

Technical Solution Overview

This document outlines the key features, system architecture, deployment scenarios, system requirements, product installation, security and privacy infrastructure, data management, and integration capabilities of ObserveIT Enterprise.

This document was written for ObserveIT Enterprise 7.12.x.

Table of Contents

Technical Solution Overview	1
Complete Insider Threat Solution	1
Key Components	2
Key Solution Features	4
Detecting Data Loss in ObserveIT	4
File Activity Monitoring	5
File Activity View	5
File History View	6
USB History View	7
Email Clients Monitoring and Visibility	8
Visual Forensics	8
MIP Integration	9
MIP Overview	9
Label Change	10
ObserveIT Keylogging	10
Insider Threat Intelligence	11
Reporting and Auditing	12
Website Categorization	13
Session and User Activity Metadata Search	14
User Activity Profile	15
Identity Theft Detection	16
User Session Locking	17
DBA Activity Audit	17
Policy Messaging and Recording Notification	18
System Architecture	20
Architecture and Components	20
ObserveIT Architecture	21
Windows Agent	22
Mac Agent	23

Mac Agent Capabilities	24
Mac Agent - Getting Started	25
Unix - Linux Agent	25
Supported Platforms	27
Windows Agent	27
Unix/Linux Agent	27
Mac Agent	28
Installation Architectures	30
All-In-One Installation	30
Small Scale Installation	30
Medium Scale Installation	31
Large Scale Installation with High Availability	32
Load Balancer Implementation	33
File System Storage	34
Large Scale Installations with Multiple Sites	34
Deployment Scenarios	36
Standard Agent-Based Deployment (Servers and Desktops)	36
Jump Server Gateway	36
Outbound Jump Server Gateway	38
Citrix Server for Published Applications	39
Hybrid Deployment - Agent Based and Gateway	40
ObserveIT Custom Installation	40
Agent Auto Upgrade	41
Upgrade Sets	41
Endpoint Upgrade Status	41
Key Configuration Settings	42
ObserveIT Web Console Users	42
SMTP Configuration	43
LDAP and Active Directory Configuration	43
Configuring Recording Policy Settings	44

Recording Policy Endpoints	44
Recording Policy Settings	45
Configuring Alert Rules	46
Ongoing Alerts Tuning	49
Implementing Lists in ObserveIT	49
Security and Privacy Infrastructure	51
Windows Agent Security	51
Mac Agent Security	51
Unix/Linux Agent Security	51
Data Security in Transit	51
Data Security at Rest	52
Installation Security	53
System Health Monitoring	53
Data Management	55
ObserveIT Database Structure	55
Database Storage	55
File System Storage	56
Metadata Storage	56
ObserveIT Data Integration	57
Integrating ObserveIT Data into 3rd-Party SIEM Systems	57
Packaged Integrations	57
Custom Integrations	57
Integration using ObserveIT RESTful API	57
Integration using CEF Logs	58
Integrating ObserveIT with a Service Desk System	58
Agent API for Integration	60

Complete Insider Threat Solution

ObserveIT's Insider Threat Management Platform provides organizations with:

- **Comprehensive Visibility:** Gain complete context into users and their data activity across Windows, Mac, Unix/Linux & virtual machine endpoints & web and cloud applications. Achieve user attribution with an easy-to-understand, visual timeline and flexible, real-time session recording.
- **Proactive Detection:** Detect unauthorized user activity, including data exfiltration, privilege abuse, unauthorized access and security controls bypass, in real-time with 320+ pre-configured indicators of risk. This is powered by an Insider Threat Library built with feedback from 1,900+ customers & leveraging NIST, MITRE & CERT guidelines.
- **Faster Investigations:** Investigate incidents efficiently with visibility into user intent and cause. Gather, package and export the necessary evidence of who, what, where, when and user intent to take action without having to jump between multiple tools. Save time and reduce cost of investigations.
- **Accelerated Response:** Respond faster to incidents by driving meaningful behavior change with built-in security awareness notifications and prevention capabilities. Integrate ObserveIT visibility and detection with your existing cybersecurity tools.
- **Fast Time to Value:** A single, lightweight user-mode agent that is easy to install, does not require reboots and is privacy compliant. Yet, the agent is invisible to the user, works across Windows, Mac, over 27 flavors of Unix/Linux, virtual machines & in your cloud infrastructure.

ObserveIT enables security and risk analysts to track and monitor file activities in order to identify and alert on instances of data exfiltration. ObserveIT significantly reduces security incidents by changing user behavior through real-time education and deterrence coupled with full-screen video capture of security policy violations; investigation time is thus reduced from days of sifting through logs to minutes of playing back video. User activity profiling of risky users enables the investigation of aggregated information about user activities in order to identify and resolve insider threats more easily.

ObserveIT monitoring of both User Activity and File Activity are critical for detecting Insider Threat and data exfiltration. File Activity Monitoring enables organizations to track and alert when files are downloaded or exported using browsers or web-based

applications, and when files are copied or moved to default local sync folders of cloud storage services or USB devices.

ObserveIT's Insider Threat Intelligence platform increases security awareness by educating employees about out-of-policy behavior whether malicious or negligent. Through policy notification and enforcement, users can be educated to change their behavior. The ObserveIT User Risk Dashboard provides Security Analysts and Investigators with an easy way to track users that have experienced any type of policy notification or enforcement as a result of violating company policy or security rules. Every user notification message triggers an alert that notifies security specialists about the incident and updates the user's risk score. Preventive actions enable security and compliance officers to stop users from breaching security or violating company policies by forcibly logging off users from unauthorized machines and closing harmful applications.

The ObserveIT monitoring software acts like a security camera on your endpoints, monitoring and recording all user activity on Windows and, monitoring and recording all user activity on Windows and Unix/Linux servers and desktops. The system generates video recordings, user activity logs, behavioral analytics and real-time alerts. The result is a complete solution for identifying and managing user-based risk. Regardless of protocol or application, ObserveIT records any window session via a terminal or console, in a compressed and searchable format. The ObserveIT software captures all activity and generates textual audit logs, even for applications that do not produce their own internal logs. Every action that is performed by remote vendors, developers, system administrators, and business users, connected via RDP, SSH, Telnet, Citrix, direct console login, or any other protocol on physical and virtual machines, such as Citrix and VMWare, is recorded by video. Video replay provides bullet-proof forensic evidence, and video content analysis can identify all actions that were performed.

ObserveIT can help satisfy compliance requirements for PCI, SOX, HIPAA and NIPSOM.

Key Components

ObserveIT provides a comprehensive solution to identify and eliminate insider threat and data exfiltration.

- **Insider Threat Library:** ObserveIT's extensive library of out-of-the-box alert rules cover the most common scenarios of risky user activities. They have built-in policy notifications that are designed to increase the security awareness of users, and reduce overall company risk. Rules are mapped to User types such as Privileged Users, Everyday Users, Remote Vendors, and so on. ObserveIT's Library of alert rules can be applied on Windows and Unix/Linux machines. They are grouped according to security Categories to help navigation and management.

- **User Activity Monitoring:** Track users with suspicious or out of policy actions on workstations and servers, including on-premise, web-based and cloud-hosted applications and systems, as well as those with no internal logging facilities of their own. Prioritize users for further investigations based on ObservelT's Risk Dashboard, which scores risky user activity across the enterprise.
- **File Activity Monitoring:** Track and alert on files that were downloaded or exported using a browser or web-based application, from the internet or intranet. Alert if a tracked file is copied or moved to the default local sync folder of cloud storage services or when a file is copied or downloaded to a connected USB device. Monitor emails sent from email clients as well as files attached to and saved from email clients.
- **Live Activity Replay:** Capture screenshots of user actions and file movement for a preset time period before and after an out of policy alert is triggered. This helps to meet privacy compliance in environments with strict restrictions on legitimate business purposes to protect against insider threats. Use session recording to monitor users and servers on a more ongoing basis.
- **Policy notification and enforcement:** Enforce company policies and security regulations by utilizing ObservelT's flexible warning and blocking notifications in real-time on any user violating your policies and security rules. Prevent malicious or unauthorized Linux commands from being executed using flexible, out-of-the-box prevention rules. Stop users from breaching security or violating company policies by forcibly logging off from unauthorized machines and closing harmful applications.
- **Website categorization:** Automatically detect categories of websites that end users are browsing, enabling alerts to be generated on browsing categories such as gaming, adult content, infected or malicious websites, phishing websites, and more. ObservelT provides 42 out-of-box website categories.
- **Maintain privacy compliance:** User anonymization in the Dashboard and Web Console protects user privacy.
- **Efficient alert rule management:** Alert rules are grouped by Categories and assigned to User Lists.
- **Department level risk management via Active Directory Group-based permissions:** Large organizations can manage the risk of their employees in departments or groups, each owned by a dedicated security team member or manager.

Key Solution Features

This section describes ObserveIT key solution features.

Detecting Data Loss in ObserveIT

ObserveIT enables the detection of potential data leaks. The ObserveIT detection mechanism prevents data exposure, data theft, and out-of-company-policy activities, by enabling security and risk analysts to track the following user actions:

ObserveIT enables detection of potential data loss when a user:

- **Attempting to move files (or folders) by copying them to the clipboard or dragging them with the mouse.**

ObserveIT immediately captures the names of the files as well as their source location and size. Thresholds can be defined to indicate a LARGE file copy based on the number of files being copied and/or their total size.

- **Connecting any USB device (including mobile phones).**

ObserveIT immediately captures the device description (i.e. model , vendor and serial number) and the mapped drive letter.

- **Copying or downloading a file to a USB device.**

ObserveIT detects any file that is copied or downloaded to a USB device. Supported devices include USBs, SD cards, smart phones, tablets, and some encrypted USBs.

- **Performing a paste operation.**

ObserveIT detects paste operation of files, folders, images, and text when paste is performed by right-click menu item **Paste**, keyboard shortcuts **Ctrl+V**, **CTRL+Insert** (Windows), menu items **Edit > Paste** and equivalent right-click menu items and keyboard shortcuts **Cmd+V** (Mac).

- **Printing of files.**

The ObserveIT detection mechanism helps to prevent data exfiltration by enabling security and risk analysts to track any user attempt to print sensitive or confidential data. ObserveIT captures the titles of the files, the printer, and the number of pages being printed.

File Activity Monitoring

ObserveIT File Activity Monitoring enables you to monitor and detect file activity so you can detect and investigate data exfiltration.

With ObserveIT, you get the full story by monitoring entry point and exit point activities providing a high level of investigative capabilities.

- ObserveIT provides visibility on users that download or export specific files from sensitive websites or web applications (such as, Salesforce, Sharepoint, CRM, ERP), whether on the internet or in the local intranet.
- ObserveIT monitors files sent from email clients, attached to emails and attachments saved from emails.
- ObserveIT tracks files copied, or downloaded to USB devices and lets you determine which devices you want to monitor, authorized and/or not authorized devices.

File Activity Monitoring 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.

Summary information about activities on tracked files is displayed in the Endpoint Diary, User Diary, and Search screens, providing an instantaneous summary view of what happens throughout the session, without having to watch the whole Video playback or run reports.

File Activity View

The ObserveIT **File Diary** provides information about all tracked file activities that occurred on ObserveIT monitored endpoints.

Tracking file-related events and metadata (including the lifecycle history of each tracked file) can help security and risk analysts potentially identify instances of data exfiltration.

From the **File Activity** view, you can:

- View details of file activities that occurred during a specified time period and according to specified criteria
 - Created
 - Downloaded
 - Uploaded
 - Copied
 - Moved
 - Renamed

- Removed
- Stopped tracking
- Sent
- Attached to an email
- Saved
- Saved to and email
- Display session time by the endpoint or server location
- Filter the tracked file activity display according to specific criteria
- Export to Excel and print selected tracked file activities

File Activity

Period: Last Between To:

Show time by: Server **Endpoint**

File name:

File path:

File extension:

User login or secondary:

File size: Any size Min Max

File operation:

Application:

Website:

Exit Point:

File MIP label:

More Filters

MIP label column: Hide Show

1-20 of 26 Items per page 1 2 Next > Last >>

Time	File Name <input type="checkbox"/> Show Path]	Label	Operation	Details	Login	Application	Session
9/22/2020							
12:14 PM	2 Files		Downloaded from	Batched download transaction	administr...	Google Chrome	
09:38 AM	confidential (3).xlsx (157KB)	Confidential (Pr...	Downloaded from	drive.google.com	administr...	Google Chrome	
9/21/2020							
05:35 PM	pp_protectedpermission.p... (826KB)	Protected Permi...	Downloaded from	10.2.2.48:8080	administr...	Google Chrome	
05:33 PM	word_protected_nooffline.... (349KB)	Protected no-O...	Downloaded from	10.2.2.48:8080	administr...	Google Chrome	
05:14 PM	rtf_demo.pfile (305KB)	ITM - Demo	Moved to	c:\users\administrator.tsta\des...	administr...	Windows Explorer	
05:14 PM	rtf_demo.pfile (305KB)	ITM - Demo	Downloaded from	10.2.2.48:8080	administr...	Google Chrome	

File History View

The **File History** view provides a full history of all operations that occurred on the alerted file and allows you to jump directly to the Video playback at any point

The **File History** view shows the lifecycle of a file's history; every instance of file download, copying, moving, renaming, or removing, is displayed as well as links to Video Playback.

File Activity | **File History**

Initial file name: DUMMY.PDF
 Initial file path: C:\USERS\ADMINISTRATOR\DESKTOP\
 Originated from: w3.org
 Original file label: Onot set

MIP label column: **Hide** Show 🔍 🖨

Date	Time	File Name [<input type="checkbox"/> Show Path]	Label	Operation	Details	LoginApplication	Video
10/08/2020	05:00 PM	DU... (13KB)		Downloaded from	🌐 w3.org	A. Google Chrome	🔍 🖨
🔔 10/08/2020	05:36 PM	DU... (13KB)		Uploaded to	🌐 app.box....	A. Google Chrome	🔍 🖨
10/08/2020	06:57 PM	DU... (13KB)	OIT Protected	Renamed as	📄 dummy-...	A. Windows Explorer	🔍 🖨
🔔 10/08/2020	06:57 PM	du... (13KB)	OIT Protected	Uploaded to	🌐 app.box....	A. Google Chrome	🔍 🖨
10/11/2020	10:57 AM	du... (95KB)	OIT Protected	Renamed as	📄 dummy-...	A. Windows Explorer	🔍 🖨

USB History View

In the **USB History** view of the File Diary, you monitor a USB. The USB History shows when a USB device was connected and detects any files copied or downloaded directly to the USB device. This feature supports USBs, smart phones, SD cards, tablets and some encrypted USB devices.

The **USB History** view shows details and the status of the USB device. Status is either white listed (authorized), not white listed (not authorized) or ignored. Details include serial number, model name, vendor name and label name of the device.

File Activity | **USB History**

Device Serial Number: CR84184A1SXW-DW
 Model Name: Transcend
 Vendor name: StoreJet
 Label Name: QA | Transcend

Status: **🚫 Unlisted**
 Add device to [White list](#)
 Ignore device

1-13 of 13 Items per page

Date	Time	File Name [<input type="checkbox"/> Show Path]	Operation	Details	Login/Seco...	Application	Endpoint Name	IP	Video
🔔	12/16/2018 12:10 PM		USBCONNECT	🚫 QA, Transcend , StoreJet...	liliya		OIT-LILIYA-LAP		🔍
🔔	12/16/2018 11:46 AM	VS_RemoteTools.exe	Copied to	🚫 E:\VS_RemoteTools.exe	liliya	Windows Explorer	OIT-LILIYA-LAP		🔍
🔔	12/16/2018 11:46 AM	tfpt.msi	Copied to	🚫 E:\tfpt.msi	liliya	Windows Explorer	OIT-LILIYA-LAP		🔍
🔔	12/16/2018 11:45 AM	HEL(7.7.0.0).txt	Copied to	🚫 F:\HEL(7.7.0.0).txt	liliya	Windows Explorer	OIT-LILIYA-LAP		🔍
🔔	12/16/2018 11:45 AM	CAP(7.7.0.0).AA9BDF3C-755A-4...	Copied to	🚫 F:\CAP(7.7.0.0).AA9BDF3...	liliya	Windows Explorer	OIT-LILIYA-LAP		🔍
🔔	12/16/2018 11:45 AM		USBCONNECT	🚫 QA, Transcend , StoreJet...	liliya		OIT-LILIYA-LAP		🔍

Email Clients Monitoring and Visibility

Email may be used as an easy exfiltration point for important data from your company. For example, employees might send confidential information via email clients, send attachments with important documents or images, or save attachments with sensitive information to their computer and later exfiltrate it. ObserveIT Email Monitoring provides visibility into this important exit point by monitoring emails sent from your email client, files attached to emails and attachments saved from emails.

From the **Email Diary** you can review and filter emails monitored to help you detect and investigate sensitive data exfiltration from your company's email client.

The screenshot displays the 'Email Activity' interface. On the left is a navigation sidebar with sections: 'Email Activity', 'Latest Sessions', 'Quick Help', 'User Guide', and 'Configuration Guide'. The 'Latest Sessions' section lists: OIT-ALON-... alon.r, MacBook-Air autouser, OIT-TEMP1 autouser, and W12-S12-Q... Administrator. The main panel features a filter section with options for 'Period' (Last 1 Weeks, Between 04/12/2019 To 05/12/2019), 'Subject', 'From', 'Recipient', 'Recipient domains' (All Selected), 'To', 'Cc', 'Attachment name', 'Attachment existence' (Any), 'Endpoint' (All), 'User login' (All), 'Recipients domains type' (Any), 'Bcc', and 'Total attachment size' (Any size, 0 KB Min, 2000 KB Max). A 'More Filters' link and 'Show'/'Reset' buttons are also present. Below the filters is a table showing 1-20 of 28 items per page, with 12 items displayed. The table columns are Time, Subject, From, Recipients, Attachments, Login, Endpoint Name, IP, and Session. The data rows are for 5/12/2019:

Time	Subject	From	Recipients	Attachments	Login	Endpoint Name	IP	Session
11:34 AM	Please add @H...	alon.r@observ...	ayelet@ob... (+1)	None	alon.r	OIT-ALON-LAP		
10:55 AM	morning	laurentobserve...	hadas.e@tsta.c...	Details... (524 B)	autouser	OIT-TEMP1		
10:48 AM	RE: Starting Me...	alon.r@observ...	anat@observei...	None	alon.r	OIT-ALON-LAP		

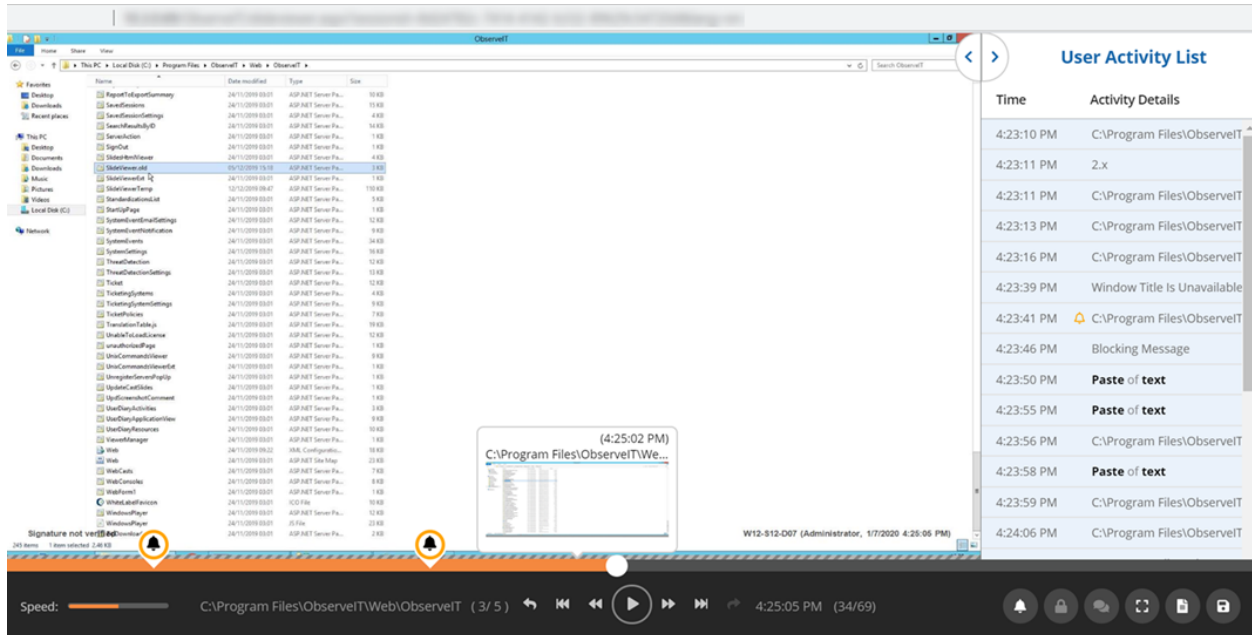
Note: Microsoft Outlook for Windows, Microsoft Outlook for Mac and Apple Mail App are supported.

Note: When using Microsoft Outlook API, a short delay may occur before full email monitoring starts. The delay of a few seconds is due to the time required b Microsoft Outlook API to establish communication.

Visual Forensics

Playing back a user session shows exactly what occurred on-screen. Playback speed is adjustable. On the right side of the player window is an activity summary panel which lists, in chronological order, every action performed during the session. Clicking an action jumps directly to that portion of the video—just like navigating chapters on a DVD. Alerts

triggered from the session are indicated on the timeline, and during playback alert details are automatically displayed at the exact time they occurred.



ObserveIT goes far beyond simply recording on-screen activity. All on-screen activity is transcribed into an easy-to-read user activity log so that you don't need to watch the video to know what the user did. User activity logs can be selected by endpoint (Endpoint Diary page), by user (User Diary page), or by keyword search (Search page). Clicking on any specific event in the log launches the video playback from that exact moment.

Note: You can see at a glance exactly what a user did during a session, and if any suspicious activities were performed.

MIP Integration

MIP integration lets you integrate the Microsoft Information Protection (MIP) Unified Labeling solution with the ITM platform providing more context about user activities.

Microsoft MIP is a cloud-based solution that lets organizations classify documents and emails by applying labels to documents. In addition, the label can have a security policy assigned to it. From Microsoft products such as Azure and Outlook, labels can be applied to files by an administrator who can also define rules and conditions and manually applied by users. This solution is available by license from Microsoft.

MIP Overview

If a file has a MIP label, the Agent captures and extract the label and its attributes when:

- a file enters (downloaded to) an endpoint you want to monitor by Web download, cloud sync folder (Box only) or as an attachment to an email (Outlook or Apple Mail)
- a tracked file is copied, moved, renamed or deleted
- a file is exfiltrated by file upload, copying or moving it to a USB, copying or moving it to a cloud sync folder of a supported vendor or sending it as an email attachment (Outlook or Apple Mail)

Label Change

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.

Note: 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.

ObserveIT Keylogging

Keylogging solutions track and record every keystroke made by a computer user. ObserveIT Keylogging is used for monitoring, root-cause analysis, data exfiltration, forensic investigation and regulatory auditing. With keylogging, you can detect keystrokes on desktop applications, websites and Windows/Mac shell command tools.

ObserveIT Keylogging solution enables you to detect and generate alerts on:

- Sensitive keywords and commands that Windows/Mac users typed
- Special keys that users pressed
 - PrtScr, Backspace, Insert, Enter, Clear, Return, Delete, End, Esc, Home, Page Up, Page Down, Tab and F1 to F12
- Key combinations that users pressed
 - Alt, Ctrl, Shift and Win with other keys (Windows) and Cmd, Control, Option, and Shift with other keys (Mac). (A key combination can be up to four keys.)

ObserveIT keylogger is supported on Windows, Mac and Unix-based operating systems. Windows keylogger data is fully captured within the main browsers (Edge, Chrome, and FireFox). Mac key logger data is supported on Safari.

Note: To prevent users who are authorized to access the database from viewing passwords or other sensitive data, data captured by the ObserveIT keylogger is hashed (using the SHA256 salted hash algorithm). ObserveIT Administrators cannot disable keylogger hashing from the ObserveIT Web Console.

Insider Threat Intelligence

ObserveIT provides an extensive library of out-of-the-box detection scenarios that can be used by Business users and Administrators to detect insider threat on Windows, Mac, and Unix/Linux systems.

The ObserveIT Analytics Library Package contains over 300 rules that cover the most common scenarios of risky user activities that might generate alerts. These rules have built-in policy notifications that are designed to increase the security awareness of users, and reduce overall company risk.

To help you use the Alert Rules, ObserveIT has determined which Alert Rules (Windows/Mac) bring the highest value to customers. These “top” 60 Alert Rules for Windows/Mac are now active by default. All other Window/Mac rules are deactivated by default.

ObserveIT’s Library of alert rule scenarios are grouped according to security Categories to help navigation and facilitate their operation and maintenance. Rules can also be mapped to types of user groups, such as Privileged Users, Everyday Users, Remote Vendors, and so on, each with a specific risk level.

Each alert rule in the ObserveIT Insider Threat Library is associated with at least one Category. Categories apply to Windows, Mac, or Unix/Linux systems; some are relevant for all systems.

The Insider Threat Library is maintained by an ObserveIT Content Manager and released as a ZIP file to customers, providing them with the most up-to-date insider threat scenarios.

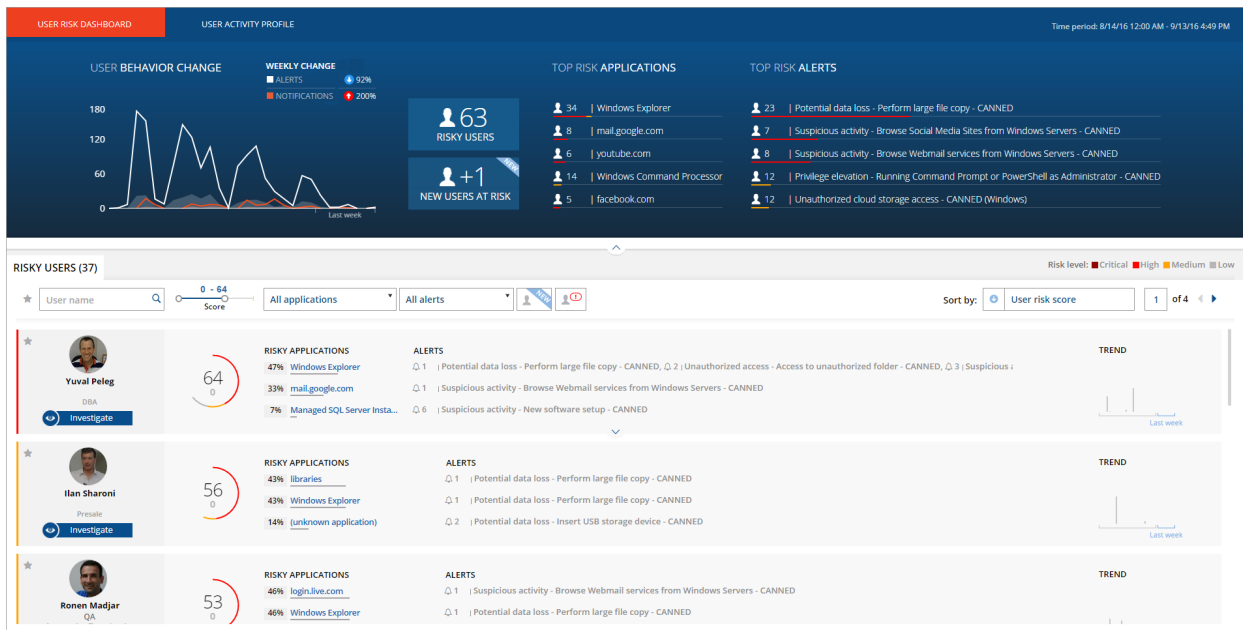
Viewing User Behavior and Risk Score

The ObserveIT **User Risk Dashboard** provides an overall view of user risk and behavior trends over a period of time. In the dashboard, you can view overall organizational risk from insider threats and view a prioritized list of users and applications that present the greatest risk to your company.

The dashboard provides a broad view of risky users and their activities. Security analysts (including security and compliance staff, and those who review insider threats,

compliance, or out-of-policy risks) can quickly locate and identify risky users and new risky users. User information is graded and presented. The dashboard is divided into areas that reflect users and their actions in relation to risk. You can understand and view the overall general risk that includes the user risk level comparison, risky users, and new risky users. You can filter and sort user information, and drill down to an individual risky user's actions to view alerts, and pinpoint exactly what actions qualify them as risky users.

Using the dashboard, security analysts and investigators can track users that have experienced any type of policy notification or enforcement as a result of violating company policy or security rules. They can also quickly pinpoint the users with the highest number of policy violations, as well as those who are not improving with time. You can filter and sort user information according to the number of out-of-policy notifications and behavior trends, providing an easy way to identify those users who constantly violate security policies and those who keep ignoring them despite being warned or even blocked.



Reporting and Auditing

ObserveIT reporting can be used by novice administrators to generate reports based on preconfigured built-in reports, or by experienced administrators and security auditors who require flexible application usage reports and trend analysis reviews. Experienced administrators and security auditors can also create comprehensive customized reports based on their own requirements. Reports can provide aggregated or summary information about all monitored user activity on Windows, Mac, or Unix-based endpoints.

ObserveIT reporting capabilities significantly enhance security operations and regulatory compliance by providing reports on alerts, websites visited, documents printed, USB

storage device connections, file/folder copying, large file/folder copying, typed keylogger data, SQL queries executed against production databases, installing and uninstalling applications, system events, user logins, and more. Captured metadata can be used to expose potential data leaks by generating reports that show for example, when corporate or sensitive files were copied or printed, when a user connected a USB storage device, when notification or blocking messages were displayed to users, when large files were copied or printed, and so on.

In addition, ObserveIT reporting on audit log information (such as, user logins, sessions, and saved sessions in which console users were active) provides valuable security auditing and change management.

The ObserveIT Web Console provides several ways to run reports and export user activity log data:

- The report generator includes built-in reports and customizable report rules for filtering by user/user group, endpoint/endpoint group, date, application, resources accessed, and more.
- Reports can be run ad-hoc or delivered on a schedule by email.
- Full-text Google-like searching allows pinpoint identification of user sessions.
- User activity log drill-down allows each session to be viewed item-by-item, to see which applications were run and which actions were performed during that session.

Website Categorization

ObserveIT provides high visibility into your employees' web browsing habits.

The ObserveIT Website Categorization module automatically detects categories of Websites that end users are browsing, enabling alerts to be generated on browsing categories such as Gaming, Adults, Infected or Malicious Websites, Phishing Websites, and more.

ObserveIT has over 28 billion indexed URLs that are updated daily with new websites and new security risks. Website Categorization supports flexible deployment modes whether your endpoint can access the internet directly or via a protected proxy.

Using URL Filtering technology, ObserveIT can automatically categorize any visited website and trigger alerts when users browse these counter-productive websites, or websites that are not allowed by policy or are suspicious for specific individuals.

Even if you have a Web Filtering solution already deployed in your organization, the ObserveIT Website Categorization capabilities can help you to detect unacceptable use of websites that you allow employees to access.

Following are some examples of scenarios for which Website Categorization would generate alerts:

- Everyday employee (not an administrator) browsing websites that describe sniffing or hacking techniques
- Employees accessing cloud storage or cloud transfer sites
- Blocking messages displayed to users when accessing malicious or phishing websites
- Using servers for non-work-related tasks such as P2P services, social media, watching online videos, etc.
- Searching for data on Darknet, illegal drug sites, violence, or any other legal-sensitive websites
- Employees wasting time on gaming, gambling, sports or news websites

Note: In order to trigger alerts on Internet browsing, the Website Categorization module must be installed.

Session and User Activity Metadata Search

ObserveIT captures all user activity, recording important information about what is seen on the screen, which applications are currently used, what actions the user has performed, the date and time of the action, and more. This "metadata" is stored in the ObserveIT database, which is located on a central SQL Server. Because metadata is centrally stored and indexed, it can be used to easily search throughout recorded sessions, and provide a textual breakdown of each user session.

The screenshot shows a search interface with the following fields and options:

- Search for:** containing text
- Within:** File attached to an email client
- Limit search to:** (expanded)
- Time:** Last period (dropdown), Of: 3 (input), Days (dropdown)
- Show time by:** Server (selected), Endpoint (checkbox)
- User (or Login):** -All- (dropdown)
- Endpoint OS:** Windows, Mac (dropdown)
- Endpoint Name:** Show IP, -All- (dropdown)
- Buttons:** Search, Reset

You can search for users who logged in, application sensitive elements that were clicked or viewed, metadata that was captured on risky user activity concerning file copying and

data exfiltration through USB storage devices or printing sensitive data, keystrokes typed, applications that were run, specific window titles or URLs viewed, browsing forbidden Website categories, SQL commands containing keywords (such as, a table name), and more. On Unix/Linux systems, you can search for users who logged in, executed specific commands (based on command name, full path, arguments, command switches) or acted under a different user's permissions.

You can limit your search by time, user, endpoint name and endpoint OS.

You can also choose to show the the time zone where the server is located of the local endpoint time zone.

ObserveIT's advanced search boosts performance by allowing you to focus a search on specific metadata.

The displayed search results provide the context of the activity, showing the exact location of searched keywords (for example, in a URL, Window title, SQL statement, and so on). Where relevant, the resulting search hit is linked directly to the portion of the video where the action occurred, making it easy to find the exact moment that an action was performed. Within each session, you can watch the full video replay of the user session and see exactly what took place.

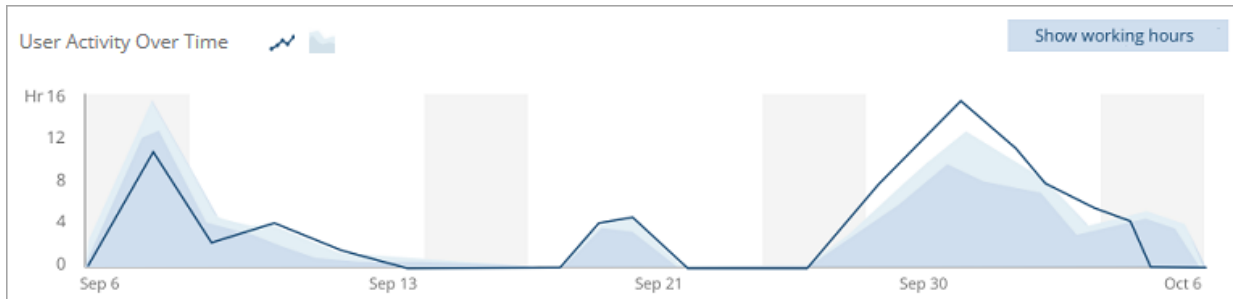
Note: For accelerated search performance, it is highly recommended that you install the Microsoft SQL Server Full Text Search (FTS) utility prior to ObserveIT installation.

User Activity Profile

ObserveIT enables you to access a risky user's profile in order to investigate and view aggregated information about the user's activities, such as:

This **User Activity Profile** information enables you to see the context of a risky user's activities, enabling you to solve incidents that might occur and identify insider threats more easily.

Dynamic filtering capabilities enable you to focus your investigation on specific applications, endpoints, login accounts, and/or remote client machines. An overall view of user activity during the specified profile period is displayed in a User Activity Over Time graph.



Identity Theft Detection

Today, security officers provide users with tools and education on how to protect their identity (such as, Two-Factor Authentication, Password complexity, reset rules, and so on). But once an identity is stolen, no tool can clearly identify or track the incident, and the responsibility for detection lies entirely on the security officer. ObserveIT enables you to include users in the detection process, and thus make users responsible for their identities. IT identity theft incidents can be detected and neutralized much quicker when users have a means to flag unauthorized logins.

The ObserveIT Identity Theft Detection solution is designed to detect access to ObserveIT monitored endpoints from unauthorized client computers.

When Identity Theft Detection is enabled, and users are logged on to ObserveIT-monitored endpoints, ObserveIT administrators or security officers will be notified about any suspicious login. A suspicious login is defined when a user tries to log in from an unauthorized client machine.

ObserveIT keeps track of authorized user login IDs and their client machines by "pairing" the domain name/login name of the user with the client computer from which the user is logged in. If a user logs in to a server from a client that is not paired to the user, an email is sent to the user, stating that there is a suspicious login with this user's credentials.

For example, if a hacker steals the credentials of a user and logs in from a remote machine, or if an internal user uses the administrator's password to log in to a server from the user's desktop, a suspicious login event is generated, and the user will receive notification about this via email. The email confirms which server the user logged on to, and from which client (user) machine they logged in. After receiving the email notification, if the user (or administrator) is indeed the person who logged in, he can ignore the email or submit another pairing request. If the user (or administrator) denies that he was the person who logged in, he should report this to the administrator.

For example, an internal user steals an administrator's password and logs in to a server from her own desktop, generating an email saying, "The user 'johnsmith' logged in to server DBPROD-4 from unauthorized desktop KATHY-DSKTP. Please confirm that it was you who performed this action."

The user can either confirm or deny the action. In parallel, an event is logged for the administrator to track and monitor unauthorized pairings. Granular security rules can be applied to specify how to manage each user confirmation.

User Session Locking

With ObserveIT, you can view live user sessions in real time. If required, you can interact with the user of each session by sending messages (for example, "You should not be running SQL queries on the production database.") and can also stop the user session entirely by locking the session.

DBA Activity Audit

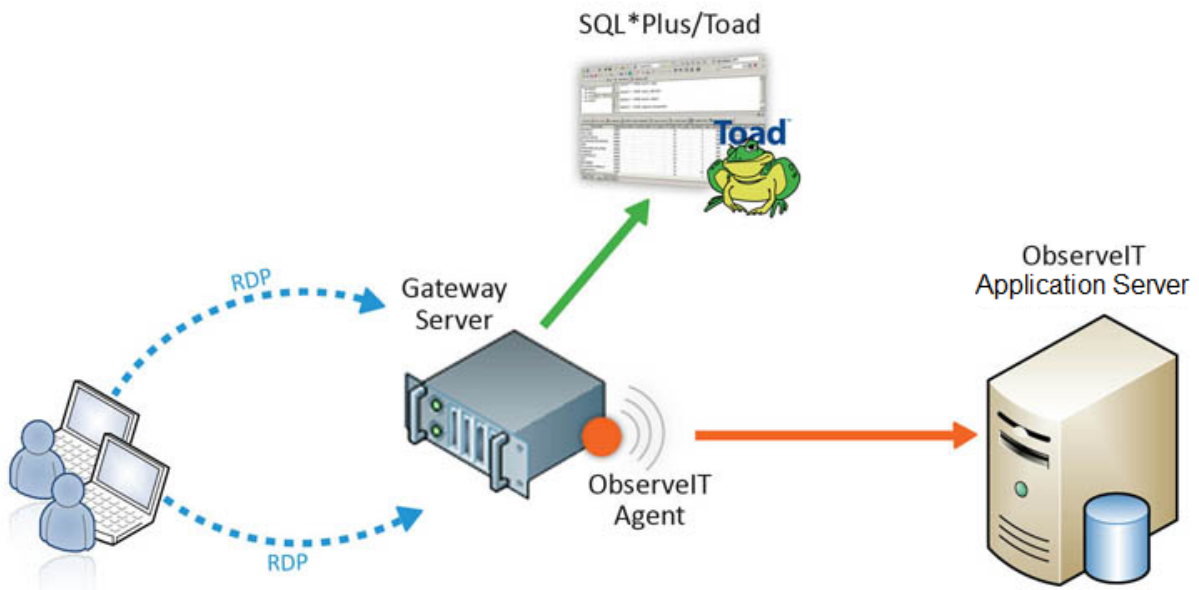
In the **DBA Activity** tab of the ObserveIT Web Console, you can monitor all SQL queries that were executed by DBAs against production databases.

DBA Activity Auditing provides monitoring of SQL queries executed by DBAs against production databases. SQL query activity is captured by ObserveIT when the DBA is using a DB management tool on an ObserveIT-monitored computer.

A recommended configuration is to ensure that all DBAs for whom recording is required must connect through a Windows gateway, on which the ObserveIT Agent and the DB management tool application are installed.

Using ObserveIT, administrators and auditors can review all SQL queries performed on a given date or filter results by database, DB User, endpoint, login ID, or any text contained within the queries. SQL queries are also included in the session activity details displayed in the Endpoint Diary and User Diary pages. When using the Search page in Metadata (user activity log) mode, text matches within SQL queries will also return the relevant sessions in the search results.

The following example illustrates how SQL queries are captured by ObserveIT:



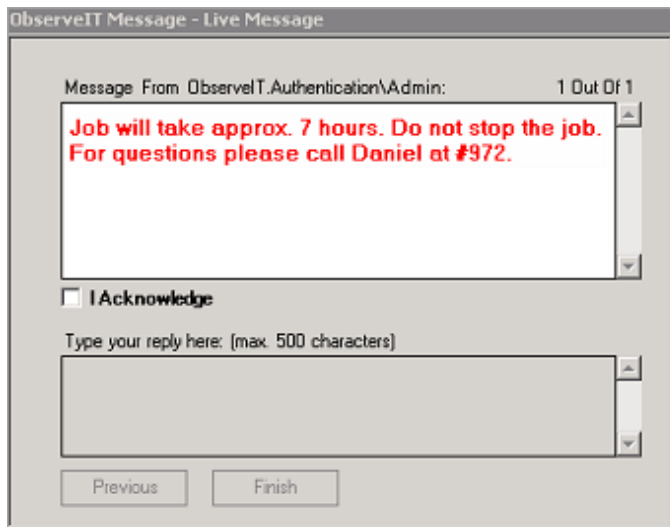
1. A user opens a remote RDP connection to the gateway in order to perform an SQL query.
2. The ObserveIT Agent captures the SQL query using the database management tool application on the gateway.

Policy Messaging and Recording Notification

Policy information can be delivered to users as they log into a server or desktop. This policy info can include notification of auditing activity (for example, “Please note that all activity on this machine is recorded.”). Policy information can also relate to company or regulatory policies (“Please note that PCI requirements mandate that no database traces be implemented on this server.”).

Policy messages can also be set to require the user’s response. This can be used to record the user’s acknowledgment that he/she is being recorded (a legal requirement in some jurisdictions). Users can optionally be prevented from completing their logon to the computer until they provide a confirmation and/or response.

Following is an example of a message that a user might receive from the administrator:



System Architecture

This section describes the ObserveIT architecture, components and supported platforms. The Windows, Mac, and Unix/Linux agents architectures are detailed.

Architecture and Components

ObserveIT is a software-based user activity monitoring and internal risk identification platform with no fixed hardware components. Software Agents running on Windows, Mac, or Unix/Linux gateways, servers or desktops capture user activity data and send it to an ObserveIT Application Server. The Application Server sends the relevant user activity log and screen video data to a Database Server for storage. All captured user activity data can be searched for, reported on, configured for alerts, and integrated with SIEM systems. Administrators manage the system and access user activity logs, screen video, reports and other features using the ObserveIT Web Console, which is served by the Application Server.

ObserveIT Application Server

The ObserveIT Application Server is an ASP.NET application that runs on a Windows Server-based computer (physical server or VM) in the context of Microsoft Internet Information Server (IIS).

Recorded data is sent by the Agents to the Application Server, which stores it in the SQL Server databases, and file system shared folders. Windows-based operating system recorded data is divided into 2 sections: the metadata (approx. 30% of the total storage size) and the graphical images (approx. 70% of the total storage size). Unix/Linux-based operating system recordings are 100% metadata.

The Application Server also maintains recording policies and other configuration data, actively communicates with Agents to deliver configuration updates and to monitor system health, handles data maintenance/archiving, and generates reports.

ObserveIT Web Console

The ObserveIT Web Console is an ASP.NET application that runs in the context of Microsoft Internet Information Server (IIS).

It is the primary interface for audit review, video replay, and reporting, as well as for configuring and administering ObserveIT. All configuration information is stored in the ObserveIT Database Server. The Web Console includes granular policy rules for limiting access to sensitive data.

In most cases, the ObserveIT Web Console component is installed on the same computer as the ObserveIT Application Server (or one of them if there are multiple Application Servers).

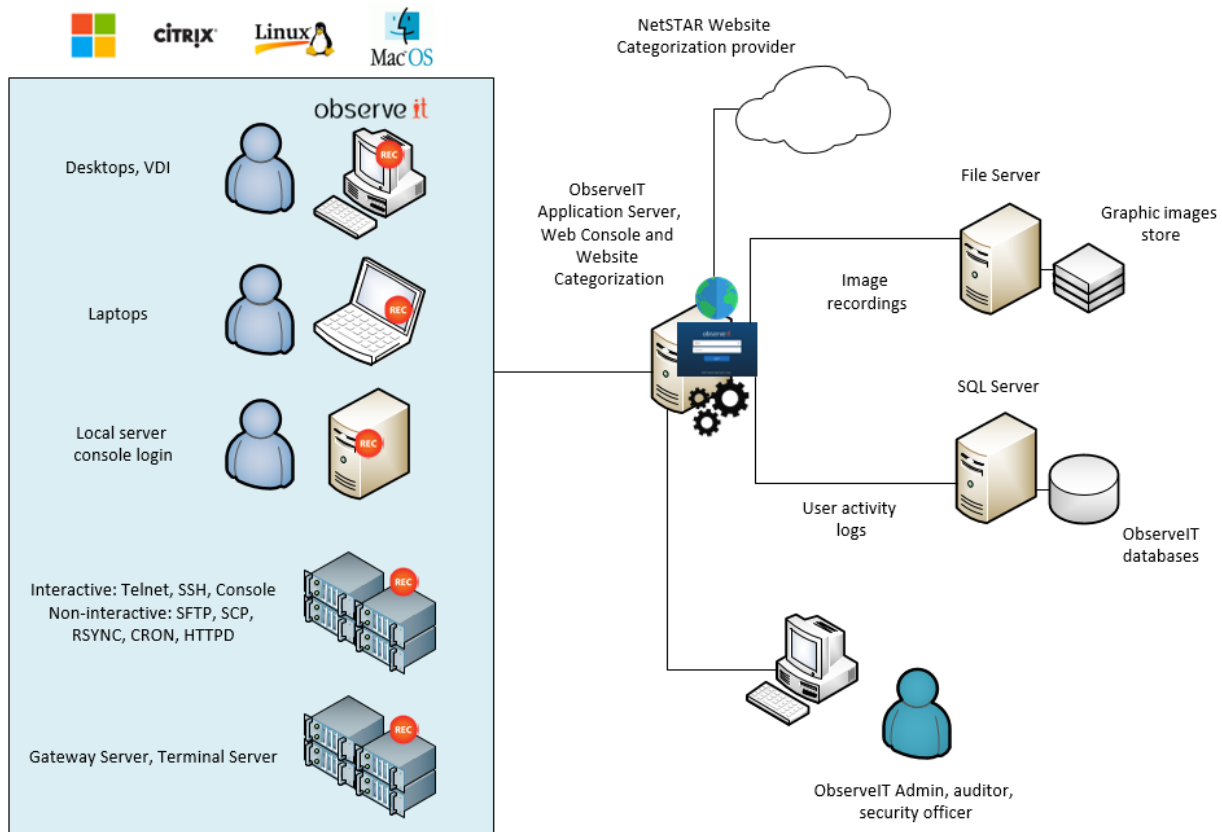
ObserveIT Database Server

By default, ObserveIT uses Microsoft SQL Server databases for data storage. This storage includes user activity configuration data, user analytics data, textual audit metadata and possibly the screenshots captured by the ObserveIT Agents for video replay.

ObserveIT can also be configured to store the video replay screenshots in file system storage instead of in the SQL database, either on the local hard drive of the ObserveIT Application Server, or on a file share in the network. In these cases, the MS SQL Server database is still used for storing user activity log and configuration data. Windows and Mac-based operating systems store approx. 20% of the total recorded data on SQL Server. The rest, approximately 80% of the total recorded data is stored on a file share. Unix/Linux-based operating system store 100% of the recorded data on SQL Server. Connectivity with the database is on standard TCP port 1433.

ObserveIT Architecture

The diagram illustrates the product architecture and flow of communication between the components.

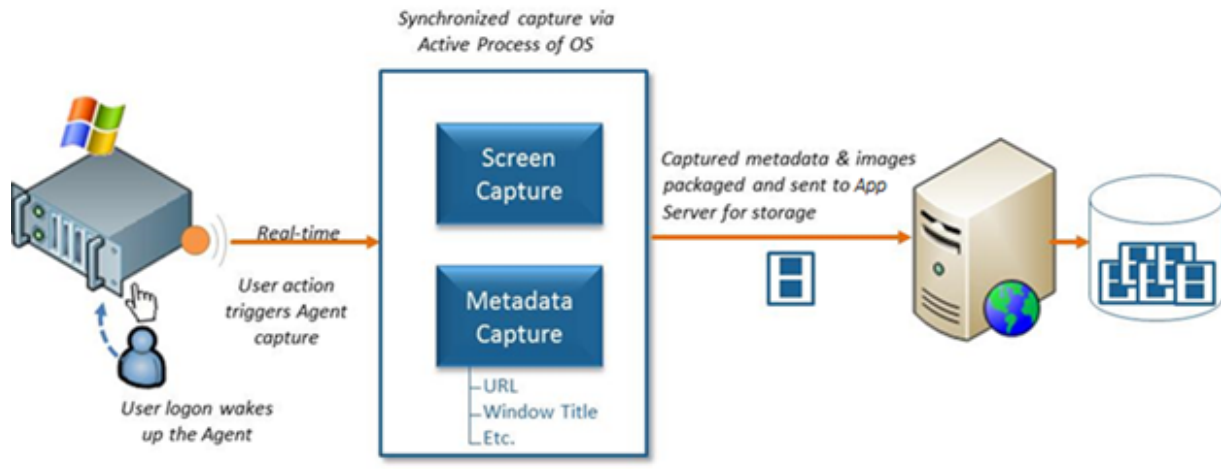


Windows Agent

The ObserveIT Windows Agent is a software component that is installed on any Windows-based operating system (server or desktop) that you want to record.

The Windows Agent is a user-mode executable that binds to every user session. As soon as a user logs into a monitored endpoint, the Agent begins recording based on the configured recording policy. From the moment a user logs on, the Windows Agent starts capturing user activity data logs and, if configured, screen video. All captured user activity data can be searched for, reported on, configured for alerts, and integrated with SIEM systems. The Agent sends all screen capture video and textual activity logs to the ObserveIT Application Server for processing and storage.

The diagram below shows the Windows Agent architecture.



By default, the Agent records the screen only when actual user activity is detected at the keyboard or mouse; during idle time (when there is no user activity on the machine), the Agent does not generate logs of screen capture data. However, optional time-based recording allows the recording of everything that appears on the screen even when the user is idle or not present – which can be useful, for example, to record the output of lengthy scripts run by IT users.

In cases when the recorded data cannot be stored on the Application Server or SQL Server (for example, the network or Application Server is down, or there is no connectivity to the database), the Windows/Linux/Unix/Mac OS Agent maintains an offline buffer to temporarily collect data. The buffer size is customizable. Once connectivity is restored, the buffered data is delivered to the Application Server.

Note: ObserveIT allows customers to monitor their users in stealth mode by deploying the Windows Agent with obfuscated names for its Agent components. To prevent innovative IT administrators or developers from discovering that the ObserveIT Agent is installed and running, ObserveIT can hide the Windows Agent by renaming processes, files and other resources, that might otherwise enable advanced users to uncover the Agent.

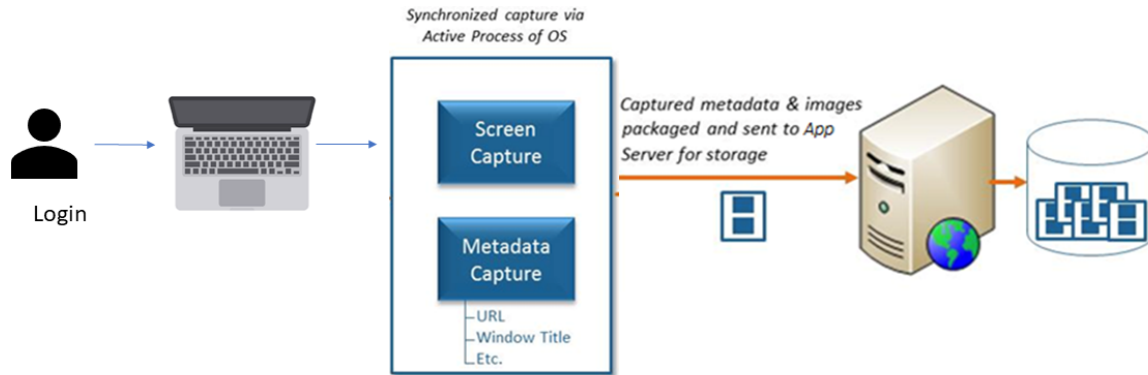
Mac Agent

The ObserveIT Mac Agent software can be installed on any Mac platform (desktop/laptop) requiring monitoring. As soon as a user logs into a monitored endpoint, the Agent begins recording based on the configured recording policy.

The diagram below shows the Windows Agent architecture.

All the metadata that is collected from the Mac Agent is searchable, reportable, can be alerted on, and can be exported to SIEM systems.

The diagram below shows the Mac Agent architecture.



Due to Apple security policy, if your organization uses the “.local” suffix, Apple devices might not resolve your unicast DNS names or bind to your Active Directory domains. (See [Apple Support](#).)

Mac Agent Capabilities

The Mac Agent has full recording capabilities and supports the features described below.

- Keylogging
- File activity monitoring
- Alerts
- Video and metadata recording
- Configurable recording policies (include/exclude users, applications, or URLs)
- Recording when Agent is offline
- Recording notification message
- Out-of-policy notifications (warning and blocking messages)
- Log Off and Close Application actions
- Health monitoring – detect if the Agent is offline or has been tampered with
- USB detection
- Email monitoring for Microsoft Outlook and Apple Mail apps

Mac Agent - Getting Started

To get started, you deploy the Mac Agent on the endpoints with one of the following methods:

- Mass deployment is used to deploy to multiple Mac OS endpoints using a deployment tool such as JAMF
- Interactive deployment is used to deploy to a single endpoint
- Offline deployment is used to install the Agent in offline mode

For more information see:

[All You Need to Know before Installing the Mac Agent](#)

[Mac Agent Deployment Overview](#)

Note: Risky activity that is performed on the Mac Agent is consolidated with other risky activities from the same user, providing a unified risk score for the user and a user-centric view in the User Risk Dashboard.

Note: For large enterprise deployments, the Mac installation package uses the JAMF management tool (and other tools that support the PKG format) to support mass deployments.

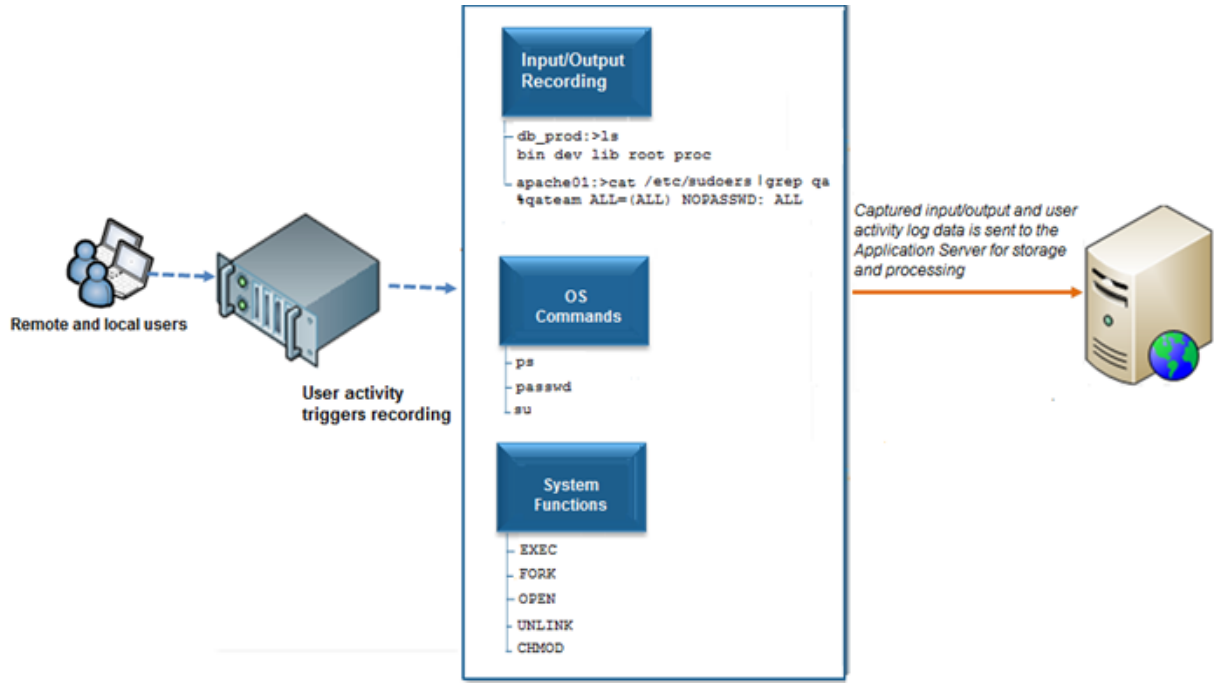
Unix - Linux Agent

The ObserveIT Unix/Linux Agent is a software component that can be installed on any supported Unix or Linux system that you want to monitor.

The Unix/Linux Agent runs in user mode and is triggered when an interactive session is created on a monitored machine (connected via SSH, Telnet, Rlogin, and so on). It records user activity inside the sessions, including interactive user activity and system functions such as OPEN, EXEC, CHMOD and others. The recorded data is sent to the ObserveIT Application Server and can be replayed or searched for input commands, system functions and output data. All recorded data can be searched, reported, configured for alerts, and integrated with SIEM systems.

When a user logs-in on a Unix/Linux machine, the Agent is started and begins recording the shell actions based on a predefined data recording policy.

The diagram below shows the Unix/Linux Agent architecture.



The ObserveIT Unix/Linux Agent captures all the internal actions and the names of files and resources that are affected by command line operations. All output, commands and important system functions inside commands are captured and forwarded to the Agent, which sends it to the ObserveIT Application Server for processing and storage.

In offline mode, the ObserveIT Agent allows local storage of the recorded data in the event of network malfunction or disconnection. When network connectivity is re-established, the ObserveIT Service transmits the locally cached data back to the Application Server. To prevent the local disk from reaching its full capacity, the volume of local data cache is limited per offline session.

Attempting to stop the recording process will terminate the user session, preventing any further user activity from not being recorded.

Supported Platforms

7.12.0 is the *last* version to support:

- SQL Server 2012/2014
- Win 32 bit agent
- Win 8.1
- Win Server 2012 (not R2)
- Debian 9

Windows Agent

You can deploy ObserveIT Agents on the following Microsoft Windows operating systems:

- Windows 10 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows Server 2016 (64-bit only)
- Windows Server 2012 R2 (64-bit only)
- Windows Server 2012 (64-bit only)
- Windows Server 2019 (64-bit only)
- Win 10 Enterprise Multi-Session
- Windows Virtual Desktop Win10
- Win 10 V1903, V1909, V2004

Unix/Linux Agent

You can deploy ObserveIT Agents on the following Unix/Linux-based operating systems:

- Solaris 11, updates 1-4; x86/x64 or Sparc
- Solaris 10, updates 7-11; x86/x64 or Sparc
- RHEL/CentOS 8.3

- RHEL/CentOS 8.2
- RHEL/CentOS 7.X
- RHEL/CentOS 6.7-6.10
- Oracle Linux 8-8.2
- Oracle Linux 7.0-7.4 x86_64
- Oracle Linux 7.8
- Oracle Linux 6.7-6.10 i386/x86_64
- SLES SuSE 15.2 32 & 64 bit
- SLES SuSE 12 i386/x86_64
- SLES SuSE 11 - 32 & 64 bit
- Ubuntu 20.04 LTS i386/x86_64
- Ubuntu 18.04 LTS i386/x86_64
- Ubuntu 16.04 LTS i386/x86_64
- Ubuntu 14.04 LTS i386/x86_64
- AIX 7.2 32-bit/64-bit
- AIX 7.1 32-bit/64-bit
- HP-UX 11.31 Itanium architecture (64-bit)
- Debian 8. 9 and 10 32-bit/64-bit
- Amazon Linux AMI 2015.03, 2017.09
- Amazon Linux 2

Mac Agent

The following versions are supported for deploying ObserveIT Agents on a Mac-based desktop, laptop, or server:

- macOS Big Sur 11
- macOS Catalina 10.15

- macOS Mojave 10.14

Installation Architectures

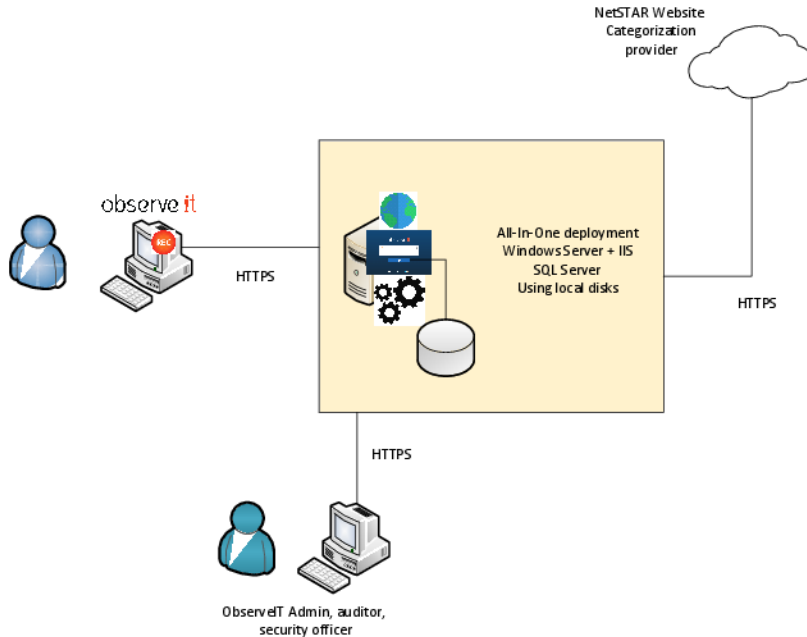
This section describes architectures for various sized ObserveIT installations.

For details and exact requirements, contact your ObserveIT representative.

All-In-One Installation

In an All-In-One installation the expected load is low, so the Application Server, Web Console and Database Server are all installed on the same platform. This includes the file share used to store the recorded images. This platform can be a physical server or it can be a virtual machine.

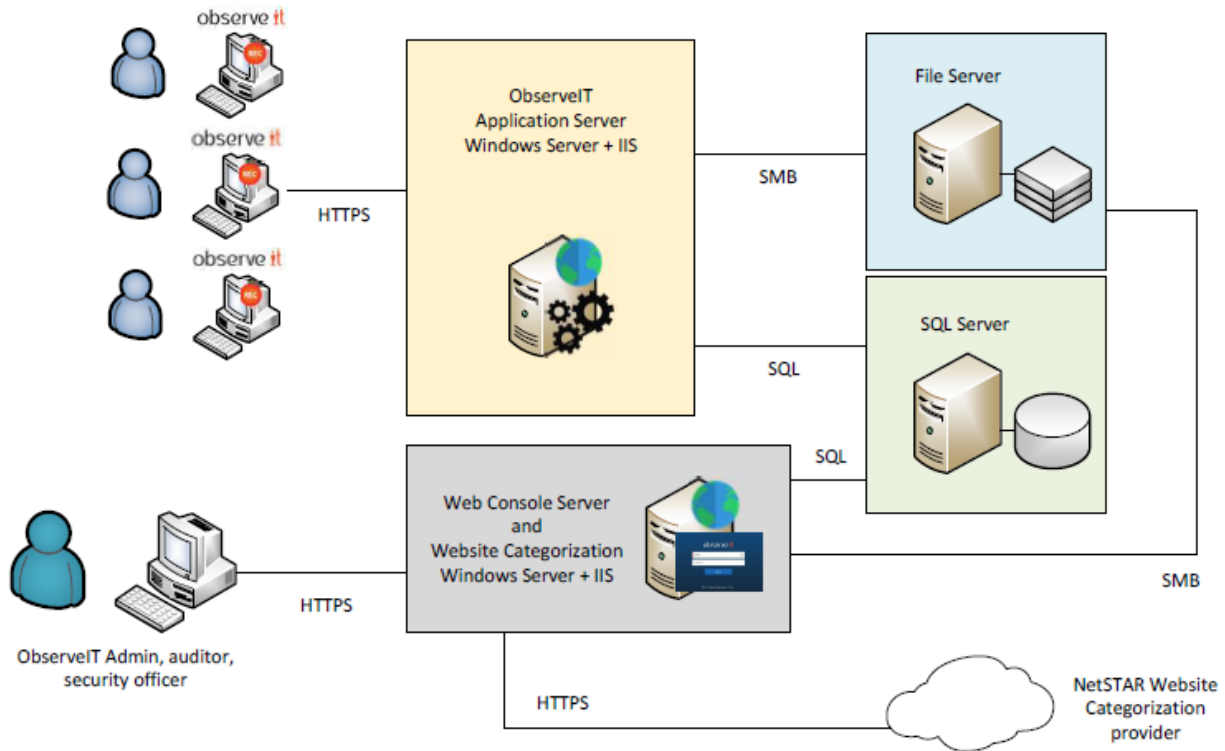
The diagram below is an example of an All-in-One installation with a single platform.



Small Scale Installation

In this example of a Small Scale installation, a separate SQL Database Server is used. All web back-end components, including the Application Server, the Web Console and the Website Categorization module (if used) are on a single machine. The file share that is used to store the recorded images may also be located on the same machine. The SQL Database Server is used to store the database.

The diagram below is an example of a Small Scale installation with a separate SQL Database Server.



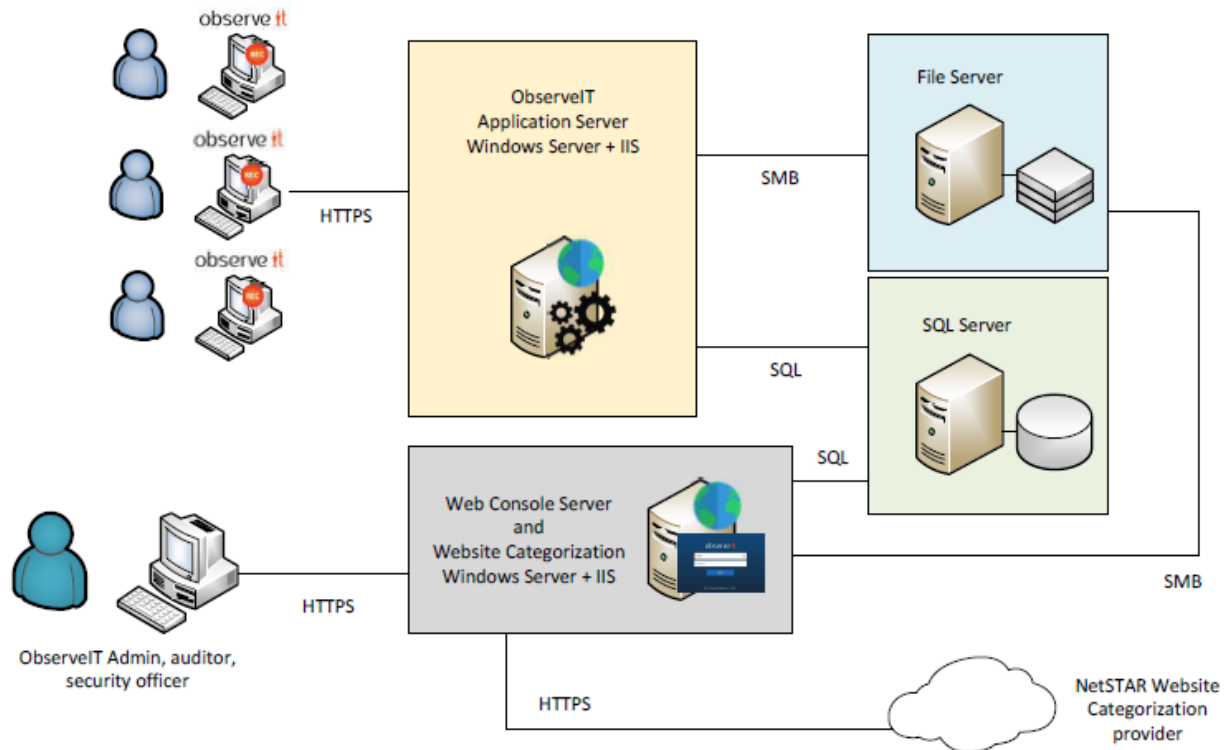
Medium Scale Installation

In a Medium Scale installation the web-based back-end components and roles of ObserveIT are deployed on 2 separate machines: Application Server is installed on the first machine and the Web Console. The Website Categorization module (if used) is on the second machine with the Web Console.

The SQL Server used to store the database is located on a separate and dedicated machine.

The file share used to store the recorded images is located on a dedicated file server machine.

The diagram below is an example of an Medium Scale Installation with 2 separate platforms.



Large Scale Installation with High Availability

This architecture fits large-scale installations and is the recommended production deployment architecture for most environments that require high availability (HA).

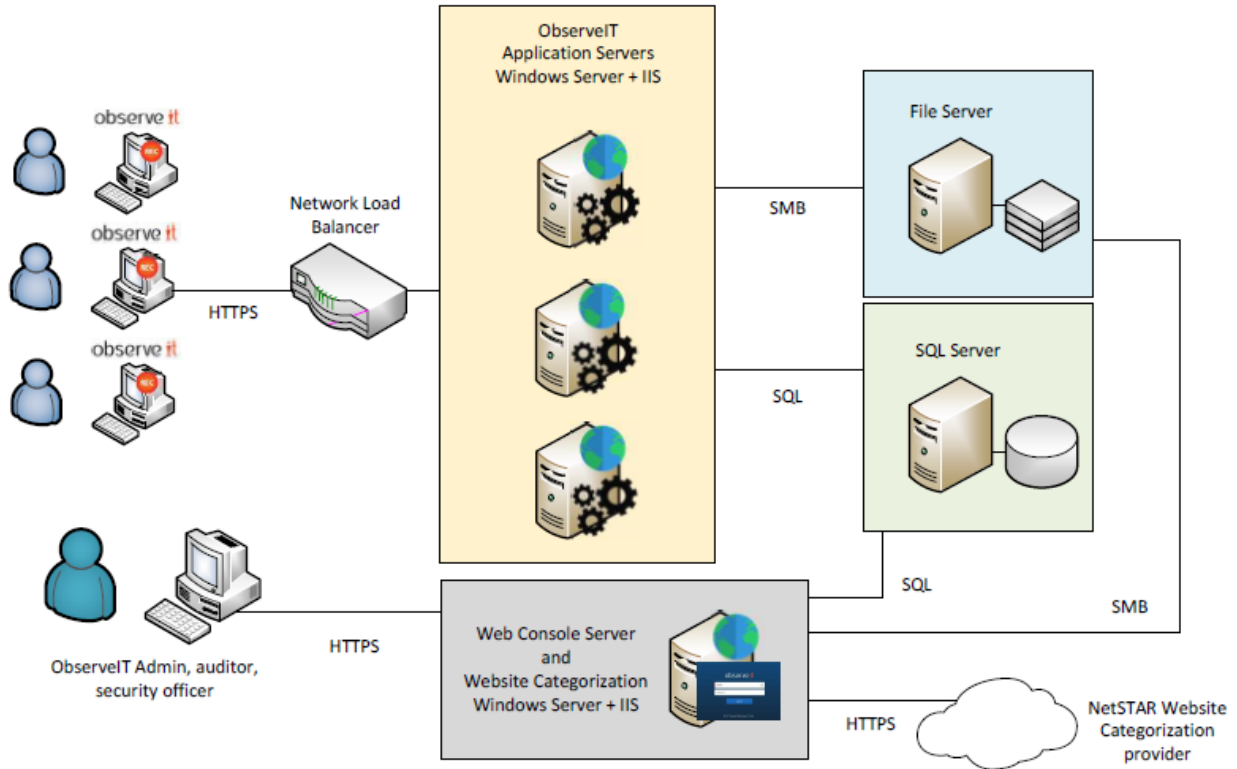
The Application Server is installed on several machines behind a network load balancer where additional Application Servers are added. The additional Application servers ensure that the expected load is distributed among remaining Application Servers in case one or more fail or are taken offline..

The Web Console and the Website Categorization module (if used) are installed on 2 separate machines, allowing high availability in case one of the machines fails or is taken offline.

The SQL Database Server used to store the database is located on a dedicated SQL Database Server Always On Availability Group, replicating the databases between the cluster members.

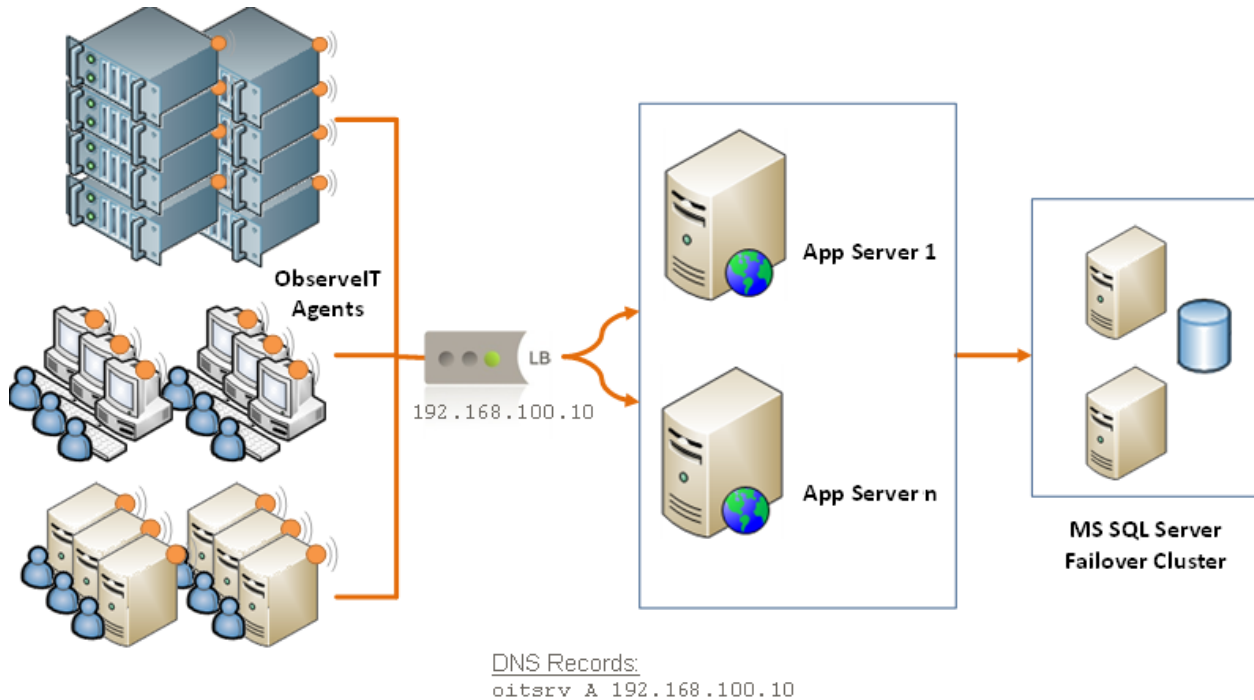
The file share used to store the recorded images is located on a dedicated file server (DFS) cluster or replicated to another server using other methods such as disk level replication or DFS.

The diagram below is an example of a Large Scale Installation with high availability.



Load Balancer Implementation

When full load balancing and high availability are required, you can use a software-based load balancer (such as Microsoft NLB) or hardware-based load balancer (such as F5). Optionally, this can be further augmented by a failover cluster for the Application Server with an active/passive cluster that has only one node operational at any given time. Also, more nodes can be added, as needed, to the failover cluster.



File System Storage

To improve performance of the MS SQL Server, it is sometimes recommended to use ObservelT's file system storage capabilities. In this Installation, the SQL Server is still used for user activity log and configuration data, but the actual screenshot images are stored in a file system directory structure, which is fully managed by ObservelT.

Large Scale Installations with Multiple Sites

This architecture fits large-scale deployments that also has one or more remote sites or branch offices where recorded endpoints reside.

Remote sites or branch offices are connected using a site-to-site VPN tunnel to the main office or datacenter.

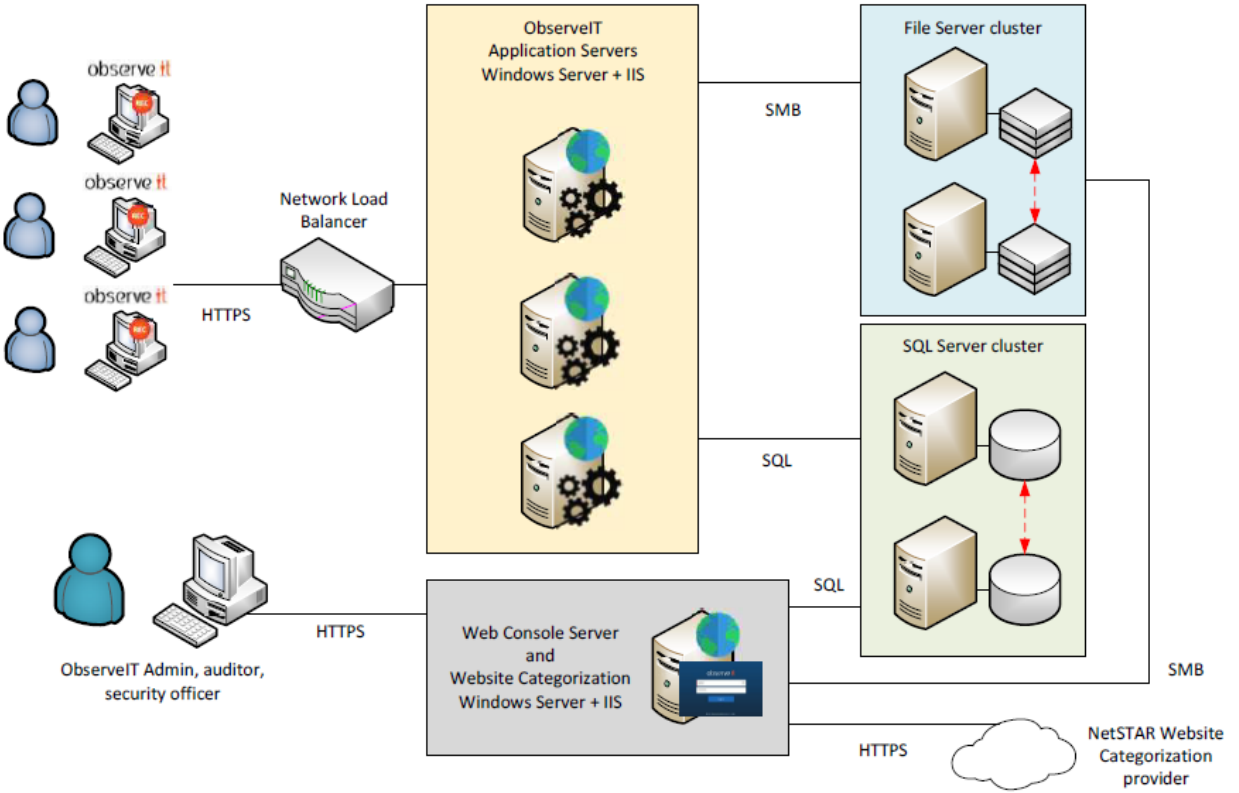
The Application Server is installed on several machines behind a network load balancer, where an additional Application Servers are added.

The Web Console and the Website Categorization Module (if used) are installed on a separate machine.

The SQL Database Server is located on a separate and dedicated machine.

The file share used to store the recorded images is located on a dedicated file server machine.

The diagram below is an example of a large scale installation with multiple sites.



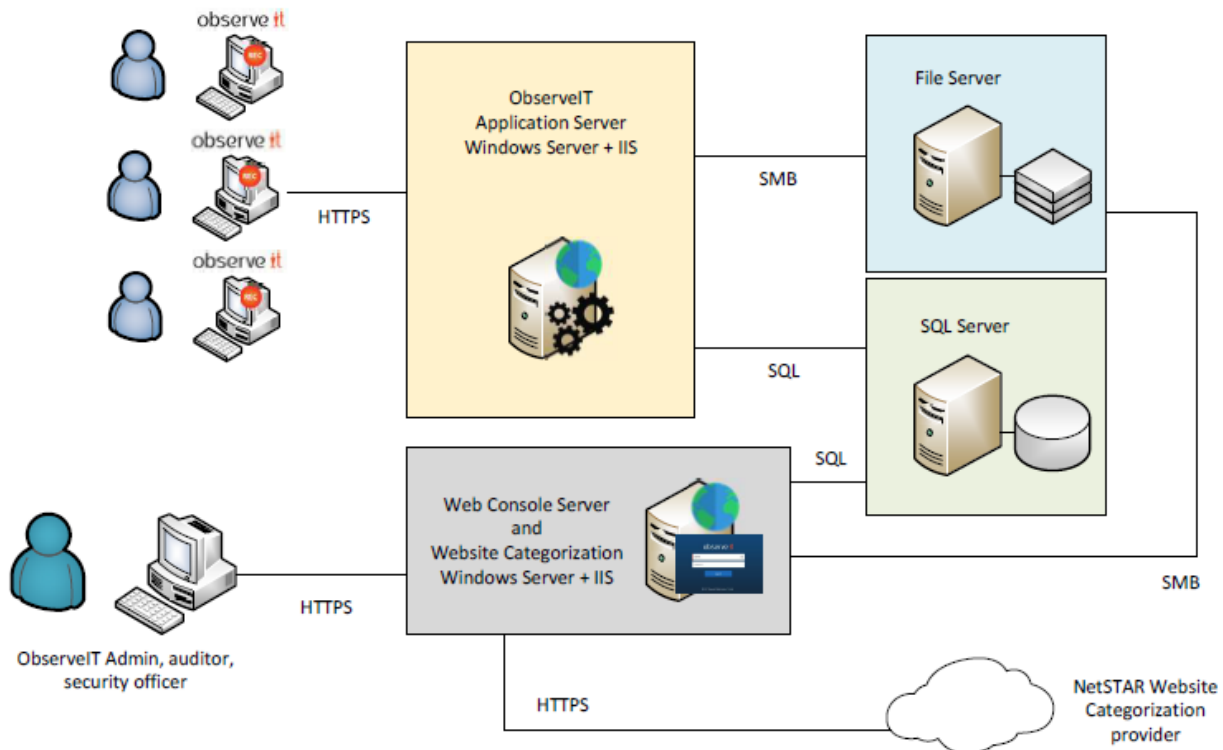
Deployment Scenarios

ObserveIT can be deployed in several different ways. The different methods are not mutually-exclusive, allowing for a hybrid deployment when required.

Standard Agent-Based Deployment (Servers and Desktops)

The standard method of deployment involves deploying the ObserveIT Agent on each machine to be monitored.

An Agent is installed on each machine that is being monitored, which captures activity on the machine and feeds the video/log data to the Application Server.



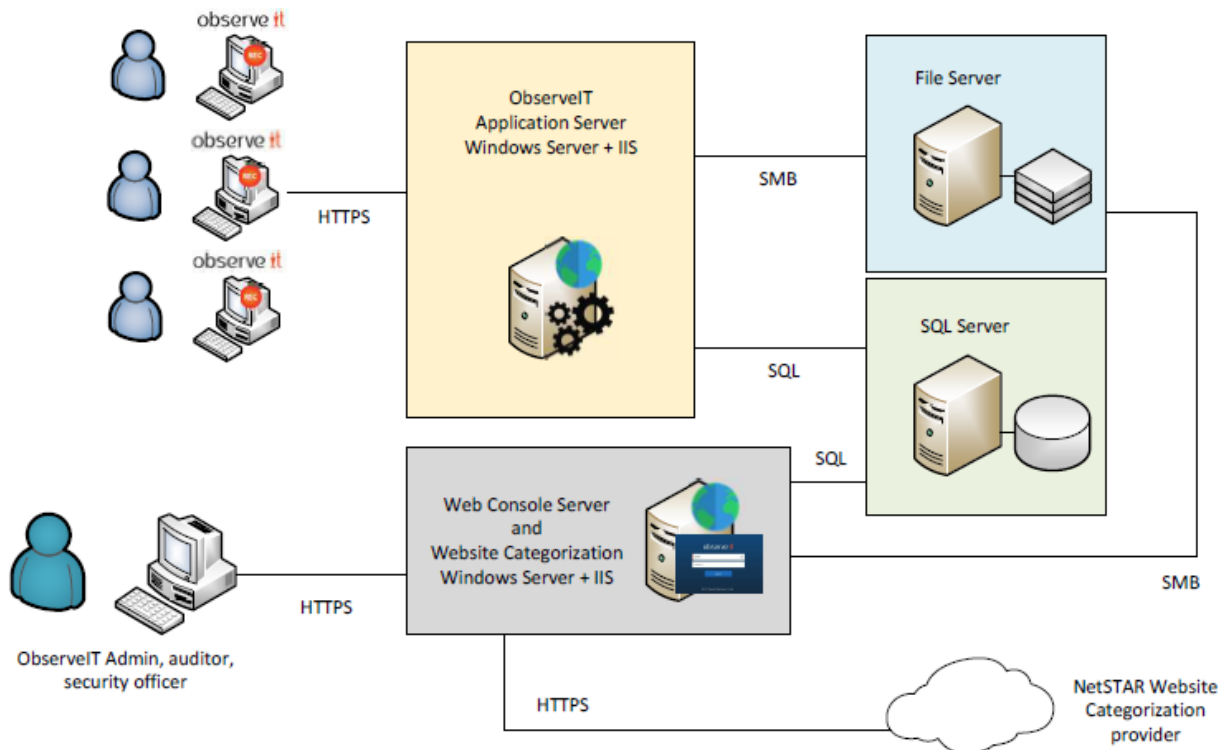
Jump Server Gateway

The Jump Server (Terminal Server) Gateway deployment is the ideal solution for logging all user configuration changes on remote network devices, servers, desktops and DB servers. In this topology, the ObserveIT Agent is deployed only on a gateway machine; only one Agent is required for recording all sessions. Users are routed via the gateway,

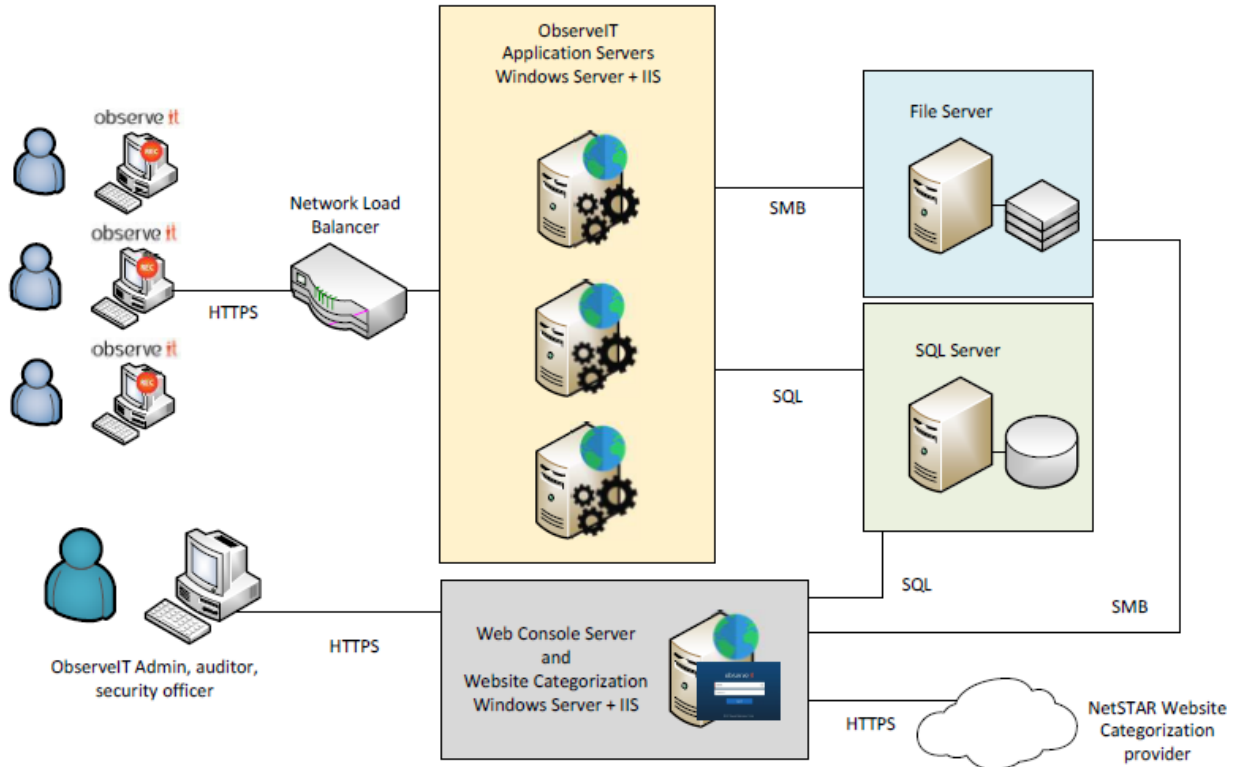
and ObserveIT records all user sessions in which the user connects to another target machine via RDP, SSH or other protocol. Client applications (such as, Microsoft SQL Server Management Studio, browsers, and others) are recorded with full user activity log analysis on the gateway.

In this deployment, ObserveIT does not record any user session in which a user logs on directly to a target machine (via local console login, or via a direct RDP/SSH/etc. window) that is not routed via a gateway. The volume of user activity log data captured is less than for the full Agent deployment because the ObserveIT Agent on the gateway does not have access to OS-specific information on the target machine. For example, it cannot detect the name of a file opened within an RDP window.

The figure below shows the Terminal Server Gateway (Jump server) deployment.



The figure below shows the Linux Gateway (Jump server) deployment.

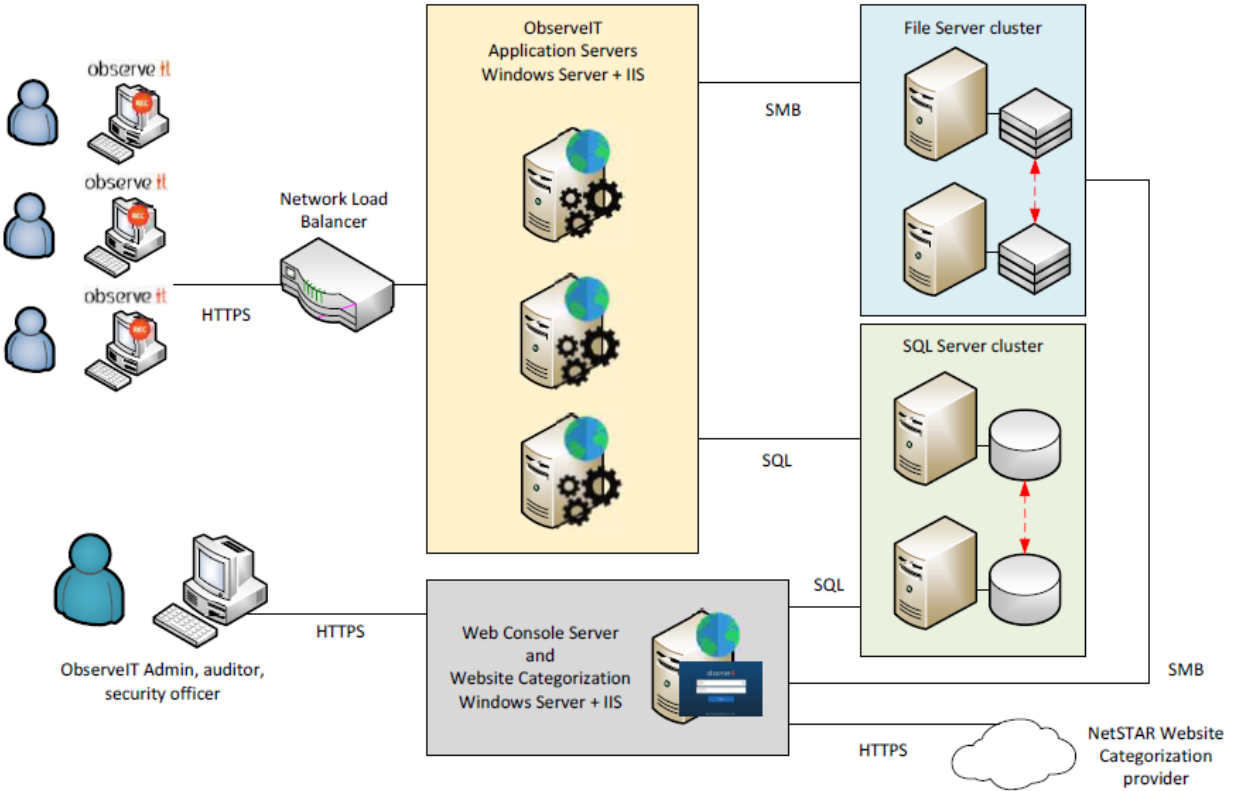


Outbound Jump Server Gateway

The Jump Server Gateway topology described above can also be used for environments in which remote users need to access multiple external resources. For example, a Managed Services Provider that needs to support multiple customers and wants to record and audit all the actions performed by the support employees.

The topology is essentially the same as for the Jump Server Gateway; the only difference is the location of each resource – that is, the Terminal Server is not on the same network as the target machines.

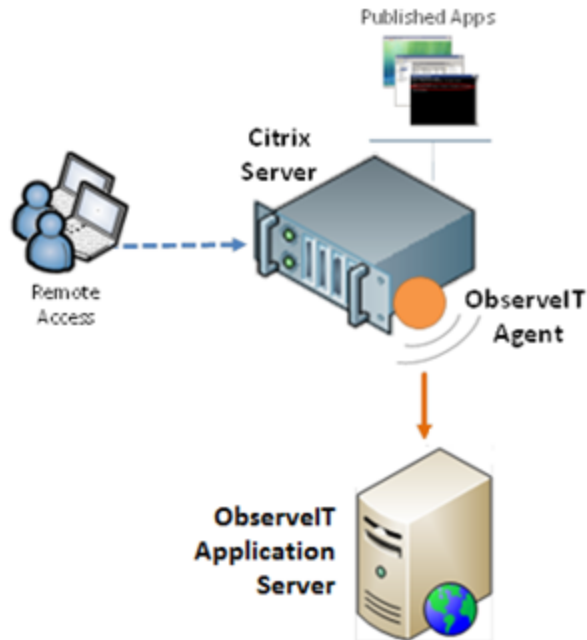
The diagram below shows the outbound Jump server.



Citrix Server for Published Applications

The ObserveIT Agent can be deployed on a Citrix Server in order to record all activities that take place within Published Applications served by the Citrix machine.

The figure below shows the Citrix server deployment.



Hybrid Deployment - Agent Based and Gateway

The Hybrid topology is the most commonly-used ObserveIT deployment because it allows you to simultaneously deploy any combination of the above topologies.

Any remote or local user can be routed via a gateway. This enables ObserveIT to capture and record every outbound session which can be replayed at any time. Agents can also be deployed on specific sensitive endpoints that require a more detailed audit, including any logins performed by privileged users with direct access to the endpoints. ObserveIT provides full user activity log data analysis and recorded video of all user actions that take place on sensitive endpoints – upon which Agents are installed – for which privileged users have direct access (and can therefore bypass the gateway).

ObserveIT Custom Installation

In a custom installation, each of the ObserveIT components can be installed separately and you can distribute the components and use advanced configuration options as needed. This is the most common type of installation.

Custom Installation is useful in environments with higher security procedures, requiring each component of the ObserveIT product to be installed separately and using dedicated service accounts; or in large-scale environments requiring custom modifications of some of the server-side components.

Agent Auto Upgrade

The Agent Auto Upgrade lets you upgrade Agents directly from the ObserveIT Web Console. Upgrading with Agent Auto Upgrade is simple. You have control over which endpoints to upgrade and when to schedule the upgrade. So when a new version of ObserveIT is released, you can easily trigger upgrades and start taking advantage of the new features.

From 7.9, Agent Auto Upgrade is available for Windows Agents only. You can use Agent Auto Upgrade to upgrade Agents from 7.1 and up.

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.

Agent Auto Upgrade supports rollback in case of failure after a number of attempts. So, if an upgrade is not successful, the previous Agent continues monitoring the endpoint. For example, if you were trying to upgrade from version 7.8 to version 7.9 and the upgrade failed, the Agent 7.8 would continue to monitor the endpoint.

Updater

The Updater is the component that manages the Agent upgrade. An Updater is installed on every endpoint.

The Updater continuously communicates with the Application Server so it knows when to update the endpoint according to settings you configure. The Updater is aware of the OS type, Agent version and bit processor, so it knows the correct upgrade version to download.

Upgrade Sets

An Upgrade Set includes the endpoints you want to upgrade and when you want that to happen. You can monitor the status of endpoints in the Upgrade Set. For example, you can review how many endpoints in the Upgrade Set have been successfully/unsuccessfully upgraded.

Endpoint Upgrade Status

You can view the upgrade progress for each endpoint. This way you know which endpoints have successfully updated, which have not and why not. In addition, you can view the upgrade history for each endpoint.

Key Configuration Settings

This section describes some settings you can use to configure the application as required by your design criteria and operational needs.

ObserveIT Web Console Users

ObserveIT administrators are also known as Console Users. Console Users can log on to the ObserveIT Web Console and view recorded sessions and other information, as well as make configuration changes based upon their role.

- The **Admin** role has the highest permissions with full control over all the management features of ObserveIT. An Administrator can make changes to the ObserveIT configuration, and is allowed to view all session recordings. This is the default role.
- The **View-Only Admin** role can view session recordings, but does not have access to ObserveIT configuration options.
- The **Config Admin** role allows administrative access to the Web Console without the ability to review user activity logs or screen recordings. Config Admin users can access specific configuration areas, and can manage other Config Admin user accounts.
- **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**.

Different levels of access can be defined for specific users or user groups. Console users can be granted permissions to view recorded sessions on one or more endpoints (on which the ObserveIT Agent is installed), endpoint groups, individual users (domain\user), or Active Directory groups. These permissions are given to users based on their defined role.

Console Users

Console Users

Create User Add AD Group

1 - 1 of 1

Name	Reports	Authentication	Permissions	Role	Create Date	Delete
Admin	Reports	ObserveIT.Authentication		Admin	4/14/2019	

SMTP Configuration

SMTP configuration enables ObserveIT to send messages and scheduled reports to Console Users.

SMTP Settings

SMTP Settings

SMTP Server Port

Mail From

User Name

Password

Please enter a valid email address for the settings verification message.

Email Address

LDAP and Active Directory Configuration

LDAP integration is commonly used for secondary user authentication.

By configuring an LDAP connection between the Application and Web Console components and an external LDAP server (such as, a Microsoft-based Active Directory Domain Controller), you can utilize user/group accounts from within an Active Directory domain, obtain access to the ObserveIT Web Console, and provide users with credentials

for ObserveIT Identification Services. Secured SSL communication to Active Directory via LDAP (LDAPS) can be configured to encrypt all communication via Active Directory.

LDAP Settings

Authentication Configuration

Automatic LDAP Target

Note: Clicking the "Detect Domain Controller" button will first detect whether the ObserveIT Application Server belongs to an Active Directory domain. If true, an automatic-type LDAP path will be added to the LDAP list below. Only automatic-type ("Auto") domains can be used for Active Directory Groups.

Manual LDAP Target

Manual LDAP targets can be used to authenticate users for 2 purposes: Console Users and Identification Services.

Type the correct LDAP path by using the following example:
LDAP://Domain_Controller_Name_or_IP/DC=Domain_Name,DC=Suffix

For example, if your Domain Controller name is OBS-DC1, and your domain name is OBSERVEIT-SYS.LOCAL, then use the following LDAP path:
LDAP://OBS-DC1/DC=OBSERVEIT-SYS,DC=LOCAL

Note: If no name resolution is possible, you might need to enter the Domain Controller IP address instead.

LDAP Path

Enter user credentials to verify the LDAP path

User Name

Password

LDAP Properties

LDAP mail field name

LDAP Targets List

LDAP Path	Domain Name	User Name	Alias	Type	Created Date	
LDAP://DC=TSTA,DC=LOCAL	TSTA.LOCAL	ObserveITApp	TSTA	Auto	4/14/2019	Delete

Configuring Recording Policy Settings

ObserveIT endpoints (or Agents) are configured by using Recording Policies, which are sets of configuration options that control aspects of how a monitored endpoint is configured. By using Recording Policies, the task of configuration is simplified since the administrator can configure one set of recording settings, and apply these settings to many monitored endpoints simultaneously. By default, all endpoints are automatically configured by one of the default Recording Policy Templates.

Recording Policy Endpoints

To see the endpoints linked to a Recording Policy template, click **Linked Endpoint** in the **Recording Policy Template** page. From here you can add, remove and review the endpoints for the recording policy.




Default Windows-based Policy - Servers

[Back to Recording Policy Templates](#)

Add Endpoints

Add Endpoints from Group

1 - 3 of 3

Endpoint Name	Version	Status	Date	
 OIT-OREL-LAP	7.11.0.41	Active	10/15/2020	Remove
 7K5TK13	7.11.0.35	Active	10/11/2020	Remove
 W19-S19-D04	7.11.0.35	Active	10/8/2020	Remove

Recording Policy Settings

Policy settings include:

- Enabling Agent Recording
- Enabling Identity Theft Detection
- Enabling Agent API
- Restricting Recording to RDP Sessions
- Enabling Email Monitoring Sessions
- Enabling Key Logging
- Enabling In-App Elements Detection
- Enabling File Activity Monitoring
- Enabling Entire Screen Capture
- Optimizing Screen Capture Data Size
- Enabling Recording Notification
- Recording in Color or Grayscale
- Setting Session Timeout
- Setting Keyboard Stroke Recording Frequency
- Setting Continuous Recording
- Enabling Live and Lock Messages from the Video Replay
- Data Recording Policy

- Offline Recording Policy
- Stealth and Privacy Policy
- Data Loss Detection Policy
- Identification Policy (Secondary User Identification/PIM)
- User Recording Policy
- Application Recording Policy
- Non-Interactive Programs Recording Policy
- Agent Logging and Debugging
- Memory Management

Configuring Alert Rules

Alert and prevent rules define the conditions under which an alert will be triggered. Alert and prevent rules help to:

- Increase security awareness through user education and policy notifications
- Prevent unauthorized and malicious activity via policy enforcement
- Detect known patterns of risky behavior using the built-in Insider Threat Library rules
- Provide dynamic forensic video for high risk activity

For each rule, you can specify a detection policy that defines the conditions that will trigger an alert, and specify additional actions to be taken when the alert is triggered. User warning notifications and blocking messages notify users in real-time about any out-of-policy behavior, enabling users to think again before performing a negligent or malicious action. Users can acknowledge a message, add a comment explaining their actions, and follow a link to view the company policy. If required, the security administrator can also select an action that will start recording a user when a security violation is detected.

Alert & Prevent Rules Notification Policies Settings

Create Alert Rule

Alert Rule Details

Name:

Description:

Category: Click [Change](#) to select or add a Category [Change](#)

OS type:

Notification policy: + -

Status: Active Inactive

Risk level:

Alert frequency: + -

Significantly affects risk score!

RULE ASSIGNMENT

Enforce this rule on: The below user list All users

Note: this rule is not assigned to any user list and will not be triggered! It can be found by filtering by "None".

[Add User List](#)

DETECTION POLICY

Who?

Did What?

On Which Computer?

When?

From Which Client?

ACTION

No Action Warning Notification Blocking Message Start Video Recording Log Off Close Application

Defining Notification Policies for Alerts

Alert notification policies enable ObserveIT administrators to define the email notifications that will be created when an alert is generated. These policies define to whom and how often emails will be sent in the event of an alert. By using configurable policies for alert notifications, they can be easily edited (for example, by changing the email address) and applied to multiple alert or prevention rules. Every rule is associated with a single notification policy.

Assigning Rules to User Lists

User Lists enhance alert rule operations by enabling you to assign rules to Lists of users, such as Privileged Users, Everyday Users, Remote Vendors, Terminated Employees, Users in a Watch-List, Executives, Developers & DevOps.

Privileged Users and Everyday Users lists are prepopulated based on common Active Directory groups. These lists can be modified, and other lists can be easily created or populated by assigning them individual users or Active Directory groups.

ObserveIT also provides an external API Web Service for customizing and managing Lists outside of the Web Console.

Assigning Rules to User Lists

The ObserveIT Insider Threat Library contains rules that cover the most common scenarios of risky user activities that might generate alerts. These rules have built-in policy notifications that are designed to increase the security awareness of users, and reduce overall company risk. ObserveIT's Library of alert rules can be applied on Windows and Unix/Linux machines.

They are grouped according to security categories to help navigation and management.

Note: Alert rules in the Insider Threat Library are already grouped into Categories and assigned to relevant User Lists with appropriate risk levels.

Categorization facilitates the operation and maintenance of rules and enables them to be grouped within similar security topics. Alert rules can be assigned to security Categories (such as, Data Exfiltration, Hiding Information and Covering Tracks, Running Malicious Software, Performing Unauthorized Admin Tasks, and more) in order to help navigation and facilitate rules operation and maintenance and enables rules to be grouped within similar security topics.

Exporting and Importing Rules


ObserveIT allows the importing and exporting of rules. Importing is managed by a wizard that notifies you in advance about any potential conflict or missing data on the target environment. Exporting rules is done by selecting the rules you wish to export and providing the location for the export file.

The ability to export and import alert and prevention rules extends ObserveIT's Insider Threat Solution, by enabling the sharing of real-time information about risky user activity and out-of-policy behavior with other departments/users in an organization and with other organizations. ObserveIT customers and business partners can use the exported/imported ObserveIT alert and prevention rules to detect risky user activity and out-of-policy behavior on their own Windows or Unix/Linux machines.

System Rules that were exported from the ObserveIT Insider Threat Library (ITL) can also be imported. After the export/import process is completed, the rules can be edited as required to suit the needs of the organization.

Alert, policy, and prevent rules can be easily migrated between staging or other environments (such as, from POC to UAT to Production). Rules can be integrated with external HR systems; ObserveIT User Lists can be exported and imported as a comma-delimited format file (CSV), so for example, you can simply export your current "Employee watch-list" from your HR system and import it into your list in ObserveIT.

Ongoing Alerts Tuning

Ongoing Alerts Tuning provides a simple way to fine-tune alert rules. You can quickly make adjustments when you come across an alert that has been triggered inaccurately. False positive alerts may clutter your Alerts list with information you don't need, causing you to miss important alerts. By clicking on the **Tuning**  icon next to an alert, you can easily make the adjustments you want and make sure the Alert rule is more accurate in the future and delete or change status of alerts already-triggered.

Implementing Lists in ObserveIT

ObserveIT allows the implementation of Lists which enable you to configure and operate alert rules more efficiently.

Using Lists enhances alert rule operations by enabling you to:

- Assign alert rules to specific users or and Active Directory groups. In this way, irrelevant "noise" is removed for other users for whom the alerts are not relevant.
- Apply the same List of users to different alert rules.
- Speed up the configuration of a long list of items by assigning them to a List.
- Easily locate and identify Lists for updating their content.
- Integrate with external HR systems. You can populate the content of a user List by importing a file of users that was exported from an HR System.

You can define the following types of Lists:

- **General:** for free text items. For example, "Keywords in sensitive file names" (this would contain a list of keywords that define sensitive file names or file extensions).
- **Users:** for users and Active Directory groups, with an option to exclude specific ones.

- **Public lists:** content can be viewed and edited by all Web Console users who have access to the ObserveIT configuration.
- **Private lists:** content can be viewed and edited (or deleted) only by the last Console User that defined the list as Private. Even Admin role users cannot view or edit the content unless they made the list Private.

ObserveIT provides a comprehensive library of alert rules configured to handle Insider Threat. These alert rules are already assigned to the relevant system-configured user lists.

Security and Privacy Infrastructure

ObserveIT is a highly-secure, enterprise-class platform designed for full reliability and non-repudiation.

Windows Agent Security

The Windows Agent is protected by a multi-layered “watchdog” mechanism that continuously monitors the recording Agent. If the Agent process is unexpectedly stopped, the watchdog immediately restarts it and reports the incident to the Application Server. If configured, the event is also reported to a SIEM system and/or an email address.

ObserveIT detects any Agent files or offline data that has been tampered with or has incurred data loss, and generates events which can be viewed in the Web Console and Administrator Dashboard. These events can also be sent to an email address and/or to an integrated SIEM system.

Mac Agent Security

The MAC Agent is protected by the OS launchd service that continuously monitors the recording Agent. If the Agent process is unexpectedly stopped, the OS immediately restarts it and the Agent continue running.

ObserveIT detects any Agent files or offline data that has been tampered with or has incurred data loss, and generates events which can be viewed in the Web Console and Administrator Dashboard. These events can also be sent to an email address and/or to an integrated SIEM system.

Unix/Linux Agent Security

The ObserveIT watchdog mechanism also continuously monitors the Unix/Linux Agent. The Unix/Linux Agent hooks to the terminal device and to the user shell. Thus, if there is any attempt to stop/kill the Agent logger process, the watchdog will immediately report the incident and terminate the shell process.

Tampering with Unix/Linux Agent files or offline data also generates events which can be viewed in the Web Console and Administrator Dashboard.

Data Security in Transit

Communication between the ObserveIT components is handled over the HTTP protocol.

SSL (Secure Sockets Layer) or TLS (Transport Layer Security) encryption protocols are fully supported for securing all HTTPS traffic between the client machine and the server running the ObserveIT Web Console.

If required, an IPSec tunnel can also be used to protect the Agent-to-Server traffic.


The figure below shows HTTPS and IPSec Security.














Data Security at Rest

Data that is stored in MS SQL Server automatically inherits all the data protection mechanisms already in place for corporate databases.

Additionally, ObserveIT will encrypt all screen recordings when the Image Security option is enabled. In this situation, the ObserveIT Agents and Application Server will use a token exchange mechanism to encrypt all session data. The recordings are digitally signed by the Application Server when stored in the database.

When ObserveIT detects any tampering with a session's data (for example, if a DBA deleted an incriminating screenshot from within the session recording), a warning indicator  appears for that session in the Web Console.

Session Duration	Login	User	Server	Client	Slides	Video
1/7/2015						
 2:17 PM - 2:45 PM	lili	n/a	 OIT-LILI	(local)	 515	
 11:53 AM - 11:54 AM	lili	n/a	 OIT-LILI	(local)	 Missing image data in session	
 11:42 AM - 11:48 AM	lili	n/a	 OIT-LILI	(local)	 77	

For privacy, all screen capture data (whether stored in an SQL database or in the file system) can be encrypted by a synchronous Rijndael 256-bit key. To further protect this key, the key itself can be encrypted by an asynchronous 1024-bit X509 certificate (with RSA encryption key). This encryption is also inherited by any sessions exported for offline viewing.

Note: ObserveIT Agents are FIPS (Federal Information Processing Standards) compliant. Both Windows and Unix/Linux Agents comply with the FIPS security standard and can be deployed on any supported FIPS-enabled machine. The TLS encryption protocol is used to secure traffic between the ObserveIT Agents and the ObserveIT Application Server.

Installation Security

The ObserveIT administrator can protect against improper or unauthorized Agent installation by requiring the person installing or uninstalling any Agent to provide a security password, which is registered on the Application Server. Requiring a password to install Agents prevents the unauthorized recording of computers and the unauthorized consumption of ObserveIT licenses. By enforcing a password also on uninstallation of an Agent, the unauthorized removal of a computer from ObserveIT's list of recorded machines is prevented.

The main ObserveIT Administrator Dashboard and mini Administrator Dashboard display the number of Agents that were recently installed and uninstalled. In addition, if configured, notifications via email can report successful or failed installation/uninstallation events due to security password enforcement.

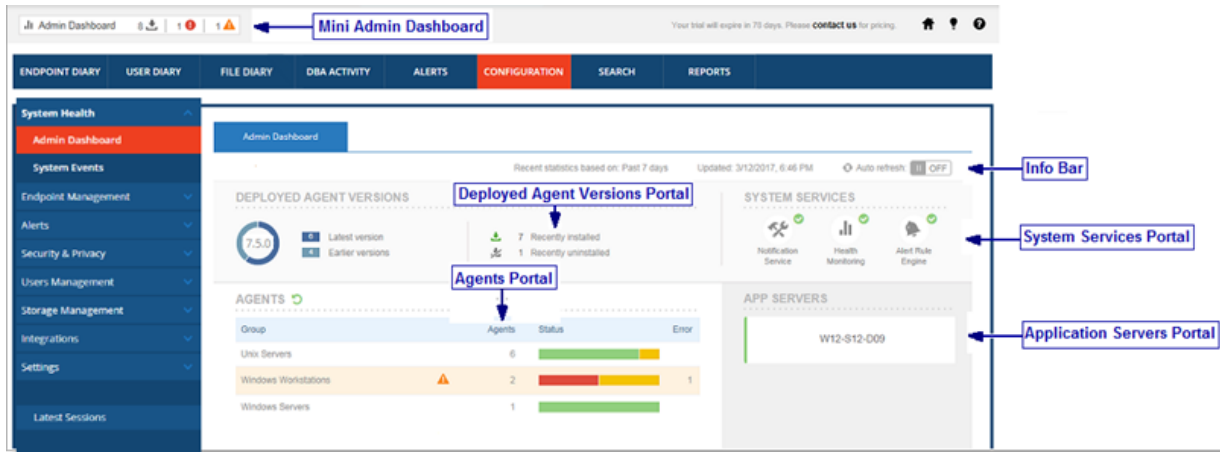
System Health Monitoring

ObserveIT provides comprehensive monitoring of all system components, providing administrators with a high-level system health overview, along with drill-down capabilities to quickly investigate any issues. An Administrative Dashboard presents administrators with graphical summaries of the operational statuses of installed ObserveIT Agents and Infrastructure, enabling you to see at-a-glance any issues requiring attention, such as communication faults, data loss, dwindling disk space or Agent tampering. Most Dashboard elements can be clicked to drill down into the details of that element.

The **Admin Dashboard** provides graphical summaries of the operational statuses of installed ObserveIT Agents and infrastructure (Application Servers, and so on), and easy navigation to drill down and perform root-cause analysis and corrective action. The **Admin Dashboard** enables you to see at-a-glance all the active Agents that are currently

installed. ObserveIT administrators can quickly identify events and statuses across the system and respond accordingly. Operational statuses and system events are color-coded according to severity (for example, "red" is the highest severity which might require immediate attention). Every change on a local Agent triggers a system event. Events that are "normal" (with **OK** status) would probably not require attention (for example, when the Agent service is started).

A **mini Admin Dashboard** (located at the upper left part of the Web Console) is viewable from every page in the Web Console. It provides a quick preview of the Agents' operational statuses and quick access to the full **Admin Dashboard**.



Data Management

This section describes ObserveIT data management.

ObserveIT Database Structure

By default, ObserveIT utilizes the following databases, which are created during installation:

- **ObserveIT:** Stores all the configuration data and all the user activity metadata captured by the ObserveIT Agents.
- **ObserveIT_Analytics:** Stores the data that is displayed in the **Insider Threat Intelligence** dashboard. This includes alerts statistics and users' score data over time, aggregated by users, applications and alert types. It also stores user profile information, such as, job title, photo, department, region, email address, and so on.
- **ObserveIT_Data:** Stores all the ObserveIT screenshot images captured by the ObserveIT Agents (by default). Screenshot images can also be stored in the file-system (for example, for large deployments).
- **ObserveIT_Archive_1:** The archive storage database stores both the archived user activity metadata and screenshot images (unless file-system storage is configured). If the archive database size reaches its maximum allocated storage, you can create a new archive database (**ObserveIT_Archive_2**, and so on.)
- **ObserveIT_Archive_template:** Template that is used for backup and restore when creating a new archive database.

Database Storage

SQL Server databases store configuration data, user analytics data, textual audit metadata and optionally (unless the file-system is used) screenshots captured by ObserveIT Agents for video replay. To prevent data loss as the database becomes full, ObserveIT enables you to configure additional storage space. You can configure a threshold (as a percentage of allocated disk space) specifying the maximum disk space that is allocated for the database. A system event is generated when the database storage threshold (%) reaches its configured limit, alerting you to configure additional storage space by updating the specified threshold or by running the archive process. Archiving older data frees up storage for more recent data.

File System Storage

In large scale deployments or when the SQL Server database has performance issues, the file-system is the preferred method for storing screen capture data. Recorded screenshots can be stored either on the local hard drive of the ObserveIT Application Server, or on a file share in the network.

Visual screenshots represent the largest portion of ObserveIT's data storage needs. For large scale deployments and/or to prevent SQL Server database performance issues, you can configure the video replay screenshots for file-system storage instead of in the SQL database, either on the local hard drive of the ObserveIT Application Server or on a file share in the network. When using file-system storage, there is still a need to maintain the MS SQL Server database, in order to store the textual metadata and the ObserveIT configuration data.

ObserveIT automatically manages the directory where you specify that screenshot data should be stored, including an auto-generated and archived subdirectory tree per date and per session.

Metadata Storage

In addition to visually recording user activity on monitored servers, ObserveIT records important information about what is seen on the screen, which applications are currently used, what actions the user has performed, the date and time of the action, and more. This information, which is called "metadata", is stored in ObserveIT's database, which is located on a central SQL Server. Because metadata is centrally stored and indexed, it can be used to easily search throughout all recorded sessions, and provide a textual breakdown of each user session.

ObserveIT Data Integration

Integrating ObserveIT Data into 3rd-Party SIEM Systems

Integration lets you leverage ObserveIT data from your other systems.

You can load user session data to a SIEM such as Splunk, McAfee ESM, or IBM QRadar and build custom dashboards and reports. You can create visualizations from data including user and file activities, alerts, lists of applications run, and more - all linked directly to session recording.

With ObserveIT integrated into your SIEM or log management solutions, you can draw a clearer picture of exactly what happened before, during, and after an insider threat incident.

Packaged Integrations

ObserveIT and our partners have built a number of integrations and plugins that work right out of the box with many popular SIEMs and other tools.

These integrations provide security analysts and investigation teams with user activity metadata, smart user behavior alerts and user context to help identify and investigate Insider Threats and other user-based threats directly from within the App. Security teams can correlate ObserveIT metadata to create smarter alerts and stop threats before they happen.

Custom Integrations

You can use the following methods to integrate ObserveIT data:

- **ObserveIT Restful API:** This is the preferred method for building integrations. You can pull reports, update rule lists, start and stop recordings, and more. You can view the public API browser to explore available endpoints.
- **CEF Logs:** Use CEF logs to integrate with SIEMs or other log aggregation systems.

Integration using ObserveIT RESTful API

You can use the ObserveIT RESTful API to leverage your ObserveIT data and integrate with other systems, including log aggregation tools and SIEMs. The Splunk and QRadar integration apps are built using this method.

The ObserveIT API is the preferred method for building integrations. You can get a feed of the latest activities and alerts in ObserveIT as well as collect user activity profiles and update alert rule lists.

Integration using CEF Logs

ObserveIT CEF Logs let you integrate with SIEMs and other log aggregation systems.

Log files are integrated into the system. The SIEM integration parses the ObserveIT log files and create events, triggers, and alerts based on text strings of information that appear inside the log file. The log files are forwarded to the remote system and ingested. Many tools, such as LogRhythm and McAfee ESM, have built-in support or a plugin available for parsing these ObserveIT CEF files. Integrated log data can be viewed, and videos of recorded sessions can be replayed directly from within the external SIEM dashboard or report environment.

Integrating ObserveIT with a Service Desk System

The integration of ObserveIT's user activity monitoring solution with an IT Service Desk system provides additional layers of security and monitoring to your organization.

When ObserveIT's session recording system is integrated with a Service Desk system, selected IT administrators or remote vendors can be requested to enter a valid ticket number in order to complete the login process to a corporate server.

The benefits of integrating a Service Desk system with ObserveIT's session recording system include:

- Enforced segregation of duties.
- Improved security by limiting server access to administrators and remote vendors who are in possession of a specific ticket number for which access to the server is required.
- Improved tracking of sessions. You can search for all sessions that relate to a specific ticket's unique reference number instead of using search key words or looking through lists of sessions.
- Faster and easier user activity auditing. By linking tickets directly to the video recording of the server session that addressed the ticket, you can easily review the exact actions performed by administrators in the context of the ticket.

When an administrator or remote vendor attempts to log in to a monitored endpoint, a message is displayed requesting the user to enter a valid ticket number from a service desk system before they can log on to the endpoint.

Ticket Window - Enter a Valid Ticket Number

Message:
In order to log in to this server, you must enter a valid ticket number from the ServiceNow ticketing system.

Ticket Number:

I don't have a ticket number. Please create a new ticket and log me in.

Comment (max 500 characters):

Agent API for Integration

ObserveIT's Agent API enables external applications to build custom logic for what and when to record. The Agent API exposes a set of classes that enable:

- Start, Stop, Pause, Resume, and End a recorded session
- Custom logic for when to start recording (based on process ID, process name, computer name, user, URL, and more)
- System health check
- Viewing recorded sessions

Recording additional processes can be tied to existing sessions or to a new session, thus creating a separate session for each recorded process. The API is built in to the Agent but not enabled by default. It can be enabled from the ObserveIT Web Console.