Teramind UAM

User Activity Monitoring

Features Guide

Version 1.3 (13 MAY 2021)

Table of Contents

1 Teramind UAM Features Overview

Teramind's UAM (User Activity Monitoring) solution comes with everything essential you will need for employee monitoring, third-party/external user monitoring, insider threat detection, and workplace productivity optimization use cases. Click on the video link below for a quick overview of Teramind UAM and its featured.

Teramind UAM Overview Video Covers:

- Activity monitoring features such as Websites, Emails, Networks, etc.
- Behavioral baseline and anomaly rules
- How to configure Teramind UAM to comply with employee privacy
- Policies & rules overview
- Forensic investigation – session recording, snapshots, reports
- Risk analysis dashboard
- How third-party monitoring works
- Productivity tools features

2 Monitoring and Detection Capabilities

Teramind UAM monitors virtually all user activity for 12 system objects such as Website, Applications, Social Media, Instant Messengers, Searches, etc. The captured data is then presented on an enterprise-grade Business Intelligence (BI) dashboard. The BI tools allow you to customize, aggregate, or group data as you need and present them in visually engaging formats. Compare trends and data movement over time and view snapshots of key metrics and KPI at a glance or drill down for in-depth analysis or export them to other applications.

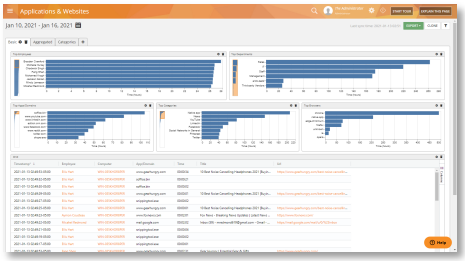
Privacy Friendly Monitoring

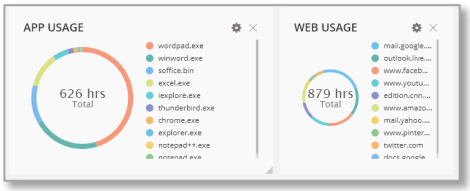
While Teramind can capture virtually all computer activity, you have complete control over privacy. Each monitored object supports monitoring profiles and granular settings to ensure user privacy. You can track as much or as little as you want based on your organization's needs and alleviate any privacy concerns. Built-in Access Control panel lets you configure what admins can view or edit eliminating privilege abuse.

On Teramind UAM, you can create behavioral rules based on user activities and work schedules. Then, receive real-time alerts and notifications when any rule is violated. Using the smart policy and rules engine, you can prevent data breaches and malicious or accidental insider threats with pre-emptive actions such as warning a user, blocking an action, or taking control over their computers at any time.

2.1 Applications & Websites

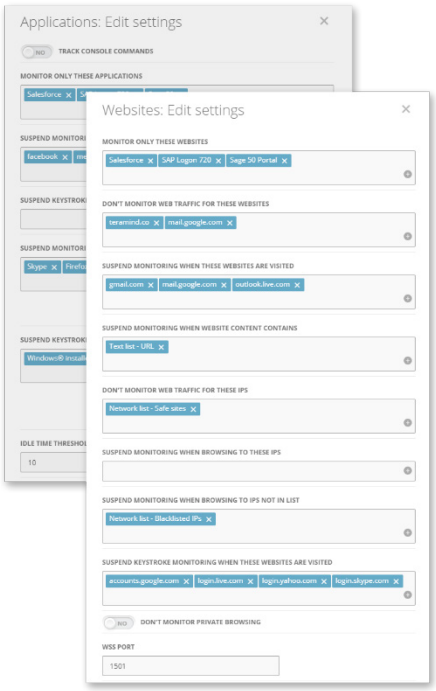
What report can I access for this activity?





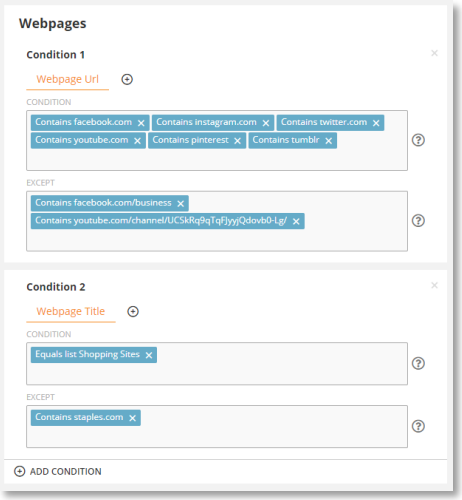
- You can view the timestamp, employee, computer, process/URL, usage duration, idle time, active time, app/webpage, title, etc.
- View top employees, departments, app/domain, categories, browsers, security categories, reputations, classification timeline, etc.
- Automatically classify apps and websites based on inCompass® NetSTAR technology.
- View individual items or aggregate and compare them in different ways.
- Filter the report by the employee, department, web/app, productive/unproductive, etc.
- Classify productive vs unproductive websites and applications.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



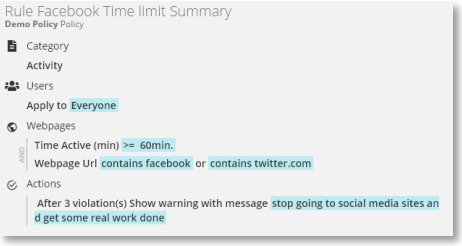
- Track all websites and applications and console commands. Or, you can configure the settings to monitor only select apps/websites.
- Monitor browser plugins and extensions.
- Suspend monitoring of keystrokes logging for certain applications/websites.
- Dynamically blackout screen recording when certain content is detected on a webpage. For example, when a user visits their bank's website or accesses a login page.
- You can suspend monitoring/keystrokes logging with extra conditions. For example, you can suspend monitoring Internet Explorer while it's used from an approved access control list (ACL).
- Option to monitor secure connections (HTTPS), SSH, and even private browsing sessions.
- Option to disable monitoring for password fields.
- Control the tracking of application idle time.

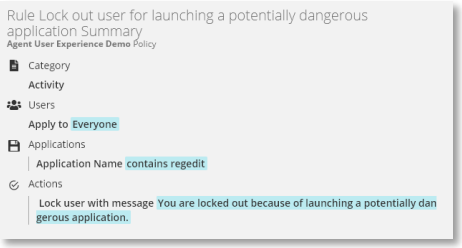
What rule and alert triggers can I use with this activity?



- On Teramind UAM, you can create Activity-based rules for the Websites and Browsers.
- For the Webpages, you can use the Webpage Title, URL, and Query Arguments (URL variables) as inputs for the rule conditions.
- For the Applications, you can use the Application Name, Application Caption, Time Active, Time Idle, etc., and detect if it's launched from a CLI (Command Line Interface).
- For the Browser Plugin, you can use the Plugin Name, Browser (i.e. IE, Firefox), Plugin Permission (i.e. Proxy VPN, Requests, User Data) as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc., and additionally a Redirect action for webpages.

What are some sample rules using this feature?





- Restrict access to non-whitelisted/unauthorized applications or websites but allow managers to override if needed.
- Detect and block when a dangerous application (e.g. Windows Registry Editor) is launched.
- Warn users when spending excessive time on social media or entertainment sites such as YouTube.
- Find out potential turnover by checking if employees are searching on job sites. Get notified if the time spent on such sites exceeds a threshold.

What are some useful resources for this feature?

- User Guide: BI Reports > Applications & Websites
- User Guide: Monitoring Settings > Applications Settings
- User Guide: Monitoring Settings > Websites Settings
- Rules Guide: Activity Rules > Applications
- Rules Guide: Activity Rules > Webpages

2.2 Browser

What report can I access for this activity?

No dedicated report

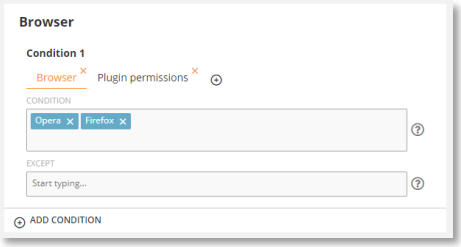
- Browser activities can be monitored under the Applications & Websites and other related BI reports (e.g. the Web File Events report shows details for all the uploads/downloads done through the browser).

What monitoring & tracking controls do I have?

No settings

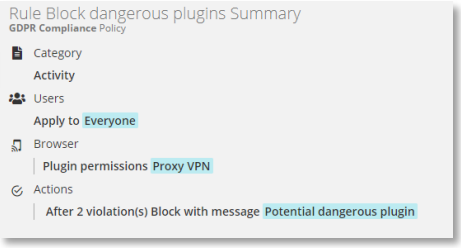
- Browser does not have a dedicated settings panel and is controlled under the Websites settings panel. Check out the Applications & Websites monitoring and tracking controls for more information.

What rule and alert triggers can I use with this activity?



- On Teramind UAM, you can create Activity-based rules for the Browser.
- You can detect specific browser name (e.g. Chrome), plugin name, and plugin permission (i.e. Proxy VPN, Requests, User Data) as inputs for the rule conditions.
- You can use Warn, Block, Notify, Lock Out User, Execute Windows Command rule Actions.

What are some sample rules using this feature?



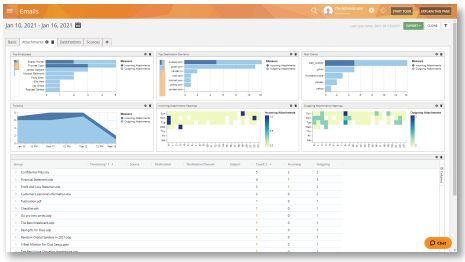
- Restrict use of certain browsers, e.g. old version of Internet Explorer.
- Block dangerous browser plugins and extensions to reduce the risk of malware infection or prevent a plugin from utilizing certain permissions such as the ability to access critical proxy settings or user data.

What are some useful resources for this feature?

- User Guide: BI Reports > Applications & Websites
- User Guide: Monitoring Settings > Websites Settings
- Rules Guide: Activity Rules > Browser

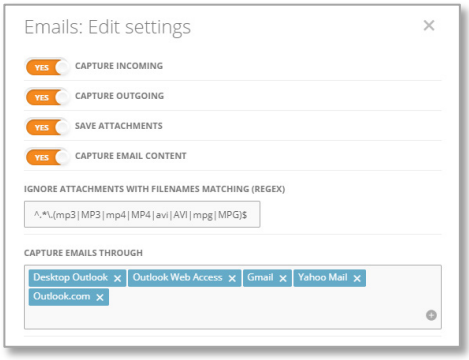
2.3 Email

What report can I access for this activity?



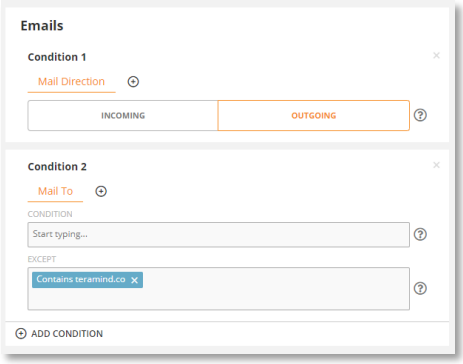
- View all emails and attachments being sent or received by employees and departments.
- View incoming/outgoing emails by timestamp, top employees/departments by no. of emails sent/received, attachment heatmaps, top domains, statistics for email sources, etc.
- Group email activities by the employee, departments, domain, source, etc. or compare trends such as outgoing vs. incoming emails.
- Save a copy of the email or attachments.
- Filter the report by the employee, department, computer, email direction, email client, etc.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



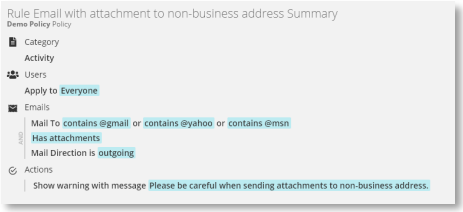
- You can select which emails to capture, incoming/outgoing, or both.
- You can decide if you want to capture the attachments or email content.
- You can use Regular Expressions (RegEx) to further filter or ignore any attachments you do not want to be captured. For example, video files.
- You can specify which email clients will be captured. Teramind supports popular clients such as Outlook, Gmail, Yahoo, etc. - both desktop and web versions.

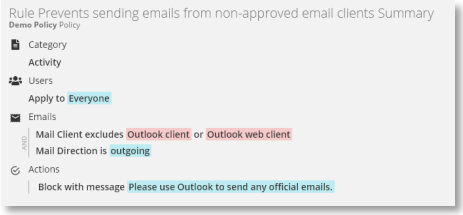
What rule and alert triggers can I use with this activity?



- On Teramind UAM, you can create Activity-based rules for the Emails.
- You can use the Mail Body, Subject, CC/To/From fields, Mail Direction, Mail Client, Mail Size fields and detect if the mail has any attachments as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc.

What are some sample rules using this feature?





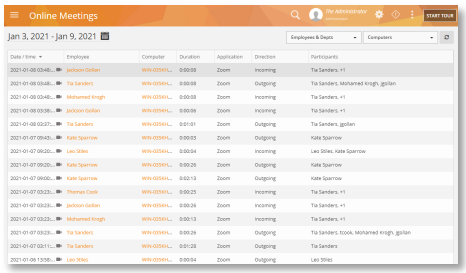
- Prevent attaching files from a certain location(s) such as local, network, or Cloud drives.
- Restrict sending work emails from personal email accounts.
- Prevent sending of attachments to non-business addresses.
- Detect if a competitor is contacting your employees or vice versa.
- Get notified if a user is sending emails with large attachments.

What are some useful resources for this feature?

- User Guide: BI Reports > Emails
- User Guide: Monitoring Settings > Emails Settings
- Rules Guide: Activity Rules > Emails

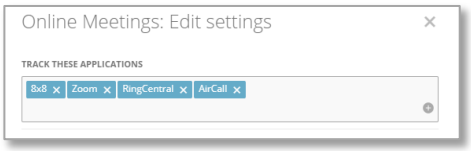
2.4 Online Meetings

What report can I access for this activity?



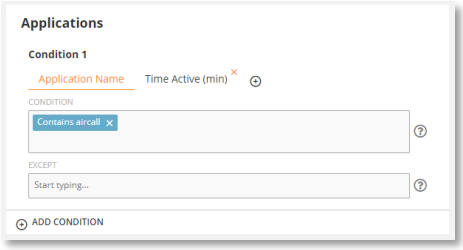
- Track online meeting activities for apps such as Zoom, AirCall, Microsoft Teams, etc.
- View employee/computer, when the meeting took place, duration, app, direction, participants, etc.
- Filter the report by the employee, department, computer, etc.
- Optionally, view and/or hear the meetings (check out the Audit & Forensics section to learn more).

What monitoring & tracking controls do I have?



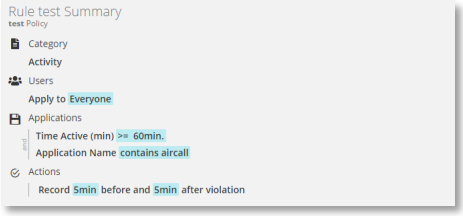
- You can select which online meeting applications to monitor such as, Zoom, Microsoft Teams, AirCall, etc.

What rule and alert triggers can I use with this activity?



- Online Meetings do not have dedicated rule triggers. However, you can use the Application category and use Activity-based rules for them.
- You can then use Warn, Block, Notify, Lock Out User, Execute Windows Command rule Actions.

What are some sample rules using this feature?



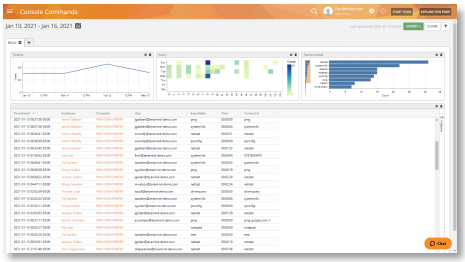
- Record the session if a user spending more than the allotted time for a meeting.
- Get notified if the total meeting duration during a day is greater than a certain value.
- Detect what files are being shared at a meeting.

What are some useful resources for this feature?

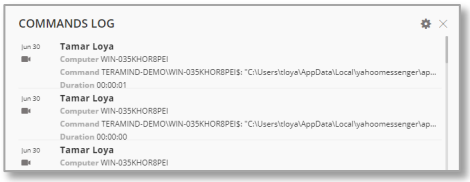
- User Guide: [Monitoring Reports > Online Meetings]
- User Guide: [Monitoring Settings > Online Meetings Settings]
- Rules Guide: [Activity Rules > Applications]

2.5 Console Commands

What report can I access for this activity?

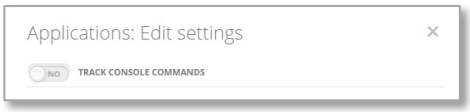


- Monitor any console commands executed by a user or an application from the command line.
- View date/time, employee, computer, username, PID (program ID), command heatmap by timeline, etc.
- Group activities by the employee, departments, app, etc. or compare trends such as top commands vs. top employees.
- Filter the report by the employee, department, computer, task, etc.



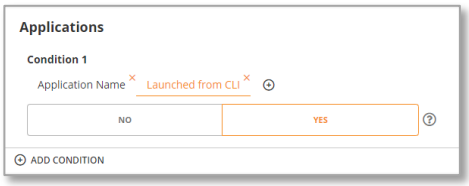
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



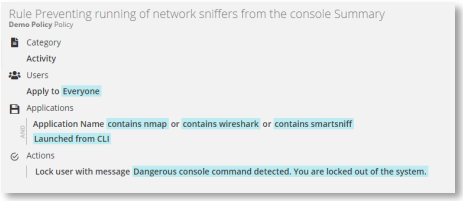
- Console commands are tracked as part of the Applications object and can be turned on/off from the Applications settings.

What rule and alert triggers can I use with this activity?



- Activity-based rules for console commands can be created under the Applications category and has the same capabilities as the application-based rules. For additional detection triggers, you can use the *Launched from CLI* condition.

What are some sample rules using this feature?



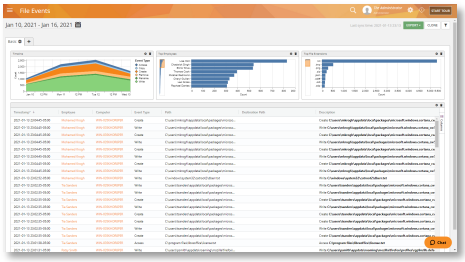
- Track privileged user activities for system-level applications.
- Block DOS commands such as *ren*, *del*, *attrib,* etc.
- Detect *ipconfig*, *nmap*, *WireShark,* or similar network scanning software.
- Prevent running of batch files and scripts.
- Block access to the command prompt entirely.

What are some useful resources for this feature?

- User Guide: BI Reports > Console Commands
- User Guide: Monitoring Settings > Applications Settings
- Rules Guide: Activity Rules > Applications

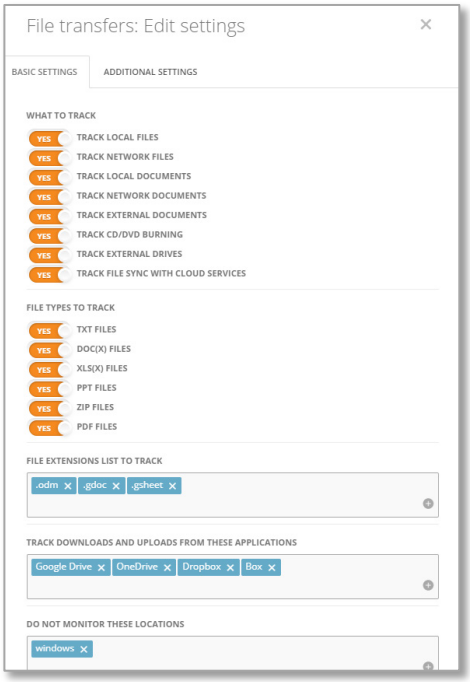
2.6 File Events

What report can I access for this activity?



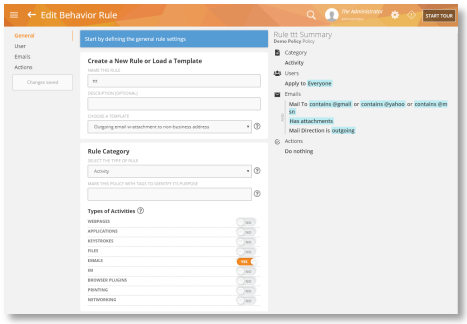
- View all file activities on the local, external, network, and cloud drives.
- View employee and computers for file actions (access, write, upload/download, etc.), source (i.e. local disk, network), the full path of the file, file name, extension, and what app initiated the file operation.
- Group by top employees/extensions or compare between two file activities such as Upload vs. Download.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



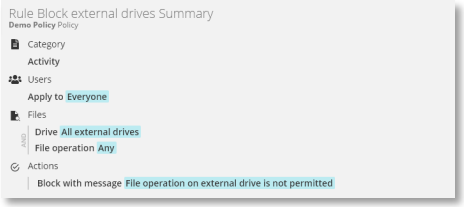
- You can specify what sources to track, such as local/network files, local/network documents, external documents, CD/DVD burning, external drives (i.e. USB / pen drives), etc.
- You can control which file types/extensions to track such as *doc*, *xls*, *ppt*.
- You can specify which applications should be monitored for upload/download activities.
- You can exclude select locations, folders, or drives from tracking.
- You can specify exactly what file operations to monitor, i.e. copy/move/upload/write.

What rule and alert triggers can I use with this activity?



- On Teramind UAM, you can create Activity-based rules for the File Transfers.
- You can use the File Operations such as access, write, rename, insert/eject), copy, upload/download, etc. as inputs for the rule conditions.
- Other conditions such as network host, file path, cloud provider, download file name, URL/size, etc. are available depending on which file operation is selected.

What are some sample rules using this feature?



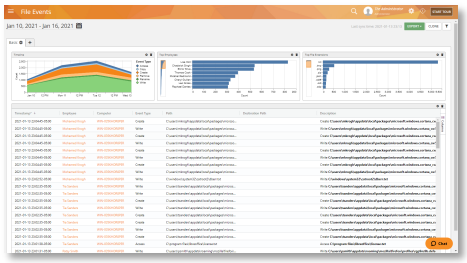
- Detect/block access to sensitive files.
- Make a folder or drive ready only, preventing any changes to the files in that folder.
- Get notified when files are uploaded to Cloud sharing sites such as Google Drive, DropBox, OneDrive, etc.
- Block files from being copied to/from removable media such as USB drives.
- Prevent changes of program settings or tampering with configuration files.
- Stop transfer of large files.

What are some useful resources for this feature?

- User Guide: BI Reports > File Events
- User Guide: Monitoring Settings > File Transfers Settings
- Rules Guide: Activity Rules > Files

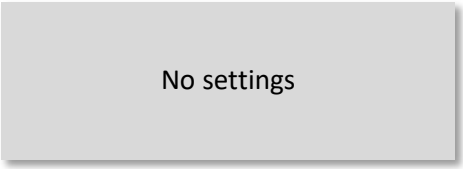
2.7 Web File Events

What report can I access for this activity?



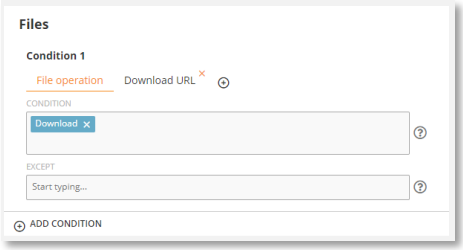
- View all web file events (upload/download, cloud sync, etc.).
- Group and compare events such as timeline (uploads vs. downloads), top employees, top domains, etc.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



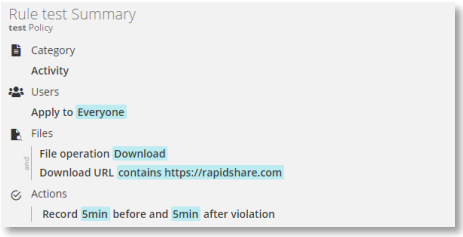
- Web File Events does not have a dedicated settings panel and controlled under the File Transfers and Websites settings panel to specify which URLs and files to track, when to track, etc. Check out the Applications & Websites and File Events monitoring and tracking controls for more information.

What rule and alert triggers can I use with this activity?



- Web File Events do not have dedicated rule triggers. However, you can use the Files category and use Activity-based rules to detect file transfer activities including web uploads/downloads.
- You can then use Warn, Block, Notify, Lock Out User, Execute Windows Command rule Actions.

What are some sample rules using this feature?



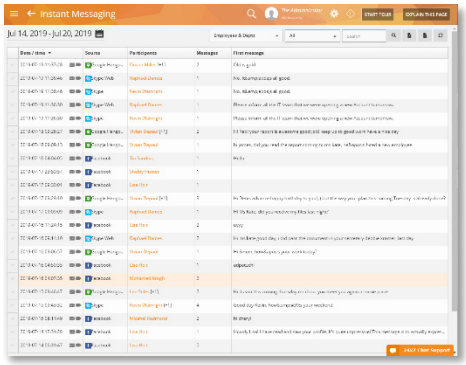
- Prevent upload or download of files to/from unknown or suspicious sites.
- Block torrent files.
- Limit the download/upload size to reduce abuse of bandwidth and storage.

What are some useful resources for this feature?

- User Guide: BI Reports > Web File Events
- User Guide: Monitoring Settings > File Transfers Settings
- User Guide: Monitoring Settings > Websites Settings
- Rules Guide: Activity Rules > Files

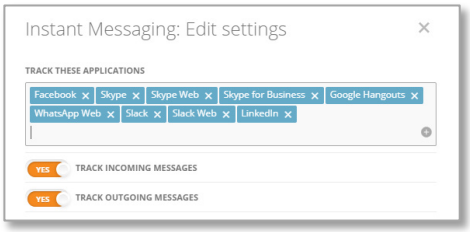
2.8 Instant Messaging

What report can I access for this activity?



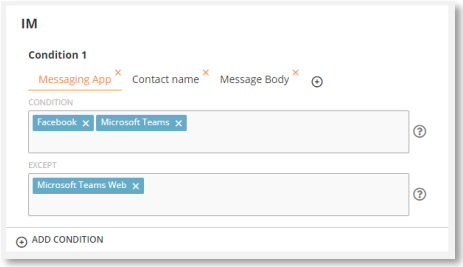
- View all conversations and group chats for popular IMs such as Facebook, Skype, Slack, etc.
- View a copy of the chat.
- View chat attachments (outgoing).
- Filter the report by the employee, computer, chat client.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



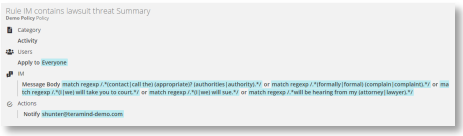
- You can select which messages to capture, incoming/outgoing, or both.
- You can specify which IM clients will be captured. Teramind supports popular clients, such as WhatsApp, Facebook Messenger, LinkedIn, Skype, Slack, Google Hangout, and Microsoft Team - both desktop and web versions.

What rule and alert triggers can I use with this activity?

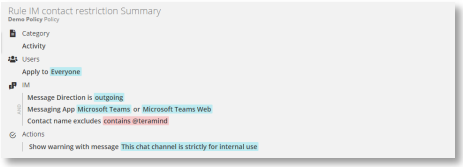


- On Teramind UAM, you can create Activity-based rules for Instant Messaging.
- You can use the Message Body, Message Direction, Messaging Application, and Contact Name as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc.

What are some sample rules using this feature?



- Restrict messages to/from select contacts.
- Detect if a user is in contact with suspicious people or criminal groups.
- Monitor support chat conversations to improve the quality of customer service and SLA.
- Get notified if the chat body contains specific keywords or sensitive phrases such as lawsuit



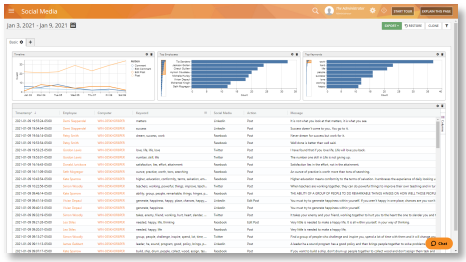
threats, angry sentiments, sexual harassment, etc.

What are some useful resources for this feature?

- User Guide: Monitoring Reports > Instant Messaging (IM)
- User Guide: Monitoring Settings > Instant Messaging / IM Settings
- Rules Guide: Activity Rules > IM - Instant Messaging

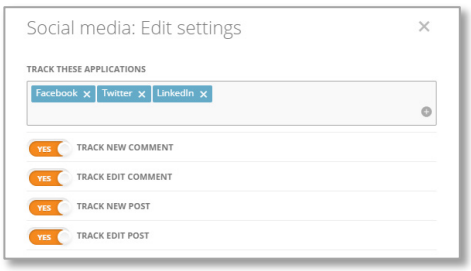
2.9 Social Media

What report can I access for this activity?



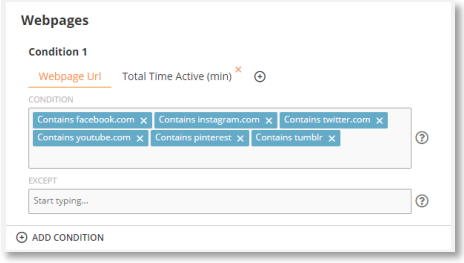
- View the source and action (post, comment, etc.) for the users' social media activities.
- View timeline (shows no. actions for the post, comment, edit post, etc.), top employees (by no. of social media activities), and top keywords, etc.
- See if any attachments are being shared.
- Aggregate or compare activities such as post vs. comments, Facebook vs. Twitter, etc.
- View the actual message.
- Filter the report by the employee, department, computer, platform, etc.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



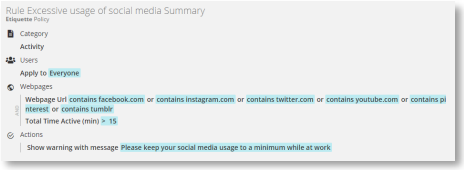
- You can specify which social media platforms to track. Teramind supports the most popular social media platforms, such as Facebook, Twitter, LinkedIn, etc.
- You can track New Comment, Edit Comment, New Post, and Edit Post activities in those applications.

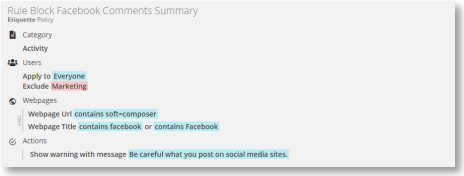
What rule and alert triggers can I use with this activity?



- Social Media does not have a dedicated rules category. However, you can create rules to monitoring social media sites using the Activity-based rules using the Webpages category. You can also create Content-based rules for social media. For example, using the Files category with a Content-based rule to detect sensitive contents and then use the *Upload URL* condition to block uploads of those files to a social media site.

What are some sample rules using this feature?





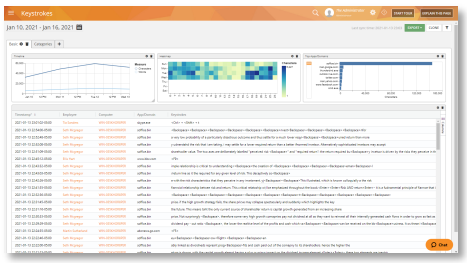
- Warn employees about excessive use of social media that might hamper productivity.
- Block posting of comments on certain social media sites such as Facebook but make an exception for the Marketing department.
- Monitor your corporate social channels. Get notified when any updates, posts, or comments are made on your social media accounts.
- Block uploading / downloading of files to/from social media sites.

What are some useful resources for this feature?

- User Guide: BI Reports > Social Media
- User Guide: Monitoring Settings > Social Media Settings
- Rules Guide: Activity Rules > Webpages

2.10 Keystrokes

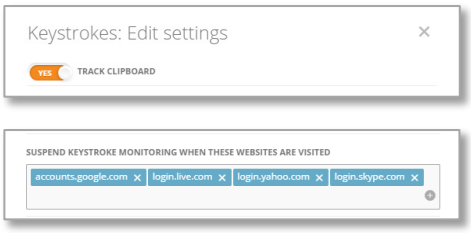
What report can I access for this activity?



- View all the keystrokes entered by the users in all apps/websites.
- In addition to regular keys, you can monitor the clipboard operations (copy/paste), use of special keys such as the Print Screen or key combinations.
- Compare items such as by timeline (e.g. no. of words vs no. of characters/letters typed for the duration), heatmap of keys pressed, top app/domains where the most keyboard activity occurred, etc.
- Group keystrokes by app/web categories, security categories, and reputation.
- Search for activities or filter the report by the employee, department, computer, etc.

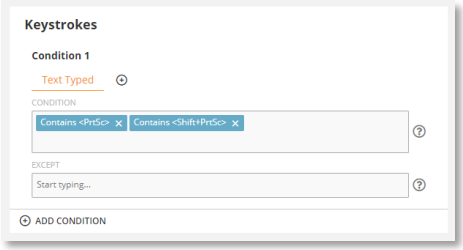
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



- You can turn the Clipboard tracking on/off.
- You can automatically suspend keylogging for certain Applications & Websites.
- Automatically suspend keylogging when certain content is detected on Applications & Websites.

What rule and alert triggers can I use with this activity?



- On Teramind UAM, you can create Activity-based rules for the Keystrokes.
- You can use Text Typed or Word Typed as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc.

What are some sample rules using this feature?

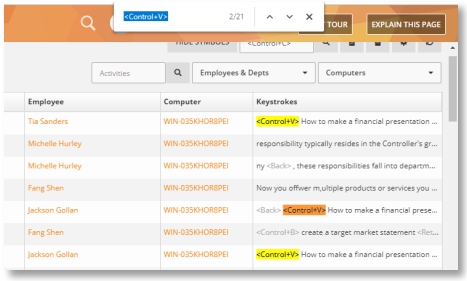
- Detect if someone is taking screenshots with the likely intention of stealing information.
- Detect if an employee is using unprofessional language with a customer on live chat.
- A user repeating easy-to-guess passwords (hence, creating a security risk).
- Disable keyboard macros or select combo keys in certain applications or for some users.

What are some useful resources for this feature?

- User Guide: BI Reports > Keystrokes
- User Guide: Monitoring Settings > Keystrokes Settings
- Rules Guide: Activity Rules > Keystrokes

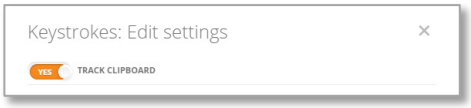
2.11 Clipboard (Copy and Paste)

What report can I access for this activity?



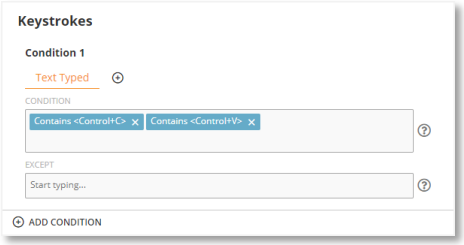
- There is no dedicated report for the Clipboard. However, you can use the Keystrokes report and search for hidden characters that indicate copy/paste operations, for example: `<Control+C>` or `<Control+V>`.

What monitoring & tracking controls do I have?



- Clipboard does not have a settings panel. However, you can turn it on/off from the Keystroke's settings panel.

What rule and alert triggers can I use with this activity?



- You cannot create any Clipboard-specific rules and alerts in Teramind UAM. You will need Teramind DLP to be able to do that. However, you can use the Keystrokes rules to detect copy/paste operations using the *Text Typed* condition and looking for values, such as `<Control+C>` or `<Control+V>`.

What are some sample rules using this feature?

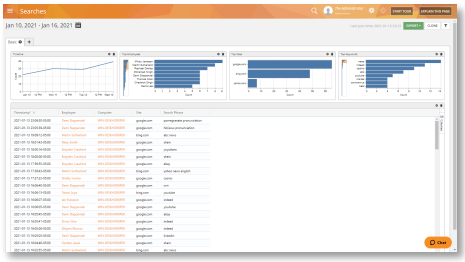
- You will need Teramind DLP for creating rules based on the Clipboard. Check out the *Teramind DLP Features Guide* for some examples of the Clipboard-based rules.

What are some useful resources for this feature?

- User Guide: BI Reports > Keystrokes
- User Guide: Monitoring Settings > Keystrokes Settings

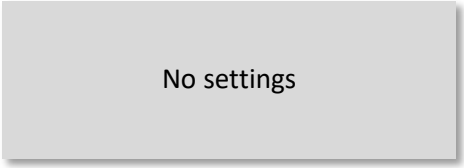
2.12 Searches

What report can I access for this activity?



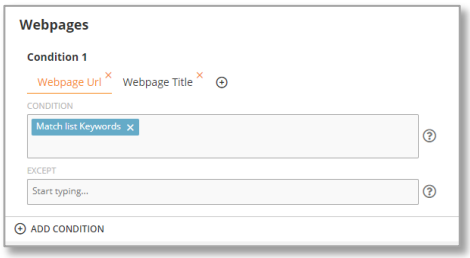
- View all the search phrases by timestamp, site, employee, department, computer, etc.
- Compare or group searches by timeline, top searches by employees, sites, keywords, etc.
- Search for activities or filter the report by the employee, department, computer, etc.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



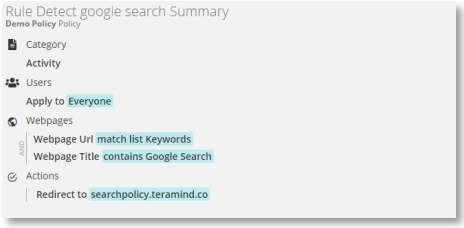
- Search does not have a dedicated settings panel. Search engines are treated like regular websites on Teramind. You can control website settings from the Websites settings panel. See the [Applications & Websites] section for more information.

What rule and alert triggers can I use with this activity?



- You cannot create any Search-based rules directly. However, in Teramind UAM you can create Activity-based rules and use the *Website URL* and *Website Title* conditions to detect a search engine and the term(s) a user is searching for.

What are some sample rules using this feature?



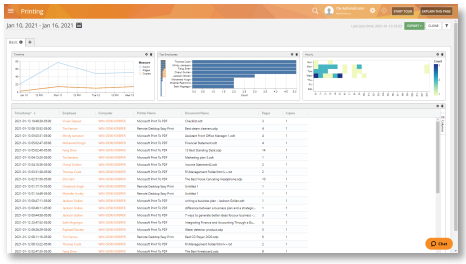
- Use the Webpages rules to detect when an employee searches for certain keywords.
- Redirect to another URL when a certain search engine is detected. For example, redirect all searches from Bing to Google.

What are some useful resources for this feature?

- User Guide: BI Reports > Searches
- User Guide: Monitoring Settings > Websites Settings
- Rules Guide: Activity Rules > Webpages

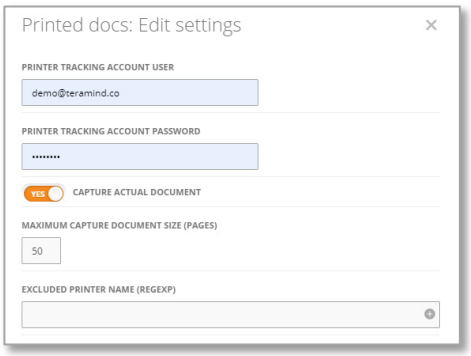
2.13 Printing

What report can I access for this activity?



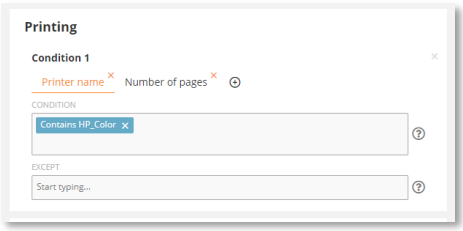
- Track all documents sent to the local or network printers including the name of the document, printer, pages, copies, computer, and the user initiating the print job.
- Compare or group print activities by timeline (e.g. no. of print jobs, pages, and copies), heatmap, etc.
- View or print a copy of the document or save it as a PDF file.
- Filter the report by employee and computer.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



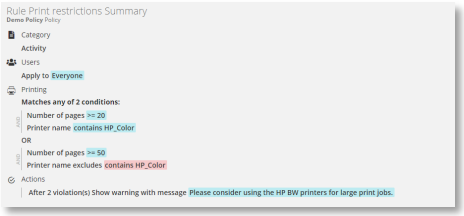
- Specify which printer account will be used for printers that require a login (e.g. network printers).
- Turn the capture of actual documents on/off.
- Specify the maximum size of the document (pages) to be captured.
- Exclude printers you do not want to track.

What rule and alert triggers can I use with this activity?



- On Teramind UAM, you can create Activity-based rules for the Printer.
- You can use the Document Name, Printer Name, and Number of Pages as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc.

What are some sample rules using this feature?



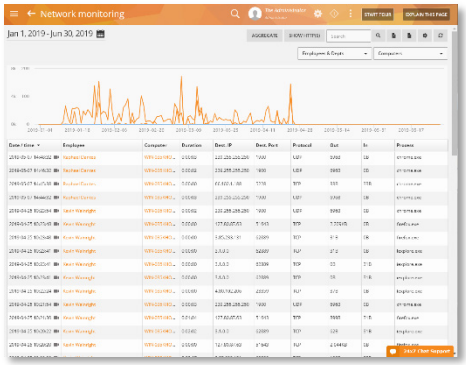
- Warn the user about large print jobs to reduce waste.
- Prevent data leaks over hardcopies by restricting what documents can be printed.

What are some useful resources for this feature?

- User Guide: [BI Reports > Printing]
- User Guide: [Monitoring Settings > Printed Docs Settings]
- Rules Guide: [Activity Rules > Printing]

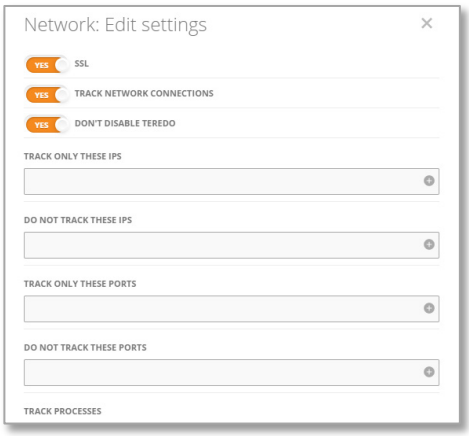
2.14 Network

What report can I access for this activity?



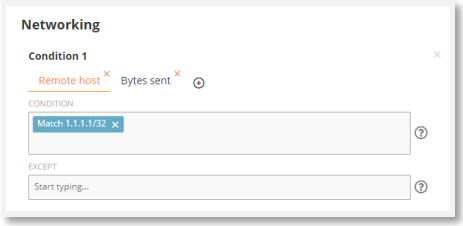
- Monitor detailed information for each network activity, such as the application process/URL, user, duration of a network session, amount of information sent or received, number of connections, port, and the protocol used.
- Aggregate similar items (i.e. sites).
- View network usage trends.
- Filter the report by employee and computer.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add a real-time *Network Usage* widget on the dashboard.

What monitoring & tracking controls do I have?



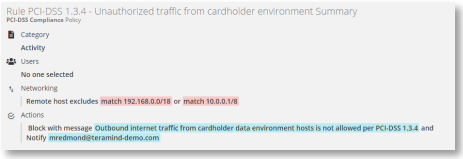
- You can turn SSL on to monitor secure connections (i.e. HTTPS).
- Select which IPs and Ports you want to track. For example, you can decide to track only external IPs or connections.
- Similarly, you can specify which network processes to track. You can use names (i.e. `svchost.exe`), Regular Expressions, Network Shared Lists, etc. to fine-tune the processes to track.

What rule and alert triggers can I use with this activity?



- On Teramind UAM, you can create Activity-based rules for the Network.
- You can use the Application Name, Remote Host and Port, Bytes Sent and Received, etc. as inputs for the rule conditions.
- You can use these rule Actions: Warn, Block, Notify, Lock Out User, Execute Windows Command, etc.

What are some sample rules using this feature?



- Implement network security-related rules, for example, restrict outgoing internet traffic from the payment server (to comply with PCI DSS regulation).
- Limit network access such as, disable login via RDP (Remote Desktop Protocol).
- Implement geo-fencing, for example, restrict access to your EU server from US users.
- Get notified when abnormal network activity (i.e. sudden spike in network traffic) is detected which might indicate an intrusion.

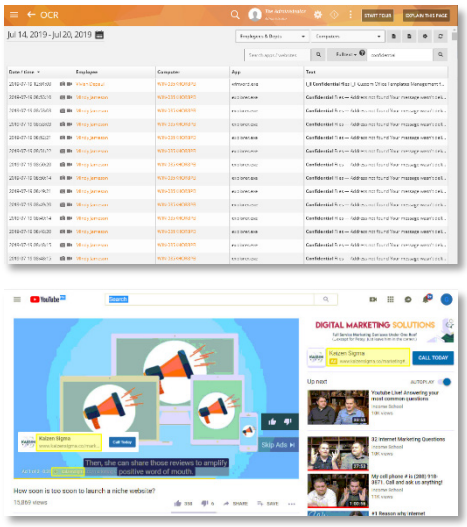
What are some useful resources for this feature?

- User Guide: Monitoring Reports > Network Monitoring
- User Guide: Monitoring Settings > Network Settings
- Rules Guide: Activity Rules > Networking

2.15 OCR

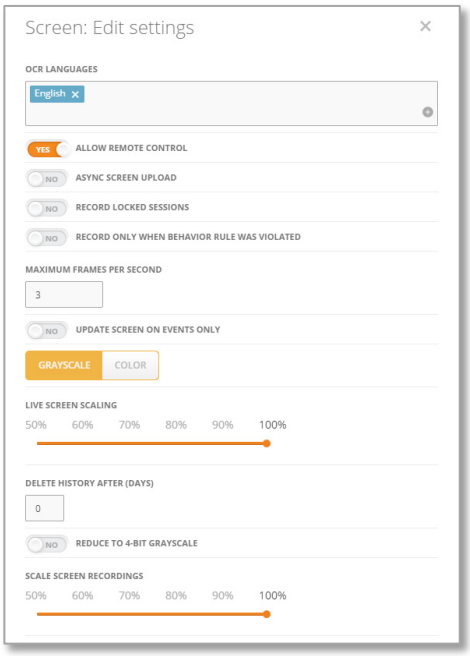
> OCR is disabled by default for the Cloud version of Teramind UAM. Please contact support@teramind.co if you need it enabled.

What report can I access for this activity?



- Detect on-screen text in real-time, even inside images or videos.
- Quickly search for information using powerful search features, such as Full Text, Wild Cards, Regular Expressions.
- Automatically identify the areas of the screen where OCR text was detected using OCR Snapshot.
- Works with multi-screen setups, virtual desktops, and Terminal Servers.
- Filter the report by employee and computer.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.

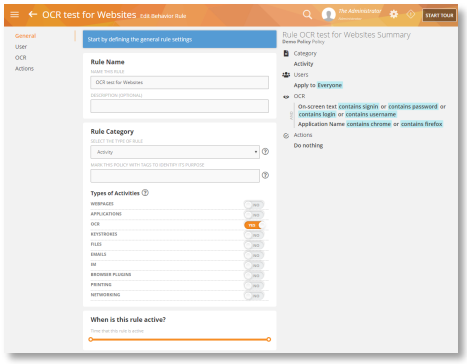
What monitoring & tracking controls do I have?



OCR settings are largely handled under the *Monitoring Settings > Screen*.

- You can specify which language will be used for the OCR. Default is English. Teramind also supports Hebrew, Russian, Dutch, Spanish, and Turkish.
- You can have asynchronized upload of OCR captured videos in case you have a slower server or limited bandwidth.
- You can enable recording only when a rule is violated to reduce the storage requirement or for privacy reasons.
- You can also control the FPS, color mode, size, bit-depth, compression, etc.
- You can specify when the recordings will be automatically deleted to reduce storage needs or to comply with privacy regulations.

What rule and alert triggers can I use with this activity?



- You can detect any text displayed on the screen by using keywords, lists, or regular expressions.
- You can use the Application Name as input for the rule condition.
- You can use the Notification Action with the OCR.

What are some sample rules using this feature?

- Generate an alert when a user sees a full credit card number on the screen violating the PCI DSS compliance requirements.
- Get notified when your employees visit sites that contain questionable content, such as hacking, pornographic, or piracy-related topics.
- Prevent steganographic data exfiltration by detecting information hidden inside images or videos.

What are some useful resources for this feature?

- Video: Intelligent User Session Mining with Teramind's patent-pending OCR features
- User Guide: Monitoring Reports > OCR
- User Guide: Monitoring Settings > Screen Settings
- Rules Guide: Activity Rules > OCR

2.16 Remote Control

Remote Control allows you to take full control of a user's computer over the internet. Additionally, you can block the user's input or freeze their screen remotely.

Remote Control is available through Teramind's Session Player and is part of Teramind's audit and forensics capabilities. Please check out the Audit & Forensics section for more information.

3 User Behavior Analytics

Teramind comes with powerful User & Entity Behavior Analytics (UEBA) to identify and alert you about a wide range of anomalous behavior and potential threats by either a malicious, inadvertent, or compromised employee or third-party entity. Predictive and situational threat information derived from machine learning, regression analysis, and risk analysis helps you detect vulnerabilities early; identify security weak spots, and develop risk mitigation plans for the future.

3.1 Insider Threat Detection

In Teramind UAM, insider threat detection works utilizing a combination of monitoring, authentication, risk analysis, and behavioral rule features. For example:

- Conduct OCR search for confidential information and see who had access to such information and when.
- Establish organization-wide visibility and control for over 12 objects including the screen, apps, websites, files, emails, etc. Locate suspicious activity in real-time.
- Detect activities of all types of insiders: employees, third-party vendors, freelancers, contracts, etc.
- Activity and Agent-Schedule-based rules to automatically detect when users violate rules.
- Utilize sophisticated anomaly rules to identify user activities outside the normal behavior.
- Real-time alerts and notifications immediately warn you about harmful insider activity.
- Use session playback, monitoring reports, and logs to investigate insider incidents and identify what happened, who, and what caused the incidents.
- Risk analysis to identify security gaps & vulnerabilities.

What are some useful resources for this feature?

- Video: Teramind: Insider Threat Prevention

3.2 Abusive Behavior

These are user behaviors that, while not malicious or particularly dangerous, still can cause your organization loss of productivity and in some cases, other damages. With Teramind UAM, you can create Activity and Agent Schedule-based rules to detect abusive behaviors easily. For example:

- Employees looking at materials online that are questionable, suspicious, or otherwise dangerous. For example, hacking sites, pornography, or piracy content.
- Workers spending too much time on Facebook, watching YouTube videos, or surfing online shopping sites.
- Employees idling too much, coming to work late, frequently absent, etc.
- Spending excess time on personal tasks such as applying for jobs.
- Abusing company resources, such as printing unnecessary copies of documents, throttling the network, etc.
- Using applications or sites that are unproductive or unauthorized.
- Not following prescribed policy when dealing with customers.

- Not following corporate etiquette policy, for example, visiting gambling sites.
- Using browser's incognito/private mode.
- Contractor submitting invoices that do match work hours or task completion status.

3.3 Malicious Behavior

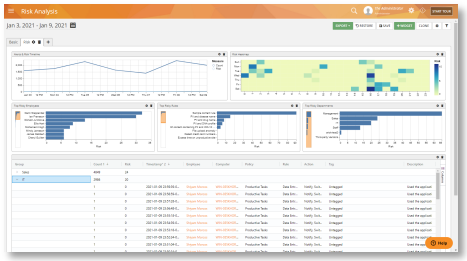
With Teramind UAM you can create Activity and Agent Schedule-based rules to detect malicious behavior or suspicious intents easily. For example:

- A user trying to hide information in an image.
- Sending out emails with sensitive files to non-corporate emails.
- Unauthorize use of Cloud sharing drives as an attempt to exfiltrate data.
- Sharing embargoed files on social media or IMs.
- Running network snooper, registry editor, or other dangerous applications.
- Running software from external media or cloud services.
- Changing the configuration of the network or system settings.
- Saving files on removable media.
- Communicating with competitors.
- RDP connection attempts to forbidden hosts or unauthorized use of RDP applications.
- Sudden change in schedules or work patterns.

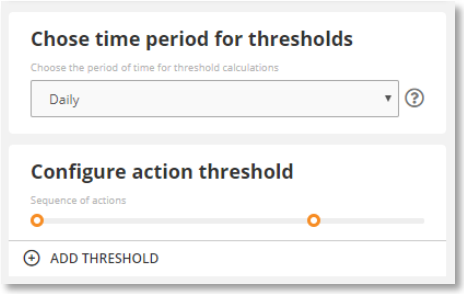
What are some useful resources for this feature?

- Video: [How to use Teramind to monitor and block data exfiltration attempts to USB/external drives]

3.4 Dynamic Risk Scoring

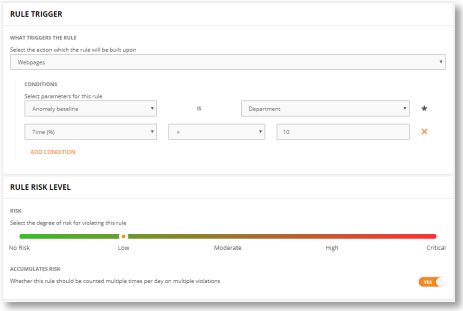


Conduct Risk Analysis:
You can use the BI Reports > Behavior Alerts > Risk screen or create your own risk analysis reports to conduct an organization-wide risk assessment. You can find out top risky users, rules, and objects (applications and websites). You can plot risk trends, for example, by department, severity, number of violations, tag, etc. Unique risk score helps you identify high-risk users or policies so that plans can be developed for treating the risks.



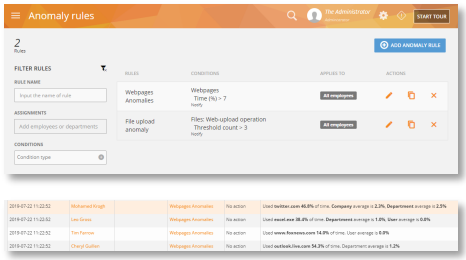
Assign Risks to Rules:
Each rule has an Advanced Action tab where you can assign risk to an activity based on frequency. You can add multiple thresholds, assign risk levels and take different actions depending on how often the rule is violated. For example, you can set an email rule that sets a Low risk when a user sends 5 emails in a day. However, if they

send more than 10 emails a day, then the rule will set a Moderate risk level and trigger a Notification action.

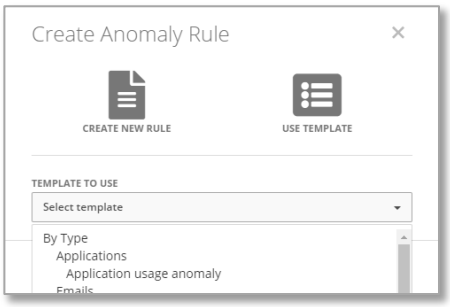


Assign Risks to Behavioral Baselines:
With the Anomaly Rules, you can assign dynamic risks to anomalous behaviors based on time and baseline compared at the user, departmental, or organizational level. For example, you can set up a website anomaly rule that assigns a high risk to a user's behavior if they spend more than 20% of their time over their departmental baseline. The risk score will then auto-adjust over time as both the user's and the department's activities change. The risk score will also reflect this on the Risk report.

3.5 Anomaly Detection



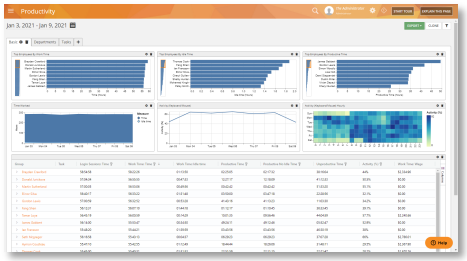
Anomaly Rules:
Anomaly Rules are special types of rules available on Teramind UAM and Teramind DLP. They allow you to identify anomalies in user behavior or application activities by utilizing behavioral baselines. An anomaly rule also allows you to assign risk levels to user behaviors and create notification actions to inform admins or managers about such anomalies. You can view the anomalies on the Alert report along with the rule violation incidents.

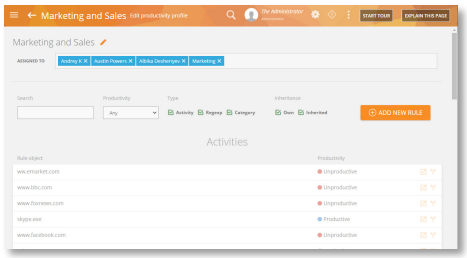


Built-in Templates:
Teramind UAM comes with many anomaly rule templates for Applications, Emails, Files, Instant Messages, Networks, Printers, etc. Using the templates, you can start creating sophisticated anomaly rules in no time.

4 Workforce Productivity

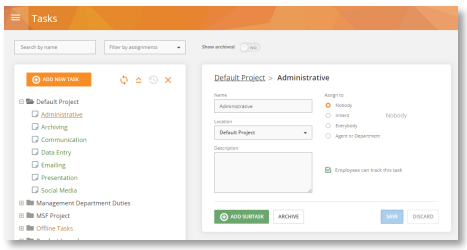
4.1 Productivity Analysis & Reporting

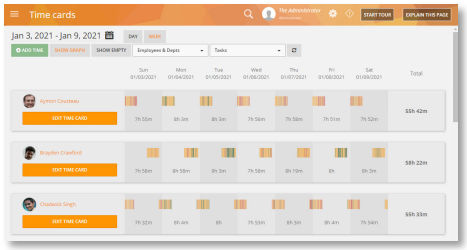




- Productivity reports allow you to track productive, unproductive, active, and idle time and performance KPIs for employees and departments.
- Create Productivity Profiles to classify productive and unproductive applications and websites and assign them to individual employees, groups, or departments.
- You can find out easily top employees by Work Time, Idle Time, Productive Time, Session Time, Activity %, etc.
- Track time spent and wages on different employees, departments, projects, or tasks.
- Understand exactly how shifts are spent through minute-by-minute activity monitoring to best utilize your workers.

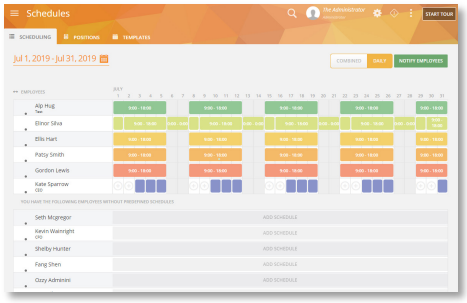
4.2 Time Tracking

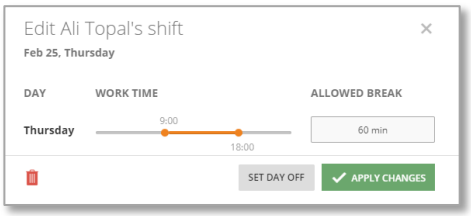




- Automatically assign tasks to employees and track time based on their activity or let them manage their clock-in.
- Comes with Time Tracker, Employee Cost, Task Cost, Time Records, and Time Card reports.
- Add missing time entries and notes such as PTO/time off, accruals, etc. for auditing and compliance purposes.
- Analyze payroll and discover your cost drivers such as unproductive hours and absence.
- View screen snapshots and session records of the selected period.
- Import projects and tasks from PM solutions such as Zendesk, JIRA, etc.

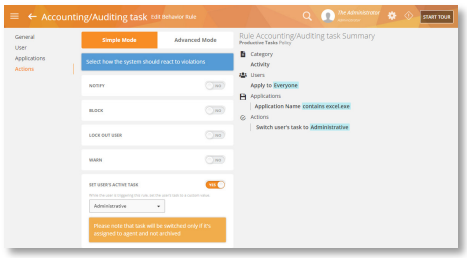
4.3 Template-Based Scheduling

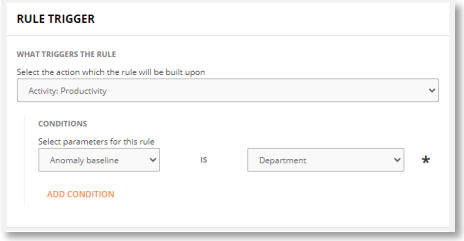




- Create daily and weekly schedules for your employees and contractors.
- Notify employees about their schedule changes automatically.
- Configure worktime, launch breaks, days off, etc.
- See who is late, stays overtime, or leaves early.
- Prevent users from using their computers or access certain apps when they are not scheduled to work.
- Batch-assign schedules to multiple employees at once.
- Create schedule-based rules such as late, absent, early start, late shift, etc.

4.4 Workflow Automation



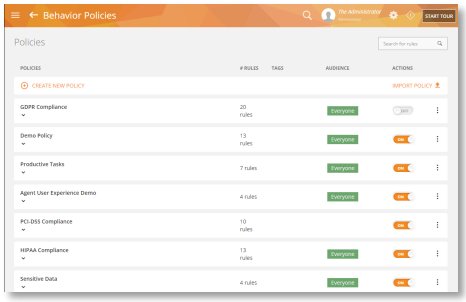


- Create productivity rules. For example, if an employee is idle for longer than a certain time, send them a warning automatically.
- Create anomaly rules to get an early warning on fringe cases. For example, employee productivity dropping below their own, departmental or organizational baseline.
- Train new staff or provide job shadowing support using the Remote Control feature. Develop training materials, demo, tutorials, etc. using the Screen and Audio recording features.
- Provide on-demand feedback and gamify performance reviews utilizing custom alert messages. For example, automatically send a congratulatory message to an employee when their productivity reaches the Top 10 spot.

5 Policy and Rules Management

The core of Teramind is its policy and rules engine which can automatically detect malicious, inadvertent, or accidental threats. You can get started right away with hundreds of pre-built rule templates and activity classification lists. Create your own policies and rules with an intuitive, visual rule editor. Use natural English, regular expressions, and sample conditions to easily define your requirements. Create monitoring profiles for individual employees, groups, or departments all from a wizard-like interface.

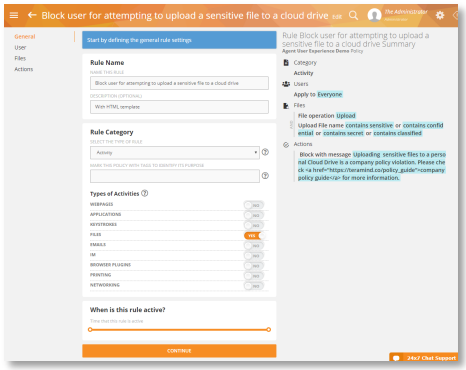
5.1 Policy Manager



Policies help you organize similar rules together or apply a set of rules to some particular users. For example, you can have all your HR-specific rules such as 'Preventing email harassment', 'Limiting social media use' etc. under the 'Business Etiquette' policy.

- You can create as many policies as you want.
- Import or export policies and share rules across them.
- Teramind UAM comes with a sample policy with some rules for you to experiment with.

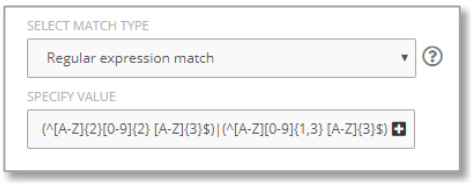
5.2 Visual Rule Editor



The Rules Editor is an intuitive, visual editor where you can create even complex rules easily without going through multiple screens or coding.

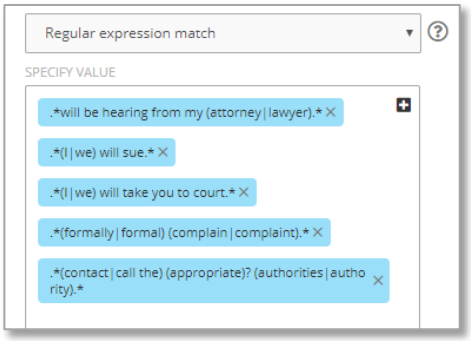
- A step-by-step wizard guides you through the entire rule creation process.
- The editor shows an easy-to-read natural language summary of the rule so anyone can follow how it works and what it does.
- Hundreds of built-in templates to choose from.
- Simple and Advanced modes for beginners and experienced users.

5.3 Regular Expression Support



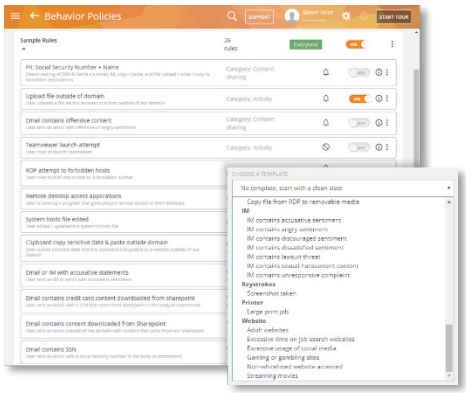
A Regular Expression or RegEx is a sequence of characters that define a pattern. Such patterns are very powerful compared to keywords or simple text searches in locating hard-to-find, repetitive information.

- Teramind UAM allows you to use Regular Expressions in rule conditions, searches, filters, monitoring settings, etc.
- You can use it to detect numeric or structured data such as credit card numbers, zip/postal codes.



- You can also detect sensitive words or phrases such as harassment or angry sentiment in emails.

5.4 Out-of-the-Box Rule Templates



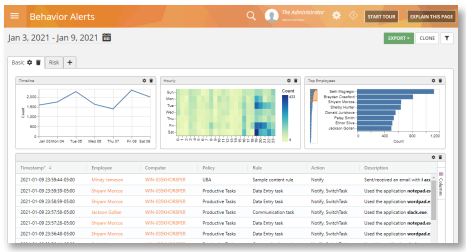
- Teramind UAM comes with hundreds of pre-defined policies and rules. For example block email containing sensitive keywords, stop the uploading of a confidential document, detect screen capture, prevent the use of external drives, etc.
- Pre-packaged sample rules ready for use.

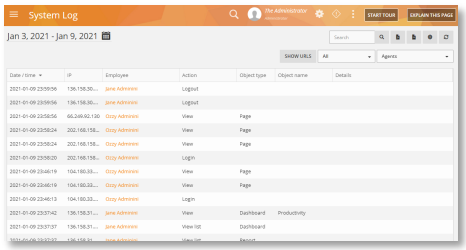
You cannot use any templates or sample rules that use the *Content-sharing* category on Teramind UAM. You will need Teramind DLP to use those templates/rules.

6 Audit & Forensics

In addition to the monitoring and alert reports, Teramind DLP comes with a Session Player that allows you to access a user's desktop live or view recordings of previous sessions. You can see all the notifications the user received and conduct powerful, on-screen content searches with OCR.

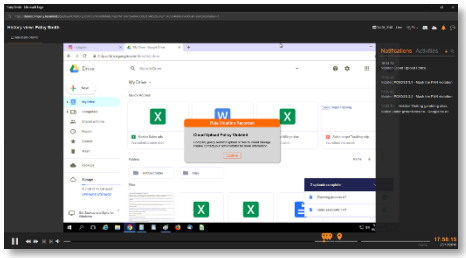
6.1 Real-Time Alerts & Logs

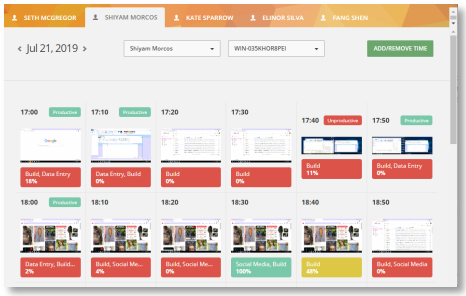




- View all rule violation incidents and alerts, actions taken by the system, alerts trend, and timeline, most violated policy & rules, most risky users, etc.
- Click on an alert to view the session recording or to investigate an employee.
- Prioritize alerts to prevent false alarms.
- Get scheduled alert digest and email notifications.
- Configure alert messages and templates with HTML.
- Immutable system and session logs.
- Export the alerts and logs as CSV or PDF.
- Integrate with SIME and log analytics systems such as Splunk to send alerts and event logs.

6.2 Video Recording of All User Activity





- Teramind visually captures every action that a user makes in real-time.
- Live View or History Playback of the user's desktop.
- Take remote control or freeze input.
- Precisely locate when a rule violation incident occurred and view the user activities leading up to the event.
- Take screenshots or export the recordings as MP4 files.
- Supports multi-screen setups and virtual desktops.
- View user activity at a glance with Live Montage and Screen Snapshots with simple color-coding.
- Access the recordings from the Monitoring Reports, Alerts, and Session Logs for any date/time and activity.

6.3 Audio Recording

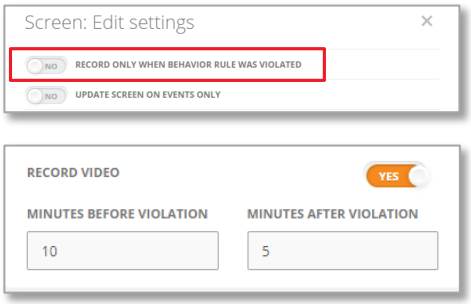
When enabled, Audio Recording captures both input (Microphone, Line-in) and output (Speakers, Line-Out, Application Sounds), etc. The audio recording is available as part of the video recordings and can be

played back with the video player. Please see the Video Recording of All User Activity section above for more information.

6.4 OCR of Screen Content

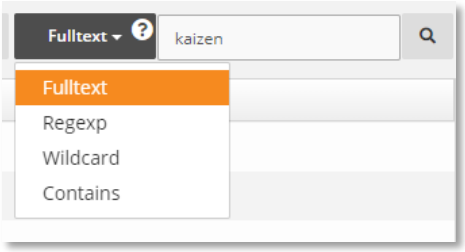
Teramind saves all the screen recordings with meta-data and indexes so that you can conduct a high-speed OCR search in the captured recordings. See the OCR section above for more information on how the OCR feature works.

6.5 Option to Record Only During Violation



- Teramind can be configured to record the Screen/Desktop only during a rule violation incident (by default Teramind records for 24/7).
- Additionally, Teramind UAM and Teramind DLP allow dynamic recording on a rule-by-rule basis. You can control how long it will record both before and after the rule violation incident.

6.6 Full-Text Search



In Teramind UAM and Teramind DLP, you can conduct OCR text searches using:

- **Fulltext:** Full-text search with natural language processing (NLP).
- **Regexp:** Regular expressions, e.g. `[a-zA-Z]{4}[0-9]{12}`.
- **Wildcard:** Use '`*`' as a wildcard, e.g. `*doe` will match `John doe`, `jdoe`, `ddoe`, etc.
- **Contains:** Find any phrase that contains the text specified. Same as `*term*`.

7 Deployment

7.1 Supported Platforms

Windows 7 & Up	Citrix XenApp® & XenDesk®	Windows Server 2012 & Up	VMware Horizon	Mac OSX

7.2 Hosting Options

Cloud	On-Premise	Private Cloud
No server maintenance, only install Teramind Agents on the machines you want to monitor and set up your users, policies, and rules and let us take care of the rest.	Control your Teramind implementation in its entirety. Leverage LDAP groups and users to identify which users and groups to apply which policies and rules to.	Use your own secure, scalable private cloud implementation including AWS, Google Cloud, Azure, and more.

7.3 Support

- Installation assistance
- We set up the host for you (for the Cloud deployment option)
- 24x7 follow-the-sun support
- Option for Enterprise SLA
- Subscription includes software updates