Privileged Account Manager 4.0 Release Notes

December 2020

Privileged Account Manager 4.0 includes new features, improves usability and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Privileged Account Manager Community Support Forum, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click the comment icon on any page in the HTML version of the documentation posted at the Privileged Account Manager Documentation website. To download this product, see the Micro Focus Downloads website.

What's New?

The following sections outline the key features and functions provided by this version, as well as issues resolved in this release:

- "New Features and Enhancements" on page 1
- "Software Fixes" on page 4

New Features and Enhancements

This release introduces the following new features and enhancements:

- "Agentless Privileged Access and Auditing" on page 2
- "Access Control - Redesigned Policy Engine" on page 2
- "Integration with ArcSight Intelligence" on page 2
- "Multiple LDAP Servers Support for Authentication" on page 3
- "User Interface Improvements" on page 3
- "Enhanced Access Control for Agents" on page 3
- "Real-Time Application Control (Allow - Deny Commands)" on page 3

Agentless Privileged Access and Auditing

Privileged Account Manager now allows administrators to provision privilege access without a need for an agent on the target host, which the provisioned users can access without the need of any client application, from within their browsers. This agentless privileged access and auditing support includes the following important capabilities:

- Live view of Privileged Sessions in real-time for administrators.
- This privileged access does not require any agent to be installed on target hosts.
- This access is clientless access (through a web browser), removing thick clients' requirements for RDP, SSH, and TELNET access.
- Auditing formats include videos and keystroke capture similar to Agent-based audits.

  For more information, see Agentless Session Management in Windows and Agentless Session Management in Unix and Linux.

Access Control - Redesigned Policy Engine

Access Control is designed to implement an organization’s security policy for Privileged Access easily. Administrators can now configure the Privileged Access intuitively by organizing their resources and users requiring privileged access in a logical manner. This new design and approach of defining policies for privileged access have the following capabilities and features:

- Type-defined Resource Pools allow the grouping of resources with similar privilege access requirements into respective groups, for privilege access provisioning.
- User Roles configuration enables grouping users with similar security requirements into User Roles.
- A one-to-one relationship between User Roles and Resource Pools using Assignments.
- An intuitive wizard-based user interface to configure Permissions with applicable attributes.
- The ability to browse the objects (users and resources) during the configuration eliminates the existing challenges of typing in object references.
- Extensive well documented REST APIs allow other systems to easily and efficiently integrate with Privileged Account Manager to drive privilege access configuration programmatically.
- Detailed reports such as "Who has access to which resources", and "Who all have access to particular resource" provides insights into provisioned Privilege accesses.

  For more information see, Access Control.

Integration with ArcSight Intelligence

Privileged Account Manager can now consider external risk scores by adding user behavior analysis (UEBA) scores in decision-making for granting privileged access rights through the integration with ArcSight Intelligence. While Privileged Account Manager has its own Risk definition and scoring, this capability enables Privileged Account Manager is to consume the Risk Scores from external systems to control privileged access to any of the target system. For more information, see Integrating with ArcSight Intelligence.

Multiple LDAP Servers Support for Authentication

Privileged Account Manager now supports adding multiple LDAP servers and uses these LDAP servers simultaneously for authentication and authorization across different features. If you upgrade to Privileged Account Manager 4.0 or later, the existing LDAP services configured in the credential vault will automatically get migrated to new LDAP server settings. For more information, see LDAP Servers.

User Interface Improvements

Privileged Account Manager has made several enhancements and user experience improvements based on feedback from customers and users.

- The console for "Framework User Manager" is migrated to the new user console, as per the latest user interface standards.
- Console permissions have been enabled on the new user console, so now the administrator can configure individual console access for various Privileged Account Manager users.
- The permission configuration has been made intuitive, by introducing more descriptive and user-friendly permission descriptions.
- With introduction of permissions, the need for two separate console landing pages (User Console and Administrator Console) has been eliminated, and new console has been merged as (https://www.netiq.com/documentation/privileged-account-manager-40/npam_admin/data/t4dytx992cxb.html#t4dytxr4yow4)a single console.

  For more information, see Managing Groups and Managing Users.

Enhanced Access Control for Agents

On the systems having Privileged Account Manager - agents, the capability to control access to various files, directories, commands within a privileged session has been enhanced significantly.

- Addition of Enhanced Access Control (EAC) capability for Windows Agents.
- New User Interface to define the type-defined EAC policies, which can be directly added to Access Control permission.
- Ability to define risk for individual granular operation (read, write, delete, and so forth).
- File and Folder control on Linux/UNIX and Windows Agents.
- Process execution control on Linux/UNIX Agents.

  For more information, see Enhanced Access Control.

Real-Time Application Control (Allow - Deny Commands)

Privileged Account Manager now has capability to define command lists and use them either as list of Allowed commands OR Denied commands within a privileged session.

- Control access to commands in agentless privileged - sessions (Terminal SSH, Telnet, and Submit user).
- Control access for agent-based sessions is easy to use with application control.
  - `usrun` is now renamed to Privileged Command
  - Run as Privileged User is now renamed to Privileged Application
- Ability to define individual risk score for each allowed or denied command.

- A new user interface to define command lists and configure those as Allow/Deny list in Access Control.

  For more information, see Application Command List.

Software Fixes

This release includes the following software fixes:

Component	Bug ID	Issue
Command Control	183329	Password checkout of Application Account Domains fails when Account Domain credential is not set.
Database Monitoring	183883	When a user tries to connect to MS SQL Server using Privileged Account Manager Database Monitoring, the session does not start if the agent is not installed on the SQL server-client system.
Administration console	183987	The behavior of the **Reset Password Age** check box and **Password Expiration** fields in the user interface is fixed.
Windows RDP Relay	278036	Access violation issue is observed in Privileged Account Manager 3.7 agent.
Credential Checkout	282417	Multiple password checkouts on the same credential using API is not sent to the Syslog server.
Descriptive Permissions	285345	Issue with a requirement to add administrative permission in Credential Vault to execute password management function.

Deprecation of Features

Support for the following features is deprecated starting this release:

- **Help Desk Role:** The help desk role which allowed a predefined set of attributes to be set on the Account Settings page so that users are assigned to the help desk group.
- **LDAP Native Map:** The Native Maps option which allowed you to map Framework User accounts to UNIX or Linux accounts and to LDAP accounts.

Deprecation of APIs

Support for old APIs (such as SPF.Util, and Java APIs) will be discontinued from the next major release of Privileged Account Manager.

For the list of supported REST APIs, see `https://<PAM_IP>/rest_api`.

System Requirements

For information about hardware requirements, supported operating systems and browsers, see *Privileged Account Manager 4.0 System Requirements and Sizing Guidelines*.

Installing Privileged Account Manager 4.0

For information about installing Privileged Account Manager 4.0, see the *Privileged Account Manager Installation Guide*.

Upgrading to Privileged Account Manager 4.0

You can upgrade to Privileged Account Manager 4.0 from Privileged Account Manager 3.7 or later. When you upgrade Privileged Account Manager to version 4.0, rollback of packages to Privileged Account Manager 3.7 or an earlier version is not supported.

WARNING: When you upgrade an Application SSO package from a previously installed version, the target server reboots automatically. Plan your downtime accordingly.

For information about upgrading to Privileged Account Manager 4.0, see Upgrading Privileged Account Manager in the *Privileged Account Manager Installation Guide*.

Upgrade Considerations

Upgrading to Privileged Account Manager 4.0 includes features and minor improvements as described below:

- LDAP Vault Migration for the authentication domain is migrated to the new user interface administration console in the **Settings > Server Settings > LDAP Servers** page.
- Permission changes on the new user interface: Some existing non-administrator users with additional console permission will get the access to the respective consoles in new user interface.

Known Issues

Micro Focus strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

- "Check-in Fails for ESXi Application with the Latest Java Version 14" on page 5
- "SSH Web Relay Session Gets Disconnected When Vault is Configured with OpenSSH Private Key" on page 6
- "MSI Upgrade Does not Work" on page 6
- "Windows Agent Sends Extra Request for Direct RDP, While Serving Web Agent RDP Session" on page 6
- "LDAP Credential Vault Set as Authentication Domain Is Not Migrated as LDAP Server on Backup Managers" on page 6
- "Video Recording is Not Captured For Web-RDP Agentless Session" on page 6
- "Enhanced Access Control Fails to Work on Solaris SPARC and HP-UX" on page 6
- "Command Control Agent Module is Not Present After a Fresh Install of the HP-UX Depot File" on page 7

Check-in Fails for ESXi Application with the Latest Java Version 14

Issue: Check-in fails for the ESXi application with latest Java version 14 when installed on Linux manager. (Bug ID: 184179)

Workaround: No workaround is available.

SSH Web Relay Session Gets Disconnected When Vault is Configured with OpenSSH Private Key

Issue: SSH Web relay session gets disconnected if vault is configured with an OpenSSH private key. (Bug ID: 189414)

Workaround: Use `ssh-keygen -m pem` format keys.

MSI Upgrade Does not Work

Issue: MSI upgrade does not work with Privileged Account Manager 4.0. (Bug ID: 286190)

Workaround: Upgrade using Package Manager.

Windows Agent Sends Extra Request for Direct RDP, While Serving Web Agent RDP Session

Issue: When Web Agent RDP session is requested, Windows Agent sends Direct RDP request, which may get authorized if a policy is created for both these permissions for same user. (Bug ID: 301071)

Workaround: There should not be Direct RDP and Web Agent RDP Permissions created to authorize same users.

LDAP Credential Vault Set as Authentication Domain Is Not Migrated as LDAP Server on Backup Managers

Issue: After upgrade, the default Authentication Domain (LDAP Credential Vault) is not migrated as **LDAP Server** under **Settings** in the backup manager. (Bug ID: 302084)

Workaround: After upgrading all the Managers, promote `auth` module in Primary Manager.

NOTE: This issue does not occur if all the Backup Managers are upgraded simultaneously using the option Update Domain Packages. Use GUI element for "Update Domain Packages".

Video Recording is Not Captured For Web-RDP Agentless Session

Issue: When using Remote Desktop Protocol (RDP) Web agentless session, the user activity is not captured in the form of a video recording. (Bug ID: 302208)

Workaround: No workaround is available.

Enhanced Access Control Fails to Work on Solaris SPARC and HP-UX

Issue: Enhanced Access Control does not work on Solaris SPARC and HP-UX. (Bug ID: 305031)

Workaround: No workaround is available.

Command Control Agent Module is Not Present After a Fresh Install of the HP-UX Depot File

Issue: Command Control Agent (`rexec`) module is not present after a fresh installation of the HP-UX depot file. (`Bug ID: 303027`)

Workaround: Upgrade from Privileged Account Manager 3.7 to 4.0 to use the HP-UX agent. For more information, see Privileged Account Manager Install Guide.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://www.microfocus.com/support-and-services/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- The Micro Focus Community pages: https://www.microfocus.com/communities/

Legal Notice