Release Notes - Privilege Manager

TITLE
Release Notes - Privilege Manager

URL NAME
PM-Release-Notes

ARTICLE

Privilege Manager Release Notes 10.6 – On-premises

Release Date: 07/11/2019

Privilege Manager is the most comprehensive least privilege and application control solution, capable of supporting enterprises and fast-growing organizations at scale.

Enhancements

Enhancements available with the 10.6 On-premises release of Privilege Manager include:

- The **Syslog integration** options have been improved and support for HTTP/HTTPS was added. The HTTPS option specifically supports integrations with DEVO. (Also available in Cloud release.)
- A **Getting Started dialog** provides information on initial configuration steps and links to documentation to guide customers through configuration, integration, and setup.
- An **Offline Approval Process** has been implemented so end users can request an approval for an application to continue to execute even if an endpoint is offline. Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. The offline approval dialog can be customized within the policy action configuration area. Summary reports for offline approvals are available via the Reports page in Privilege Manager. This feature requires the latest Agents.
- **Filters/Actions have been added** in support of various new Privilege Manager functionality:
  - Application Approval Request (with Offline Fallback) Message Action (Windows, macOS): This action is for application approval requests, online and offline, allowing a customized message to be displayed to the user.
  - Copy Install Application (macOS): This filter detects if an application is installed via copy.
  - User Requested Run As Administrator Filter (macOS): Detects if a user right-clicked on an application and used Privilege Manager's custom "Request Run as Administrator" option.
  - Executable Declared as Privileged Filter (macOS): This filter checks the info.plist at execution time to determine if the applications requires administrative rights.
  - Codesign Elevated Application Filter (macOS): This filter detects codesign entitled applications to determine if the application requires administrative rights.
- **Direct approval process selection for ServiceNow** is now available in the Privilege Manager UI, and no longer requires Silverlight.
- The Windows agent supports the **display of the ServiceNow approval request ID** after the approval has been submitted.
- **Integration to use Azure AD as an authentication provider has been improved.** It is now possible to specify the Client ID and the Client Secret in the configuration for Azure AD. If not specified, the associated user credential will be used. This enables customers to use just one credential for both import and login, or use separate ones based on preference. https://thycotic.force.com/support/s/article/PM-How-to-Configure-Privilege-Manager-with-Secret-Server (https://thycotic.force.com/support/s/article/PM-How-to-Configure-Privilege-Manager-with-Secret-Server)
  Local Active Directory accounts can be imported and synchronized with Azure AD. Tasks have been added to support importing a subset of the directory instead of needing to import the entire directory. https://thycotic.force.com/support/s/article/PM-Setting-Up-Azure-Active-Directory-Sync (https://thycotic.force.com/support/s/article/PM-Setting-Up-Azure-Active-Directory-Sync)
- **New macOS features** (refer to the Mac User Guide (https://thycotic.force.com/support/s/article/PM-Macs) for detailed information):
  - A policy can be created to allow or deny standard users to install specific applications by copying the application into the Applications folder.
  - Just as on Windows endpoints, users can request application self-elevation via a context menu action on macOS system endpoints. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.
- A setting was put in place to **cap the maximum number of events** that can be sent back to the server at 1 Million events. Once that threshold is reached, the oldest event is purged from the list. This setting can be adjusted in the Advanced section of the Configuration page.
- A **browser-based server Log Viewer** is now available from the Admin menu.
- **Error notification and performance in high latency environments** have been greatly improved in this release.
- The **Application Justification Summary Report** was added to the reports page.
- **Bulk delete actions** have been added to support the removal of large numbers of file resources without timeouts.
- The Resource Targets on the Conditions tab of an ACS policy has been renamed to "when ANY match" for clarification of scope.
- General improvements have been made to the Groups view within the Local Security area.
- The Privilege Manager feature to support RDP session monitoring is being discontinued.

Bug Fixes

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items.

- In the Privilege Manager UI domain, users cannot be added to TMS Roles, only groups may be added.
- When the URI information is deleted from an existing SMTP server configuration, the URI entry box disappears from the UI.
- The Privilege Manager UI does not correctly load policy details with large numbers of filters configured. Paging functionality has been added, defaulting to 10 items per page viewed. This can be customized on any given list page to a view of up to 100 items per page.
- Unable to edit configuration of "All Other Users and Groups" for groups in local security from "Ignore if found" to "Remove if found". When this issue occurs, Privilege Manager will show an error, which then allows the user to fix the error by navigating to the "RemoteScheduledClientCommandContract" for the group that is having the issue, removing the input parameters for the provisioned group, and then retrying the change.
- Error upgrading to 10.5 U3 Directory Services for some specific conditions.
- LSS Member filter does not work if the number of members across endpoints and the number of endpoints is large.
- The Privilege Manager Remove Program Utility displays incorrect buttons for NoModify and NoRepair registry keys.
- The Add/Remove Programs Utility is preventing repairs to Microsoft Office products.
- The User Context Filter via SID Filter "create page" validation causes an error, which prevents the SID to be saved.
- After reboot, the endpoint agent creates a certificate based on the UUidCache information causing an invalid agentID error.
- A macOS account with a computed RelativeId (RID) that is null results in an exception that causes Local User Inventory to fail.
- MacOS: The Administrator account (500) is required to be added to the managed Administrators (544) group.
- After editing a managed local group, the list of members will sometimes expand to include what appears to be the entire list of all users in the system. Refreshing the console will return to showing just the members that were configured.
- During Event Discovery, if the same file is discovered from 2 policies, only one file entry will be removed but receive an Acknowledge All. The second listing of the same file cannot be removed.
- Built-in Privilege Manager User does not have read access to policies.
- Privilege Manager relies on the "Require Folders for Secrets" Secret Server setting during integration set-up.
- Login button is displayed after authentication with Secret Server.
- Customers upgrading from version 8.x have issues deleting or saving items with GUID 71f3e19c-625c-4696-80e6-c9616554cb3c.

AGENT OFFLINE

- UAC Override policy does not go into effect until UAC Override scheduled task is run.
- Event discovery resources stuck in Pending Assignment status.
- On macOS endpoints with agent version 10.6.19 installed, depending on the user interaction with the approval dialog, it is possible that after clicking Continue or Cancel the dialog is redisplayed and cannot be dismissed.

Known Issues

- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.6 macOS endpoint agent.
- If a customer implementation uses the Microsoft Azure Service Bus for their Internet connected clients, the clients will **NOT** be able to communicate with the Privilege Manager server after an upgrade to 10.6. Contact Thycotic Support if you are using Microsoft Azure Service Bus and are planning to upgrade. This does not impact implementations using a Reverse Proxy.
- Privilege Manager macOS Administrator and Privilege Manager Windows Administrator roles:
    - If you are using the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles, you must also add those members to the Privilege Manager Users role or they may not be able to view some of the application filters or actions. If you are using Secret Server authentication, restarting the Privilege Manager app pools may be required to have this take effect.
    - Members of the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles may not be able to delete some items such as policies, actions and filters, even though they are editable. Have a member of the Privilege Manager Administrators role delete those items if this occurs.

Privilege Manager Release Notes 10.6 – Cloud

Release Date: 05/30/2019

Privilege Manager is the most comprehensive least privilege and application control solution, capable of supporting enterprises and fast-growing organizations at scale. In this new release, Thycotic expands its Enterprise-Grade Privileged Access Management (PAM) as a Service, offering Privilege Manager in the cloud and building upon its industry-leading cloud-ready solutions.

Enhancements

Enhancements available with the 10.6 Cloud release of Privilege Manager include:

- A **Getting Started dialog** provides information on initial configuration steps and links to documentation to guide customers through configuration, integration, and setup steps.
- An **Offline Approval Process** has been implemented so end users can request an approval for an application to continue to execute even if an endpoint is offline. Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. The offline approval dialog can be customized within the policy action configuration area. Summary reports for offline approvals are available via the Reports page in Privilege Manager.
- **Clear communication for regularly scheduled or emergency maintenance tasks:**
    - In Privilege Manager Cloud environments **regularly scheduled maintenance tasks** will be announced via a maintenance banner at least 14 days prior to the maintenance window being in effect.
    - Thycotic will announce any **regularly scheduled and emergency maintenance** to inform customers when maintenance is performed on the cloud instance.
- **Filters/Actions have been added** in support of various new Privilege Manager functionality:
    - Application Approval Request (with Offline Fallback) Message Action (Windows, macOS)
    - Copy Install Application (macOS)
    - User Requested Run As Administrator Filter (macOS)
    - Executable Declared as Privileged Filter (macOS)
    - Codesign Elevated Application Filter (macOS)
- **Direct approval process selection for ServiceNow** is now available in the Privilege Manager UI, and no longer requires Silverlight.
- The Windows agent supports the **display of the ServiceNow approval request ID** after the approval has been submitted.
- **Thycotic One** is the access portal to Privilege Manager Cloud and provides data center access/support via Thycotic One US East, EU, and Australia Azure geo locations.
- **Integration to use Azure AD as an authentication provider has been improved.** It is now possible to specify the Client ID and the Client Secret in the configuration for Azure AD. If not specified, the associated user credential will be used. This enables customers to use just one credential for both import and login, or use separate ones based on preference. https://thycotic.force.com/support/s/article/PM-How-to-Configure-Privilege-Manager-with-Secret-Server (https://thycotic.force.com/support/s/article/PM-How-to-Configure-Privilege-Manager-with-Secret-Server)
  Local Active Directory accounts can be imported and synchronized with Azure Active Directory. Tasks have been added to support importing a subset of the directory instead of needing to import the entire directory. https://thycotic.force.com/support/s/article/PM-Setting-Up-Azure-Active-Directory-Sync (https://thycotic.force.com/support/s/article/PM-Setting-Up-Azure-Active-Directory-Sync)
- **macOS**, refer to the Mac User Guide (https://thycotic.force.com/support/s/article/PM-Macs) for detailed information on the new macOS features.
    - A policy can be created to allow or deny standard users to install specific applications by copying the application into the Applications folder.
    - Just as on Windows endpoints, users can request application self-elevation via a context menu action on macOS system endpoints. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.
- A policy was put in place to **cap the maximum number of events** that can be sent back to the server at 25000 events. Once the 25000 event comes in, the oldest event is purged from the list. For troubleshooting purposes this can be temporarily adjusted by Thycotic support.
- A **browser-based server Log Viewer** is now available from the Admin menu.
- **Error notification and performance in high latency environments** have been greatly improved in this release.
- The **Application Justification Summary Report** was added to the reports page.
- **Bulk delete actions** have been added to support the removal of large numbers of file resources without timeouts.
- The Resource Targets on the Conditions tab of an ACS policy has been renamed to “when ANY match” for clarification of scope.
- General improvements to the Groups view within the Local Security area.
- The Privilege Manager feature to support RDP session monitoring is being discontinued.

Bug Fixes

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items

- In the Privilege Manager UI domain users cannot be added to TMS Roles, only groups may be added.
- When the URI information is deleted from an existing SMTP server configuration, the URI entry box disappears from the UI.
- The Privilege Manager UI does not correctly load policy details with large numbers of filters configured. Paging functionality has been added, defaulting to 10 items per page viewed. This can be customized on any given list page to a view of up to 100 items per page.
- Unable to edit configuration of "All Other Users and Groups" for groups in local security from “Ignore if found” to “Remove if found”. When this issue occurs, Privilege Manager will show an error, which then allows the user to fix the error by navigating to the “RemoteScheduledClientCommandContract” for the group that is having the issue and removing the input parameters for the provisioned group and then retry the change.
- Error upgrading to 10.5 U3 Directory Services for some specific conditions.
- LSS Member filter does not work if the number of members across endpoints and the number of endpoints is large.
- The Privilege Manager Remove Program Utility displays incorrect buttons for NoModify and NoRepair registry keys.
- The Add/Remove Programs Utility is preventing repairs to Microsoft Office products.
- The User Context Filter via SID Filter "create page" validation causes an error, which prevents the SID to be saved.
- After reboot, the endpoint agent creates a certificate based on the UUidCache information causing an invalid agentID error.
- A macOS account with a computed RelativeId (RID) that is null results in an exception that causes Local User Inventory to fail.
- MacOS: The Administrator account (500) is required to be added to the managed Administrators (544) group.
- After editing a managed local group, the list of members will sometimes expand to include what appears to be the entire list of all users in the system. Refreshing the console will return to showing just the members that were configured.
- During Event Discovery, if the same file is discovered from 2 policies, only one file entry will be removed but receive an Acknowledge All. The second listing of the same file cannot be removed.
- Built-in Privilege Manager User does not have read access to policies.

Limitations in Privilege Manager Cloud 10.6 vs. On-prem

AGENT OFFLINE

- The Local Active Directory features exists, but requires a direct connection to the domain controller, which is often not permissible due to firewall configurations.

- Secret Server integration for authentication and vaulting of local account credentials is not presently available.
- All license key management is done via Thycotic and license keys are not visible on the licensing page. There are not presently options for customers to add additional licenses directly.
- Access to the Security Manager console (Silverlight version) is not available.
- Personas are not available.
- Server-side Powershell scripts not signed by Thycotic are not allowed. Custom server-side work can be done via Professional Services engagements.
- The setup is managed by Thycotic and installations, upgrades, and repairs are unavailable to the customer directly, this includes setup, add/remove feature options, and connection option to existing Secret Server. Upgrade notices and banners are removed with upgrades being handled by Thycotic during maintenance periods.

All other features and functionality of Privilege Manager On-premises and Cloud are the same.

Known Issues

- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.6 macOS endpoint agent.

Release Notes 10.5.4

Release Date: 12/11/2018

Enhancements

Listed below are the enhancements being provided in this release:

- When creating a resource target for a policy, the “Groups” option is available to allow targeting of organization units (OUs). See article: https://thycotic.force.com/support/s/article/User-Defined-Resource-Targets-and-Collections (https://thycotic.force.com/support/s/article/User-Defined-Resource-Targets-and-Collections)
- A new report called “Server Node Status” will show the version installed on each server node in high availability environment. This report will inform customers of the installed version of Privilege Manager across multiple instances for high availability.

Bug Fixes

Listed below are the bugs that have been fixed in this release. (The product behavior is described as it was prior to the fix. In a few of the items below, the specific fix is also described.)

- Users with the Privilege Manager Helpdesk Users role are unable to approve items; get an error message.
- Authenticated XAML message does not work if agent cannot connect to domain. Fix: When validating credentials, if the domain is not available Privilege Manager will now authenticate against the operating systems so that (if the domain isn't available) the agent will use the local database SAM cache.
- Purge Maintenance task times out on extremely large tables when performing a deletion of millions of records.
- Exporting the Application Summary Report to CSV fails.
- During upgrade, some servers don't have proper permissions to allow writing new certificates to C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys. Fix: A new error message was added for Privilege Manager servers that do not have proper permissions during the upgrade to write new certificates to: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys.
- After successfully adding the first license, message saying “No records to display” is still displayed.
- Licensing page does not display an error if importing an invalid or duplicate license.
- On some reports, some valid filterable values are not being displayed as a selectable option after selecting the “Filter Report” button.
- Labels and information displayed when viewing a task does not properly align when the screen size is small.
- Option to “Backup the System” under “Client System Settings” policies does not elevate without selecting to apply to child processing. Fix: Elevation will now occur automatically without having to change the child processing setting.
- Some Role membership group names are in all lowercase, not Pascal case.
- On the Help page, the link for the user guide is pointing to the Preferences page instead of the actual user guide.
- User is unable to press the ‘Cancel’ button on the Preferences page.
- When the browser is made smaller, the page to create scheduled tasks has overlapping text.
- When editing a copy of the “Approval Request Form Action”, the selected value in the “Approval type” disappears when switching from view mode to edit mode.
- Changing the “Minimum Security Level” field in the console log settings is not limiting the records displayed in the logs.
- “Base URL” field for Privilege Manager server under Foreign systems reads as “Base URI”. Fix: Text of the “Base URI” label in a Foreign System has been changed to “Base URL”.
- Selecting options besides the “Upper Case” option when configuring a user’s password results in “Undefined” being displayed as a selected option.
- Incorrect error messages are displayed if a new User credential is saved without or with an incorrect password.
- After clicking “Import” on the Import Items page, the import button does not grey out to display feedback that the import is processing.
- Exception is thrown on “Client System Settings” page when the Assign Filter field is left blank.
- Assigning filters to any of the items in “Client System Settings” can cause the page to become unresponsive.
- On the Time of Day filter, changing the time under “Different Periods on Different Days” also incorrectly changes the times under “Same Period Every Day”.
- Clicking the Sort column of an empty report causes page to error.
- When deleting a filter or an action that is used in a policy, Privilege Manager correctly prevents the deletion but displays an incorrect error message.
- When building resource target queries, starting with “All Computers” causes poor performance. Fix: This been removed from the default way resource target queries are built.
- “OU Directory Scope Collection Update” task fails if Collection.LastUpdated is null.
- Applications hang if a new certificate is created and the agent requests new client items before it updates applicable policies or registers with the server.
- Installing a new agent on a Mac endpoint results in a corrupted schedules.plist file.
- Azure AD tokens are expiring within minutes. Fix: Azure AD will now last as long as normally issued tokens.
- If the “UNC Elevation Policy Template” Config Feed is imported, the "UNC Content Query" is erroring.
- When Secret Server and Privilege Manager are installed together using the combined installer, and a separate domain account without write permissions is used, subsequent upgrades fail if the domain account running the application pool does not have Write permissions on the TMS web folder.
- “Advanced Deny Notification Actions” are not included in dashboard counts and the list of denied files.

Release Notes 10.5.000003

Release Date: 9/25/2018

Bug Fixes

- Fixed issue where the Mac agent configuration did not have a default task check in interval saved.
- Fixed issue where queries for reports that are scoped to display only certain resources will fail if the Default Security Descriptor ID is null or empty.
- Fixed issue where large Active Directories caused the Collection and Resource Targeting Update task to run for too long.
- Fixed issue where Privilege Manager’s authentication provider screen would crash if incorrectly configured. When Privilege Manager cannot reach an Active Directory domain, a useful error message is now displayed.
- Fixed issue where Privilege Manager task schedules are not properly saved and displayed.
- Fixed issue where the dashboard would display an unexpected error in a modal popup the state of a gauge undefined.
- Fixed issue where the sign-in page URL query string could be used to redirect a user to another URL by only allowing relative URLs.
- Fixed issue where Telerik grids were not able to be resized when zoomed in or out in Chrome, Firefox, and Edge.
- Fixed issue where the GetToken API returned an invalid token for unauthorized requests instead of a 401 response code.
- Fixed issue that allowed Privilege Manager to be embedded inside of an iframe.

AGENT OFFLINE