

# Proofpoint | ObserveIT On-Premises Release Notes version 7.12.0

## Version 7.12.0

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

For information about how to install and upgrade, see:

- [Installation Guide](#)
- [ObserveIT Upgrade](#)

For the online documentation, click [here](#).

This version includes security fixes.

## New Features and Enhancements

### *New Console Users Roles*

Console User roles have been added. These roles are in addition to the already existing roles.

- **Alerts Analyst:** This role can access **Alert & Prevent Rules** and **Lists** and view session recordings, but cannot gain access to any other ObserveIT configuration options.
- **Settings Admin:** This role can see all users and their permissions, but can create or delete only "Settings Admin" users. Settings users are unable to view session recordings, **Alert & Prevent Rules** and **Lists**.

See: [Creating and Managing Local Console Users](#)

### *MIP Labels*

The Agent also detects MIP label changes on tracked files. This provides additional visibility when monitoring suspicious activity on sensitive files. Using label change detection when a file is exfiltrated lets you fine tune alerts, reduce noise and gives you a more comprehensive view of file activity. Label changes display in the File Diary and File History, User and Endpoint Diary and in the Session Player views.

See: [MIP Integration](#)

## *Linux Desktop UI Monitoring is now GA*

Linux Desktop UI Monitoring provides a graphical view for Linux systems that support a graphical environment. The Linux Desktop Agent captures screenshots and metadata for application usage and Web browsing.

See: [Linux Desktop UI Monitoring Overview](#)

## *USB Device ID*

USB Device ID is now stored and displayed as a separate field. Previously, it was included in the USB Label field.

USB Device ID displays in Endpoint and User Diary views, in the USB History tab and in the Session Player. The reporting field **Device ID** is available for USBConnect and File Activity type reports. You can also search by a USB Device ID.

USB Device IDs can be used when defining alerts for files exfiltrated to a USB device (**Exfiltrated File > To USB device > USB whose Device ID**) and detecting connected USBs (**Detect connected USB > USB ID**)

## *Audit Screen Enhancement*

In the **Operator** column of **Audit Sessions** list, (**Configuration > Security & Privacy > Audit > Sessions**), the text "this screen" displays next to an operator who opened a video session player from the Audit Sessions screen.

In addition, you can filter the view to show:

- Any screen (the default): Shows video sessions played from the Audit Session screen and any other screen
- This screen: Shows only video sessions played from the Audit Sessions screen
- Other screens: Shows only video session played from any screen other than the Audit Sessions screen

See: [Auditing Session Replays](#)

## *Extract Email for AD Group*

For console users who are part of an AD group that is defined in the Console User Group, the email that is saved with the AD group can be extracted and downloaded. This enables emails to be sent to all users in an AD Group when a recorded session is saved.

## *Custom Group View Enhancement*

You can see which endpoints belong to which groups when you add endpoints to a group (**Configuration > Endpoint Management > Endpoint Groups**).

In addition, the **Check All** selection option, now lets you choose to show all pages or just the current page.

The screenshot shows the 'Add Endpoints to Group' interface. At the top, there is a 'My Endpoint Group' section with a 'Filter by Endpoint Group' dropdown set to 'All' and a 'Search by name' input field. Below this is a table with the following data:

Endpoint Name	Latest IP	Version	Monitor Status	Custom Endpoint Groups
<input type="checkbox"/> DEMO-SE-SERVER	104.130.219.150	7.11.1.69	Active	-
<input type="checkbox"/> WINDOWS8	N/A	7.0.0.2	Active	-
<input type="checkbox"/> DESKTOP-EVMI1NU	192.168.202.128	7.6.1.35	Active	Group A
<input type="checkbox"/> TERMINAL1	192.168.2.36	Uninstalled	Active	Group A
<input type="checkbox"/> SALES-RDP-ONLY	N/A	7.4.1.27	Active	-
<input type="checkbox"/> a-3bo2cvsf1b7w5	N/A	Uninstalled	Active	Group A, Group B, Group C
<input type="checkbox"/> ubuntu1804	172.16.220.173	Uninstalled	Disabled	-
<input type="checkbox"/> Q8-W08SQ08-2	10.2.56.76	Uninstalled	Disabled	-
<input type="checkbox"/> OIT-DEMO-12	192.168.253.247	Uninstalled	Disabled	Group A, Group C

Below the table, there is a 'Select All - Clear All' link and a 'Total selected endpoints: 0' indicator. At the bottom right, there are 'Close' and 'Add Selected Endpoints' buttons.

See: [Modifying Members in Endpoint Groups](#)

### *Windows and Mac Agent Installation Modification*

Before installing Windows or Mac Agents, from **Configuration > Settings > Service Settings**, download configuration files containing authentication details.

See: [Configuring Service Settings](#)

### *System Event for mTLS Server-Side Validation*

A system event is sent when the server-side does not enforce mTLS indicating that you need to configure the server-side for mTLS.

See: [Enforcing mTLS by the Server](#)

### *Archiving/Deleting Process Status Enhancement*

Archiving/Deleting process now handles Alerts and Agent updates with statuses.

## Supported Platforms

Release 7.12.0 supports Agents from release 7.8.0 and above.

7.12.0 is the *last* version to support:

- SQL Server 2012/2014 Enterprise
- Win 32 bit Agents
- Win 8.x 64 bit
- Win Server 2012 (not R2)
- Debian 9.1 and lower

## Resolved Issues

- ✓ [Issue 420]: Fixed application error when setting up MTLS password on Web Console.
- ✓ [Issue 394]: Printing sessions from the Endpoint and User Diary pages fixed to respect the time filter.
- ✓ [Issue 376]: Fixed high CPU issue when killing non-interactive session on Linux.
- ✓ [Issue 360]: Issue with installing Agent on an endpoint that was renamed has been resolved.
- ✓ [Issue 359]: Performance issue when querying file activity when using API reports has been resolved.
- ✓ [Issue 357]: High latency when deleting metadata as part of archiving with legal hold has been resolved.
- ✓ [Issue 353]: Default time period in various Web Console screens has been changed to "last 3 days".
- ✓ [Issue 248, 349]: In the Video Player, the issue of the Alert overlay that did not fully collapse has been resolved.
- ✓ [Issues 340, 338]: The issue of missing screenshots that arrive after the session was signed has been resolved.
- ✓ [Issue 336]: Fixed memory issue for RDCL process on RDS Citrix machine.
- ✓ [Issue 329]: Fix display issue with Database path field has been fixed.
- ✓ [Issue 327]: High CPU usage for Linux endpoints when registration fails, has been fixed.
- ✓ [Issue 323]: Issue of documenting file attaching to email and switching quickly to browser associated as an email not as an upload. (Mac Agent)
- ✓ [Issue 321]: Issue with installing the Agent based on Master Image on Turkish-based OS was fixed.
- ✓ [Issue 303]: Fixed detecting monitoring of Web browsing during offline Activity Replay.
- ✓ [Issue 265]: The Admin Dashboard screen was fixed to show earlier version fields correctly.
- ✓ [Issue 264]: Non-USB hard drives are no longer recognized as USB devices.

- ✓ [Issue 198]: Fixed login issue on Linux when all Application servers are in down.
- ✓ [Issue 194]: The issue that triggered Alert based on keylogger XQurartz terminal on Mac was fixed.
- ✓ [Issue 161]: Archiving and deleting process is now handled
- ✓ [Issue 182]: The detection of the correct URL when uploading files and switching to other tabs was significantly improved.
- ✓ [Issue 446]: Resolved issue of possible MacOS pop-up for screens recording permissions for metadata.
- ✓ [Issue 439]: Removed duplicate file copies.
- ✓ [Issue 438]: Issue resolved when Activity Replay to stop recording as configured.
- ✓ [Issue 426]: Performance issue was resolved when processing email activity.
- ✓ [Issue 420]: Issue was resolved in Security & Privacy screen when setting mTLS password.
- ✓ [Issue 417]: Issue of error messages during installation of Linux Agent to non-default location was resolved.
- ✓ [Issue 411, 399]: Partial documentation of massive file copy was fixed, recovering all files.
- ✓ [Issue 380]: A performance issue on archiving process was fixed.
- ✓ [Issue 320, 319]: Test files created by the system are no longer left on screenshot storage devices.

## Limitations and Known Issues

### Release 7.12.0

- For files with any of the following extensions: RTF, TXT, PNG, BMP, JPG, JPEG, XML, ZIP, upon adding or removing a label that has protection in a way that the file is renamed (for example, from .txt to .ptxt), the indication for Label Change in some cases is not displayed in the **File History** tab.
- If you perform a backup and restore of the SQL database, Upgrades registered by the Updater before the restore, will not re-register and any Upgrade Sets will not be assigned to the Upgrade Updaters.

You will need to force the Updater to re-register the Upgrades server.

For each endpoint, delete `oitsettings.json` file located in <updater installed location>\Updater Utility\config

For example (default location):

C:\Program Files\Windows Client Utility\Updater Utility\config