ObserveIT 7.6.2 Release Notes

This document lists new and deprecated supported platforms, issues that were discovered and fixed since the release of the previous release of ObserveIT, and known issues and limitations. It is important that you read this document before you install and configure ObserveIT version 7.6.2.

Documentation for release 7.6.2 is available here.

New Features in this Release

ObserveIT 7.6.2 release includes the following new features:

- Silent Installation and silent installation with obfuscation: From macOS Mojave 10.14, the mass deployment procedure has been streamlined so the ObserveIT process controller is automatically granted access. For more information and instructions, click here.
- ObserveIT Agent has been certified on the following platforms:
    - Linux RedHat 7.5
    - Linux RedHat 7.6
    - Ubuntu 18.04

ObserveIT 7.6.2 also includes the following 7.6.x features:

- Enhanced performance for File Activity Monitoring (FAM): FAM is no longer in Beta. Monitoring. Performance as well as diagnostics fine-tuned to perform at GA level.
- New screens allowing granular control of the File Activity module:
    - Viewing and controlling FAM tracked files per endpoint
    - Ignoring file activity originating from other endpoint solutions
- File Activity Monitoring upload and download tuning and diagnostics: Added diagnostics log to understand the internal FAM rules and events.
- File Activity Monitoring performance enhancements: Improved handling of FAM service events enabling FAM to perform under a higher load.
- File Activity Monitoring policy updates include:
    - Ability to control number of tracked files and the retention policy
    - Option to enable advanced file tracking control
    - Option to control tracked files and exclude bypassed files
- Implementation of enhanced auditing of ObserveIT Console Users activity (GDPR compliance).
- Timeline view provides a chronological view of all activity within the session: Provides a view of the exact flow of user actions.
- Password complexity has been upgraded: Provides better security and decreased vulnerability.

- A link to the Support Portal was added to the Help menu via the (?) icon on the top right of the Web Console screen.

Resolved Issues

- [Issue #63033] – Modified Chrome URL detection mechanism for to improve performance when using ObserveIT Hidden Installation with Chrome.
- [Issue #63233] – Added authentication certificate to WebsiteCategory request.
- [Issue #63478] – Session closes only after all files are transferred.
- [Issue #63485] – Duration time for execution of Splunk integration improved.
- [Issue #63600] – Alerts generated for File Activity Monitoring with Website categorization.
- [Issue #63548] – Alerts generated for excluded applications defined by Recording Policies.
- [Issue #64054] – Links to updated online documentation validated.
- [Issue #58364] – Windows Agent popup messages (secondary authentication, ticketing, alert notifications, etc.) appear in the correct language for a localized installation.
- [Issue #61248] – Active Directory users can authenticate to use Credential config part of the Dev portal after logging into Web Console.
- [Issue #55384] – Services responsible for File Activity Monitoring start correctly after reboot on Windows 10 machines.
- [Issue #62150] – Secure Print is now supported.
- [Issue #56959] – In order to support special Chinese characters in exported PDFs, you need to install the "arial-unicode-ms" font. This font is not included with ObserveIT.
- [Issue #62064] – All applications can be run as Administrator when User Access Control Local Policy is set to Disabled.
- [Issue #62017] – On AIX, when there is communication problems with the ObserveIT Application server register over https mode, there is no core dump of obitd.
- [Issue #62393] – When using non-default names for the network interface on Linux, the correct host IP is used instead of 127.0.0.1.
- [Issue #50542] – The correct page count is now captured, even for very large print jobs.
- [Issue #61382] – Clipboard issues with Excel are resolved.
- [Issue #62628] – Opening pictures using the Photos application in Windows 10 is no longer recognized as a file upload, same for PDFs and HTML files.
- [Issue #59785] – Blocking messages now support Chinese characters.
- [Issue #58309] – Stability issues with the Notification service after restarts have been resolved.
- [Issue #60865] – On a Mac agent, when only metadata is being recorded, recording is started after a Start Video Recording alert is issued.
- [Issue #63226] – In Excel, moving a value in a cell, no longer results in the following error:

  "There's a problem with the clipboard, but you can still paste this content within this workbook"

Known Issues

- [Issue #56098] – When upgrading from a version earlier than 7.1, changes that were made in the assignment of Insider Threat Library (ITL) alert rules to User Lists (from a version earlier than 7.1) will be reset to their default assignment.
- [Issue #58105] – During installation of the Website Categorization module on machines that are using TLS version 1.2, the following error message might be displayed:

  "The update service could not be accessed. Please check Internet connectivity. If this machine…"

This error message can be ignored as the Website Categorization module will still function properly in this environment.

- [Issue #58607] – When accessing a Linux agent using sftp protocol and an alert notification has been configured for GET and PUT commands, the user receives an "access denied" message but the warning notification is not displayed.
- [Issue #60392] – Upload tracking with Firefox on Windows 10 does not work due to permissions issues.
- [Issue #61186] – When using the Edge browser, the "Save as photo" command is not detected as a file event. The downloaded file is not tracked.
- [Issue #60137] – Searching for a part of a filename together with the file extension may not return correct results.
- [Issue #62197] – When moving from using a combined mode of screenshot storage (SSD "Hot" storage together with standard "Warm" storage), to using only standard file system storage, IIS must be restarted after the change is applied in Screenshot Storage configuration.
- [Issue #62988] – The apis folder and its sub-folders remain after uninstall.
- [Issue #62720] – Uploads from Firefox (below Firefox release 33) are not tracked.

Limitations

- For Asian languages that use a virtual keyboard, key logging data is captured by "writing" on the keyboard, but typed characters cannot be captured by mouse clicks.
- Graphical (X) applications are not recorded except for the supported X terminals, such as GNOME-terminal or dtterm.

File Activity Monitoring

- New File Activity metadata is not yet fully integrated in API for SIEM integration.
- When copying a tracked file to a network share or to a local drive mapped to a network shared drive, tracking is discontinued.
- File tracking is lost after deleting (i.e., moving to the Recycle Bin) and then restoring the file.
- Modifications of file content are not tracked.
- Changes to file permissions are not tracked.
- Performing a "Save As" on a tracked file will not track the newly created file
- Upgrading an Agent will sometimes stop tracking of files that were tracked before the upgrade
- Cloud Sync & Share:
  - Only the default installation folders are supported. For example, if you install Dropbox in a non-default folder an alert will not be triggered when copying a tracked file to this folder.
- FAM Undetected Scenarios
  - USB/Network drive upload is detected, however the source of the file is sometimes not detected correctly.
  - The TOR browser is not supported.
- When using Edge browser (Win 10), Upload events are filtered out and not marked. This occurs when using File Picker activity and does not occur with Drag and Drop activity. This limitation applies to OS builds before 1709 only.

Anonymization Limitations (from ObserveIT 6.7)

The following are known issues that relate to the ObserveIT Anonymization feature:

- When an "Anonymized" Web Console user logs in to the Web Console, the following features are disabled: Reports, Archive, DBA Activity, Saved Sessions, Audit Sessions, Audit Saved Sessions, and Inventory view in the Endpoint Diary.

In-App Elements

- [Issue #22203, #22873] – Applications that were developed using the following technologies are not supported for marking and capturing user interactions with applications:
  - Java-based apps, desktop and web (Java applets)
  - JTK-based apps
  - Flash-based app (Adobe Air, web)
  - Proprietary windows-based technologies such as SAP Business One
- [Issue #31562] – Capturing In-App elements metadata on user interactions with applications/websites is disabled on Citrix and Terminal Servers.
- [Issue #31561, #31563, #31564] – The Internet Explorer 9, Opera, and Firefox browsers are not supported for marking In-App elements data.
- [Issue #31652] – Alert rules cannot be created from an In-App element password field using the "empty" or "not empty" operator.

Active Directory Limitations

- The Application Server must have access to at least one Domain Controller of the 'Login Domain', otherwise the old Agent will fail to retrieve the user's group membership. This also occurs when there is "One Way Trust" between forests.
- In order that the Application Server/Web Console will refresh the Active Directory networking topology (for example, when there is a new Domain Controller, forest trust relationship, etc.), the user must reset the IIS (Microsoft Internet Information Server).

Mac Printing

- Printing directly from Chrome browser is not tracked.
- Printing from Finder using right-click-Print, without opening the document is not tracked.
- Printing from the Mail application may not be tracked at times.
- When printing from OneDrive, the document name is sometimes missing.

Endpoint IP

- The Additional IPs displayed in Configuration>Endpoints screen may include some non-real IPs (starting with "169.254").

Product Architecture

- [Issue #63625] – Agent remote control for start/stop activities is not supported on Amazon Web Server (AWS) environment.