Privileged Account Manager 3.7 Patch Update 2 Release Notes

September 2020

Privileged Account Manager 3.7 P2 resolves several previous issues and contains improvements to existing features.

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" on page 1
- "Software Fixes" on page 2
- "Security Vulnerability Fixes" on page 3
- "System Requirements" on page 3
- "Upgrading Privileged Account Manager" on page 3
- "Updated Modules" on page 3
- "Known Issues" on page 4
- "Contacting Micro Focus" on page 4
- "Legal Notice" on page 4

What's New

This release includes the following enhancements:

- "Support for Verifying Certificate Authority Certificates" on page 2
- "Support to Display Credential Vault Name Using Tooltip" on page 2

Support for Verifying Certificate Authority Certificates

Privileged Account Manager now provides an option to verify the server's certificate for outgoing TLS connections to LDAP authentication Domains. This option is selected by default. You can deselect this option to disable certification verification for LDAP Credential vaults. If you enable certification verification, you must perform the following steps:

For Linux Manager

1. Place the LDAP CA certificate in the `/etc/ssl/certs/` folder.
2. Run the command `c_rehash`.
3. Restart the Privileged Account Manager service by using the `/etc/init.d/npum restart` command.

For Windows Manager

Add the LDAP CA certificate to the Trusted Root List.

1. Right-click the cert format certificate.
2. Install the certificate and follow the subsequent steps to add it to the Computer level trusted root list.

NOTE: You can also run the certificate management tool **mmc** > **Add the Certificates Snapin** or `Certim.msc`. Import the CA certificate into the trusted tool certificate list.

For SLES

Run the `update-ca-certificates` command. The directory of CA certificates trust anchors used by administrators is `/etc/pki/trust/anchors.`

For RHEL

To add a certificate in PEM or DER file format to the CA trusted list on the system:

1. Add the certificate as a new file to `/etc/pki/ca-trust/source/anchors/` directory.
2. Run `update-ca-trust`.

For more information, see "Verifying and Installing LDAP Certificate Authority Certificates" in the *Privileged Account Manager Install Guide*.

Support to Display Credential Vault Name Using Tooltip

A tooltip is added in the credential vault resource name to display the complete vault names.

Software Fixes

Privileged Account Manager 3.7 P2 includes software fixes that resolve the following issues:

Component	Bug ID	Issue
	226784	Privileged Account Manager Credential check-ins delegated to Identity Manager fail.
Identity Manager	267004	Checkout fails for a custom Application credential vault when password change is set to `never`.
SSH	282060	SSH relay `Submit User` as `Run User` fails with JNLP file from Privileged Account Manager User Console.
Windows and Linux Manager Agent	1173205	Certificate validation made more robust for communication between managers and agents.
Windows Manager and Agent	239124	Error handling for some scenarios causing access violation in the Windows agent and Windows manager.

Security Vulnerability Fixes

Privileged Account Manager 3.7 P2 fixes the following potentially vulnerable security issue:

A possible DoS attack in the HTTPS communication is handled by providing an option to disable the client initiated renegotiation. (CVE-2020-11862). Perform the following steps to set this option:

1. Edit the `unifi.xml` file located at `/opt/netiq/npum/config/unifi.xml` and replace '`0`' with '`1`' in the `<SSL b.changed="1" i.reneg_dos_protection="1"/>`command.
2. Restart the Privileged Account Manager service by using the command: `/etc/init.d/npum restart`.

System Requirements

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

Upgrading Privileged Account Manager

You can upgrade to Privileged Account Manager 3.7.0.2 from Privileged Account Manager 3.7 or later. When you upgrade Privileged Account Manager to version 3.7, a rollback of packages to version 3.6 or an earlier version is not supported.

For information about upgrading to Privileged Account Manager 3.7 P2, see"Upgrading Privileged Account Manager" in the *Privileged Account Manager Installation Guide*.

Updated Modules

This version updates the following modules:

- Registry Client for registering and location framework services. `<regclnt>`
- Administration interface `<admin>`
- Provides storage and reporting of system and application audit events `<audit>`
- Remote execution for the command control agent `<rexec>`
- Provides a protocol relay for managing privileged RDP sessions `<rdp>`

- Provides mechanism to request for resources `<resreqagnt>`
- Agent console `<servers>`
- Registry Manager `<registry>`
- Framework package `<spf>`
- Command control manager module `<cmdctrl>`

Known Issues

Micro Focus strives to ensure our products provide quality solutions for your enterprise software needs. There are no new issues other than the issues mentioned in the Privileged Account Manager 3.7 Release Notes. If you need further assistance with any issue, please contact Technical Support.

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

© 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/.