WHAT’S NEW IN OBSERVEIT 7.4

Insider Threat Management is a growing concern as organizations are becoming increasingly aware of the potential risks imposed by their trusted employees and external workers. To mitigate the risk posed by insiders, companies are looking to deploy and expand ObserveIT within their organization by monitoring a broader user population who are accessing servers and desktops, and to protect data from being exfiltrated or misused in various ways.

ObserveIT 7.4 focuses primarily on improving the scalability and performance of the product to better support large number of agents and concurrent users with lower infrastructure costs and faster Management Console.

ObserveIT 7.4 integrates seamlessly into your security and IT environments now supporting the automatic update of Lists via API (e.g., sensitive machine IPs, files that need tracking), the mass deployment of Mac agents using JAMF, the obfuscation of the Windows Agent component to hide it from advanced users, and the introduction of a new ObserveIT QRadar App.

ObserveIT 7.4 helps Security Analysts and Investigators to better detect and manage Data Exfiltration by the improvement of the Diaries and Search screens to provide summary information on downloaded and exfiltrated files – directly from a Session Summary view.

OBSERVEIT 7.4 KEY NEW FEATURES

Scale better in large deployments on a single environment – support deployment size growth

- ✓ Significantly increase metadata ingestion capacity in a single database environment (lower TOC)
- ✓ Faster Management Console that better handles large set of users (Search, Diaries, etc.)
- ✓ Configure keyboard frequency to take screenshots only every few seconds
- ✓ Enable the Windows Agent API to work in a multi-site ObserveIT deployment

Obfuscation of the Windows Agent – better hide the agent from advanced users

- ✓ Hide agent DLLs, EXE files processes and services
- ✓ Hide or rename log files, event viewer logs, registry entries, etc.
- ✓ Do not show error messages on the monitored user screen while running in Stealth mode

Data Exfiltration – provide a quick summary in the Diaries and Search

- ✓ Show a summary of risky file activities (e.g., web downloads, moving files to the cloud) as part of the session summary in the User Diary, Endpoint Diary, and Search
- ✓ Provide the application/website context in session summaries
- ✓ Enhance the Alert Rule Editor for file activity alerts
- ✓ Introduce a new and modern UI design for the Diaries and Search

Integration and Enterprise Readiness – address IT and security needs raised by customers

- ✓ APIs for List management to cover a broad spectrum of use cases
- ✓ Deliver updated native IBM QRadar App (Alerts, metadata, not including File Diary metadata)
- ✓ Support IP range (CIDR) definition for alert rules to support large server deployments

Privacy – help protect employee privacy

- ✓ Protect user privacy when switching to full-recording upon an alert, by reverting to metadata-only recording after a predefined time
- ✓ Allow more granular web categories for creating accurate web browsing alerts

Mac Agent

- ✓ Support Mac agent mass deployment using the JAMF management tool
- ✓ New metadata for copy/move of any file or folder
- ✓ Support MacOS High Sierra (10.13)

SCALE BETTER IN LARGE DEPLOYMENTS ON A SINGLE ENVIRONMENT

ObserveIT deployments keep growing as customers protect larger areas of their organization from Insider Threat and specifically Data Exfiltration.

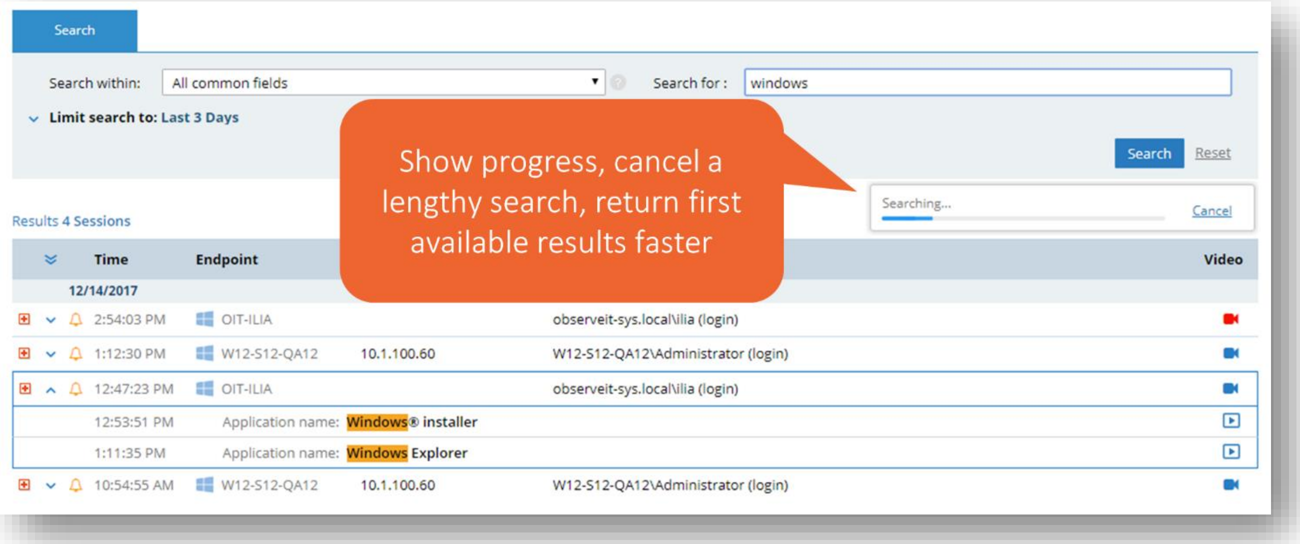
Compared to the earlier 7.1 release, ObserveIT 7.4 provides key improvements relating to metadata ingestion and responsiveness of the Management Console; even customers recording full video (not only metadata) will experience reduced load on the backend and faster responsiveness of the Management Console:

- Deployments with 5,000+ monitored users running on high-end machines (e.g., 32 cores SSD) can now handle 3-4 times more metadata ingestions on the same hardware.
- Lower scale deployments running on low-end servers can now handle twice the capacity compared to the 7.1 release.
- Management Console response time is significantly improved. The improvement is more noticeable in deployments with a large volume of recording data in a live database than in small deployments.
- Example: In some scenarios, with 3 months of data recorded for 12K monitored users, working with the User or Endpoint Diaries works even 10 times faster.

  These improvements allow you to expand your existing ObserveIT implementation by adding more agents using the same infrastructure. If you are setting up a new ObserveIT site, your infrastructure costs can be significantly lower; as mentioned, the larger the deployment size – the more significant the change.

For a specific sizing assessment, please approach the Support and Customer Success teams.

User and Endpoint Diaries are optimized to work faster, and the Search page has been redesigned to return the first matching results as soon as they occur, without forcing the user to wait for the full query to end. The search query can be cancelled by the user at any time.



Search within: All common fields

Search for : windows

Limit search to: Last 3 Days

Show progress, cancel a lengthy search, return first available results faster

Searching...

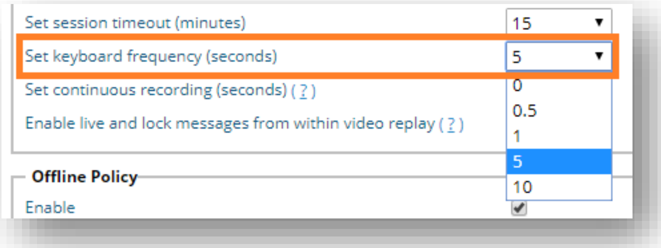
Results 4 Sessions

Time	Endpoint			Video
12/14/2017				
2:54:03 PM	OIT-ILIA		observeit-sys.local\ilia (login)	
1:12:30 PM	W12-S12-QA12	10.1.100.60	W12-S12-QA12\Administrator (login)	
12:47:23 PM	OIT-ILIA		observeit-sys.local\ilia (login)	
12:53:51 PM	Application name: Windows® installer			
1:11:35 PM	Application name: Windows Explorer			
10:54:55 AM	W12-S12-QA12	10.1.100.60	W12-S12-QA12\Administrator (login)	

Search Working for Any Scale

ADDITIONAL LARGE-SCALE ENHANCEMENTS

- **Reduce the frequency of screenshot captures to less than once per second** – by configuring the keyboard frequency to record every few seconds customers can reduce the volume of data sent by the agents – hence balancing recording quality and system load.



Set session timeout (minutes) 15

Set keyboard frequency (seconds) 5

Set continuous recording (seconds) (?)

Enable live and lock messages from within video replay (?)

0
0.5
1
5
10

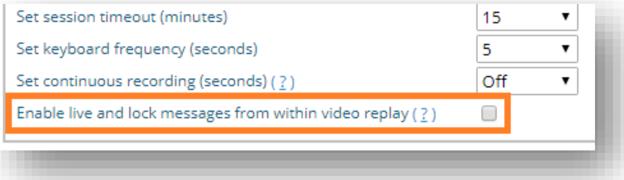
Offline Policy

Enable ☑

- **Enable the Windows Agent API to work in a multi-site ObserveIT deployment** – when using Agent API to start/stop recording in a multi-site ObserveIT environment, the API now returns the location (URL) of the site in which the agent's sessions will be stored so it can also be retrieved later via API.

  In addition, the recording policy now fully applies to sessions that are started via Windows Agent API, including specific users to record, applications to exclude from recording, and so on.

- **Enable Live and Lock messages via Recording Policy** – ObserveIT has the capability to send live messages to recorded users directly from the Video Player. In order to reduce the load on the backend when this feature is not in use, this capability can now be disabled via a recording policy.



Set session timeout (minutes) 15

Set keyboard frequency (seconds) 5

Set continuous recording (seconds) (?) Off

Enable live and lock messages from within video replay (?) □

OBFUSCATION OF THE WINDOWS AGENT

Monitoring highly technical users in full stealth mode can be challenging as IT administrators or developers could use creative ways to uncover the installation of the ObserveIT agent on the endpoint. ObserveIT 7.4 introduces obfuscation capabilities that hide the agent binaries and configuration files, making it much more difficult for highly technical users to find.

Obfuscation of the Windows Agent includes:

- Removing the term "ObserveIT" from agent binary files so they cannot be found easily
- Renaming installation files, processes and service names so they cannot be identified by searching on the internet – e.g. using Google Search.
- Hiding or renaming log, trace, and configuration files
- Removing the term "ObserveIT" from the content of configuration and dynamically created files
- Removing the term "ObserveIT" from registry key entries and Windows Event Viewer's logs
- Avoiding the showing of error messages on the monitored user's screen while running in stealth mode

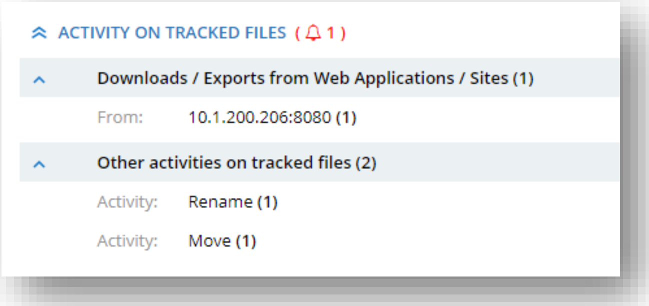
Obfuscation capabilities are available for both stealth and non-stealth agent versions. Please contact ObserveIT Support to obtain the obfuscated agent version (a.k.a. "No Label").

DATA EXFILTRATION – ENHANCED DIARY VIEWS AND ALERTS

The **Session Summary** in the User Diary, Endpoint Diary, and Search screens is a highly used feature as it provides customers with an instantaneous summary view of what happens throughout the session, without having to watch the whole Video playback or run reports.

ObserveIT 7.4 significantly enhances the Session Summary by providing:

- Visibility on files that were downloaded from the Web during the session, including a breakdown by website which enables you to quickly understand how many files where downloaded from each website.
- Visibility to tracked files that were exfiltrated to Cloud Sync & Share local folders (e.g., Dropbox, Box) during the session. Breakdown by cloud vendors shows how many files were copied to each cloud vendor.
- Visibility to other activity performed on tracked files, such as copy, move, rename or delete, allowing you to easily spot user attempts to move data around or to hide tracks by renaming or deleting files.



ACTIVITY ON TRACKED FILES (🔔 1)

Downloads / Exports from Web Applications / Sites (1)

From: 10.1.200.206:8080 (1)

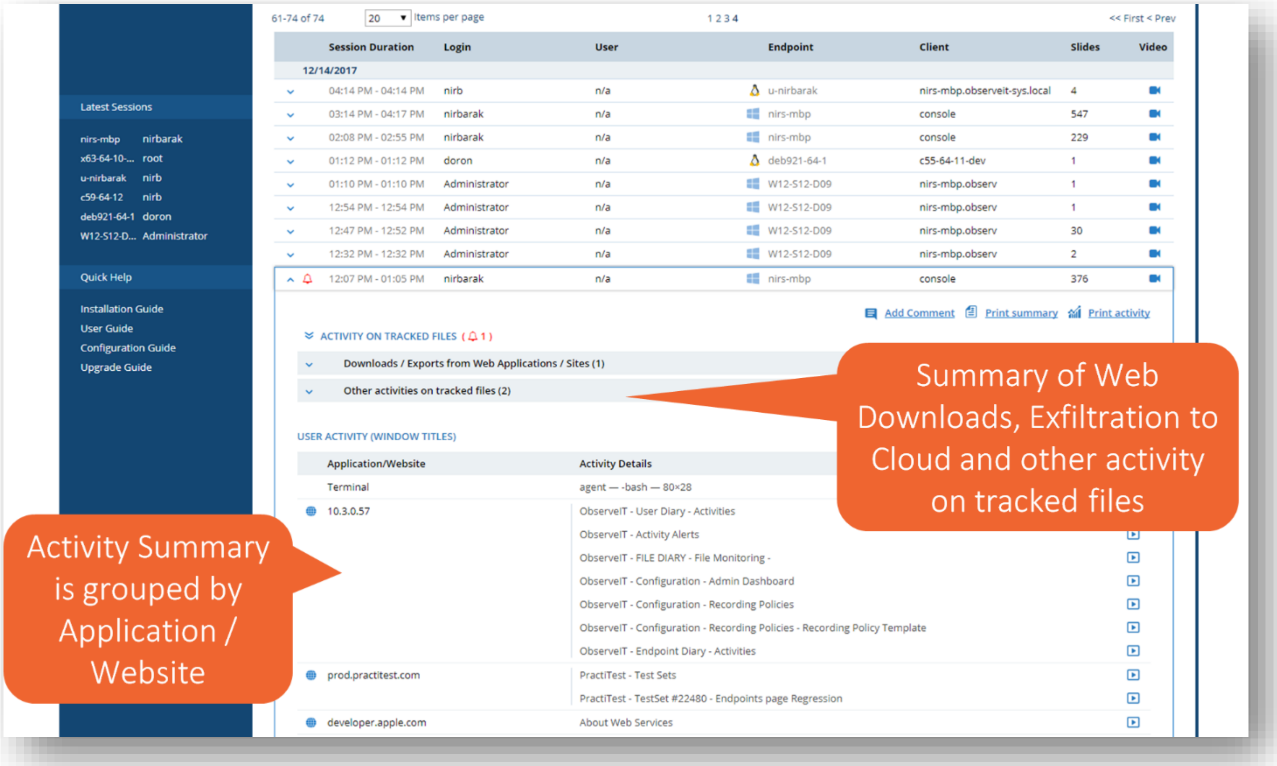
Other activities on tracked files (2)

Activity: Rename (1)

Activity: Move (1)

The above FAM summaries are linked to the File Diary, Video Player, and Alerts, allowing you to fully understand the user activity around the file action, view a complete history of the tracked file, and quickly investigate any alerts associated with file activity.

The summary of user activity is now grouped by the application or website in which the activity occurred. This provides a much better context for understanding user activity during the session especially when interacting with websites and web applications (in earlier versions, the site URL was not displayed).



Session Duration	Login	User	Endpoint	Client	Slides	Video
12/14/2017						
04:14 PM - 04:14 PM	nirb	n/a	u-nirbarak	nirs-mbp.observeit-sys.local	4	
03:14 PM - 04:17 PM	nirbarak	n/a	nirs-mbp	console	547	
02:08 PM - 02:55 PM	nirbarak	n/a	nirs-mbp	console	229	
01:12 PM - 01:12 PM	doron	n/a	deb921-64-1	c55-64-11-dev	1	
01:10 PM - 01:10 PM	Administrator	n/a	W12-S12-D09	nirs-mbp.observ	1	
12:54 PM - 12:54 PM	Administrator	n/a	W12-S12-D09	nirs-mbp.observ	1	
12:47 PM - 12:52 PM	Administrator	n/a	W12-S12-D09	nirs-mbp.observ	30	
12:32 PM - 12:32 PM	Administrator	n/a	W12-S12-D09	nirs-mbp.observ	2	
12:07 PM - 01:05 PM	nirbarak	n/a	nirs-mbp	console	376	

ACTIVITY ON TRACKED FILES (1)

Downloads / Exports from Web Applications / Sites (1)

Other activities on tracked files (2)

USER ACTIVITY (WINDOW TITLES)

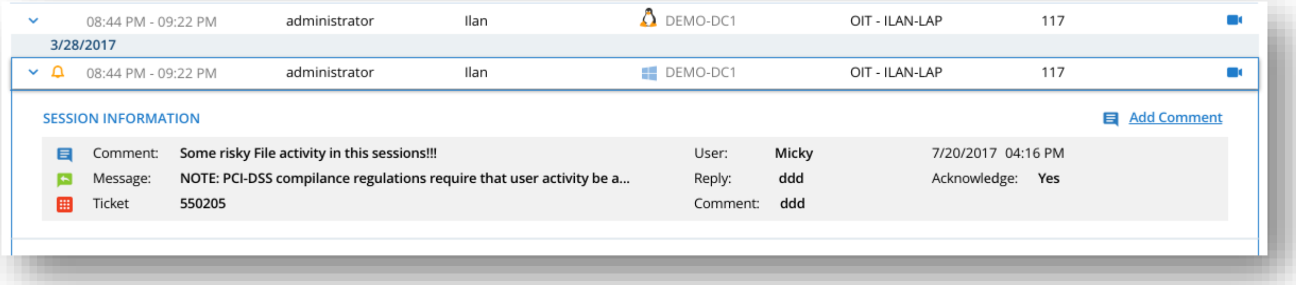
Application/Website	Activity Details
Terminal	agent — -bash — 80×28
10.3.0.57	ObserveIT - User Diary - Activities
	ObserveIT - Activity Alerts
	ObserveIT - FILE DIARY - File Monitoring -
	ObserveIT - Configuration - Admin Dashboard
	ObserveIT - Configuration - Recording Policies
	ObserveIT - Configuration - Recording Policies - Recording Policy Template
	ObserveIT - Endpoint Diary - Activities
prod.practitest.com	PractiTest - Test Sets
	PractiTest - TestSet #22480 - Endpoints page Regression
developer.apple.com	About Web Services

Summary of Web Downloads, Exfiltration to Cloud and other activity on tracked files

Activity Summary is grouped by Application / Website

New Sessions Summary in Diaries and Search screens

A fresh UI provides a modern user experience, also allowing users to easily spot session-level comments, tickets, and messages, which are now more visible on-screen.



08:44 PM - 09:22 PM	administrator	Ilan	DEMO-DC1	OIT - ILAN-LAP	117	

3/28/2017

08:44 PM - 09:22 PM	administrator	Ilan	DEMO-DC1	OIT - ILAN-LAP	117	

SESSION INFORMATION

Add Comment

Comment:	Some risky File activity in this sessions!!!	User:	Micky	7/20/2017 04:16 PM	
Message:	NOTE: PCI-DSS compilance regulations require that user activity be a...	Reply:	ddd	Acknowledge:	Yes
Ticket	550205	Comment:	ddd		

INTEGRATION & ENTERPRISE READINESS

ObserveIT 7.4 introduces several enhancements requested by customers allowing them to use ObserveIT more effectively and seamlessly integrate with other IT and Security systems.

API'S FOR LIST MANAGEMENT

Lists are used in alerts for a broad spectrum of use cases. Often, the content of a list is provided by another system in the organization. This could include a watch-list of users from HR that need to be monitored closer, a list of source files to track, sensitive server IP addresses to which restricted access is required, keywords on which to alert, and so on.

ObserveIT 7.4 allows customers to automate list management by providing API's to query the lists and their content, and update list contents (add, replace, and remove list items).

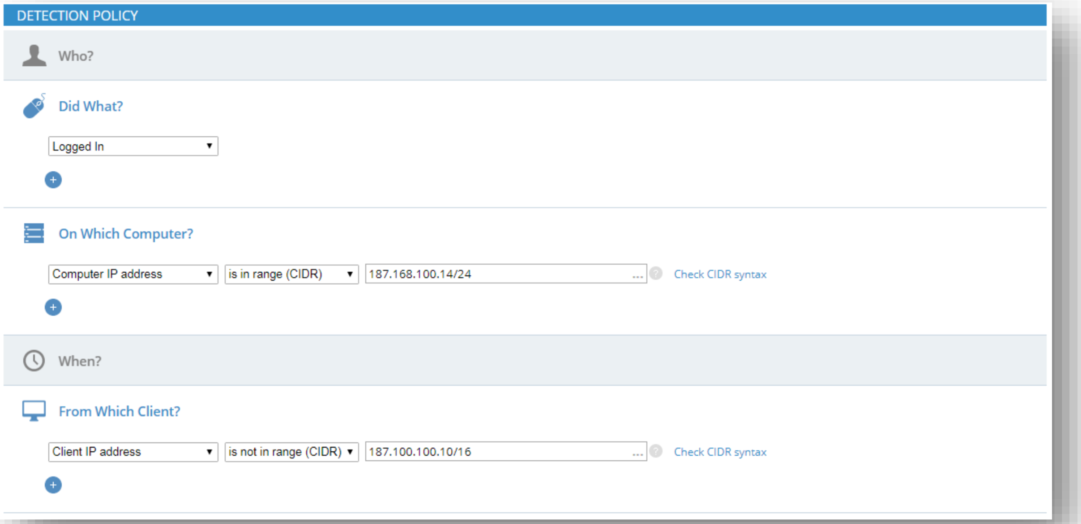
For technical documentation of the ObserveIT API, please refer to:
https://docs.preview.observeit.net/apis/index.html?url=apis/control-7.4.yaml

SUPPORT IP RANGE (CIDR) DEFINITION IN ALERT RULES

Some IT environments manage their computers by IP addresses instead of machine names, thus requiring security policies to be built around a range of IPs.

For example: Only members of the "ITSec" AD group can access the range of machine IPs defined as 187.168.100.14/24 (CIDR).

ObserveIT 7.4 allows you to define alert rules utilizing the CIDR format for both endpoint and client computers, as well as managing IP ranges via lists.



DETECTION POLICY

Who?

Did What?

Logged In

On Which Computer?

Computer IP address | is in range (CIDR) | 187.168.100.14/24 | Check CIDR syntax

When?

From Which Client?

Client IP address | is not in range (CIDR) | 187.100.100.10/16 | Check CIDR syntax

Alert Rule Based on IP Ranges (CIDR)

SIEM – NATIVE IBM QRADAR APP

A new ObserveIT QRadar App is available in the IBM Security App Exchange, enabling a faster and simpler integration of ObserveIT and QRadar.

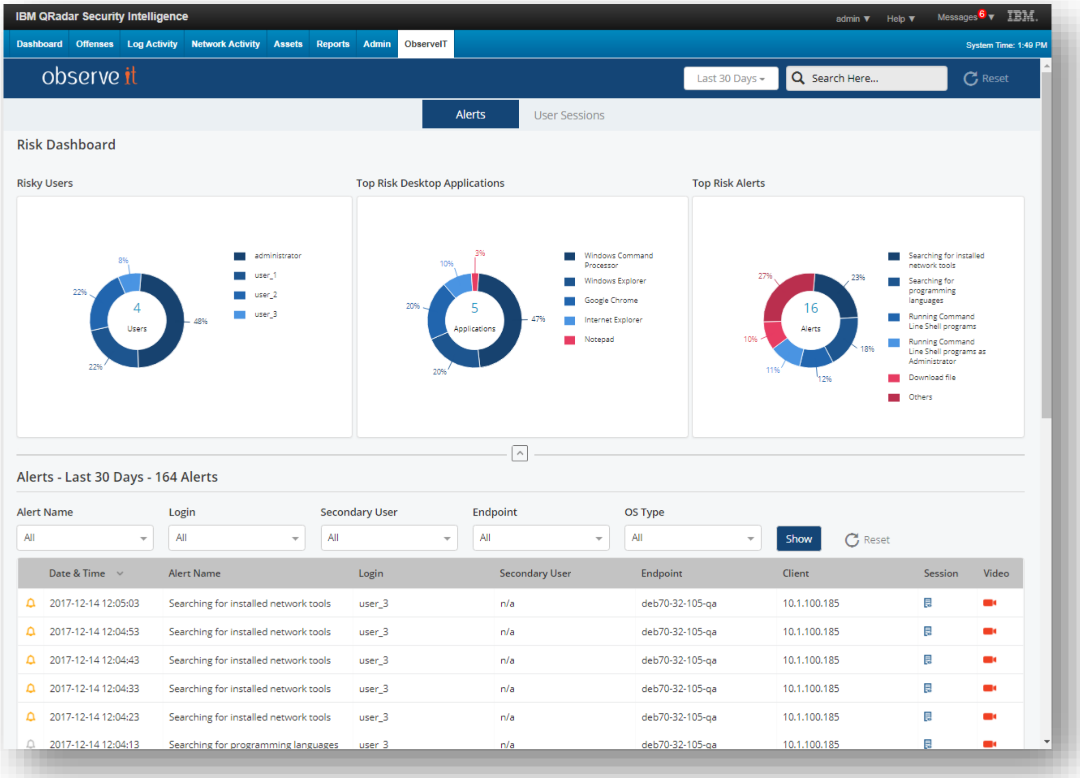
Click here to access and download the new app.

The ObserveIT QRadar App is supported on ObserveIT 7.1 or higher, and IBM QRadar 7.2.8 or higher.

When using the App, ObserveIT metadata is pulled into QRadar making it available for further correlation and analysis. The ObserveIT QRadar App has two main views:

Alerts

- Show a summary of top alerts by user, application, and alert type
- Filter the list of alerts by login, user, endpoint, date range, and so on.
- Drill down to see details of each alert
- Link to view the video playback and the session summary in ObserveIT



Alerts - Last 30 Days - 164 Alerts

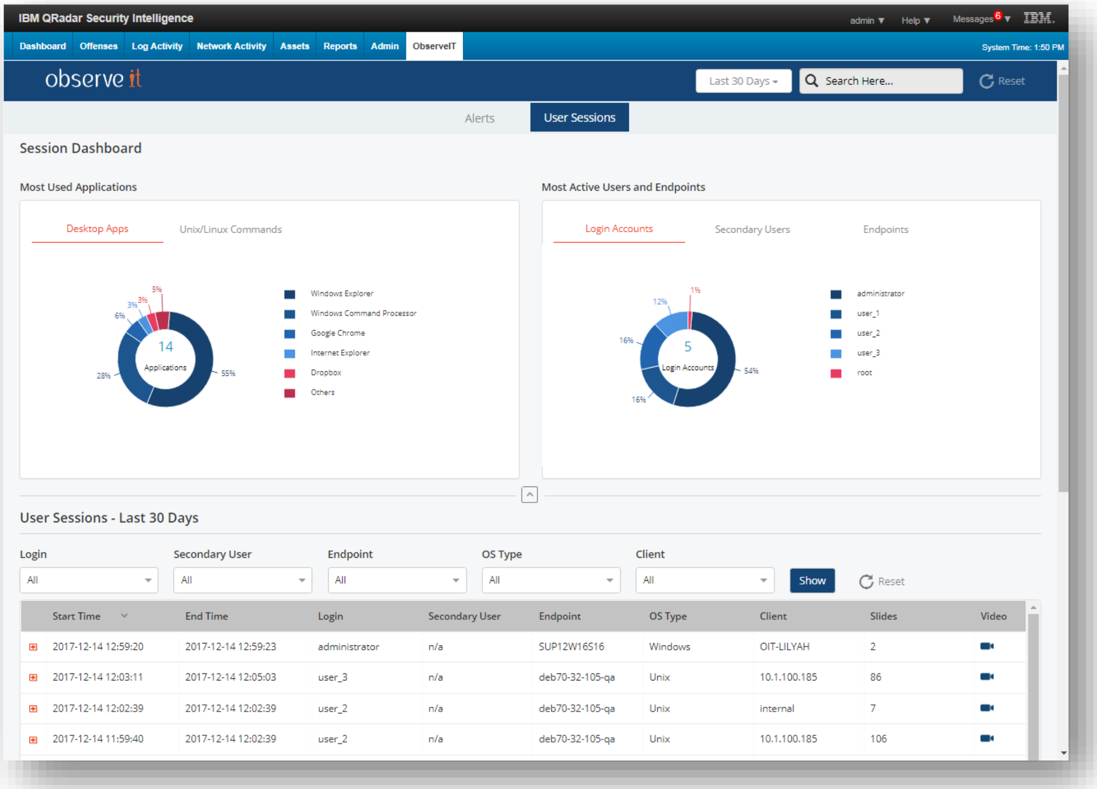
Alert Name: All ▾
Login: All ▾
Secondary User: All ▾
Endpoint: All ▾
OS Type: All ▾
Show
Reset

	Date & Time	Alert Name	Login	Secondary User	Endpoint	Client	Session	Video
🔔	2017-12-14 12:05:03	Searching for installed network tools	user_3	n/a	deb70-32-105-qa	10.1.100.185	🗎	🎥
🔔	2017-12-14 12:04:53	Searching for installed network tools	user_3	n/a	deb70-32-105-qa	10.1.100.185	🗎	🎥
🔔	2017-12-14 12:04:43	Searching for installed network tools	user_3	n/a	deb70-32-105-qa	10.1.100.185	🗎	🎥
🔔	2017-12-14 12:04:33	Searching for installed network tools	user_3	n/a	deb70-32-105-qa	10.1.100.185	🗎	🎥
🔔	2017-12-14 12:04:23	Searching for installed network tools	user_3	n/a	deb70-32-105-qa	10.1.100.185	🗎	🎥
🔔	2017-12-14 12:04:13	Searching for programming languages	user_3	n/a	deb70-32-105-qa	10.1.100.185	🗎	🎥

ObserveIT QRadar App – Alerts Dashboard

User Sessions

- Show a summary of most used applications and Unix/Linux commands
- Show a summary of most active users and endpoints
- Show the list of sessions and filter it by user, endpoint, client computer, and more
- Expand each session to see the session summary. User activity is grouped by applications and websites
- Link to view the full video playback



User Sessions - Last 30 Days

Login: All
Secondary User: All
Endpoint: All
OS Type: All
Client: All

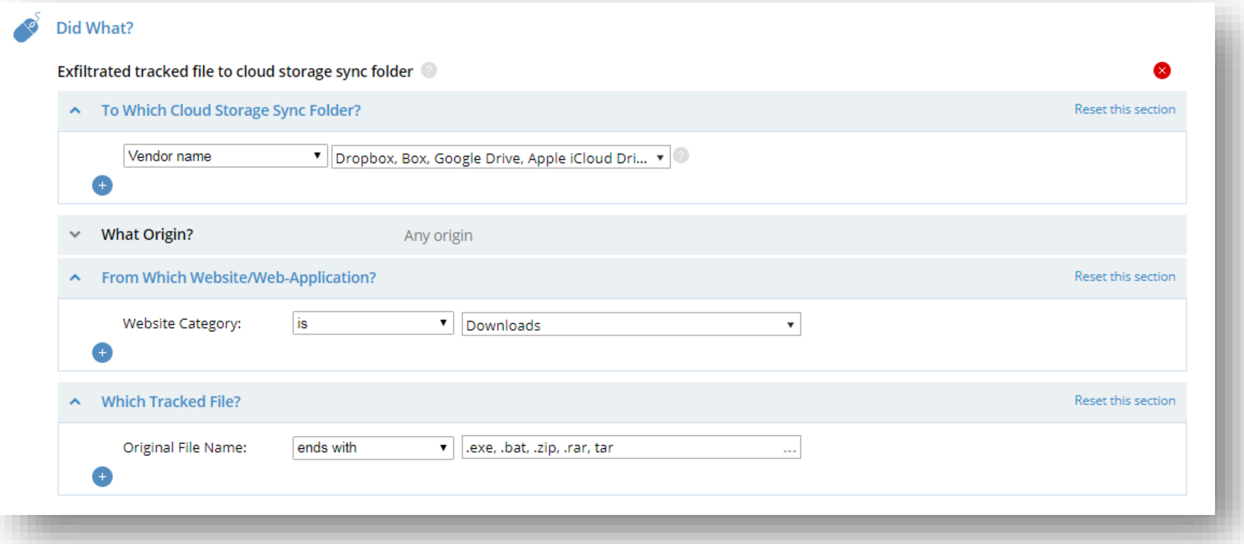
	Start Time	End Time	Login	Secondary User	Endpoint	OS Type	Client	Slides	Video
⊞	2017-12-14 12:59:20	2017-12-14 12:59:23	administrator	n/a	SUP12W16S16	Windows	OIT-LILYAH	2	■
⊞	2017-12-14 12:03:11	2017-12-14 12:05:03	user_3	n/a	deb70-32-105-qa	Unix	10.1.100.185	86	■
⊞	2017-12-14 12:02:39	2017-12-14 12:02:39	user_2	n/a	deb70-32-105-qa	Unix	internal	7	■
⊞	2017-12-14 11:59:40	2017-12-14 12:02:39	user_2	n/a	deb70-32-105-qa	Unix	10.1.100.185	106	■

ObserveIT QRadar App – User Sessions Dashboard

ENHANCED FAM ALERT RULES

ObserveIT 7.4 enhances the way alert rules are defined on file activity metadata (FAM).

Rules are defined in a hierarchical and dynamic UI providing security admins with an intuitive, flexible, and consistent way to define FAM alerts.



Did What?

Exfiltrated tracked file to cloud storage sync folder

To Which Cloud Storage Sync Folder? — Reset this section

Vendor name: Dropbox, Box, Google Drive, Apple iCloud Dri...

What Origin? — Any origin

From Which Website/Web-Application? — Reset this section

Website Category: is — Downloads

Which Tracked File? — Reset this section

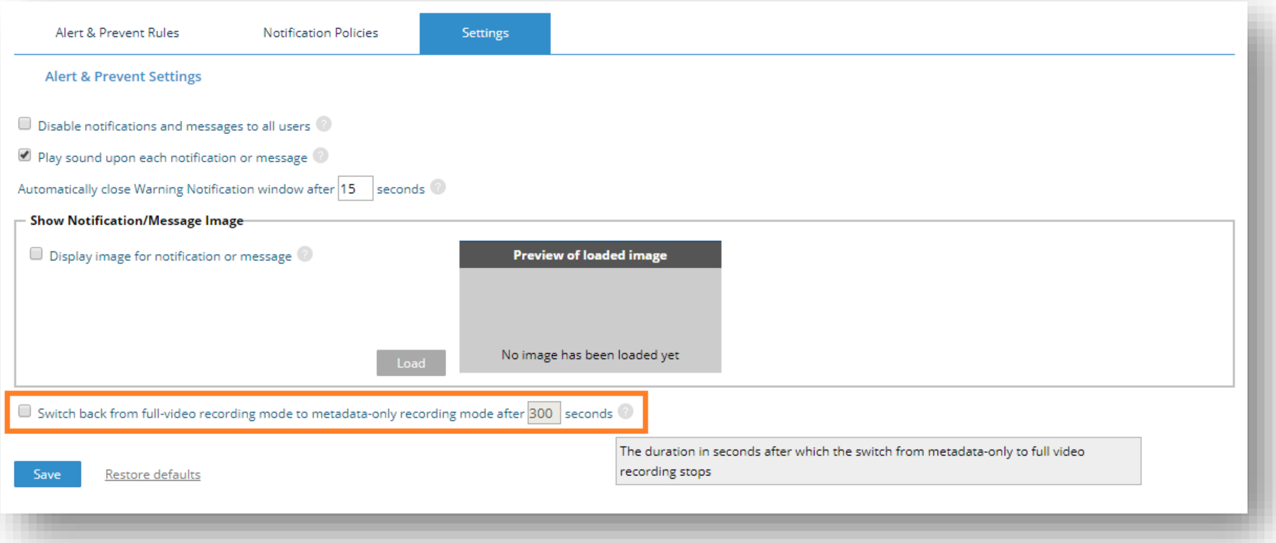
Original File Name: ends with — .exe, .bat, .zip, .rar, tar

FAM Alert Rule – Intuitive and Flexible

PRIVACY – TURN OFF VIDEO AFTER PREDEFINED PERIOD

When recording in metadata-only mode and switching to full-recording (with video) upon alert, to protect user privacy there is a need to switch back to metadata-only recording after a predefined time period.

ObserveIT 7.4 provides this capability allowing you to configure the time interval that suits your need.



□ Disable notifications and messages to all users

☑ Play sound upon each notification or message

Automatically close Warning Notification window after 15 seconds

□ Display image for notification or message

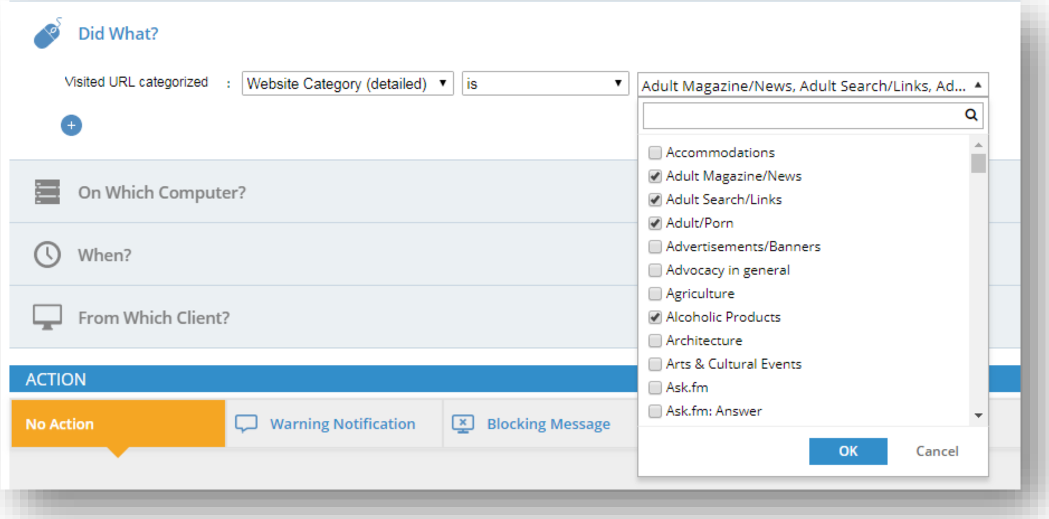
□ Switch back from full-video recording mode to metadata-only recording mode after 300 seconds

The duration in seconds after which the switch from metadata-only to full video recording stops

Switch Back to Metadata-Only Recording after a Specified Period

GRANULAR WEB CATEGORIES

ObserveIT 7.4 provides customers with a more granular list of Website Categories, which are more specific and accurate for defining alerts based on web browsing.



Visited URL categorized : Website Category (detailed) ▾ is ▾ Adult Magazine/News, Adult Search/Links, Ad... ▴

- ☐ Accommodations
- ☑ Adult Magazine/News
- ☑ Adult Search/Links
- ☑ Adult/Porn
- ☐ Advertisements/Banners
- ☐ Advocacy in general
- ☐ Agriculture
- ☑ Alcoholic Products
- ☐ Architecture
- ☐ Arts & Cultural Events
- ☐ Ask.fm
- ☐ Ask.fm: Answer

More Granular Website Categories

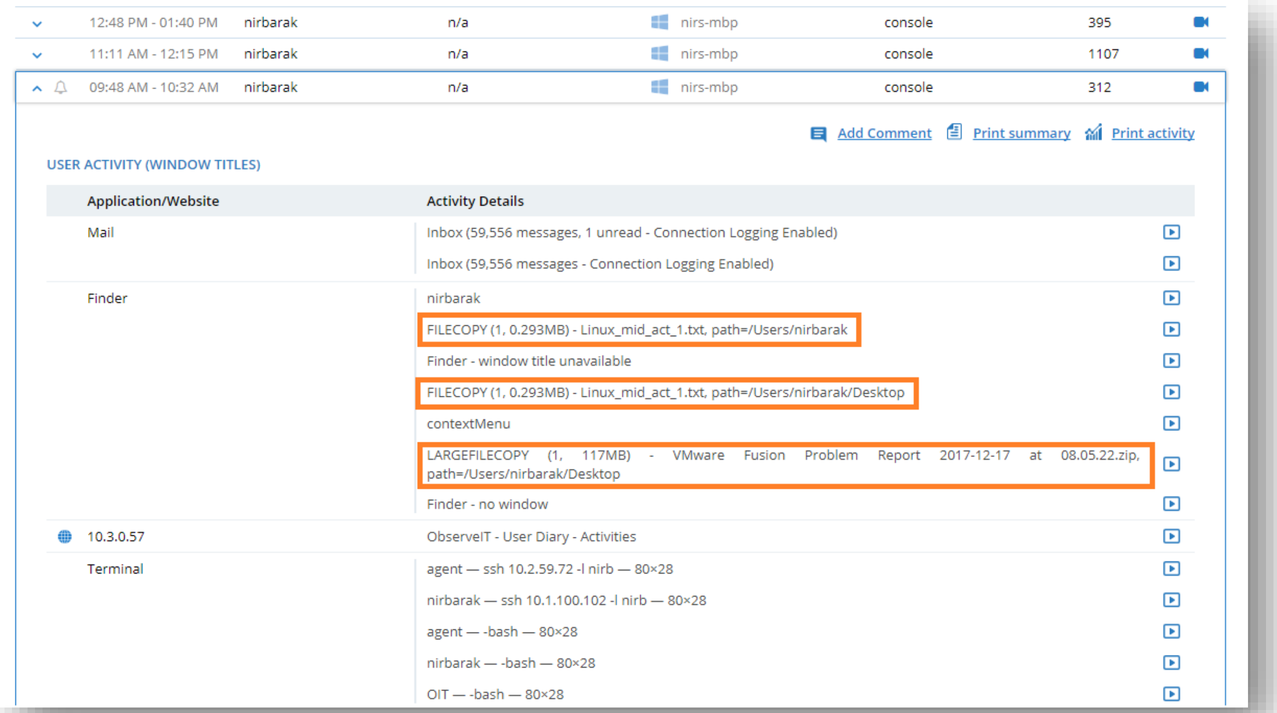
✓

✓ *Note: The less granular list of categories that was available before this release can still be used.*

MAC AGENT

With the growing use of Mac agents in larger deployments, ObserveIT 7.4 keeps improving the Mac agent to address market needs.

- New supported platform: MacOS High Sierra (10.13)
- Mass agent deployment
  - Restructure the Mac installation package to support mass deployments using the JAMF management tool, and other tools that support the PKG format.
- Capture file copy activity on Mac
  - When a file or a folder is copied/moved using drag & drop in the Finder application or using the Pasteboard, this activity is now recorded.
  - The captured metadata contains the number of files being copied, their total size, the names of the files and the folder from which they were copied or moved.
  - Large file copies (configured via recording policy) are indicated as such.
  - The captured metadata is search-able, alert-able, report-able, and can be exported to SIEM.



12:48 PM - 01:40 PM	nirbarak	n/a	nirs-mbp	console	395
11:11 AM - 12:15 PM	nirbarak	n/a	nirs-mbp	console	1107
09:48 AM - 10:32 AM	nirbarak	n/a	nirs-mbp	console	312

USER ACTIVITY (WINDOW TITLES)

Application/Website	Activity Details
Mail	Inbox (59,556 messages, 1 unread - Connection Logging Enabled)
	Inbox (59,556 messages - Connection Logging Enabled)
Finder	nirbarak
	FILECOPY (1, 0.293MB) - Linux_mid_act_1.txt, path=/Users/nirbarak
	Finder - window title unavailable
	FILECOPY (1, 0.293MB) - Linux_mid_act_1.txt, path=/Users/nirbarak/Desktop
	contextMenu
	LARGEFILECOPY (1, 117MB) - VMware Fusion Problem Report 2017-12-17 at 08.05.22.zip, path=/Users/nirbarak/Desktop
	Finder - no window
10.3.0.57	ObserveIT - User Diary - Activities
Terminal	agent — ssh 10.2.59.72 -l nirb — 80×28
	nirbarak — ssh 10.1.100.102 -l nirb — 80×28
	agent — -bash — 80×28
	nirbarak — -bash — 80×28
	OIT — -bash — 80×28

Mac Captures Metadata of File Copy and Large File Copy

NEW INSIDER THREAT LIBRARY (ITL) RULES

ObserveIT 7.4 keeps adding out-of-the-box scenarios to detect insider threats. Existing rules and lists are updated based on customer feedback and continuous learning. Many of the Windows rules are enhanced to provide better detection on Mac.

Following is a taste of the enhancements:

Windows

- Adding or modifying Roles and Features in IIS Manager (PERFORMING UNAUTHORIZED ADMIN TASKS)
- Opening ObserveIT Agent folder (BYPASSING SECURITY CONTROLS)

Mac

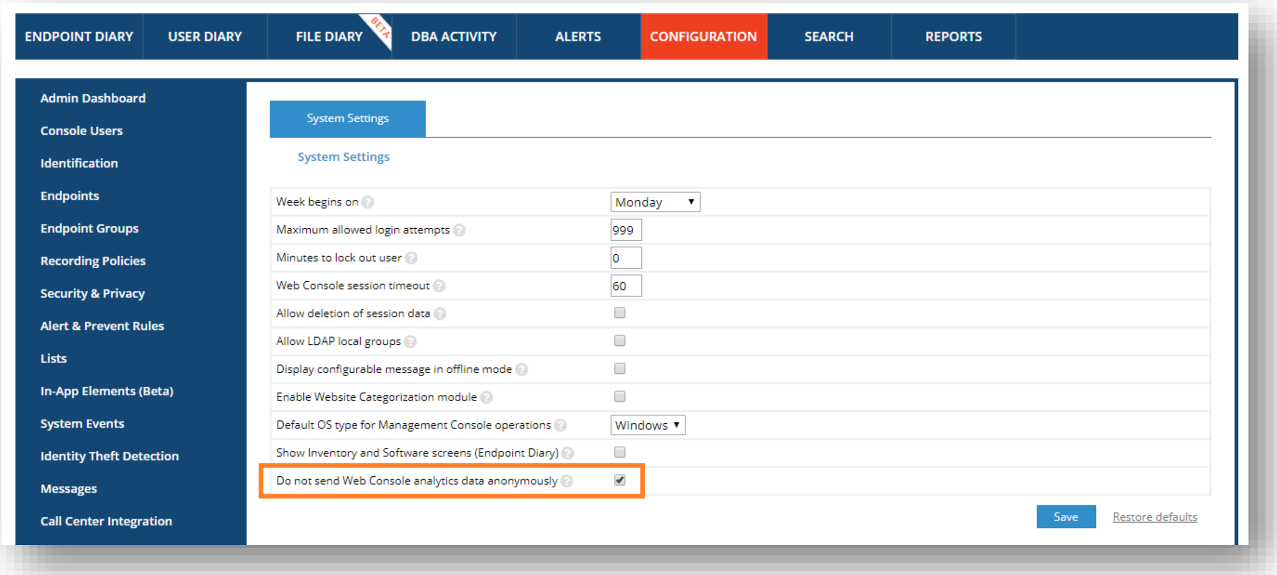
- Opening sharing settings on Mac (CARELESS BEHAVIOR)
- Taking control on remote machine from Mac (UNAUTHORIZED MACHINE ACCESS)
- Taking screenshot using keyboard shortcut on Mac (DATA EXFILTRATION)
- Many rules and lists were updated to support Mac specific tools and keywords. Few examples:
    - Mac command line admin tools
    - Mac cloud backup tools
    - Mac email clients
    - Mac SQL tools
    - Mac Hacking/Spoofing keywords
    - Mac Instant Messengers
    - …and more

FEATURE ANALYTICS

We want to make ObserveIT better for our customers. For that, we need better visibility on how users interact with the Management Console – how often, which screens are used most, and so on.

ObserveIT 7.4 anonymously collects feature usage data that can be later analyzed by the ObserveIT team and used as valuable input for future product enhancements.

ObserveIT appreciates your willingness to help improve our product; however, if you decide to opt-out, you can do so during the installation (via a dedicated checkbox option) or at a later stage by using the System Settings option (shown below).



System Settings

Week begins on	Monday
Maximum allowed login attempts	999
Minutes to lock out user	0
Web Console session timeout	60
Allow deletion of session data	☐
Allow LDAP local groups	☐
Display configurable message in offline mode	☐
Enable Website Categorization module	☐
Default OS type for Management Console operations	Windows
Show Inventory and Software screens (Endpoint Diary)	☐
Do not send Web Console analytics data anonymously	☑

If you agree to help ObserveIT by sending us anonymized usage data, please make sure to white-list the ***api.mixpanel.com*** *domain in your environment*

Thank you for your help in making ObserveIT a better product!