Korean, making it impossible for single-byte codes to accurately represent them. The system employs 2 bytes per character to represent them in...
coded character sets for such languages. Double-byte characters are those that use the two-byte encoding method. Privileged Account Manager now helps you define and get privileged access to various features containing non-English characters.

As a Privileged Account Manager user you can now define and procure SSH, RDP access with objects containing non-English characters. You can also define authentication to various authentication types containing non-English characters.

**Language Support**

The Privileged Account Manager installation software is not localized and is available only in English. Whereas, the Privileged Account Manager Administration Console and the User Portal and its help files are localized.

Privileged Account Manager also supports localizing error messages and login prompts.

Privileged Account Manager supports localization in the following languages:

- German
- French
- Spanish
- Canadian French
- Italian
- Japanese
- Portuguese
- Brazilian Portuguese
- Chinese (Simplified, PRC)
- Chinese (Traditional, Taiwan)
- Swedish

The preferred language must be set in the client's browser to display the text in respective language other than English.

**Legal Notice**

*Copyright 2009 - 2023 Open Text.*

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see [http://www.microfocus.com/about/legal/](http://www.microfocus.com/about/legal/).