ObserveIT Version 7.9.0 Release Notes

This document provides information about new features, issues that were discovered and fixed since the previous release of ObserveIT, and limitations of the release. It is important that you read this document before you install and configure ObserveIT version 7.9.0.

Documentation for the release is available here.

For information about how to install and upgrade, see:

- ObserveIT Installation
- Upgrading ObserveIT

NEW FEATURES AND ENHANCEMENTS

✓ *Agent Auto Upgrade (Beta)*

Agent Auto Upgrade lets you upgrade Agents directly from the ObserveIT Web Console. You have control over which endpoints to upgrade and you schedule when the endpoints will be upgraded. Agent Auto Upgrade is intuitive and easy to use.

- Create Upgrade Sets: Create a policy that defines which endpoints you want to upgrade and when. Allows you to create multiple Upgrade Sets to define specific policies for specific endpoints.
- Upgrade Sets Status: Review and monitor the Upgrade Sets you create so you know which are successful and which are not. You can access additional information about specific endpoints directly from this view.
- Endpoint Upgrade Status: Review and monitor the upgrade progress and history of each endpoint so you know which endpoints have successfully updated, which have not and why not.
- Retry and Rollback: If an endpoint cannot be upgraded, Agent Auto Upgrade, retries. If still not successful, the Agent version is rolled back so that it can continue monitoring the endpoint.

Prerequisite: The first time you use Agent Auto Upgrade, you must install the Updater component on each endpoint. (See Installing the Updater for Agent Auto Upgrade.)

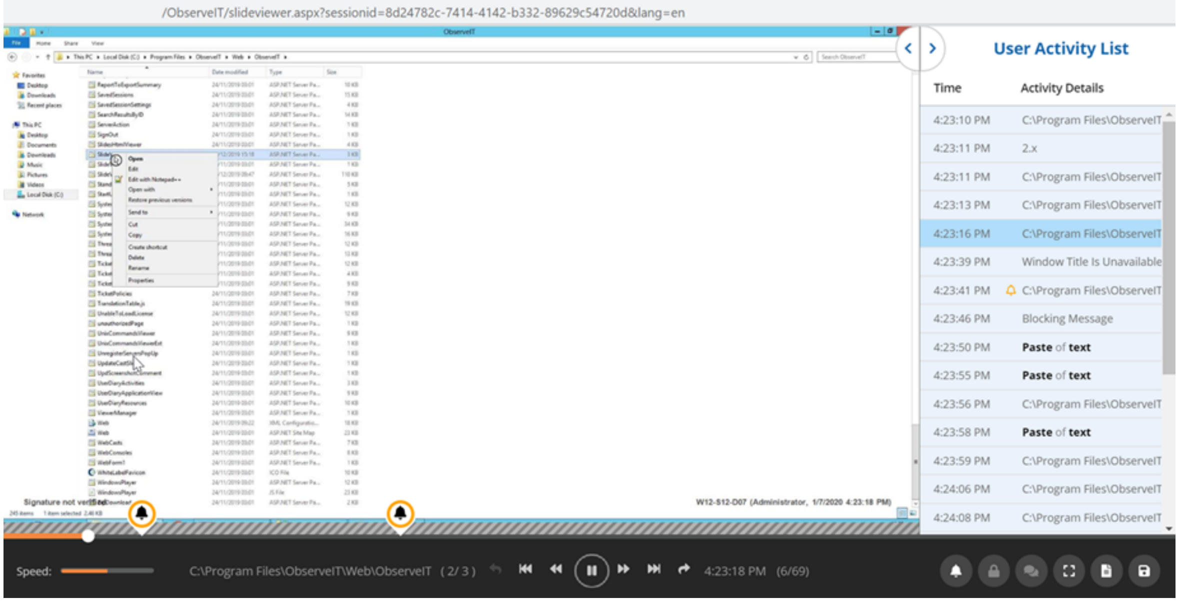
See: Agent Auto Upgrade

✓ *Session Player Updated*

The look & feel and usability of Session Player have been updated using new back-end technologies providing more secure and enhanced performance.

Here are some of the enhancements that have been introduced with this version:

- Look & feel have been modified (especially the bottom controls area)
- Thumbnails of activities can be viewed when hovering with the mouse over the progress bar
- Navigation time to various activities has been boosted



/ObserveIT/slideviewer.aspx?sessionid=8d24782c-7414-4142-b332-89629c54720d&lang=en

User Activity List

Time	Activity Details
4:23:10 PM	C:\Program Files\ObserveIT
4:23:11 PM	2.x
4:23:11 PM	C:\Program Files\ObserveIT
4:23:13 PM	C:\Program Files\ObserveIT
4:23:16 PM	C:\Program Files\ObserveIT
4:23:39 PM	Window Title Is Unavailable
4:23:41 PM	🔔 C:\Program Files\ObserveIT
4:23:46 PM	Blocking Message
4:23:50 PM	**Paste** of **text**
4:23:55 PM	**Paste** of **text**
4:23:56 PM	C:\Program Files\ObserveIT
4:23:58 PM	**Paste** of **text**
4:23:59 PM	C:\Program Files\ObserveIT
4:24:06 PM	C:\Program Files\ObserveIT
4:24:08 PM	C:\Program Files\ObserveIT

W12-S12-D07 (Administrator, 1/7/2020 4:23:18 PM)

Speed: C:\Program Files\ObserveIT\Web\ObserveIT (2/3) 4:23:18 PM (6/69)

See: Using the Session Player

✓ *Mac No Label (NL)*

Improved Mac No Label (NL) version introduced.

✓ *Continued Tracking when Copy File to Network Drive*

File tracking continues to the network drive. When a tracked file is moved or copied to a network drive, tracking is supported.

All file activity (rename, delete etc) executed from the same endpoint will be tracked by the Agent.

✓ *Enable Box sync folders monitoring as entry point*

You can enable tracking files copied from Box cloud storage sync folder to local or network drive (as a new entry point). From the time a file is infiltrated from the Box cloud storage sync folder, all its activities are tracked. You can review the tracked events from File History and the Diary views.

Select **Enable Box sync folders monitoring as entry point**, from **Recording Policies**, in **File Activity Global Monitoring Settings** section,

> This feature is currently only supported for Box Drive and Box Sync applications.

See: File Activity Monitoring Global Settings

✓ *Alert Download by Full URL*

When defining alert rules, you can now create Alerts by setting a specific **Website URL** from which a file has been downloaded, in the conditions for the Exfiltrated File and **Downloaded/Saved** categories.

See: Exfiltrated File - Did What and Downloaded/Saved File - Did What

✓ *ObserveIT dedicated driver used for optimized file activity monitoring*

- **ObserveIT Proprietary Driver**: From this release only, ObserveIT dedicated driver (Next-Gen FAM driver), is used for optimized file activity monitoring. The option to select/unselect Next-Gen FAM driver has been removed from the **Recording Policy**.

✓ *Enabling Screen Recording with macOS Catalina*

You can enable screen recording permissions for Mac Agents in macOS Catalina.

From the ObserveIT Web console, select **Enable Automatic Security and Privacy Update** in **Stealth and Privacy Policy** section of **Recording Policies**.

See: Enabling Screen Recording (Catalina)

✓ *Continue recording after locking and then unlocking the screen*

You can enable a recorded session that was locked and then unlocked, to continue being recorded.

Select **Continue recording after locking and then unlocking the screen**, from **Recording Policies**, in the **System Policy** section.

> This option is displayed only when **Enable recording** is disabled. To turn this option on, you must uncheck the **Enable recording** checkbox, and then check **Continue recording after locking and then unlocking the screen**.

QUALITY RESOLVED ISSUES AND ENHANCEMENTS

Release 7.9x includes improvements and enhancements to Agents, Alerts and Health Monitoring mechanisms.

Alerts Enhancements

- [Issue 63825]: In the **Create Alert Rule** area for **Did What** > **Logged In**, the actions: **Warning Notification**, **Blocking Message**, **Start Video Recording** and **Log Off** actions are now supported.
- [Issue 64308, 66799]: For the Alert Rule **Bypassing Security Control** > **Logging in with local user account**, description was updated to clarify how this Alert Rule should be used.
- [Issue 65717]: Users with the role **View-only Admin**, can now add comments to already triggered alerts.
- [Issue 66161]: Tuned the Alert weight that are used by the formula that calculates. the user's risk score in the Risk Dashboard. Previously, the mechanism was too sensitive to high-severity Alerts (High & Critical). The risk score was not reduced when an already triggered alert was set to non-issue status. For example, 3 Critical Alerts calculated to a score of 100. If there were more than 3 critical Alerts, and one of them was marked as Non-Issue, the score remained 100. That was adjusted, by tuning the weight (the effect on the score) of Alerts with severity of High (from 30 to 15) and Critical (from 90 to 30).

Alerts Resolved Issues

- [Issue 61486]: IP of endpoint is displayed correctly on triggered Alerts.
- [Issue 61586]: Printing to Cloud Printer is now captured. Print server credentials must be added in the Windows Credential Manager.
- [Issue 62031]: In some cases, after upgrade, Web Categorization stopped responding. The issue was resolved.
- [Issue 62699]: Alert on print screen issue resolved.
- [Issue 65480]: Dates and times set within rules are saved correctly.
- [Issue 66900]: Issues with synchronization and capturing key logger activity on PuTTy were resolved.
- [Issue 67698]: When assigning rules to Users Lists, by clicking the **Exiting Rules** button, the displayed pop-up no longer shows rules that are already assigned. Pop-up now shows only rules not yet assigned.
- [Issue 67844]: When expanding Alert Rules, the description is also displayed.

Agent Resolved Issues

- [Issue 60120]: Copying and Drag & Drop on Mac, no longer reported as a download event.
- [Issue 61542]: Users who are configured in the Recording Policy as "excluded", are no longer displayed in the Last Sessions area or the various Login features in the Web Console.
- [Issues 61975, 61993]: When the Activity of file downloads is followed by a quick tab switch in the Web Console browser, file downloads are detected more accurately.
- []Issue 62717]: When File Rename activity is performed fast, the event is detected and not overlooked.
- [Issue 64326]: When downloading files via Edge on Mac, the URL is detected accurately.

- [Issue 64771]: Multiple upload of the same file is now reported correctly - not only one time.
- [Issues 65000, 66901, 66975]: When uploading/downloading files, URL is taken correctly from the expected tab when multiple tabs are open.
- [Issue 65067]: Alert Rule with Close Application Action now successfully closes the browser when triggered.
- [Issue 65343]: When copying files to USB, File Copy activity is no longer reported twice in Diaries.
- [Issue 65562]: There are no longer empty lines in the Endpoint/User Diaries when a user clicks on a minimized Explorer application.
- [Issue 65683]: High memory consumption and large amount of window handles were resolved when connecting using Remote Desktop Protocol with multiple screens.
- [Issue 65767]: On Windows 32-bit, the problem of ever-growing log files has been resolved.
- [Issue 65832]: Paste activity is now successfully detected even after session timeout.
- [Issue 66882]: When connecting a USB to a mac endpoint, the application name is "Finder", not "Windows Explorer".
- [Issue 67219]: During Mac installation, installation password supports special characters such as !.
- [Issue 67898]: The correct URL is taken when uploading a file and navigating during upload (Firefox).
- [Issue 68187]: The activity of email sending is displayed immediately in the Web Console.
- [Issue 68609]: Email sending using email keyboard shortcuts on Mac, now detects keyboard shortcuts CMD + Enter, Shift + CMD + d
- [Issue 68900]: Download of image via Microsoft Edge browser is now accurately captured.
- [Issue 68952]: Download Activity is fully captured with all details, such as Application Name
- [Issue 69032]: BitLocker encrypted USB device is successfully recognized when plugged in.

Health Monitoring Resolved Issues

- [Issues 63127, 55098, 67777, 68636, 57894, 46286, 49106, 46073]: Accuracy of "Unreachable" status in **Configuration** > **Endpoints**, has been fixed.
  The threshold after which the Application Server makes the decision to change the status to "Unreachable" has been increased to 24 hours.

  Note that, if the user is offline during the 24-hour period, recording continues offline as usual.

- [Issue 56704]: The issue that occurred when an Agent that was installed on Windows 10 was not reported in some cases has been resolved.
- [Issue 66050]: False positive that occurred in the reporting of tampering has been resolved.
- [Issue 66659]: The issue of Heartbeat handling has been improved for large scale environments (above 10K endpoints).
- [Issues 68849, 53058]: Sending of a system event for Tampered offline files has been resolved.

Other Enhancements

- **Mac Agents - support for MTLS** (See Configuring ObserveIT to use mTLS (Mac))
- **Screenshot Storage Optimizer was enhanced to comply with higher security standards**.

  The updated Screenshot Storage Optimizer module that is part of 7.9 requires a token for authentication during interaction with the ObserveIT Application Server. This token can be downloaded from the **Service Settings** screen in the **Configuration** area from the ObserveIT Web Console.

  Notes:

  If this is the first time that Screenshots Storage Optimizer is used, make sure you've installed the **Advanced Web Console Setup**.

  ObserveIT version can be upgraded to version 7.9 without upgrading the Screenshot Storage Optimizer. In this case the old Screenshot Storage Optimizer will not be affected and will continue to operate.

  Installing Screenshot Storage Optimizer

Additional Resolved Issues 7.9.x

- ✓ [Issue 64326]: Improved URL detection on Mac machines
- ✓ [Issue 65039]: Improved Web Categorization of URL also based on subdomains.
- ✓ [Issue 65040]: Fix stability of DLMonitor.
- ✓ [Issue 65067]: Alert detection with Close Application actions on browser has been fixed.
- ✓ [Issue 65396]: Opening Alert screen in IE and searching for Rule Name in Filters area functions correctly.
- ✓ [Issue 65562]: Empty Windows title in Diary screen fixed.
- ✓ [Issue 67811]: When changing logger process name, system no longer creates tampering alert.
- ✓ [Issue 67991]: Issue in Firefox where some user activity was reported as upload incorrectly. This has been resolved.
- ✓ [Issue 68145]: Optimized database clean-up.
- ✓ [Issue 68673: Changes to keyboard settings will apply in the next session.
- ✓ [Issue 68683]: Improvements to Installer.
- ✓ [Issue 68817]: Freeze issue in SSMS on old Agents has been resolved.
- ✓ [issue 68920]: Improve Print Job detection when multiple users are connected to the same endpoint.
- ✓ [Issue 68901]: In the Email Diary view, the Endpoint filter is not populated accurately.
- ✓ [Issue 69844]: Improved storage when using Keylogger data.
- ✓ [Issue 70150]: Keylogger detection has been improved in multi-field forms in when the user switches between the fields using the keyboard (TAB).

Release 7.10.0

- Agent Updater: Version 7.10 requires deployment using third party tools.
- In some cases, when creating a new Upgrade Set, the default Target Version is set to 7.9 instead of 7.10. You can choose the correct version (7.10) manually by clicking the **Change** hyperlink next to the version number.
- DBA Activity: In SQL2017, **Execute** button not supported for DBA Activity in Web Console, Use F5 to execute query.
- In mTLS setup, if you want to replace the Client certificate, add the new certificate and remove the older certificate. This allows the connection to resume.