ObserveIT 7.1 Release Notes

In This Document

About This Release

This document lists the new features and enhancements, issues that were discovered and fixed since the release of ObserveIT version 7.0.0, and known issues. It is important that you read this document before you install and configure ObserveIT version 7.1.0.

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

New Features and Enhancements

This release includes several major new features and enhancements.

- **File Activity Monitoring (BETA feature)** – Enable security analysts to detect data exfiltration before it happens, with full file audit.
  - Track and alert on files that were downloaded or exported using a browser or web-based application, from the internet or intranet.
  - Alert if a tracked file is copied or moved to the default local sync folder of cloud storage apps: Dropbox, Google Drive, iCloud, Box (Windows only), OneDrive (Windows only).
  - Track activities on downloaded/tracked files – copy, move, rename, delete.
  - File Diary – browse and filter activities on tracked files. Print and export to Excel.
  - File History – view full history of each tracked file and link to Video playback for more context.
- **Enhanced Alert Review Workflow** – enable Incident Response teams to drive incident investigation.
  - Export alerts metadata and screenshots to PDF file – share real-time information on risky user activity and specific incidents with people in the organization who do not have access to ObserveIT.
  - Add comments to alerts, view comments, and filter by comment text.
- **Alert when Copying Text to Clipboard** – Alert when text that contains sensitive or confidential content is copied to the clipboard.
- **New Reports** – New reporting capabilities that enable compliance teams to meet the regulatory requirements.
  - Typed text (key-logger)
  - SQL Queries (DBA Activity)
  - User Text Feedback (Notifications and Preventive Actions)
- **Enhanced Insider Threat Library (ITL)** – Additional out-of-the-box insider threat scenarios are provided by new system rules to prevent data exfiltration, enabling compliance teams to meet the regulatory requirements.
- **Detect & Prevent SFTP commands (Linux) –** sent from remote servers with intent to bypass security controls.

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, 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 supported platforms provide coverage for the latest OS and application versions:

- Agent support for Windows Server 2016
- DBA Activity support for MS SQL Server Management Studio 2016
- 64-bit Application Server

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

Resolved Issues

- [Issue #46809] – When Session Data Integrity is enabled, the Console now loads data at the normal speed.
- [Issues #48676, 53251] – ObserveIT now supports complex Active Directory passwords and special characters upon Web Console login.
- [Issue #49965] – Uninstalling the Web Console now completes properly.
- [Issue #53072] – When ObserveIT is active, starting the tomcat browser on Linux as a regular user (not root) no longer fails.
- [Issue #53247] – The Website Categorization module is updated properly when running under the SSPI service user.
- [Issue #53252] – The Unix Agent now registers properly for Fully Qualified host names.
- [Issue #53272] – After unregistering an Agent, 3-999 days of inactivity are supported.
- [Issues #53366, 53998] – Agent installation no longer fails on HTTPS port 443 when TLS 1.1/1.2 is enabled.
- [Issue #53637] – Lists can now be configured properly in the Chinese version of ObserveIT.
- [Issue #53692] – Out-of-the-box alerts are triggered for all regular users; Unix/Linux users are now automatically added to the Everyday Users list.
- [Issues #53794, 53795, 53796] – The status of Agents is now reflected properly in the Health Monitoring Admin Dashboard – the numbers of recently installed/uninstalled Agents are displayed correctly in the Deployed Agent Versions portal.
- [Issue #54027] – User notification feedback messages now support the use of Chinese characters.
- [Issue #54093] – When key logging is disabled, alerts are now generated when a user executes an SQL command.
- [Issue #54707] – In the User Risk Dashboard, filtering the display of users by Endpoints now works correctly.
- [Issue #54846] – Windows commands are now captured properly in Putty applications that use uncommon prompts.
- [Issue #55231] – On RHEL/CentOS 7.0, unnecessary audit logs are no longer generated.
- [Issue #55475] – In the User Activity Profile, an error no longer occurs when choosing the Date in a specific language.
- [Issue #55622] – ObserveIT Website Categorization now works properly when installed in proxy mode.

Known Issues

- In rare cases, when File Activity Monitoring (Beta version) is enabled, Agent CPU utilization shows an increase. This issue will be fixed in the next version.

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, Session Diaries, Video Player, and SIEM integration.
- 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.

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).