observeIT
a division of Proofpoint

ObserveIT Version 7.10.0 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 7.10.0.

Note: If the ObserveIT SaaS Feeder is currently installed in your environment, you must uninstall it before upgrading to ObserveIT version 7.10.
After the SaaS Feeder is uninstalled, you can install the new version of SaaS Feeder.
(The ObserveIT SaaS Feeder can be downloaded from ObserveIT Support Portal.)

Note: HTTP as communication protocol between the agent and the Application Server is no longer supported. Since Agents Auto Upgrade provides remote installation using highly secure credentials, it must be deployed using HTTPS or a higher security protocol.

For information about how to install and upgrade, see:

- Installation Guide
- ObserveIT Upgrade

New Features and Enhancements

Agent Auto Upgrade is GA

Agent Auto Upgrade is now GA for Windows. This feature 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.

From version 7.10, you will no longer need to use a 3rd party deployment tool. The upgrade is completed and deployed from the Web Console.

Note: When upgrading to 7.10, you will still need to deploy the agent with a 3rd party tool, such as Microsoft SCCM.

Note: If you have already deployed the Agent Updater from version 7.9.x, it is not supported with OIT server side 7.10.0. To use the feature and have the ability also

to update the Agent Updater remotely, you must update the Agent Updater to 7.10.0 with a 3rd party tool.

Updater Enhancements for 7.10 include:

- Updater Health Monitoring: The health status of the endpoint is displayed in the ObserveIT Web Console in the **Updater Status** column of the **Endpoint Upgrade Status** view. This view provides a quick way to find out the update status of an endpoint. In addition, you can easily check the update version by hovering over the **Updater Status** column.

  See: Endpoints Upgrade Status

- Auditing Capabilities: ObserveIT tracks **Upgrade Set** changes that were made while working in the Web Console, including Stop/Resume Upgrade Set, Delete Upgrade Set, and Create Upgrade Set. This information is available from the **Configuration Changes** tab in the **Audit** option of the Web Console.

  See: Auditing Configuration Changes

- Security Enhancements:

  - MSI validation checks the signature and certificate for the Agent and Updater
  - Secured API communication by using JSON Web Token (JWT)
  - mTLS authentication added

  See: Agent Auto Upgrade

Legal Hold

When you schedule archiving to move data from the main ObserveIT database automatically or deletion to remove data automatically, you can choose to exclude all sessions for specific users/endpoints. User activity data that you may not want to include in the scheduled archiving or deletion will remain available. The excluded data will continue to be available from the Web console diaries, alerts, search and reports.

See: Archiving ObserveIT Data and Deleting ObserveIT Session Data

Alert on Upload/Download by Website URL or Window Title

You can create alert rules for downloading and uploading (file exfiltration) by the website full URL and/or the website's Windows title.

This allows you to create rules that are much more specific and less noisy. For example, by looking for a window title that contains an email address string, you can create a rule that detects upload to personal Gmail but not to corporate Gmail.

See: Exfiltrated File - Did What

Alert on Taking a File from Box (Entry Point)

Box is a new entry point supported from version 7.9. In version 7.10, you can create an alert when files are taken out of a local Box folder.

The Brought in a File option lets you define an alert rule for the already supported following entry points (download from web, saving email attachment) and for this new one as well.

From the time a file is infiltrated from the Box cloud storage sync folder (entry point), all its activities are tracked (copy/move/rename/delete) until it is exfiltrated via one of the supported exit points (upload, send as email attachment, copy to USB, copy to local sync folder).

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

See: Brought in a File - Did What

Work from Home Optimization (WFH)

As many companies are implementing Work from Home (WFH) policies, new challenges are presented, such as:

- Higher networking from outside the organization into the organization
- Delays in seeing captured user activity in the Web console (because VPN is not always turned on from home)

ObserveIT has optimized Agent-server networking as follows:

- Redundant overhead on networking volume was removed
- Number of calls from Agent to server in idle time was reduced
- Flattening the curve of volume sent by the Agent upon recovery from offline

For more information about ObserveIT and WFH, see ObserveIT Remote Architecture.

Website Categorization Enhancement

The following categories have been added to Website Categorization and are available in Alert Rules and Recording Policies:

- CBD & Hemp Products
- Guns
- Ammunition
- Knives
- Paintball
- Self-Harm

- Abortion
- Child Abuse
- Tracking Sites
- Fitness
- Home & Garden
- DoH/DoT
- Infrastructure & Backend Services
- Newly Registered Domains
- Fireworks
- Cyberbullying

Note: If you are using the Website Categorization module, after installing or upgrading to version 7.10, contact ObserveIT Support to help you complete the update with the 16 new categories.

See: Website Categorization

USB Storage Device Additional Identifier

User activity related to usage of USB (connect to USB, copy to USB) has been enhanced by extracting the USB Device ID and adding it to the end of the USB Label field in parentheses.

Overwriting Old Activity in Offline Recording Policy

To prevent offline mode from filling up your disk drive, you can set a threshold for available disk space. When the threshold is reached, offline data starts to overwrite old activity.

See: Offline Recording Policy

Updated Configuration Screen in the Web Console

The Configuration screen in the Web Console has been updated. Now the left menu provides a more compact view and improving navigation. Previously, the left-menu was a flat list of about 30 screens. In the new hierarchical menus, all screens are grouped into sections by their topics (System Health, Endpoint Management, Alerts, etc). Each section can be expanded to view the associated screens or collapsed to hide them.

Security & Privacy Enhancements

You can turn on server certification validation to force Windows Agents to validate the server certificate.

See: Securing Server Certificate Validation

In a mTLS Mac environment, you can set passwords for up to 4 different certificates.

Note: For Mac Agents in an mTLS environment, the server certificate must comply with Apple Application transport Security (ATS) requirements.

See: Securing Mac Agent Certificate for mTLS

Resolved Issues

- ✓ [Issue 1233]: Removed notification that Linux trace file was too large.
- ✓ [Issue 1128]: Resolved Agent obfuscation issue by automating screen recording (Catalina).
- ✓ [Issue 1102]: Live playback issue on IE11 has been fixed.
- ✓ [Issue 1099]: Export of CSV from configuration endpoint has been fixed to support Chinese characters.
- ✓ [Issue 1082]: Time of an alert exported to CEF log file is set to the local time zone.
- ✓ [Issue 68377]: Cases of missed emails in Email Diary was resolved.
- ✓ [Issue 802]: Leftovers from Mac uninstall removed.
- ✓ [Issue 697]: Fixed false positive FAM events when files selected for uploading.

Limitations

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.

Deprecation

The following have been deprecated as they are no longer supported from version 7.10.0:

- ✓ Windows 2008 supported for ObserveIT Agent 7.9.1 on best effort
- ✓ Windows 7.8 supported for ObserveIT Agent 7.9.1 on best effort
- ✓ macOS Sierra 10.12 supported for ObserveIT Agent 7.9.1 on best effort
- ✓ Oracle Linux 5
- ✓ Ubuntu 12.04
- ✓ RHEL/CentOS 5.10-5.11