ObserveIT 7.5.2 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 7.5.2.

For details of the new features and enhancements that are provided in this release, please refer to What's New in ObserveIT 7.5.

The most up-to-date release documentation is available here.

New Features in this Release

This release includes the following new features:

- Monitor any file being uploaded to any website – Provides better detect data exfiltration attempts by getting full visibility to any file sent out via webmail, social media, cloud storage, file sharing sites, and more.
- FAM is easily accessible across the Management Console – Enables security analysts and investigators to resolve incidents faster.
- Cut down archive processing time – Archiving and deleting large amounts of recording data can now be completed much faster and within the allocated nightly time slot.
- Search includes File Activity Metadata (FAM) – Security analysts can search for any user activity including file downloads & uploads, copy to cloud, etc. without losing the context of all other user activities.
- Integration – Larger scale and new APIs for SIEM and User Activity Profiles. Easily integrate large amounts of user activity data with other security tools and processes.
- Video Player – Richer context in the User Activity List. Understand exactly, step-by-step, what the user is doing.
- Privacy – Protect user privacy by excluding categories of personal websites (e.g. banking, social media) from being recorded or record them as meta-data only instead.
- Mac Agent Enhancements – Print activity is monitored and detected as data exfiltration. The printer name, document name and number of pages are recorded.
- Mac presence in the Management Console – The Mac icon is displayed in recorded sessions to indicate the Mac platform and the Mac OS type is available in various filters and in Search.
- Configuration for File System storage has been moved from the database configuration file to a new screen in the Web Console (Configuration > Storage > Screen Capture Data > Change storage mode popup). All configuration is now done using the Web Console.

Supported Platforms

New Platforms

- MS SQL Server 2017 as the ObserveIT Application database
- Microsoft SSMS 17.x (17.1, 17.2, 17.3) for DBA Activity
- Linux Agent installation and activity on Debian 9
- Linux Agent installation on Oracle Linux 6.9
- The latest version of Amazon Linux (currently 2017.09)

Deprecated Platforms

- Database/Application Server: Microsoft SQL Server 2008 will not be supported starting with ObserveIT release 7.5.
- RHEL/CentOS 6.6
- Oracle Linux 6.6
- Internet Explorer 9

A full list of all the currently supported platforms and their update versions is provided in the ObserveIT Product Documentation.

Resolved Issues

- [Issue #59467] – Uninstall now removes all recact.exe entries from the Windows registry.
- [Issue #59088] – Permissions have been hardened for an internal UNIX agent file.
- [Issue #58940] – The Mac agent supports TLS 1.1 and 1.2.
- [Issue #57060] – ObserveIT monitor logs support CEF format.
- [Issue #58391] – The Website Categorization Module can now be installed when using custom SQL ports.
- [Issue #59518] – CPU performance has been improved in cases when Session Data Integrity is enabled.
- [Issue #58825] – When saving rules using the "Time of day" and the operator "is between" is selected, the time fields are saved correctly.
- [Issue #60026] – This fix added one more program to our supported login program binary named "Terminal".
- [Issue #60975] – Screenshots Storage Optimizer can now post "processed-tasks" to the Task service in SSPI.
- [Issue #61489] – Installation of the Web Console proceeds in a normal amount of time and is no longer delayed by unzipped files.
- [Issue #62094] – When using the GetImageList API with a valid ObserveIT token, users receive the data for the requested session.
- [Issue #61782] – When using the REST APIs to pull the User Activity Profile details, the netActiveTime is correctly calculated. A field displays the daily time spent in the application.
- [Issue #60206] – Results from commands entered into PowerShell now display correctly, including the Clear Screen (cls) command, when the KeyLogger is enabled.

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 #58364] – Windows Agent popup messages (secondary authentication, ticketing, alert notifications, etc.) appear in English even on a German localized installation.
- [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.

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 (Beta)

- New File Activity metadata is not yet fully integrated in all modules across the Web Console – including Search, Reports, Video Player, and SIEM integration. The following limitations also apply:
  - All downloaded files are tracked – the download action cannot be limited to specific websites. However, the Alerts configuration can be limited to files that originate from specific websites.
  - When a file is downloaded to a folder, file activity on the folder is not recorded.
  - If a tracked file is added to a folder, any actions on the folder will appear as actions on the tracked file. Renaming the folder will stop file tracking.
  - 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 stop the tracking.
  - Upgrading an Agent will sometimes stop tracking of files that were tracked before the upgrade.
  - Sessions with no file activity to display may be included in search results when the keyword in the "Search for" field is also the title of a window that is unrelated to file activity and the "Within" field is set to "All file activity".
- 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.
  - It is not possible to add another Cloud Sync & Share vendor to the 5 currently supported vendors.
- Tracked files are kept at the Agent level, therefore, files that are downloaded from one monitored computer will not be tracked when they are accessed from another monitored computer. Files accessed by different users from the *same* monitored computer are tracked properly.
- FAM Undetected Scenarios
  - Download of files with the .pdf extension in Internet Explorer are not tracked.
  - USB/Network drive upload is detected, however the source of the file is sometimes not detected correctly.
  - The TOR browser is not supported.
- FAM – Silent Mode
  - When CPU reaches above 15% (configurable), or the Agent receives 200 events in 3 secs, whichever comes first:
    - FAM Driver moves into "silent mode" for 10 sec (configurable).
    - FAM events during this time will not be monitored.

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.

- When Anonymization is enabled, Web Console users who are "Anonymized" can see previously scheduled reports in the clear (i.e., not anonymized).
  To prevent Anonymized users from viewing data that is not anonymized, disable the Reports feature or remove the relevant Web Console users from the distribution list ("*Scheduled Reports for Console User*") in the Reports page.

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

- User domain is NOT equal to group domain:
- *Old Agent*: Only when USER domain is nested in DL (different domain to USER) that is nested in another DL (different domain to USER).
- User domain is NOT equal to resource domain (domain of the Agent machine):
- *New Agent*: DL group from USER domain will not work (see Microsoft known behavior: http://technet.microsoft.com/en-us/library/cc755692%28v=ws.10%29.aspx.)
- 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").