Privileged Account Manager 3.6 Release Notes

June 2019

NetIQ Privileged Account Manager 3.6 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:

1.1 Password Management

PAM now provides the capability to automatically rotate the password of credentials managed by PAM. For password change (rotation), PAM has introduced tasks which contain password change script and scheduling options to execute the script. By default, PAM provides out-of-the-box scripts to change password of the following:

- Windows: Local and Service account
  - **Service accounts:** COM+, Windows Services, IIS Pool, and Task Scheduler

- Linux, UNIX and Network Devices which can be connected using SSH
- Active Directory

In addition, you can also create custom script to change password. If the password change operation fails, it is recorded in the failed reports, using which you can analyze the failure. For more information, see Password Management in the Privileged Account Manager Administration Guide.

1.2 Support for Federal Information Processing Standards (FIPS)

PAM offers enhanced protection against security threats and compliance with United States federal government standards by supporting Federal Information Processing Standards (FIPS). PAM leverages the FIPS 140-2 compliant features to meet the security requirements of United States federal agencies and customers with highly secure environments. Enabling FIPS mode in Privileged Account Manager causes the communication between product components such as PAM Manager, PAM Agent, PAM Administration Console, PAM User Console, and target applications to use FIPS 140-2 certified OpenSSL algorithms.

For more information about enabling FIPS, see Enabling FIPS Mode in the *Privileged Account Manager Installation Guide*.

1.3 User Experience Improvements

The new administration console of PAM, which can be accessed using the URL `https://`*`<PAM server host name/IP address>`*`/pam`, includes the following:

- Access
- Reports
- Credential Vault

You can access all other features from the legacy administration console.

1.3.1 Access

Access has now been completely migrated to the new administration console. In addition to the existing features, you can review the usage of generated API tokens and revoke the tokens if you detect malicious activities. You can also transfer all the tokens of a user to another user.

For more information about Access, see the Contextual Help.

1.3.2 Reports

The **Reports** tab now contains all the reports that are available in the **Reporting Console** along with an enhanced user experience.

In addition to using built-in reports, you can also create new reports by defining the desired criteria for the following reports:

- **Sessions:** Helps you track all the actions performed by a user in a privileged session. You can configure rules to record user actions such as keystrokes, screen shots, or videos.
- **Administrator Activities:** Helps you track all the activities performed by administrators through the UI, command line, and APIs.

- **Credential Checkouts:** Helps you track all the credential check in and check out operations performed by users.
- **Shared Key Checkouts:** Helps you track all the shared key check in and check out operations performed by users.

However, the report settings, such as encryption, audit, and syslog settings, are in the old administration console.

Performance has been enhanced to reduce the time taken during pagination and loading of data in reports.

For more information about Reports, see the Contextual Help.

1.3.3 Credential Vault

Credential Vault formerly known as Enterprise Credential Vault is enhanced and moved to the new administration console. The credential vault is no longer available in the old administration console. The credential vault is now organized as a collection of vault types, where vault type contains vaults of similar type and vault (formerly known as profiles) is a collection of resources (formerly known as account domain) of similar type. For example, LDAP (Vault Type) > Active Directory (Vault) > Active Directory server (Resource).

In Credential Vault, you can manage all resources and their respective credentials, which are used to provide privileged access. In addition, you can also manage scripts, password policies, and tasks that are used to rotate privileged account password. For more information about the Credential Vault, see the Contextual Help.

In this release, the capability to migrate the Credential Vault objects to external LDAP directory is not available.

1.4 Integration with ServiceNow

PAM provides the capability to integrate with ServiceNow, which allows you to use ServiceNow for creating and approving privileged access requests. By integrating with ServiceNow, the organization can utilize their current ticketing system to process privileged access requests. When you integrate with ServiceNow, the request details are recorded in the ServiceNow incident and the session activities are recorded in PAM.

In this release, you can use ServiceNow to create and manage only Linux terminal access requests. PAM also allows the terminal users to create ServiceNow incident directly from the terminal instead of ServiceNow UI. For more information about integrating with ServiceNow, see Integration with Ticketing Systems in the Privileged Account Manager Administration Guide.

1.5 OpenLDAP Support

In addition to Active Directory and eDirectory, PAM now authenticates and authorizes the users and groups of OpenLDAP.

For more information about configuring OpenLDAP, see the Contextual Help.

1.6 Support for Custom RDP Port through PAM RDP Relay Functionality

For better security in your organization you can now connect to a custom RDP ports through RDP relay.

1.7 Updates to Supported Platforms

There are several updates to the Privileged Account Manager supported platforms. For the complete list of supported platforms, see the Privileged Account Manager 3.6 System Requirements.

1.8 Package Rollback Is not Supported

Rolling back packages from version 3.6 to 3.5 using the UI is not supported, as there are several schema changes in the product.

1.9 Software Fixes

Privileged Account Manager 3.6 includes software fixes that resolve several issues.

1.9.1 When Creating an Emergency Access Request for Database the Available Databases are not Displayed

Fix: The available databases are displayed when creating an emergency access request. (Bug 1101185)

1.9.2 Although the Changes to Audit Log Settings are Saved They are not Displayed in the UI

Fix: Changes are displayed correctly in **Audit Log Settings**.(Bug 1114751)

1.9.3 Application SSO Does not Launch from the User Console

Fix: Application SSO can be launched from the User Console.(Bug 1106413)

1.9.4 Unable to Access RDP Relay that is a part of a Domain Though the Emergency Access Request is Approved

Fix: RDP relay to the target that is a part of a domain can be accessed after the emergency access request is approved.`(Bug 1112011)`

1.9.5 Data displayed in the Reporting Console is inconsistent

Issue: Data displayed in the Reporting Console is inconsistent because the data is retrieved from audit managers in different audit zones.`(Bug 1041844)`

Fix: Data displayed in the Reporting Console is consistent because data is retrieved from audit managers within the same audit zone.

1.9.6 Secondary Authentication Popup Displays Unsupported Authentication Methods

Issue: When secondary authentication is enabled, the secondary authentication popup displays unsupported authentication methods. `(Bug 1113789)`

Fix: The secondary authentication popup window displays only supported authentication methods.

1.9.7 Session Reports in the New Administration Console do not display any data if there are only Unauthorized Sessions

Fix: Session reports in the new Administration Console displays all the sessions. `(Bug 1107120)`

1.9.8 Command Execution Fails when a Policy is Associated with a Rewrite Command and an Enhanced Access Control script on AIX Operating Systems

Issue: When a policy is associated with a `rewrite` command and an Enhanced Access Control script on AIX operating systems, command execution fails with an error. `(Bug 1120492)`

Fix: When a policy is associated with a `rewrite` command and an Enhanced Access Control script on AIX operating systems, command execution is successful.

1.9.9 Unable to Launch RemoteApp from User Console if Application Name and Alias are not Identical

Fix: You can now launch remoteApp even with a different application name and application alias.`(Bug 1106413)`

1.10 Security Vulnerability Fix

Fix: Privileged Account Manager 3.6 resolves the Privileged Account Manager authentication token vulnerability (CVE-2019-3491) with PAM endpoints.

2 System Requirements

For information about hardware requirements, supported operating systems and browsers, see Privileged Account Manager 3.6 System Requirements.

3 Installing Privileged Account Manager 3.6

For information about installing Privileged Account Manager 3.6, see the Privileged Account Manager Installation Guide.

4 Upgrading to Privileged Account Manager 3.6

You can upgrade to Privileged Account Manager 3.6 from Privileged Account Manager 3.5 or later. Rollback of packages 3.6 to 3.5 is not supported, as there are several schema changes in the product.

For information about upgrading to Privileged Account Manager 3.6, see Upgrading Privileged Account Manager in the *Privileged Account Manager Installation Guide*.

5 Known Issues

NetIQ Corporation 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 5.1, “Privileged Single Sign-on to Microsoft Edge is not Supported,” on page 7
- Section 5.2, “Secure Shell Java Terminal Displays Random Characters Instead of the Typed Characters,” on page 7
- Section 5.3, “Unable to Refresh Data In Access page While Using Internet Explorer 11,” on page 7
- Section 5.4, “Time Zones Are Different In Reports and Keystrokes,” on page 7
- Section 5.5, “All Registered Agents become Unregistered after License is added to Privileged Account Manager,” on page 7
- Section 5.6, “Audit Videos do not Play in Microsoft Edge,” on page 7
- Section 5.7, “PAM User Console cannot be Custom Branded,” on page 7
- Section 5.8, “Unable to Log into PAM Console by Using Firefox Quantum and Edge browser, When Secondary Authentication is Enabled for Biometric Devices,” on page 8
- Section 5.9, “Newly Created Reports are not Listed Under My Reports in Internet Explorer 11 Browser,” on page 8
- Section 5.10, “New sessions are not Updated in Session Table in Internet Explorer 11 browser,” on page 8
- Section 5.11, “Moving Multiple Objects Does Not Work,” on page 8
- Section 5.12, “The Run as privileged user Option Is Not Displayed on a Windows 2012 Server Start Menu,” on page 8
- Section 5.13, “The Command Control Objects Are Not Displayed When Large Number of Objects Are Added Simultaneously,” on page 8
- Section 5.14, “The Unregistered Hosts List Is Not Working,” on page 8
- Section 5.15, “The Changes to the Syslog Settings Do Not Get Applied,” on page 9
- Section 5.16, “RDP Relay Does Not Work When Network Level Authentication Is Enabled,” on page 9

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

Workaround: Use any supported browser other than Microsoft Edge. `(Bug 1079379)`

5.2 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.

5.3 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.

5.4 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.

5.5 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)`

5.6 Audit Videos do not Play in Microsoft Edge

Workaround: Use any of the other supported browsers to view Audit videos. `(Bug 1037322)`

5.7 PAM User Console cannot be Custom Branded

Workaround: There is no workaround at this time.`(Bug 1094124)`

5.8 Unable to Log into PAM Console by Using Firefox Quantum and Edge browser, When Secondary Authentication is Enabled for Biometric Devices

Issue: When you use Privileged Account Manager in Microsoft Edge or Firefox Quantum, after you install AAF 6.0, you are unable to enroll biometric devices. (`Bug 1097960`)

Workaround: There is no workaround for Firefox Quantum at this time. For the workaround while using Microsoft Edge, see the Privileged Account Manager 3.6 System Requirements.

5.9 Newly Created Reports are not Listed Under My Reports in Internet Explorer 11 Browser

Use browsers other than Internet Explorer 11. To view the list of supported browsers, see the Privileged Account Manager 3.6 System Requirements. (`Bug 1100985`)

5.10 New sessions are not Updated in Session Table in Internet Explorer 11 browser

Use browsers other than Internet Explorer 11. To view the list of supported browsers, see the Privileged Account Manager 3.6 System Requirements. (`Bug 1100970`)

5.11 Moving Multiple Objects Does Not Work

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.

5.12 The Run as privileged user Option Is Not Displayed on a Windows 2012 Server Start Menu

Issue: When you right-click **Start** menu on a Windows 2012 server, the **Run as privileged user** option does not get displayed. (`Bug 901032`)

Workaround: To workaround this issue, right-click the application in the folder where the application is installed to execute **Run as privileged user**.

5.13 The Command Control Objects Are Not Displayed When Large Number of Objects Are Added Simultaneously

Issue: When Command Control Objects are added simultaneously in large numbers, the objects do not appear in the console. This is an intermittent behavior. (`Bug 908307`)

Workaround: There is no workaround at this time.

5.14 The Unregistered Hosts List Is Not Working

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`)

Workaround: Ensure that when you install Agents, you register it with the Manager for Privileged Account Manager. However, there is no workaround to register multiple unregistered hosts at the same time.

5.15 The Changes to the Syslog Settings Do Not Get Applied

Issue: In the Reporting console of Privileged Account Manager when you save the changes to syslog settings, such as select **SSL**, or **Allow Persistent Connections,** the changes are not applied. (`Bug 895993`)

Workaround: To workaround this issue, restart Privileged Account Manager.

5.16 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

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

Issue: The NPAM service commands such as start, stop, restart, and status do not work in SUSE Linux Enterprise Server 12 or later. (`Bug 1041284`)

Workaround: To workaround this issue, perform one of the following:

- Reboot the system using the following command:

  ```
  reboot
  ```

  (or)

  ```
  shutdown -r now
  ```

- Kill and restart the NPAM process using the following command:

  ```
  pkill unifid
  /etc/init.d/npum start
  ```

After performing one of the preceding steps, you can verify the NPAM process running status by executing the following command:

```
/etc/init.d/npum status
```

5.18 Cannot Launch SSH Relay Session from User Console in FIPS mode

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

6 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/

7 Legal Notice

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/.