observe it

ObserveIT 7.0 Release Notes

In This Document

About This Release

This document lists the new features, enhancements, known issues, and issues that were discovered and fixed since the release of ObserveIT version 6.7.2. It is important that you read this document before you install and configure ObserveIT version 7.0.0.

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

New Features and Enhancements

This release includes several major new features and enhancements.

New Features

- User Activity Profile
  - Enable security analysts to see exactly where users are spending their time
  - Investigate employee or remote vendor productivity by examining how much time they spend in applications, their working days/hours, and idle time
  - Dynamic application and device filtering capabilities
  - Identify risky user activity such as applications/websites/Unix commands that are abnormally used, or run on infrequently used computers
- Key Logging Alerts
  - Detect and alert on sensitive keywords & commands typed in desktop applications, websites and shell command tools
  - Detect and alert on data exfiltration attempts by users typing protected keywords in emails or chat applications, social media sites, etc.
  - Identify and alert on commands executed in CLI tools such as Windows CMD, PowerShell, PuTTY or Mac Terminal
  - Identify and alert on Unix level commands running from Mac terminal applications
- Preventive Actions
  - Stop users that breach security or violate company policies
  - Force users to log-off when connecting to unauthorized computers
  - Close applications or websites that are involved in unauthorized activity
  - Collect valuable user feedback before the application is closed or the user is logged-off
- Insider Threat Library (ITL) maintained by a Content Manager and released as a ZIP to customers
  - Customers receive regular updates with no need for software upgrade
  - Security administrators are kept up-to-date with new insider threat scenarios

Enhancements

- Revamped Web Console UI
  - Enhanced Web Console UI look & feel consistent across the product
  - High resolution screens accommodating more data
  - Improved terminology changes – "Endpoints" and "Recording Policies"
- ObserveIT Insider Threat Library (ITL)
  - Additional out-of-the-box insider threat scenarios provided by new system rules for key logging, unauthorized DBA and Active Directory activity.
- New and Improved Reports
  - New reporting capabilities on websites visited, printed documents, USB storage device connections, file copying, installing and uninstalling applications, and so on, significantly improving security operations and regulatory compliance.
- The deletion of data from the Archive database can now be done by users who are members of Active Directory groups.
- Solaris 10 with OpenSSL version 1.0.1 is now supported.

Backward Compatibility

Most features, functions, and capabilities of ObserveIT are backward compatible, which means that you can use an earlier version of the ObserveIT Agent with the current version of the ObserveIT server-side components. However, in order to maintain full feature compatibility, it is highly recommended that you use the most current version of the product.
Following are the minimum server-side and Agent components versions that are supported in this release:

Component	Minimum Supported Version	Upgrade Requirements
Server-Side	5.8.3 is the oldest version that can be upgraded to version 7.x.x.	If you have an earlier version that is not supported, first upgrade to the minimum supported version, and then upgrade to the latest version.
Agents (Windows or Unix)	5.8.3 is the oldest version that can work against Server 7.x.x (backward compatibility of Agents).	If you have an earlier version that is not supported, uninstall it, and then install the latest version.

New Supported Platforms

The following new platforms are supported in this release:

- RHEL/CentOS 7.3 x86_64
- Oracle Linux 7.3 i386/x86_64
- Solaris 10 with OpenSSL version 1.0.1
- Windows Server 2016 on the Server-side (Application Server and Web Console)

  Note: Windows Server 2016 will also be supported on the Agent from version 7.0.1.

- Microsoft SQL Server 2016

The following platforms are no longer supported or have limited support:

- User Activity Profile is not supported on Microsoft SQL Server 2008/R2 does not support the User Activity Profile feature.
- Solaris 10 with OpenSSL version 0.9.7/0.9.8 is supported ONLY for ObserveIT Agents up to 6.7.2 on best effort.
- HP-UX 11.23 is no longer supported

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

Resolved Issues

- [Issue #46606] – The export of report files via Excel now works properly.
- [Issue #47246] – Sessions in the User Diary are now displayed properly in the Japanese UI.
- [Issue #47942] – The Admin Dashboard in the Japanese UI now works properly.
- [Issue #49370] – The Secondary Authentication window no longer disappears when the RDP client is closed.
- [Issue #49723] – Key Logger search performance was significantly improved.
- [Issue #50041] – The size of the trace file from the Rule Engine Service was significantly reduced.
- [Issue #50757] – The ObserveIT Agent now supports color recording in high screen resolutions.
- [Issues #50837 & 51809] – The size of the trace file from the User Analytics Service was significantly reduced.
- [Issue #51114] – When opening a report in Excel, header images now display properly.
- [Issue #51115] – Uninstallation of an AIX Agent no longer changes file permissions in the `sshd_config` file.
- [Issue #51512] – The ObserveIT Agent tray icon is now displayed correctly as configured in the Stealth and Privacy recording policy.
- [Issues #52222 & 48979] – From ObserveIT version 7.0.0, the Agent on Solaris 10 supports OpenSSL version 1.0.1. For earlier versions, please contact ObserveIT support.

Known Issues

- [Issue #28607] – When using a Remote Desktop connection on an Agent endpoint with key-logging enabled, when the RDP window is maximized, the Agent does not capture keystrokes and the Search feature doesn't work as it should.
- [Issue #31072] – Health monitoring does not monitor the User Analytics Service.
- [Issue #31297] – When returning online from offline recording mode, changes in the Recording Policy are not always implemented.
- [Issue #39746] – When copying a file from a mobile storage device to the desktop/folder/USB storage, the FILECOPY window title is not displayed.
- [Issue #40351] – When running a command from the Unix shell that produces output for another shell command, the name of the Top Level Command (application name) for the secondary shell command is incorrect.
- [Issue #41443] – When a security password for Agent uninstallation is configured, upgrading the Agent using the "One Click" installation does not work.
- [Issue #41582] – In the Alerts page, the "Status", "Alert/Prevent", "OS Type" and "Action" filters do not return their default values after clicking Reset.
- [Issue #45438] – On Unix sessions comprising 20,000 commands, only 1,500 commands are displayed in the "Print Detailed Information" report.
- [Issue #45955 & 52746] – In some cases, window titles which contain special characters do not display properly.
- [Issue #46258] – When defining an Archive schedule with job frequency set to "Once" (i.e., a one-time job), the Data Type section should not be displayed.
- [Issue #47055] – In rare cases, when there are many concurrent users and the recording policy is configured to use color compression for images, some of the recorded chunks appear as grayscale.

- [Issue #47393] – When using the "Login/Secondary user [domain\]name" option to define the "Who?" condition, and the operator is negative (for example, "is not", "is not a member of group" etc.), alerts are not triggered in cases of no Secondary Authentication.
- [Issue #47657] – Restoring archived screenshots is not possible when the File System archiving mode is used.
- [Issue #48348] – Archiving screenshots to the File System Archive takes longer than to the Database Archive.
- [Issue #48353] – No system event is generated for a failed Archive job.
- [Issue #49997] – The "Visited URL" condition appears twice in the "Did What?" condition of an alert rule, if a Website Category condition is also defined for the alert rule.
- [Issue #51072] – In the Windows Session Player, the screenshots scroll bar does not scroll up or down automatically.
- [Issue #51248] – In the Filter section of the Alerts page, the content of the Action field disappears after clicking Reset.
- [Issue #52468] – Data from offline user sessions that were previously online is not displayed in the User Activity Profile.
- [Issue #52555] – By default, alert rules that were updated more than one year ago are not displayed due to the default filter period. To change the default filter period, open the More Filters section of the Alert & Prevent rules tab, and change the value in the "Updated on" field.
- [Issue #52657] – In some cases, the User Activity Profile shows "Unknown application" instead of the specific application name in the list of user applications.
- [Issue #52867] – When the Website Categorization module fails to download the initial data, the "Website Categorization Last Update" date in the About page is displayed incorrectly.
- [Issue #53043] – The day of the week system setting "Week begins on" is not reflected in generated alerts and reports.
- [Issue #53082] – On Mac Agents, users that belong to an Active Directory group that was excluded from being recorded in the User Recording Policy, are still recorded.
- [Issue #53211] – When defining a date range for a report, the end date for the defined period is not saved.
- [Issue #53214] – If the Agent is in a different time zone to the Application Server, the number of alert instances in the Application Activity List of a user's activity profile may show inconsistencies.
- [Issue #53076] – When a notification message is too long, the Preview popup does not display properly.
- [Issue #53089] – The Login/User filter in the Archive Diary does not include user names.
- [Issue #53122] – User Risk Dashboard shows incorrect application name on Unix systems.
- [Issue #53125] – The ObserveIT Key Logger does not capture text on remote sessions to Windows 8, 8.1, or 10 machines on which an Agent is installed.

Limitations

- SQL Server 2016 is not supported for DBA Activity in the Web Console.
- The Windows Key Logger functionality does not support Asian languages, such as Korean, Chinese (Traditional/Simplified), and Japanese, etc.
- Graphical (X) applications are not recorded except for the supported X terminals, such as GNOME-terminal or dtterm.

Anonymization Limitations (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 Server Diary.
  - After Anonymization is enabled, Web Console users who are "Anonymized" are able to see previously scheduled reports in the clear (i.e., not anonymized).
    In order 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).