observe IT
a division of Proofpoint

ObserveIT Version 7.11.0 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 7.11.0.

For information about how to install and upgrade, see:

- Installation Guide
- ObserveIT Upgrade

New Features and Enhancements

MIP Integration

MIP integration integrates the Microsoft Information Protection (MIP) Unified Labeling solution into the ObserveIT platform providing more context about user activities. If a file has a MIP label, the Agent captures and extract the label and its attributes upon file exfiltration of tracked and non-tracked files and file entry of tracked files. MIP labels are visible in the User, Endpoint, Email and File diaries and you can create alerts by MIP labels. In addition, you can use the MIP labels when searching the ObserveIT database and include them when creating reports.

- See: MIP Integration

Activity Replay Offline Mode

Activity Replay protects employee's privacy and reduces storage requirements. When Activity Replay is turned on in the Recording Policy, only metadata is captured, and only when specific Alerts are triggered. The video recording before and after the time of alert is captured and sent from the endpoint to the server. This feature was introduced in version 7.8.0.

From version 7.11.0, Activity Replay is supported also in offline mode providing a broader solution for users working offline and is useful when working from home. In off-line mode, to prevent data from filling up your disk drive, new screenshots overwrite the old screenshots when the maximum limit for screenshot storage is reached. By default, Activity Replay storage has been increased to 300MB in addition to the offline data limit of 500MB.

- See: Activity Replay

Endpoint IP Visibility

Since users may work with their endpoint from different locations (usually laptops), a different IP may be assigned to the same endpoint based on the location. For example, the same endpoint may have one IP when working from within the office, and a different IP when working from home.

From version 7.11.0, the IP of the endpoint in each session is stored and displayed separately per session. The endpoint IP is displayed, in addition to the endpoint name in all the diaries screens, and in Alert, Search and Report screens.

In the diaries screens, when **Show IP** is selected, the Endpoint filter at the top allows you to view multiple entries for the same endpoint when more than 1 IP was assigned. In the Reports screen, a new field **Endpoint IP in Session** was added to Session report parameters.

Multiple Hotspots

To enhance screenshot storage efficiency and boost storage performance in large scale deployments, you can now have up to 4 hot storage locations for screenshot storage. From version 7.11.0, the Screenshot Storage screen (**Configuration** > **Storage Management** > **Storage**) has been enhanced to allow you to configure multiple hot storage space for screenshots.

- See: Configuring SSD-based Hot Storage

Security Enhancement

For increased security, .NET Framework 4.7.2 or higher must be installed. Earlier versions are no longer supported.

Support for macOS Big Sur 11

macOS Big Sur 11 is now supported. An updated MDM configuration profile file grants the required permissions.

- See: macOS Big Sur 11 Solution

Note:
When installing Windows Agents to a custom location:

- include a subfolder in the path, for example C:\custom path\Sub folder for Observeit agent \{agents files and folders}
- use the installation script and include the INSTALL parameter (see Installation Parameters)

Resolved Issues

- ✓ [SUP-19, SUP-166]: Loading time issue for Alert page with many alerts has been resolved.
- ✓ [SUP-21]: New threshold added for winserv trace file with control for maximum size on the Agent.
- ✓ [SUP-30, SUP-125]: In some cases, in the Email Diary, recipient information was missing for contacts that were already in the local address book. This has been resolved.
- ✓ [SUP-106]: Opening a PDF file in a browser is no longer reported as Upload.
- ✓ [SUP-114]: Improved tracking on Linux when opening a shell from a sudo command.
- ✓ [SUP-128]: Resolved tampering message when Agent offline data was sent in Activity Replay mode.
- ✓ [SUP-138]: When using Agent API, you are not able to activate Key Logger
- ✓ [SUP-148]: Fixed printer detection when regular user (not admin user) send to the printer.
- ✓ [SUP-150]: Resolved issue when user reached Dashboard page and no users displayed.
- ✓ [SUP-155]: After upgrading backend, some inactive alerts during duplication were reactivated. This has been resolved.
- ✓ [SUP-159]: Fixed partial screen for 4K monitor with 150% scale.
- ✓ [SUP-152]: Improved processing offline data.
- ✓ [SUP-154]: Issue of missing screenshots after changing sessions after a session timeout, has been resolved.
- ✓ [SUP-156]: Resolved multiple Updater issue.
- ✓ [SUP-163]: Device ID field is extracted consistently for both USB connect and copy to USB
- ✓ [SUP-164]: All Agent DLLS are now monitored for tampering.
- ✓ [SUP-168]: Resolved issue of non-interactive SSH taking too long to complete on Linux.

- ✓ [SUP-169]: ObserveIT TA has been updated to support Python to integrate with Splunk 8.0 and higher.
- ✓ [SUP-172]: Improved indexing of a few key tables to improve DB performance.
- ✓ [SUP-174, SUP-177]: In reports on Endpoints, in some cases, the value of the recording status showed as active. The issue was resolved.
- ✓ [SUP-176]: In some cases, timeline displayed empty in User and Endpoint diaries. This has been resolved.
- ✓ [SUP-178]: Improved screenshot storage during data movement from Hot to Warm.
- ✓ [SUP-193]: Archiving issue after upgrade has been resolved.

Limitations

Release 7.11.0

The Application Server cannot be installed on a servers with WebDAV enabled.

The Web Console cannot be installed on servers with WebDAV enabled.

MIP Limitations and Known Issues

- Alert rules configured using the **MIP Label of the file** option are currently not supported for user file activity on the Mac.

  In the File Diary, **File MIP Label** filter includes all the labels available in the database. This list is populated whenever there is file activity for file with a MIP label and on the tenants configured. This list can't be managed/cleaned.

- For tracked files: the Agent only reads MIP labels when there is file activity. If an MIP label is changed in the background, for example in MS Azure, and there is no file activity, the label may not be updated.

- If MS Office is not installed on the endpoint, the Agent may not be able to extract files.

- The Agent extracts sub-labels (for MIP) for AIP. The Agent extracts the lowest sub-level, so the child label, not the parent label is extracted.

- Label name and label display name: the Agent extracts the label name. This may differ from the display name (You can check the name in the Microsoft 365 Security Console – Sensitivity Labels)

- Label name changes: Agent sees Microsoft's label name and not the display name, in MIP as an admin you can change only the display, the label name remains the same.

- With Azure Information Protection (AIP): the Agent can extract labels and sub-labels, because of the metadata on file for files labels coming from AIP.

Deprecation

The following have been deprecated as they are no longer supported from version 7.11.0:

Internet Explorer is no longer supported for viewing the ObserveIT Web Console.