Privileged Account Manager 3.7 Release Notes

December 2019

Privileged Account Manager 3.7 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.

1 What's New?

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

- Section 1.1, "Dashboard for Administrators," on page 1
- Section 1.2, "Enhancements to Multi-Factor Authentication," on page 2
- Section 1.3, "Enhancements to Database Monitoring," on page 2
- Section 1.4, "Enhancements to Credential Checkout and Emergency Access," on page 2
- Section 1.5, "SSH Relay Enhancements," on page 3
- Section 1.6, "Framework Administrator Roles for LDAP Users," on page 3
- Section 1.7, "Quick Reference Videos," on page 3
- Section 1.8, "Improved Report Export Capability," on page 3
- Section 1.9, "Software Fixes," on page 4
- Section 1.10, "Security Vulnerability Fix," on page 5

1.1 Dashboard for Administrators

PAM now offers a new dashboard that serves as a single, quick access console, enabling PAM administrators to quickly identify any potential security issues and administrative tasks that need immediate attention.

For more information about the dashboard, see the Contextual Help in the administration console.

1.2 Enhancements to Multi-Factor Authentication

- Section 1.2.1, “Radius Client Method Support in Advanced Authentication,” on page 2
- Section 1.2.2, “Multi-Factor Authentication using RADIUS server,” on page 2

1.2.1 Radius Client Method Support in Advanced Authentication

In addition to existing Advanced Authentication methods, PAM now supports RADIUS Client method.

For more information, see “Supported Authentication Methods” in the *Privileged Account Manager Administration Guide*.

1.2.2 Multi-Factor Authentication using RADIUS server

PAM now supports Multi-Factor Authentication using a RADIUS server, enabling easy integration with any third-party RADIUS supported Multi-Factor Authentication products.

For more information, see “Multi-Factor Authentication” in the *Privileged Account Manager Administration Guide*.

1.3 Enhancements to Database Monitoring

Database monitoring capabilities are now extended to the IBM Db2 database.

For more information about configuring privileged access to databases, see “Privileged Access to Databases” in the *Privileged Account Manager Administration Guide*.

1.4 Enhancements to Credential Checkout and Emergency Access

- Section 1.4.1, “Enhancements to Credential Checkout,” on page 2
- Section 1.4.2, “Credential Checkout for Microsoft Azure,” on page 2
- Section 1.4.3, “Enhancements to Emergency Access Request and Credential Checkout,” on page 3
- Section 1.4.4, “Credential Checkout for Windows, Linux, and AIX Local Accounts,” on page 3

1.4.1 Enhancements to Credential Checkout

Credential checkout capabilities are now extended to the IBM Db2 database. PAM supports only the TCP protocol in this release.

For more information about configuring privileged access to databases, see “Privileged Access to Databases” in the *Privileged Account Manager Administration Guide*.

1.4.2 Credential Checkout for Microsoft Azure

PAM now enables credential checkout for Microsoft Azure in addition to other cloud services such as Red Hat OpenStack and Amazon Web Services (AWS). To get privileged access to these cloud services, you can now check out privileged account credentials from the user console.

For more information about configuring password checkout for Microsoft Azure, see “Enabling Credential Checkout for Microsoft Azure” in the *Privileged Account Manager Administration Guide*.

1.4.3 Enhancements to Emergency Access Request and Credential Checkout

Minimum access duration of emergency access request and credential checkout is reduced to 1 hour from 6 hours.

1.4.4 Credential Checkout for Windows, Linux, and AIX Local Accounts

PAM now supports credential checkout for Windows, Linux, and AIX local accounts.

For more information, see "Configuring Credential Checkout for Applications" in the *Privileged Account Manager Administration Guide*.

1.5 SSH Relay Enhancements

- Section 1.5.1, "Ability to Connect Submit User to Target Systems," on page 3
- Section 1.5.2, "OpenSSH Upgrade," on page 3

1.5.1 Ability to Connect Submit User to Target Systems

PAM now enables `Submit User` to connect to target systems. The administrators can now provide privilege access to multiple users with a single command control rule.

For more information, see "Secure Shell Relay Usage Scenarios" in the *Privileged Account Manager Administration Guide*.

1.5.2 OpenSSH Upgrade

OpenSSH has been upgraded to version 7.9p1.

1.6 Framework Administrator Roles for LDAP Users

LDAP users (Microsoft Active Directory, NetIQ eDirectory, or OpenLDAP) can now get administration privileges for PAM framework through their LDAP group membership. This ability significantly simplifies the configuration process for providing framework roles to LDAP users.

For more information, see "Assigning Framework Roles for LDAP Users" in the *Privileged Account Manager Administration Guide*.

1.7 Quick Reference Videos

PAM now provides short quick reference videos that serve as self-learning tutorials for PAM administrators.

To access these videos, in the administration console, click <*user_name*> at the top-right corner and select **Getting Started**.

1.8 Improved Report Export Capability

PAM now enables you to export keystrokes in a CSV format.

1.9 Software Fixes

Privileged Account Manager 3.7 includes software fixes that resolve the following issues:

- Section 1.9.1, “Privileged Sessions Are Not Audited When Secure Boot is Enabled,” on page 4
- Section 1.9.2, “Changes Made in the Backup Manager Through REST API Are Not Replicated in the Primary Manager,” on page 4
- Section 1.9.3, “Access As Column of Approved Windows Emergency Access Session Does not Display the Domain Name,” on page 4
- Section 1.9.4, “Users in the Account Group Are Not Authorized to Access the pcksh Session,” on page 4
- Section 1.9.5, “Agent Crashes with Access Violation Error,” on page 5
- Section 1.9.6, “Re-Login is Required After Registering the License,” on page 5
- Section 1.9.7, “The Unregistered Hosts List Using IP Range Does Not Work,” on page 5
- Section 1.9.8, “SSH Relay Adds a root Login Entry to Syslog in PAM Server,” on page 5
- Section 1.9.9, “NPAM Service Commands Do Not Work In SUSE Linux Enterprise Server 12 or Later,” on page 5
- Section 1.9.10, “SSH Relay to a SSH Target Host Fails if You Use a Custom Port Other Than Port 22,” on page 5
- Section 1.9.11, “When Secondary Authentication after Login, is in Progress, Accessing PAM Through Another Tab Displays Your Landing Page Without Data,” on page 5

1.9.1 Privileged Sessions Are Not Audited When Secure Boot is Enabled

Audits are now captured successfully when Secure Boot is enabled. `(Bug 1105024)`

1.9.2 Changes Made in the Backup Manager Through REST API Are Not Replicated in the Primary Manager

Changes made in either the Backup Manager or the Primary Manager using REST API are replicated in all the other managers.`(Bug 1101042)`

1.9.3 Access As Column of Approved Windows Emergency Access Session Does not Display the Domain Name

Issue: The approved emergency access sessions listed under **Windows** tag does not display the domain name in the **Access As** column. Instead, it displays only the user name. For example: Instead of `Domain/Administrator`, **Access As** displays only `Administrator`. `(Bug 1147175)`

Fix: **Access As** column now displays domain name/user name.

1.9.4 Users in the Account Group Are Not Authorized to Access the pcksh Session

Issue: Users who are part of an account group are not authorized to access the `pcksh` session when the account group is added to the **runuser** of the `pcksh` policy. `(Bug 1131566)`

Fix: Users in the account group are authorized to access the `pcksh` session.

1.9.5 Agent Crashes with Access Violation Error

The random agent crash issue observed on multiple Windows servers has been fixed. (`Bug 1134687`)

1.9.6 Re-Login is Required After Registering the License

After registering the license, you now see the license information without a re-login. (`Bug 1096076`)

1.9.7 The Unregistered Hosts List Using IP Range Does Not Work

Issue: In the administration console, when you search for unregistered hosts by clicking **Hosts > List Unregistered Hosts > IP Range**, the `Failed to list unregistered agents` error is displayed. (`Bug 832747,790444,1104360`)

Fix: The unregistered hosts are displayed correctly.

1.9.8 SSH Relay Adds a root Login Entry to Syslog in PAM Server

SSH Relay adds a root login entry instead of PAM user login entry in the syslog of PAM server. To overcome this issue, the default log level of Syslog is set to `QUIET`. For more information, see the Knowledge Base Article 7023749.(`Bug 1126023`)

1.9.9 NPAM Service Commands Do Not Work In SUSE Linux Enterprise Server 12 or Later

The NPAM service commands such as start, stop, restart, and status now work in SUSE Linux Enterprise Server 12 or later. (`Bug 1041284`)

1.9.10 SSH Relay to a SSH Target Host Fails if You Use a Custom Port Other Than Port 22

SSH Relay to custom ports on target SSH hosts works successfully. (`Bug 1155401`)

1.9.11 When Secondary Authentication after Login, is in Progress, Accessing PAM Through Another Tab Displays Your Landing Page Without Data

When secondary authentication after login, is in progress, accessing PAM through another tab displays the login screen. (`Bug 1146114`)

1.10 Security Vulnerability Fix

Privileged Account Manager 3.7 fixes the issue of potentially unsafe CBC encryption (CVE-2019-0169).

For more information, see Disabling CBC Mode.

2 Deprecation of APIs

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

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

3 System Requirements

For information about hardware requirements, supported operating systems and browsers, see *Privileged Account Manager 3.7 System Requirements and Sizing Guidelines*.

4 Installing Privileged Account Manager 3.7

For information about installing Privileged Account Manager 3.7, see the *Privileged Account Manager Installation Guide*.

5 Upgrading to Privileged Account Manager 3.7

You can upgrade to Privileged Account Manager 3.7 from Privileged Account Manager 3.6 or later. When you upgrade PAM to version 3.7, rollback of packages to PAM 3.6 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 3.7, see Upgrading Privileged Account Manager in the *Privileged Account Manager Installation Guide*.

6 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.

- Section 6.1, “Privileged Single Sign-on to Microsoft Edge is not Supported,” on page 7
- Section 6.2, “Replication Issue in Command Control Module,” on page 7
- Section 6.3, “Secure Shell Java Terminal Displays Random Characters Instead of the Typed Characters,” on page 7
- Section 6.4, “Unable to Refresh Data In Access page While Using Internet Explorer 11,” on page 7
- Section 6.5, “Time Zones Are Different In Reports and Keystrokes,” on page 7
- Section 6.6, “All Registered Agents become Unregistered after License is added to Privileged Account Manager,” on page 7
- Section 6.7, “Moving Multiple Objects Does Not Work in Command Control Console,” on page 7
- Section 6.8, “RDP Relay Does Not Work When Network Level Authentication Is Enabled,” on page 8
- Section 6.9, “Audited Command Filter and Session End Filter Are Not Available in the New Administration Console,” on page 8
- Section 6.10, “PAM Fails to Send Emails When SMTP Has SSL and Authentication Enabled,” on page 8
- Section 6.11, “Cannot Launch SSH Relay Session From User Console in FIPS Mode,” on page 8
- Section 6.12, “Password Management and Windows Credential Checkout is Not Working With Latest Updated SLES 12 SP4,” on page 8

6.1 Privileged Single Sign-on to Microsoft Edge is not Supported

Workaround: Use any supported browser other than Microsoft Edge. (Bug 1155981)

6.2 Replication Issue in Command Control Module

Issue: In some rare scenarios, replication in Command Control module is inconsistent due to which the Backup Manager inconsistently processes the newly created Command Control rules, hence they are intermittently failing. (Bug 1039518)

Workaround: Promote the existing Primary Command Control module so the replication thread pushes the latest configuration to all the Backup Managers.

For more information, see the Knowledge Base Article 7022994.

6.3 Secure Shell Java Terminal Displays Random Characters Instead of the Typed Characters

Issue: SSH Java terminal displays random characters instead of the typed characters on Java SSH relay connection to certain network switches. (Bug 1086870)

Workaround: Use alternative SSH clients such as command line SSH or PuTTY, or MobaXterm, instead of Java SSH.

6.4 Unable to Refresh Data In Access page While Using Internet Explorer 11

Issue: When you click **Refresh** in the **Access** page, the updated data is not displayed.(Bug 1095367)

Workaround: Click **Refresh** in Internet Explorer browser instead of **Refresh** in the **Access** page.

6.5 Time Zones Are Different In Reports and Keystrokes

Issue: For certain Linux and Unix sessions, the time zone for Start Time is different in the Reports and Keystrokes. (Bug 1041802)

Workaround: There is no workaround at this time.

6.6 All Registered Agents become Unregistered after License is added to Privileged Account Manager

Workaround: Install PAM License immediately after deploying PAM manager. If license is added later, re-register the agents after you add a new license. (Bug 1100050)

6.7 Moving Multiple Objects Does Not Work in Command Control Console

Issue: Selecting and moving multiple objects by using the Shift/ Ctrl key does not work. (Bug 915307)

Workaround: There is no workaround at this time.

6.8 RDP Relay Does Not Work When Network Level Authentication Is Enabled

Issue: RDP Relay fails with the error `The remote computer requires Network Level Authentication, which your computer does not support.` when Network Level Authentication (NLA) is enabled on the host. (`Bug 774061`)

Workaround: Perform the following to disable NLA on the remote desktop session host:

1. Click **Control Panel > System > Remote Settings**.
2. Deselect **Allow connections only from computers running Remote Desktop with Network Level Authentication** and click **OK**.

For more information about using PAM application SSO where NLA can be enabled, see the Knowledge Base Article 7020137

6.9 Audited Command Filter and Session End Filter Are Not Available in the New Administration Console

Issue: `Audited Command Filter` and `Session End Filter` are not available in the new administration console. (`Bug 1130821`)

Workaround: Continue using `Audited Command Filter` and `Session End Filter` in the old administration console. For `Session End Filter`, the alternate solution is to use `Session Start Filter` with the `before` and `after` match conditions in the new administration console.

6.10 PAM Fails to Send Emails When SMTP Has SSL and Authentication Enabled

Workaround: Use an SMTP server that does not have SSL and Authentication enabled. (`Bug 1128134`)

6.11 Cannot Launch SSH Relay Session From User Console in FIPS Mode

Workaround: Launch SSH relay session using any standard SSH clients.(`Bug 1109771`)

6.12 Password Management and Windows Credential Checkout is Not Working With Latest Updated SLES 12 SP4

Issue: When SLES 12 SP4 is upgraded to the latest `krb5` package, the Password Management and Windows Credential Checkout stops working. (`Bug 1158344`)

Workaround: Downgrade the krb5 package to the one supplied with Base SLES 12 SP4. This functionality is validated against the `krb5-1.12.5-40.28.2.x86_64` package.

For more information, see the Knowledge Base Article 7024313.

7 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/

8 Legal Notice

© Copyright 2019 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus 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/.