ACTIVTrak

GETTING STARTED WITH ACTIVTRAK ALARMS

Alarms are the single most versatile tool that ActivTrak provides. Alarm configuration takes ActivTrak from a simple monitoring tool, and turns it into a versatile suite capable of performing tasks for every department in your company. Trigger security protocols, ensure policy compliance, and analyze adherence or deviation from established workflows.

Alarms give administrators the control and visibility to make informed decisions.

ACTIVTRAK HAS 3 MAJOR ALARM TYPES

ACTIVITY ALARMS

Activity alarms allow you to capture nearly any activity that happens on a monitored computer. Triggers on any behavior-based activity from your monitored computers.

AUDIT ALARMS

Used to detect changes within your ActivTrak Account.

USB ALARMS

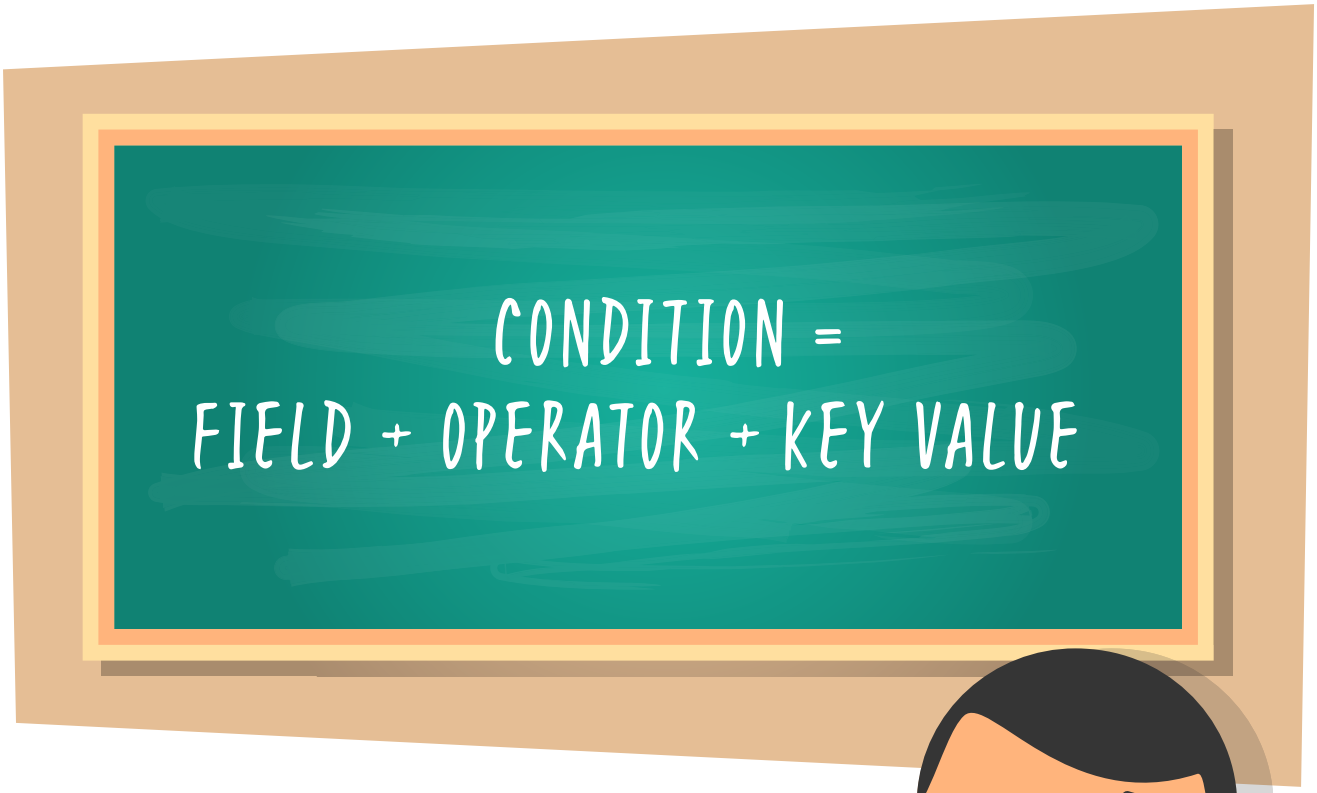
Used to detect when a USB is used on any of your monitored workstations. The alarm will trigger when a USB device is inserted, written to, or both.

HOW TO SET AN ALARM

1. **Set Your Alarm Conditions**
2. **Choose Your Reactions**
3. **Set it Live!**

ALARM CONDITIONS

Conditions tell ActivTrak when to trigger your alarm and begin your alarm reactions. Add as many conditions as needed to capture the activity you're looking for. You can choose to trigger an alarm when 'any' one condition is met, or when 'all' conditions are met together.



FIELDS

Choose from one of ten predefined fields to pinpoint nearly any activity on a computer.

Field Options

- User
- Titlebar
- URL
- Computer
- Description
- Duration
- Executable
- Private IP Address
- Logon Domain
- Primary Domain

ALARM REACTIONS

CAPTURE SCREENSHOT OR VIDEO

Screenshot

When an alarm is triggered you have the option of taking one or multiple screenshots from the computer that triggered the activity. If you choose to take multiple screenshots, ActivTrak will take a screenshot at any interval you set that is greater than or equal to 10 seconds.

Video

When an alarm is triggered you have the option of recording a video. Unlike screenshots that only capture activity after an alarm is triggered, videos provide context 15 seconds before the alarms is triggered, and 15 seconds after the alarm is triggered, which provides much more context into the activity taking place.

EMAIL ADMINISTRATORS

Send an email with Alarm details to administrators in your system.

NOTIFY THE USER

Send an informative pop-up message to the computer that triggered the event. Create your own custom message, and insert field values from the triggered activity.

NOTIFY EXTERNAL SYSTEMS

Send a Webhook with Alarm information to any destination. Use an optional parameter to send specific information with your webhook.

SET ACTIVITY RISK POINTS

Set an alarm risk level to signify the how risky you consider the activity. When a user triggers the alarm this will increase their user risk score, and add to the alarm risk score, allowing you to efficiently keep track of how often risky activity is happening, and who is doing it.

TERMINATE THE APPLICATION

Immediately close the application that triggered the alarm.

ACTIVITY ALARM CHEAT SHEET

TRACK WORKFLOW ADHERENCE

Purpose

- **Sales reps shouldn't be on LinkedIn for more than ten minutes at a time.**

Conditions

- Match All: URL contains LinkedIn AND Duration greater than 600.

Reactions

- Pop-up: You've been here for over ten minutes, are you running into a problem?
- Capture multiple screenshots (Interval: 10 seconds).

TRACK SENSITIVE FILE ACCESS

Purpose

- **Understand unauthorized access to privileged information.**

Conditions

- Match All: Titlebar contains [Sensitive file name]
  AND user is not [Users with privilege to access file]

Reactions

- Pop-up: You do not have permissions to view this file. Your actions are being recorded.
- Capture Video
- Email Alert: To: All Admins, Body: $User$ has opened $Titlebar$.
  Additional info: $Titlebar$ | $Description$ | $Executable$ | $Time$ | $Computer$
- Webhook to security system to shut down activity in progress.
- Terminate application

VIDEO ALARM

Purpose

- **Understand unauthorized access to privileged information.**

Conditions

- **Match Any:** Titlebar contains export OR URL contains Export
  OR Description contains Export

Reactions

- Capture Video
- Email: $User$ Requested an export from $Titlebar$.
  Additional info: $Titlebar$ | $Description$ | $Executable$ | $Time$

AUDIT ALARM CHEAT SHEET

DELETED DATA

Purpose

- **Trigger an alarm when someone deletes an alarm.**

Conditions

- Match All: Event equals ‘DeleteAlarm’ AND User not equal to [admins]

Reactions

- Send an Email to Administrators
- Set Alarm Risk Level

DELETED USERS

Purpose

- **Trigger an alarm when someone deletes users.**

Conditions

- Match All: Event equals ‘DeleteUsers’ AND User not equal to [admins]

Reactions

- Send an Email to Administrators
- Set Alarm Risk Level

UPDATED LIST OF BLOCKED WEBSITES

Purpose

- **Trigger an alarm when someone edits your blocked websites list.**

Conditions

- Match All: Event equals ‘UpdateBlockingDomain’ AND User not equal to [admins]

Reactions

- Send an Email to Administrators
- Set Alarm Risk Level

USB ALARM CHEAT SHEET

USB USAGE

Purpose

- **Alert external systems when a USB device is used.**

Conditions

- Select ‘USB Storage is Inserted’ AND User Does not Contain [users with privilege to use USB devices]

Reactions

- Capture Video When the Alarm is Triggered
- Send an Email to Administrators
- Webhook to External Security Systems to trigger security Protocol
- Set Alarm Risk Level

TRANSFERRING DATA TO USB

Purpose

- **Understand when someone transfers data to an external device.**

Conditions

- Match All: Select USB Storage is inserted, Also select USB Storage is written.

Reactions

- Capture Video
- Send Email: $User$ is Transferring files from $Titlebar$ to a USB. $Description$