Teramind User Guide

Version 2.6 (8 JANUARY 2022)

TERAMIND

Table of Contents

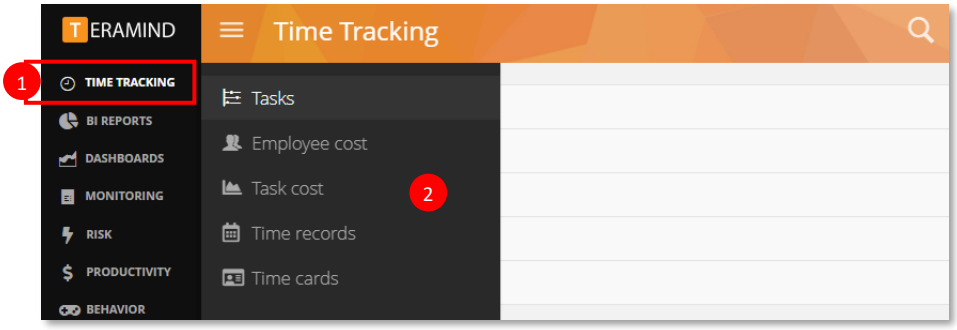
1 Time Tracking

1.1 Introduction to Time Tracking

The Time Tracking menu offers you with several time and task management features. You can create and manage tasks and timesheets, and track costs by employees or tasks. Employees can also access the web-based time tacker from this menu to clock in their time without installing the Teramind Agent.

These features are seamlessly integrated with the Teramind Agent, Behavior Policies & Rules, Scheduler, Employee Profiles/Departments, and other Teramind productivity features. This makes time tracking and reporting autonomous and easy to use.

1.2 Accessing the Time Tracking Menus



1. Hover your mouse over the **Time Tracking** menu, then
2. Select an option from the **sub-menu**, such as *Tasks*, *Employee cost,* etc.

> If you are a regular employee or an external user and an administrator has enabled the *User can clock in and out using the web interface* option and the *User can clock in and out using Web interface* option on your employee profile, you will see a **Time tracker** sub-menu instead of the **Tasks** sub-menu.

1.3 Tasks

The Tasks screen allows you to create and manage tasks and subtasks. You can also assign these tasks/subtasks to specific employees, departments or the entire organization.

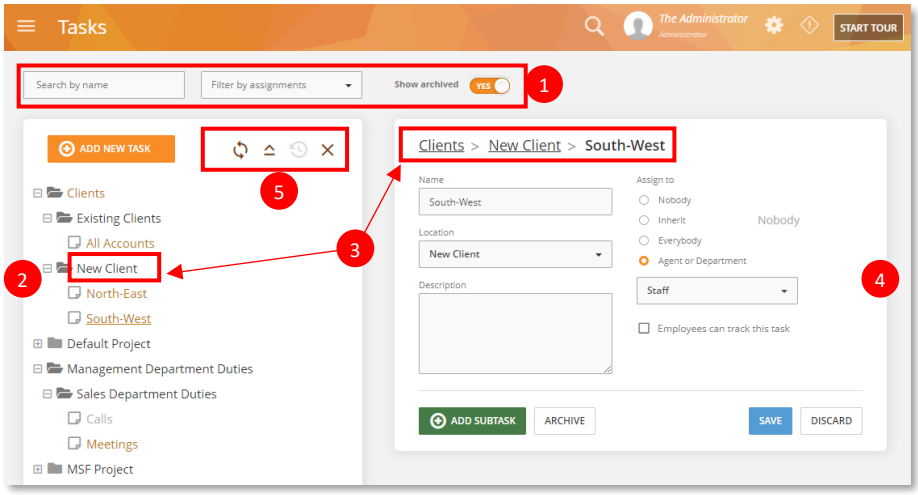
> The *Tasks* screen is accessible to the *Administrators* and *Operational Administrators* only (check out this Knowledge Base article to learn about access roles and permissions).

1.3.1 What You Can Do with Tasks

You can utilize tasks in various ways. For example:

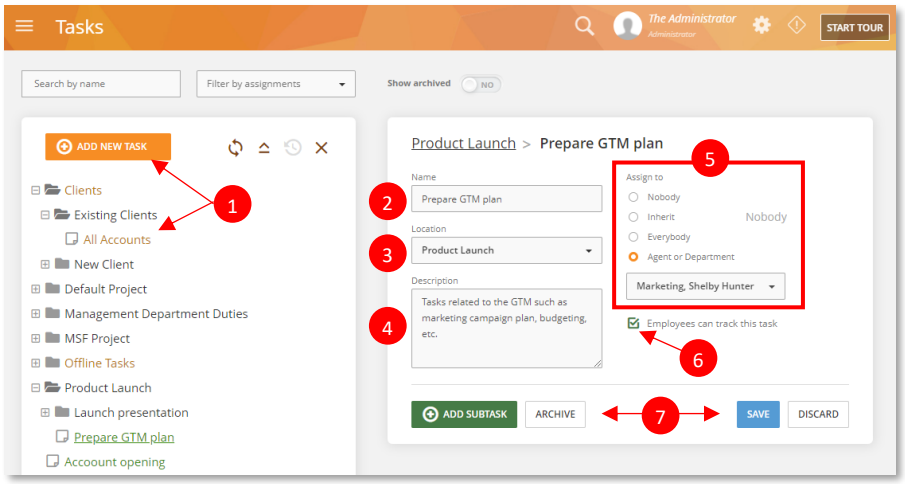
Assign tasks with the Revealed Agent You can create and assign tasks that will become available on the Revealed/Visible Agent so that employees can select them.	See Using the Revealed Agent section for more information.
Assign Tasks with Rules Any tasks you create from the *TIME TRACKING* > *Tasks* menu will be available to the Policy & Rule Engine so that you can automatically assign a task to an employee with the *Set User's Active Task* action. This is particularly useful for the Silent/Hidden Agent as it does not allow employees to select their tasks.	See the Action tab - Responding to Rule Violation Incidents section for more information on rule actions.
Set the Default Task You can set the default task for an employee or the entire organization.	*For Individual Employees*: from the employee's profile under the ACCOUNT INFO tab > DEFAULT TASK option. *For All Employees*: from the Settings > Agent Default option.
Use the Web-Based Time Tracker Allow employees to clock in/out from a web interface without requiring Teramind Agents to be installed on their computers – useful when hiring external consultants or contractors.	See the Time Tracker section for more information.
Import Projects/Tasks from 3rd Party Solutions Import projects and tasks from an external Project Management solution such as Jira.	See the Setting Up a New PM integration with Jira section for step-by-step instructions.
View Productivity Reports Tracking employee times with tasks help you get better understanding of your organizational productivity and how your employees spend their time.	See the BI Reports > Productivity for more information.

1.3.2 Navigating the Tasks Screen



1. Using the options from the the top of the screen, you can filter by list of tasks by task name or assignments (employees). You can also show/hide archived tasks (if you enable *Show archived* tasks, they will be displayed as light grey color).
2. On the left side of the screen, you can see the list of existing tasks. If a task has subtask(s) it will show a **Folder** icon with a small **+** or **–** sign in front. You can expand/collapse the folder by clicking the **+/-** sign.
3. You can select a task/subtask by clicking on its **name** from the left panel or by clicking a link from the **breadcrumb** from the right panel.
4. When you select a **task/subtask**, you can view/edit its details on the right panel of the screen. See below for details.
5. You can refresh the list of tasks, scroll to the top of the list of tasks, or scroll to the selected task by clicking these icons. If you click the **X** icon, it will hide the task details panel on the right (select a task/subtask or create a new task to show the panel again).

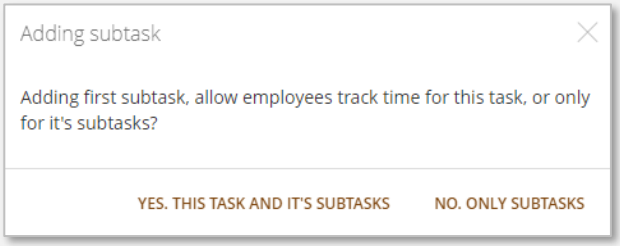
1.3.3 Creating / Editing a Task or Subtask



1. Click the **ADD NEW TASK** button to create a new task or select an existing task/subtask from the left panel. You will be able to edit the task on the right panel.
2. Enter a **Name** for the task.
3. Select a **Location** for the task. The location decides the level at where the task will be added. If you select 'Top level' it will be added at the top-most level without any parent task. If you select an existing task, then the task you are currently editing will be added as a subtask/child task under that task (note: you can also create a subtask by clicking the **ADD SUBTASK** button. See below for more information).
4. You can optionally provide a **Description** for the task.
5. Select an option from the **Assign to** section. Here's the explanation for each option:
    - *Nobody* = the task will not be assigned to anyone.
    - *Inherit* = the task will get its assignments from its parent task. This option is only available for subtasks.
    - *Everybody* = all employees will have this task assigned.
    - *Agent or Department* = you can assign the task to one or more employees or departments when you choose this option.
6. If you enable the **Employees can track this task option**, the employees will be able to select this task from their Revealed/Visible Agent. This does not apply to the Silent/Hidden Agent.
7. Click the **SAVE** button to save the task or the **DISCARD** button to cancel your edits. If you are editing an existing task or subtask, you will see two more buttons: **ADD SUBTASK** to add this task as a subtask, and an **ARCHIVE** button to archive the task.

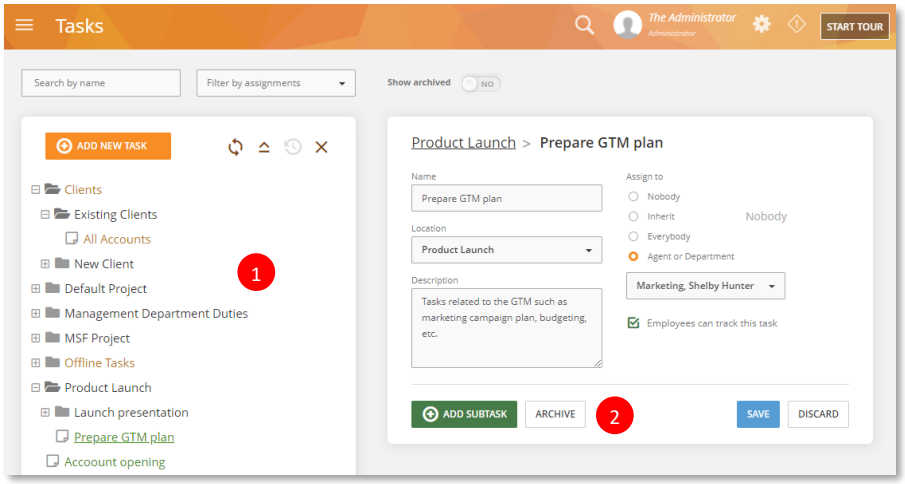
Subtasks and Employee Assignments

When you create a subtask under a task for the first time, you will see a pop-up message:



Select the **YES** option to allow employees to track their time for the parent task and the subtask. Select the **NO** option to allow them to track only the subtasks.

1.3.4 Archiving / Unarchiving a Task or Subtask



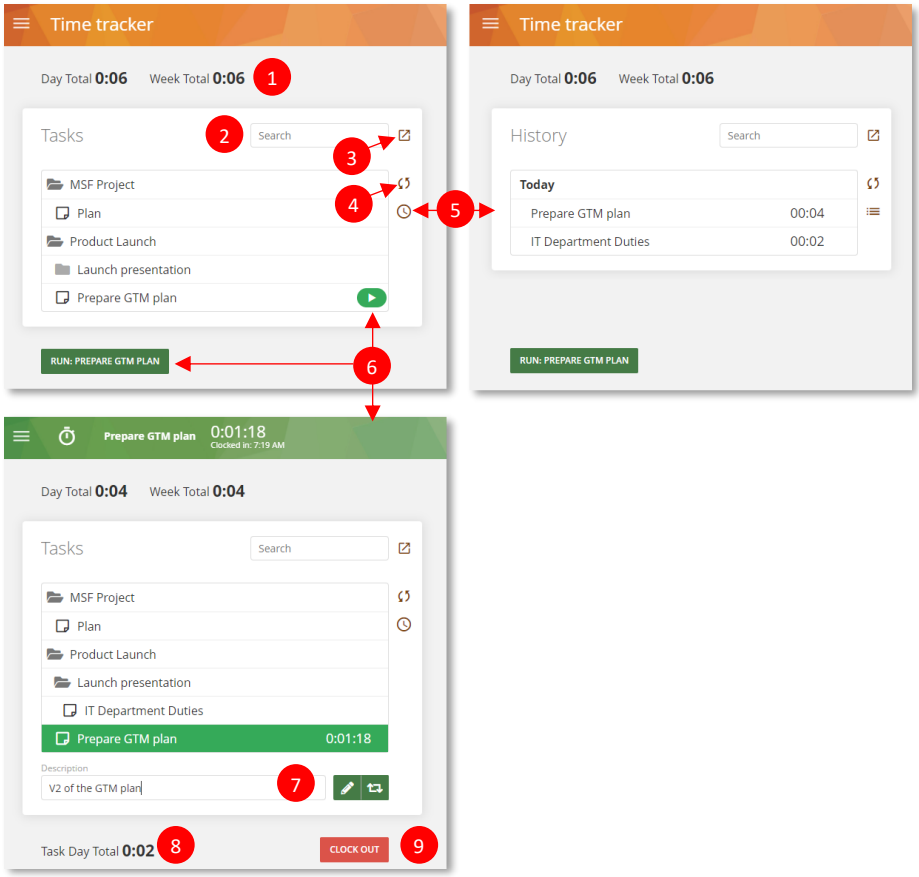
1. Select a **task/subtask** from the left panel.
2. Click the **ARCHIVE** button to archive it. Or, if it's already archived, click the **UNARCHIVE** button to restore it.

- An archive task will not show up on any of the places where tasks are used. For example, on the Revealed Agent's task list, on the *Set User's Active Task* rule action, on the employee's profile under the *ACCOUNT INFO tab* > *DEFAULT TASK* option, or on the *Settings* screen's *Agent Default* option.
- If you archive/unarchive a task that contains subtasks, all those subtasks will be archived/unarchived too.

1.4 Time Tracker

The Time Tracker screen allows employees to clock in or out and log their tasks from the web without having to install the Teramind Agent. This is particularly useful for tracking the time of consultants, freelancers, and other external users.

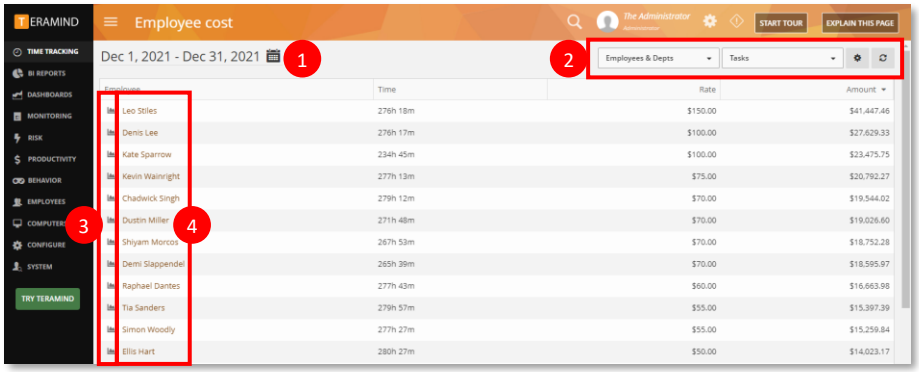
The *Time Tracker* screen is only accessible to an employee if you enable the *User can log in to the Teramind Dashboard* option and the *User can clock in and out using Web interface* option from their Employee Profile (under the *ACCOUNT INFO* tab).



1. On top of the Time Tracker screen, you will see the total hours for all tasks under the **Day Total** and **Week Total**.
2. You can search for a task using the **Search** field.
3. You can open the Time Tracker in a new browser window by clicking the **Pop-Out** icon.
4. You can refresh the task list by clicking the **Refresh** icon.
5. Click the **Clock** icon to view your work history. Once on the *History* view, click the **List** icon to go back to the *Tasks* view.
6. When you hover over a task, a **Play** button will be displayed. Click this button to start a task. You can also click the **RUN:** button to restart the last task. This will switch the window to a green theme and start the clock-in timer.
7. You can enter a **Description** for the current task in progress. This description will show up on the Time Records report under the *Notes* column.
   When you enter a description, you have two options to record it:
   - Click the **Pencil** icon to update the current time record with the description. You can also press the **CTRL** + **Enter** keys.
   - Click the **Refresh** icon to create a new time record with the description. You can also press the **Enter** key.
8. You will be able to see the total time spent for the currently running task under the **Task Day Total**. Note that, this time includes all sessions for the task. For example, if you worked on this same task on and off several times during the day, it would show the total time.
9. Click the **CLOCK OUT** button to stop the timer and clock out.

1.5 Employee Cost

The Employee Cost screen shows a report of time worked, rate, and the cost by employees for a period.

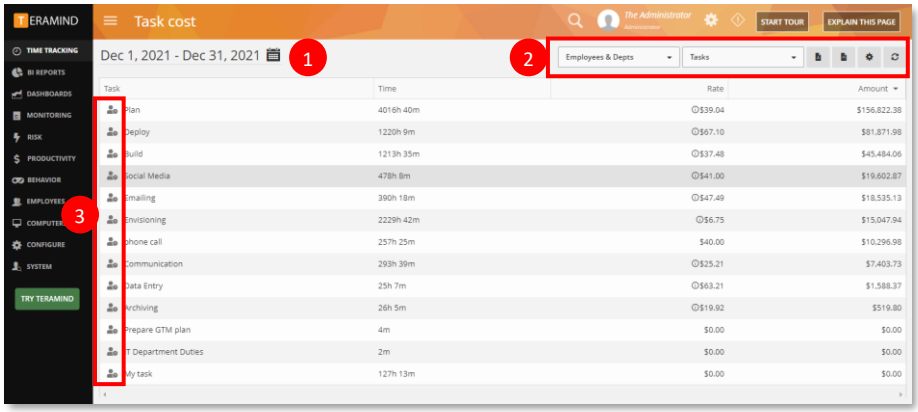


1. You can set a reporting period by clicking the **Calendar** .
2. By accessing the options at the top-right corner of the screen, you can filter the report by employees/departments, and tasks. You can also export the report in CSV/PDF format and specify what columns the report will display or export.
3. Clicking the small **Graph** icon in front of an employee's name will open a pop-up window where you can view a breakdown of cost by tasks and time records for that employee. See the Task Cost and Time Records sections to learn more.
4. Clicking an **employee's name** will open the activity history for that employee. Check out the Viewing an Employee's Monitoring Report section to learn more.

> To calculate the employee costs properly, you need to set the RATE option from the employee's profile > PERSONAL INFO tab.

1.6 Task Cost

The Task Cost screen shows a report of time worked, rate, and the cost by tasks for a period.

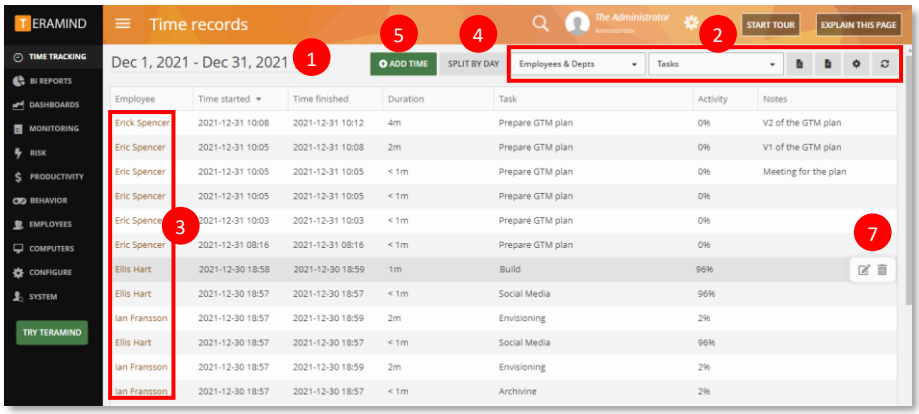


1. You can set a reporting period by clicking the **Calendar** .
2. By accessing the options at the top-right corner of the screen, you can filter the report by employees/departments, and tasks. You can also export the report in CSV/PDF format and specify what columns the report will display or export.
3. Clicking the small **Person with Clock** icon in front of a task will open a pop-up window where you can view a breakdown of cost by employees and time records for that task. See the Employee Cost and Time Records sections to learn more.

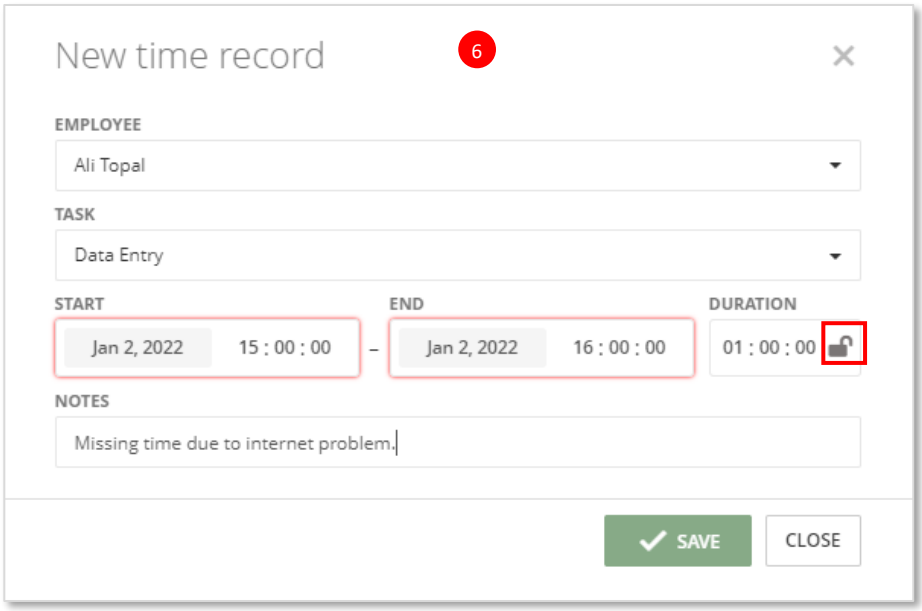
> To calculate the task costs properly, you need to set the RATE option from the employee's profile > PERSONAL INFO tab.

1.7 Time Records

The Time Records screen shows a report of time started, time finished, duration, task, activity %, etc. by employees for a period.



1. You can set a reporting period by clicking the **Calendar** .
2. By accessing the options at the top-right corner of the screen, you can filter the report by employees/departments, and tasks. You can also export the report in CSV/PDF format and specify what columns the report will display or export.
3. Clicking an **employee's name** will open the activity history for that employee. Check out the Viewing an Employee's Monitoring Report section to learn more.
4. Turing the **SPLIT BY DAY** toggle button on will group the rows by date.
5. **Adding Time:** You can click the **ADD TIME** button on top of the report. A pop-up window will appear:



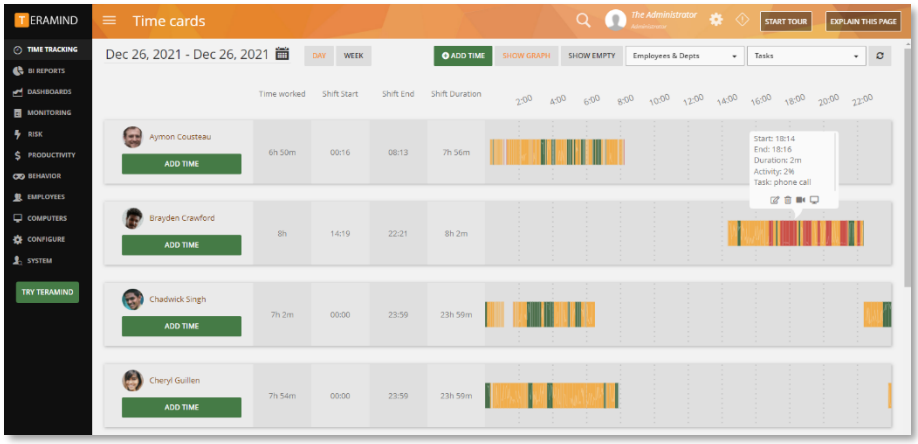
6. Select the **EMPLOYEE**, **TASK**, and enter a **START** date/time and **END** date/time. Click the **Locked** or **Unlocked** icon to lock/unlock the **DURATION** field. If it's unlocked, you can enter a duration manually, otherwise, it will be calculated automatically. You can optionally add **NOTES** to the time record.
7. **Editing/Removing Time:** Hovering over a time record/row will show two small icons on the right side of the screen. Click the **Pencil** icon to edit time. You can then edit the time the same way you would add time.
   Click the **Trash Can** icon to delete the highlighted time record.

> You can also add/edit/remove time from the Time Cards and the Employees > Snapshots screens.

1.8 Time Cards

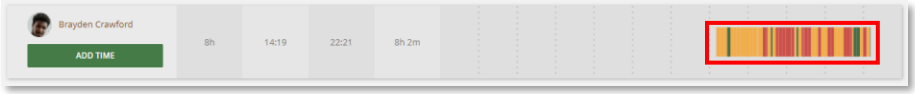
The Time Cards screen shows a detailed report of time worked and activity % of the employees. You can also add/remove time, view session records, and key monitoring reports from this screen.

You can switch the view between the Day View and Week View.



1.8.1 Activity Graph Color Guide

The Time Cards report shows the activity level on a colored bar graph:



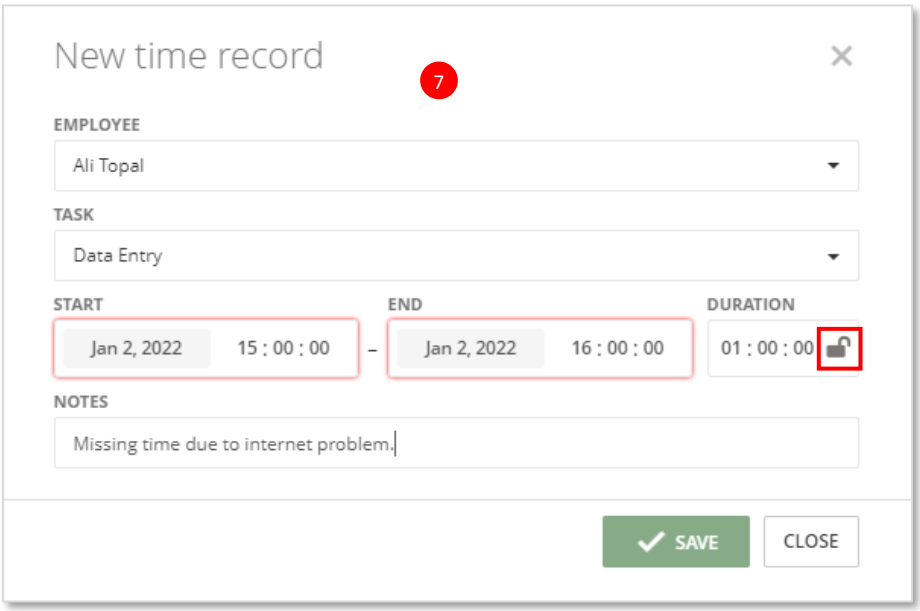
The table below shows what each color bar represents:

	Green	70% – 100% activity
	Orange/Yellow	11% – 69% activity
	Red	0% – 10% activity
	No Color/Gap	No data available / user was offline

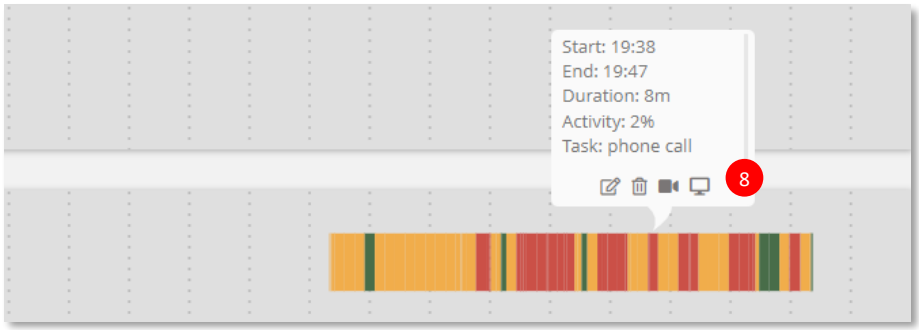
1.8.2 Day View

The Day view shows the time worked, shift start, shift end, shift duration, and detailed breakdown of activity for a single day.

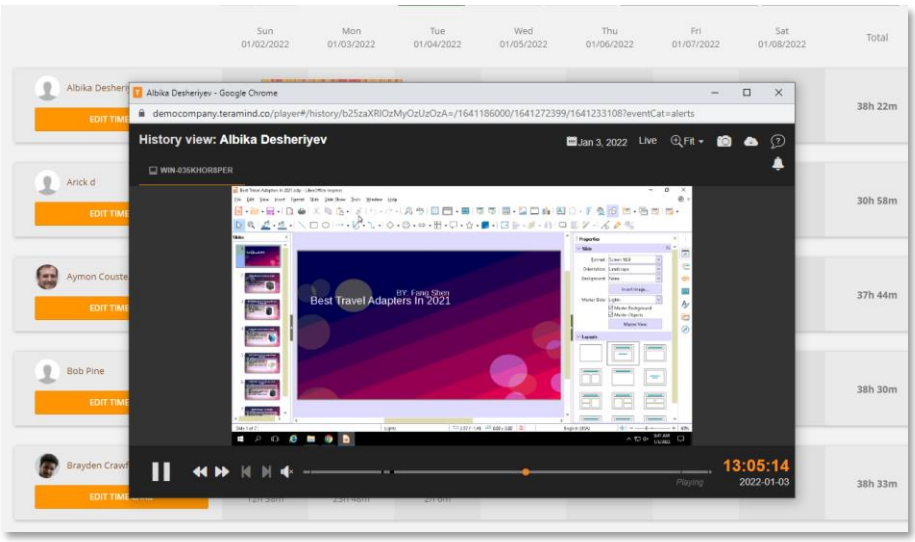
1. Click the **DAY** button to switch the view to the daily view.
2. You can set the report date by clicking the **Calendar** . Note that if you select a period instead of a single day from the calendar, the view will automatically switch to the Week View.
3. Clicking the **SHOW GRAPH** button to show/hide a white line graph overlaid on top of the activity bar graph. While the bar graph shows the activity level as a color chart (see Activity Graph Color Guide above), the line graph shows the actual activity %.
4. Click the **SHOW EMPTY** graph button to show/hide empty days.
5. You can filter the report by employees/departments, and tasks by using the filter options near the top-right corner.
6. **Adding Time:** Clicking the **ADD TIME** (either on top of the report or under an employee's name on the left) button will pop up a *New time record* window:



7. Select the **EMPLOYEE** and **TASK** and enter a **START** date/time and **END** date/time. Click the **Locked** or **Unlocked** icon to lock/unlock the **DURATION** field. If it's unlocked, you can enter a duration manually, otherwise it will be calculated automatically. You can optionally add **NOTES** to the time record.
8. Hovering over the activity graph will show a small pop-up window where you can see the details for that time slot such as start time, end time, duration, activity %, and task. At the bottom of that window you will also see several icons:

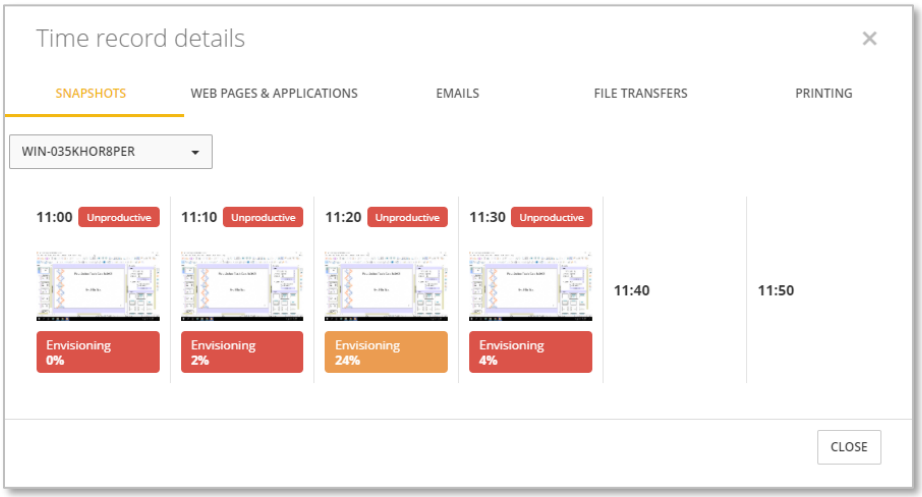


- **Editing Time:** Click the **Pencil** icon to edit time. An *Edit time record* similar to the *New time record* window will pop up where you can change the time.
- **Deleting Time:** Click the **Trash Can** icon to delete the selected time slot.
- **Viewing the Session Records:** Click the **Movie Camera** icon to view the session recording of the employee for the selected timeslot:



Check out the Session Player section for more information.

- **Viewing the Monitoring Reports:** Clicking the **Monitor** icon will pop up a window that will display some key monitoring reports, such as the Snapshots, Web Pages & Applications, Emails, etc. for that employee:

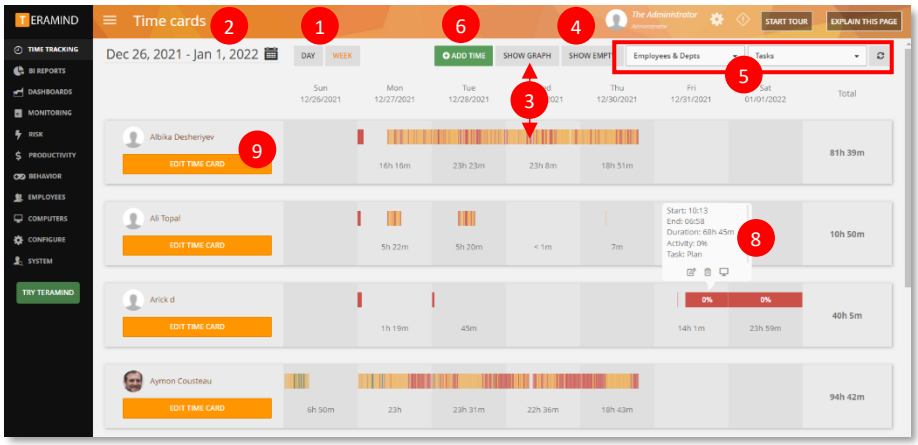


Check out the Viewing an Employee's Monitoring Reports section to learn more.

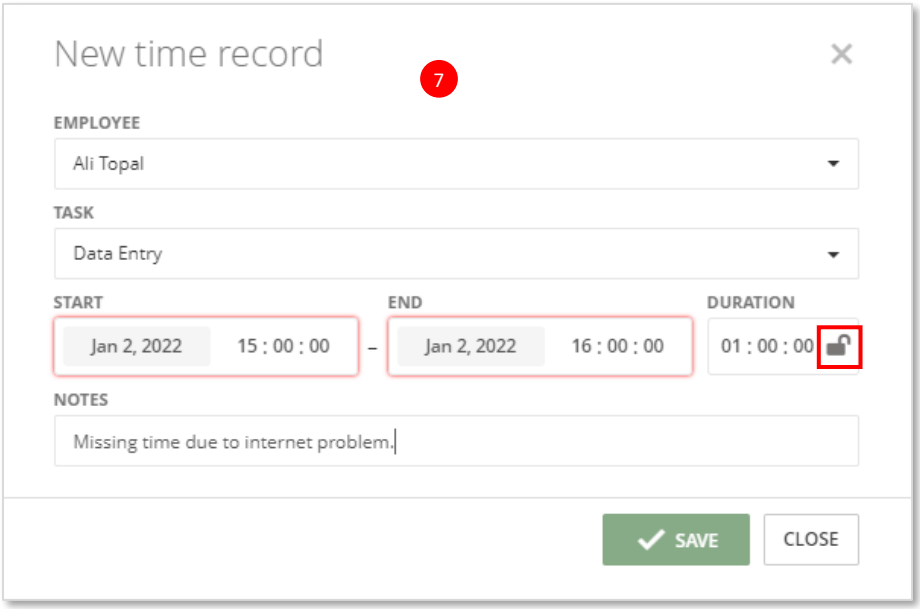
You can also add/edit/remove time from the Time Records and the Employees > Snapshots screens.

1.8.3 Week View

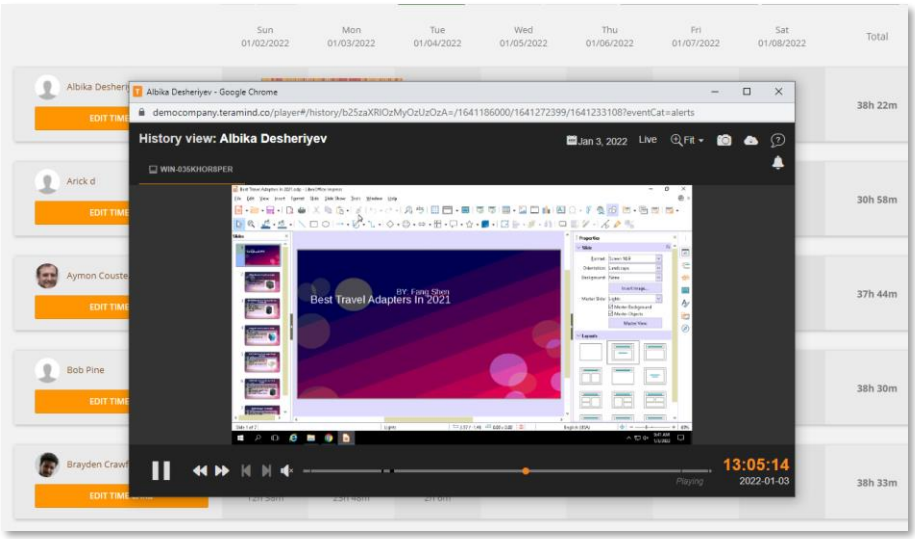
The Week view shows the time worked, shift start, shift end, shift duration and detailed breakdown of activity.



1. Click the **WEEK** button to switch the view to the weekly view.
2. You can set the reporting period (max 7 days) by clicking the **Calendar** 📅. Note that if you select a single day from the calendar, the view will automatically switch to the [Day View](#).
3. Clicking the **SHOW GRAPH** button to show/hide a white line graph overlaid on top of the activity bar graph. While the bar graph shows the activity level as a color chart (see [Activity Graph Color Guide](#) above), the line graph shows the actual activity %.
4. Click the **SHOW EMPTY** graph button to show/hide empty weeks.
5. You can filter the report by employees/departments, and tasks by using the filter options near the top-right corner.
6. **Adding Time:** Clicking the **ADD TIME** (either on top of the report or under an employee's name on the left) button will pop up a *New time record* window:

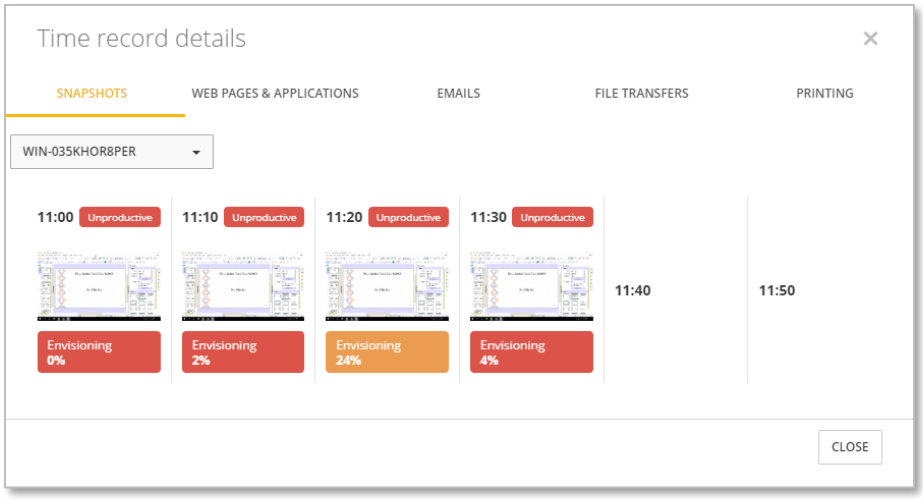


7. Select the **EMPLOYEE** and **TASK** and enter a **START** date/time and **END** date/time. Click the **Locked** or **Unlocked** icon to lock/unlock the **DURATION** field. If it's unlocked, you can enter a duration manually, otherwise, it will be calculated automatically. You can optionally add **NOTES** to the time record.
8. Hovering over the activity graph will show a small pop-up window where you can see the details for that time slot such as start time, end time, duration, activity %, and task. At the bottom of that window you will also see several icons:
    - **Editing Time:** Click the **Pencil** icon to edit time. An *Edit time record* similar to the *New time record* window will pop up where you can change the time.
    - **Deleting Time:** Click the **Trash Can** icon to delete the selected time slot.
    - **Viewing the Session Records:** Click the **Movie Camera** icon to view the session recording of the employee for the selected timeslot:



Check out the Session Player section for more information.

- **Viewing the Monitoring Reports:** Clicking the **Monitor** icon will pop up a window that will display some key monitoring reports, such as the Snapshots, Web Pages & Applications, Emails, etc. for that employee:



Check out the [Viewing an Employee's Monitoring Report](#) section to learn more.

9. **Adding/Editing Time in Batch Mode:** Clicking the **EDIT TIME CARD** button under an employee's name will expand the row to show a breakdown view of all the tasks and time entries for the week. You can then edit existing tasks/time entries or add new entries if wanted:

10. Select an existing task or choose a new task by clicking the *Choose task* pull-down menu.
11. Enter time in the fields marked with seven dots.
12. Click the **SAVE** or **DISCARD** button to save or discard the time entry.

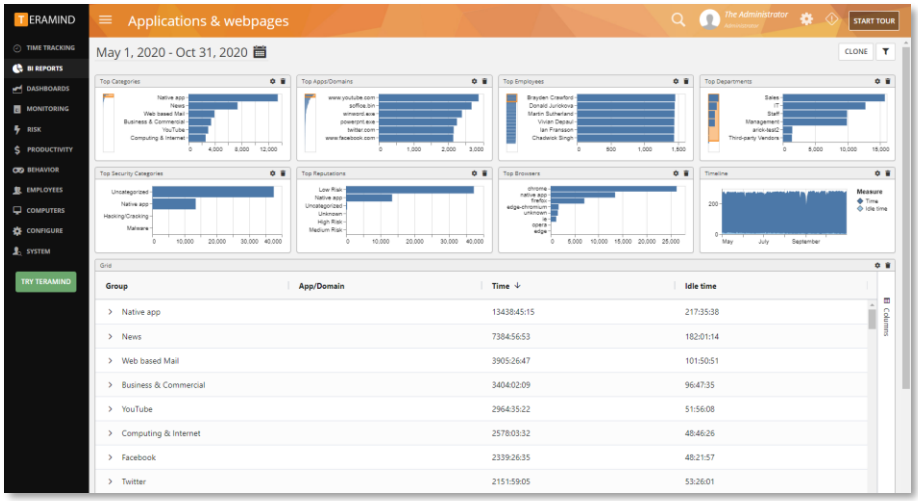
> You can also add/edit/remove time from the [Time Records](#) and the [Employees > Snapshots](#) screens.

2 BI Reports

2.1 Introduction to BI Reports

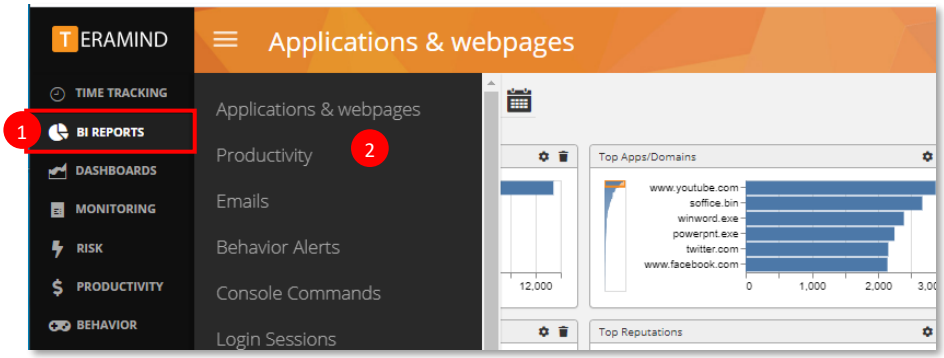
BI (Business Intelligence) Reports are powerful tools that simplify visualization and analysis of complex data. With these reports, managers can get timely and quick access to key information such as app and online activity, task and project engagement, work time analysis, security risks and more.

Teramind comes with several pre-built BI report templates for common KPIs important to any business, such as Applications & Webpages, Productivity, Emails, Behavior Alerts, Login Sessions, File Events etc. You can also 'clone' any of these built-in reports and customize them to your needs.



You can quickly create your own reports with easy to use widgets in visually engaging formats using bars, charts, heatmaps, and tables. The reports can be filtered by employees, departments, computers and other data points. Each report screen also has its own settings you can use to finetune what data it displays and how.

2.2 Accessing the BI Reports Menus

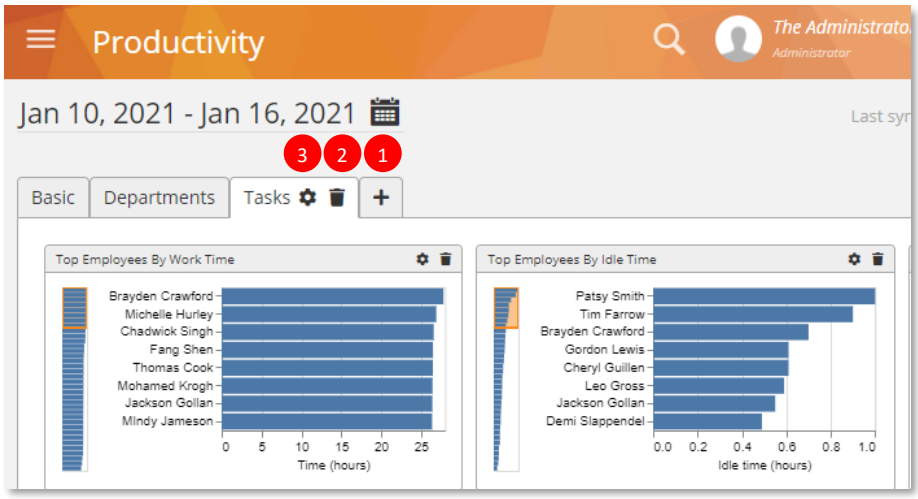


3. To access a BI Report, hover your mouse over the **BI Report** menu, then

4. Select a report from the **sub-menu**, such as *Applications & webpages*, *Productivity* etc.

2.3 Report Tabs

Each Pre-Built BI Report comes with one or more tabs. This is to help you organize your information and quickly add different views for the data. You can also add your own tabs on a Custom BI Report.



1. Click the small **+** icon on top to add a new tab. After you have added a tab, you can then add widgets to populate it. Check out the BI Widgets section to learn more about widgets.
2. Click the small **Trash Can** icon to delete a tab.
3. Click the small **Gear** icon to rename the tab.

2.4 Pre-Built BI Reports

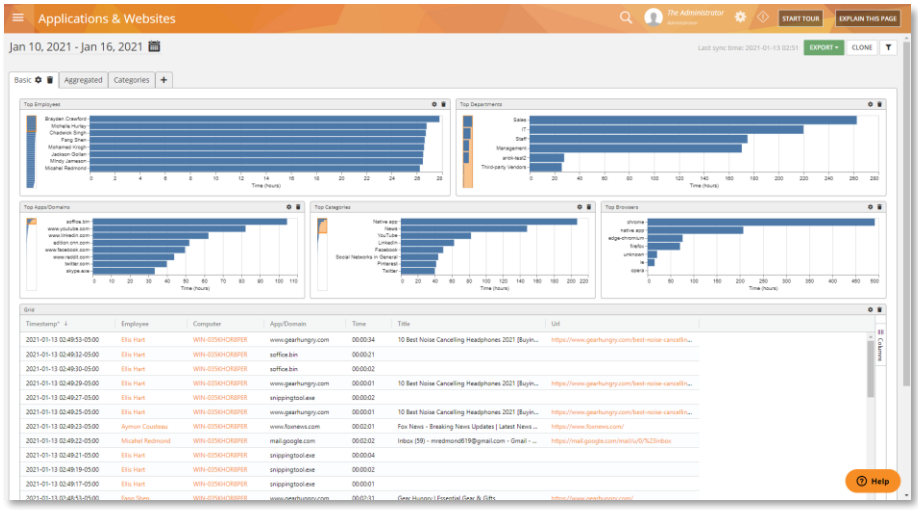
Teramind comes with several pre-built BI reports. You can use them as-is or configure or use them as templates for creating your own Custom BI Reports.

> While Teramind allows you to edit the Pre-Built BI Reports, the changes are temporary and only available as long as you are on the report page. If you refresh the page or log out, the changes will be lost. To make the changes permanent, use the Custom BI Reports instead.

2.4.1 Applications & Websites

This report highlights app and web usage statistics for employees and departments. It comes with three tabs: *Basic*, *Aggregated* and *Categories*. The *Basic* tab and the *Aggregated* tab both contain the same widgets such as Top Employees, Top Departments, Top App/Domains, Top Categories*, Top Browsers etc. The only difference is the *Grid Widget*(table) that groups employees by App/Web category. For the *Basic* tab, the *Grid Widget* shows all employees by timestamp whereas the *Grid Widget* on the *Aggregated* tab groups it by app/website. The third tab, *Categories* has few more *Chart Widgets* such as

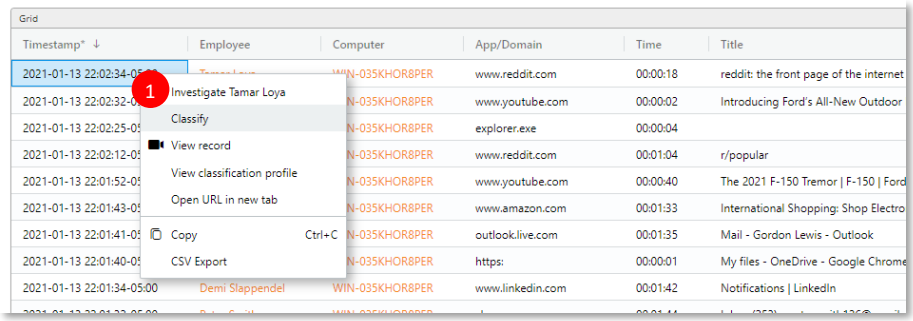
Top Security Categories*, Top Reputations*, Classification Timeline etc. And the *Grid Widget* on this tab groups employees by web/app Categories.



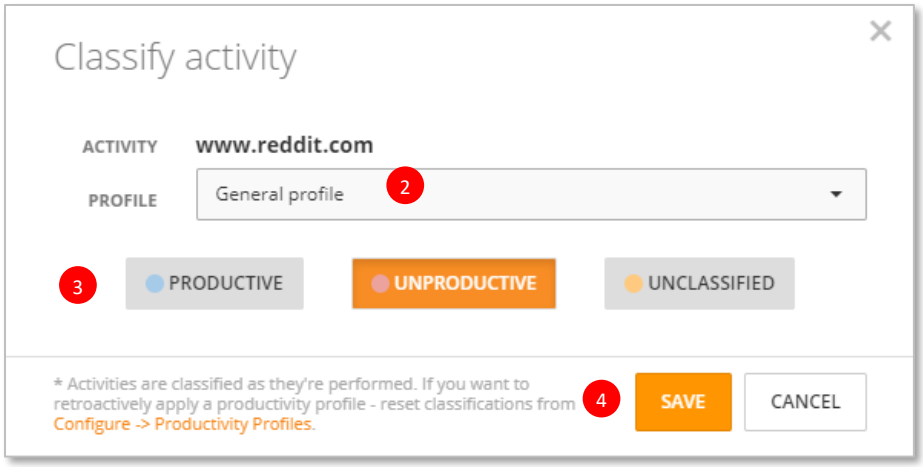
***About Security Categories and Reputations Widgets**
Teramind uses inCompass® NetSTAR, a comprehensive web categorization and filtering technology to automatically classify websites and their reputations.

2.4.1.1 Classifying Web Pages & Applications as Productive/Unproductive

Productivity Profiles determine how apps/websites are classified as productive/unproductive. This, in turn, will affect how Productive Time, Unproductive Time etc. are reported. You can also quickly classify an item from the *Grid Widget* on any of the tabs:



1. Right click on a row on any of the Grid Widgets and select the **Classify** option from the pop-up menu.



4. Select a productivity **PROFILE**.
5. Select any of the **PRODUCTIVE**, **UNPRODUCTIVE** or **UNCLASSIFIED** option.
6. Click **SAVE** to save the classification. Note that activities are classified as they are performed. If you want to retroactively apply a productivity profile - reset classifications from Configure -> Productivity Profiles.

To learn how to classify a group of activities, configure the productivity profiles or reset them, check out the Productivity Profiles section of the User Guide.

2.4.1.2 Aggregating Similar Items

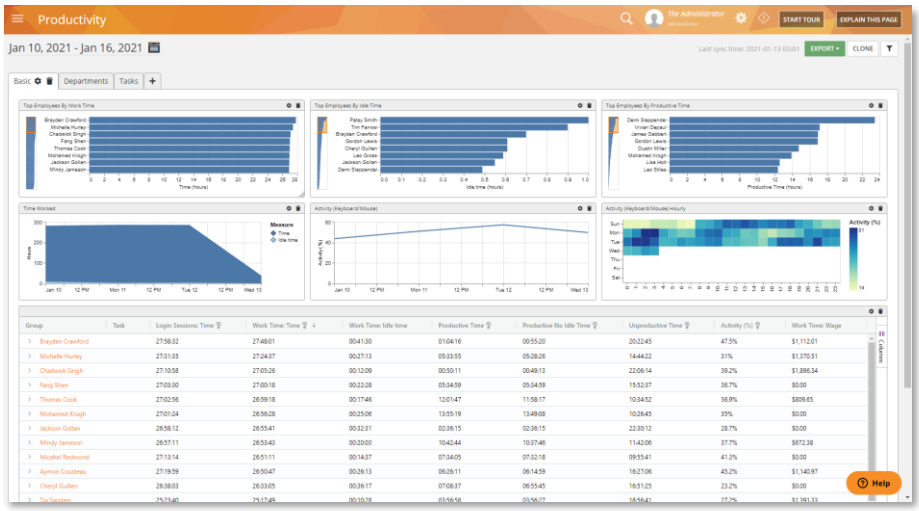
Both the *Aggregate* and *Categories* tabs shows employee times grouped by app/web and category. You can, of course, create a custom report and add your own widgets on it to show aggregated items.

2.4.1.3 Showing Idle Time

Both the *Aggregate* and *Categories* tabs shows idle time on the *Grid Widgets*. You can, of course, create a custom report and add your own widgets on it to show idle times and compare it with other data points such as Idle Time vs Active Time.

2.4.2 Productivity

This report highlights productivity and performance KPIs for employees and departments. It comes with three tabs: *Basic*, *Departments* and *Tasks*. The *Basic* tab shows several *Chart Widgets* such as, Top Employees by Work Time, Idle Time and Productive Time, Time Worked, Activity % etc. The tab also contains a *Grid Widget* showing Task, Login Sessions Time, Work Time, Idle Time etc. by employees. The *Departments* tab shows similar information except the Grid Widget groups the information by department. There are also three widgets (Classification, Activity and Top By Idle Time) that shows information by department. The *Tasks* tab shows similar information like the Basic and Departments tabs but groups them by tasks.



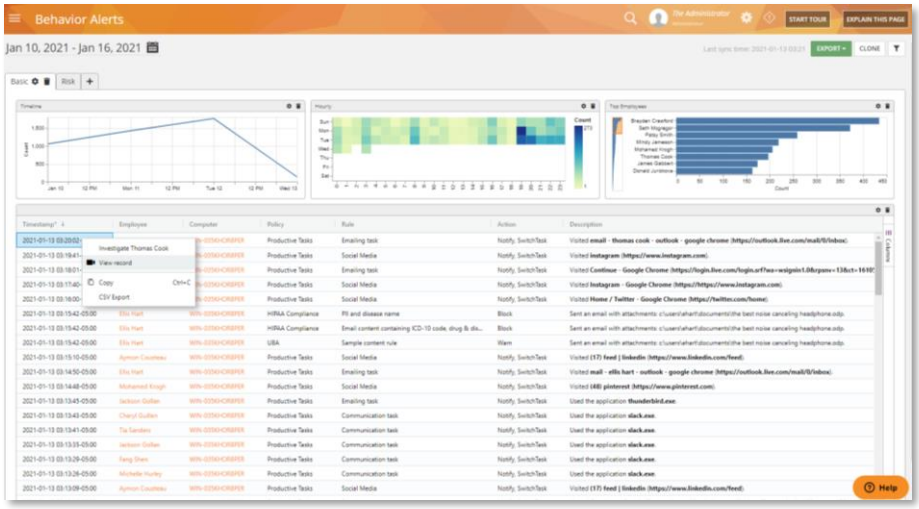
For an explanation of the productivity metrics, check out the Productivity Report Explained section on the User Guide to learn more.

Productive Time, Unproductive Time etc.
Productivity Profiles determine how apps/websites are classified as productive/unproductive. This, in turn, will affect how Productive Time, Unproductive Time etc. are reported.

2.4.3 Behavior Alerts

This report shows all the rule violation incidents (triggered by the regular Rules) and any anomalies (triggered by the Anomaly Rules). This report shows details for all alerts, actions taken by the system and risk information for employees and departments. It comes with two tabs: *Basic* and *Risks*. The *Basic* tab contains several *Chart Widgets* that shows no. of alerts (count) for the timeline, Hourly and Top Employees. There is also a *Grid Widget* (table) that show the Timestamp, Employee, Computer, Policy, Rule, Action taken by the system and a Description of the alert.

The *Risk* tab allows you to conduct organization-wide risk assessment. It contains several *Chart Widgets* that shows various alert and risk comparisons such as Alerts & Risk by timeline, Risk Heatmap, Top Risky Employees/Departments etc. It also has a *Grid Widget* that shows information similar to the *Grid Widget* on the *Basic* tab but shows risk details grouped by tags.



2.4.3.1 Plotting the Risk Trend

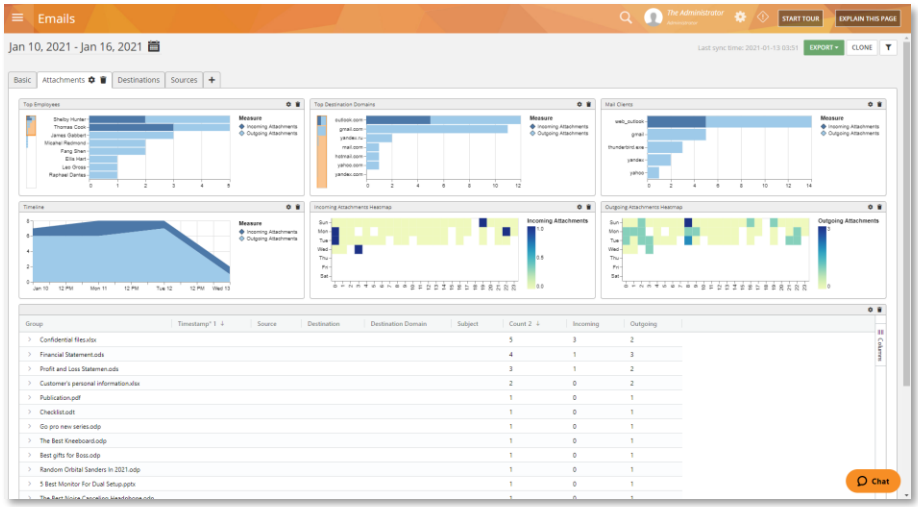
The Alerts & Risk Timeline and the Risk Heatmap shows risk trends. You can also create your own custom report and add any trends you want to plot. For example, Risk Score by Departments, Frequency of Risk Violation by Tags etc.

2.4.3.2 Identifying High Risk Users, Rules and Objects

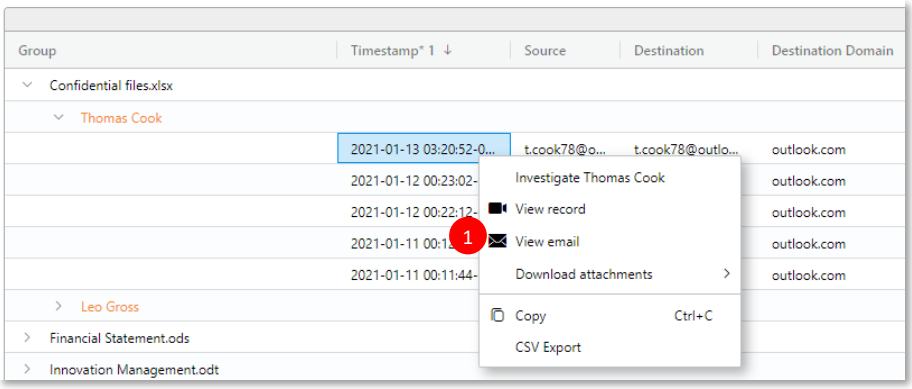
The Top Risky Employees, Top Risky Departments, Top Risky Rules etc. shows these. You can also create your own custom report and add any rated items you want. For example, Top Risky Object, Top Risky Object Type etc.

2.4.4 Emails

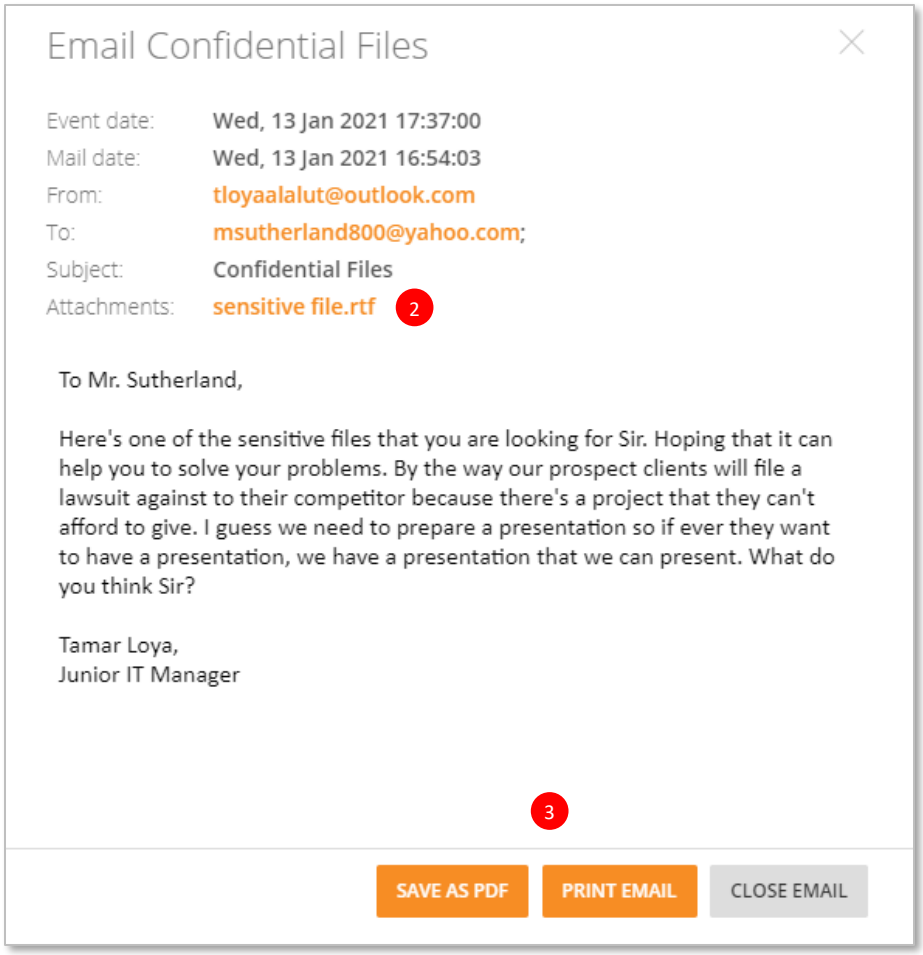
This report displays all the email activity for employees and departments. It comes with several tabs such as *Basic*, *Attachments*, *Destinations*, *Sources* etc. Each tab contains various *Chart Widgets* to give you all the details you might need of the email activities of your employees such as incoming/outgoing emails by Timeline, Top Employees by no. of emails sent/received, Attachment Heatmaps, Top Destination Domains, statistics for email Sources etc. There is also a *Grid Widget* (table) on each tab that shows all the incoming and outgoing emails with timestamps that can also be grouped employees by employee, attachment, destination, source etc.



2.4.4.1 Viewing / Saving / Printing Email Contents and Attachments

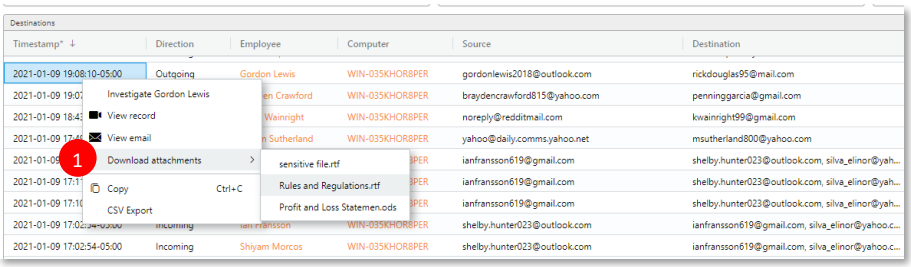


1. Right click on a row on any of the *Grid Widgets* and select the **View email** option from the pop-up menu (you might need to expand a grouped row until you see the Timestamps to be able to see this option). A pop-up window will open:



2. If there are any attachments (and you have enabled attachment captures on the [Email Monitoring Settings]) then, you can click on the attachment(s) to download them.
3. You can save a copy of the email by clicking the **SAVE AS PDF** button or print it with the **PRINT EMAIL** button.

2.4.4.2 Saving Email Attachments

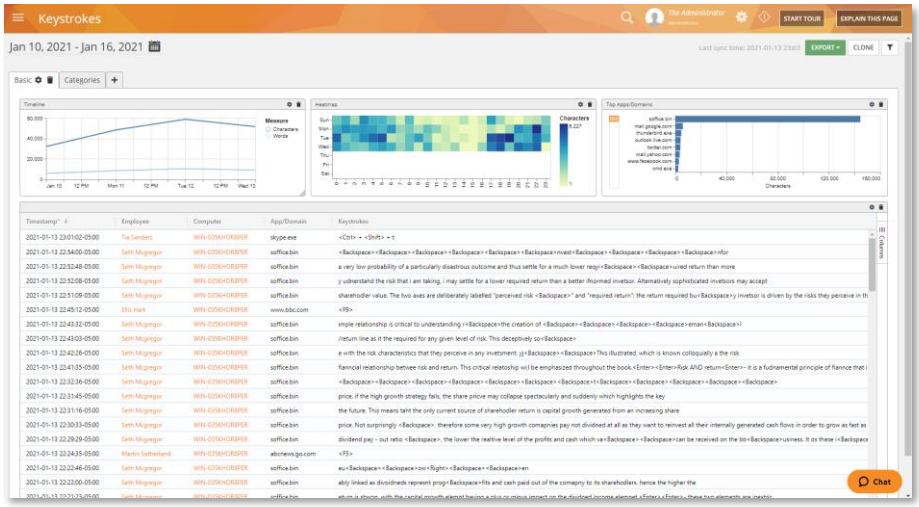


1. Right click on a row on any of the *Grid Widgets* and select the **Download attachment** option and the file to download (you might need to expand a grouped row until you see the Timestamps to be able to see this option). Note: you can also save an attachment from the [email view window].

2.4.5 Keystrokes

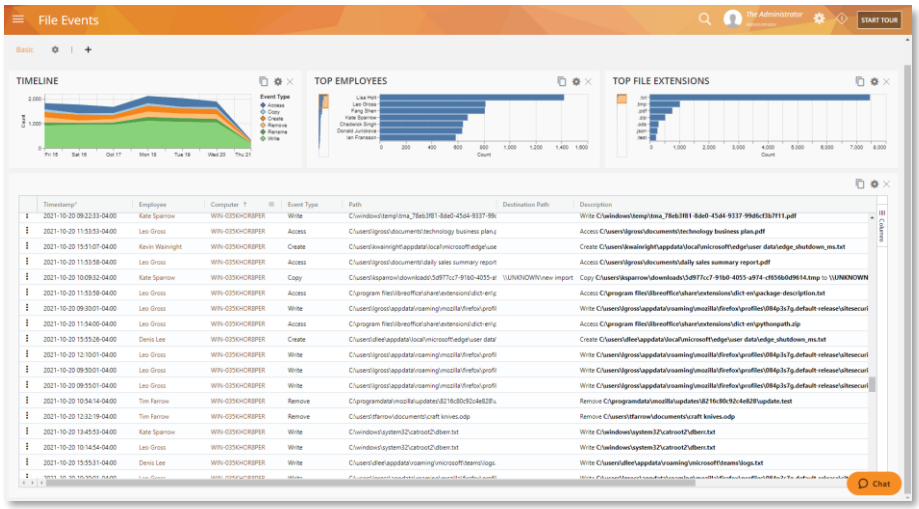
This report shows statistics of all keystrokes entered by the users. In addition to regular characters the report also tracks words and phrases, special commands (i.e. clipboard copy/paste), use of special keys and hidden symbols such as the <Print Screen>, <CapsLock>, <Backspace> etc. etc. The repot comes with two tabs: *Basic* and *Categories*. The Basic tab comes with several *Chart Widgets*: Timeline (shows no. of words vs no. of characters/letters typed for the duration), a Heatmap of no. of characters typed and a Top App/Domains where the most keyboard activity occurred. There is also a *Grid Widget* (table) that shows all keystrokes by Timestamp, Employee, Task and App/Domain etc.

The *Categories* tab shows similar information but for app/web Categories, Security Categories and Reputation Categories.



2.4.6 File Events

This report shows statistics of all file events on the local drives, external drives (such as USB drives), network and even Cloud files. The report comes with only one tab, *Basic*, that shows several *Chart Widgets*: Timeline (by the volume of file activities such as Access, Copy, Create, Rename, Remove/Delete, Upload etc.), Top Employees (who had the most file activities) and Top File Extensions. There is also a *Grid Widget* (table) that shows all file events by Timestamp, Employee, Process, Description etc.



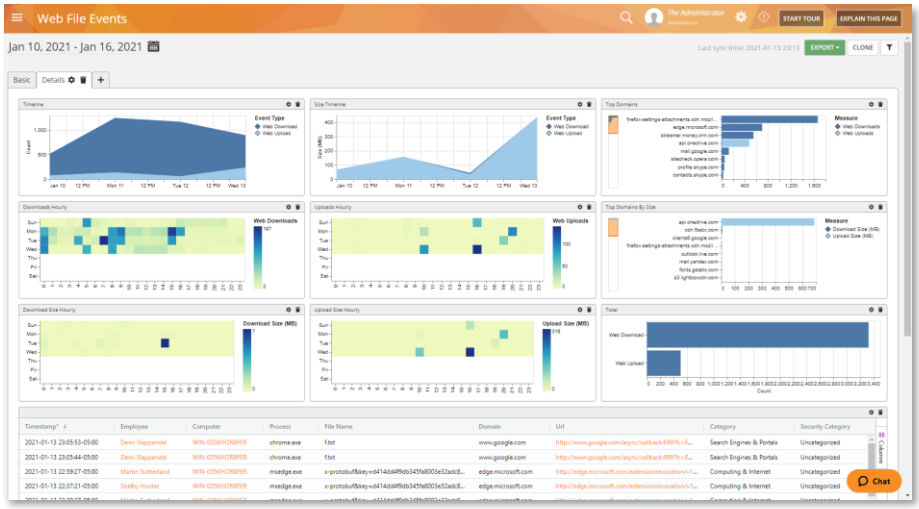
Note that Teramind cannot track the copy operation for a file from one network server to the same network server (e.g. source and destination is the same). For example, copying of a file from `\\103.247.55.101\source_folder` to `\\103.247.55.101\destination_folder` cannot be tracked. Copy to and from same local drives is detected as usual.

Also copying of an empty file cannot be tracked since it will be impossible for the system to distinguish between the file *create* and *copy* operations due to the zero size of the file.

2.4.7 Web File Events

This report shows statistics of all web file events (upload/download, cloud sync etc.). The report comes with two tabs, *Basic* and *Details*. The *Basic* tab shows several *Chart Widgets*: Timeline (by the volume of web upload and web download), Top Employees (who had the most web file activities) and Top Domains (by uploads/downloads). There is also a *Grid Widget* (table) that shows all web file events by Timestamp, Employee, Event Type, Domain, File etc.

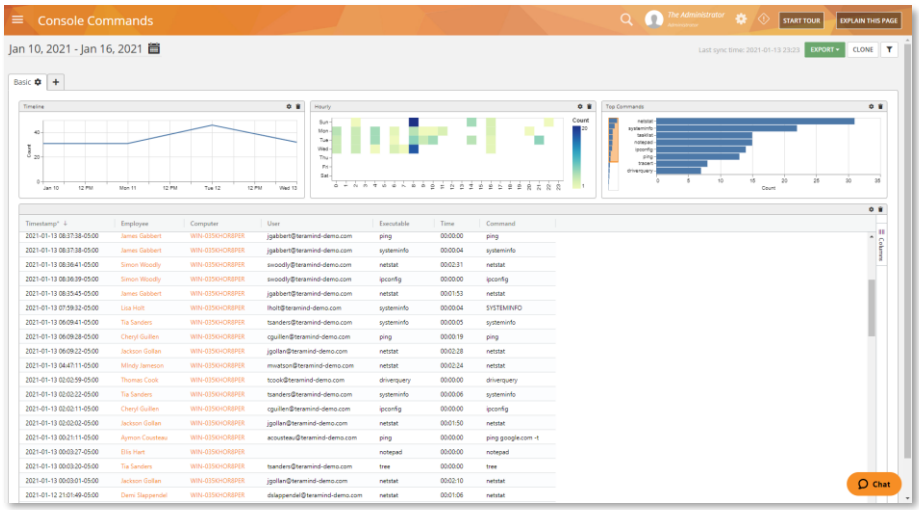
The second tab, Details, shows more details related to web file events such as charts for the size of uploads/downloads, volumes of upload/download by hour, top domains by size etc.



2.4.8 Console Commands

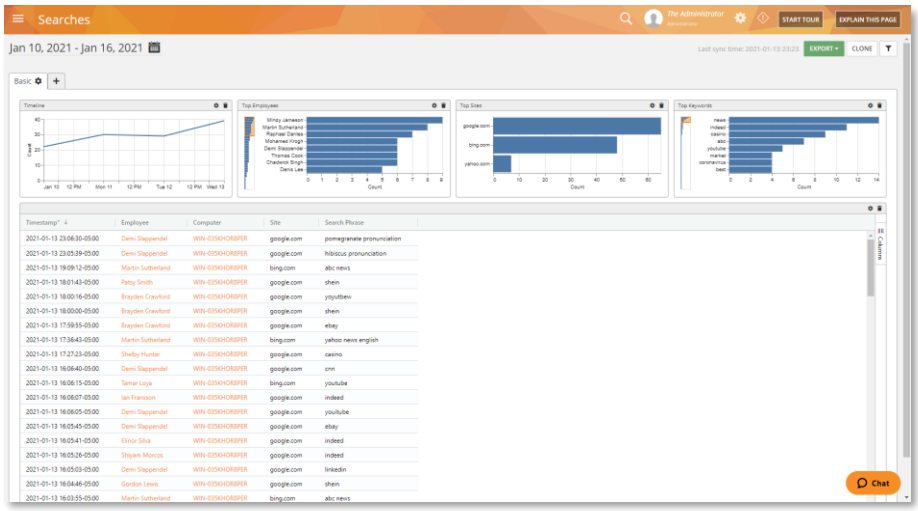
This report shows statistics of console/terminal commands executed by a user or an application from the command line. Console Commands can be useful to keep an eye on privileged users (system admins, power users etc.) as these commands are often used to execute system-level applications and scripts. In the wrong hands, such commands can be dangerous and need overseeing.

The report comes with only one tab, *Basic*, that shows several *Chart Widgets* for no. of commands for the Timeline, Hourly and Top Commands. There is also a *Grid Widget* (table) that shows all console commands by Timestamp, Employee, Executable (app), the actual Command etc.



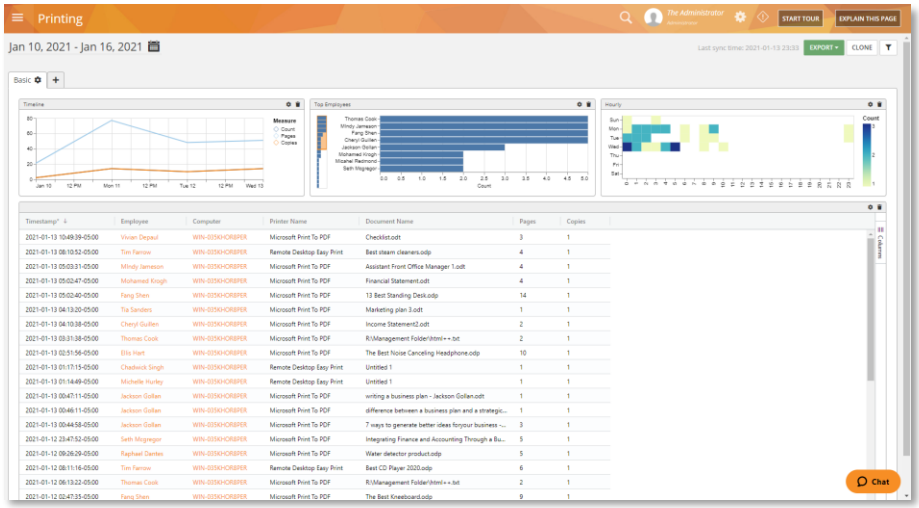
2.4.9 Searches

This report shows statistics on user searches on sites like Google, Bing, YouTube etc. The report comes with only one tab, *Basic*, that shows several *Chart Widgets* for no. of searches for the Timeline, Top searches by Employees, Sites and Keywords. There is also a *Grid Widget* (table) that show all searches by Timestamp, Employee, Site, Search Phrase etc.

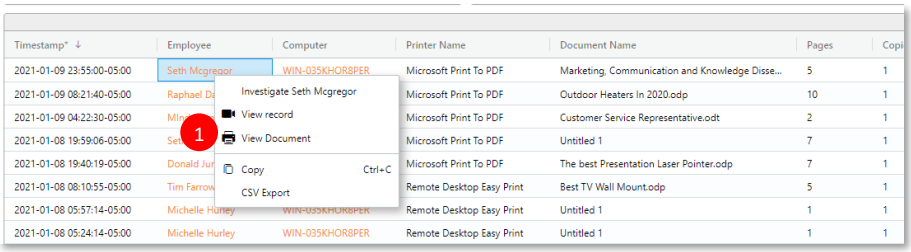


2.4.10 Printing

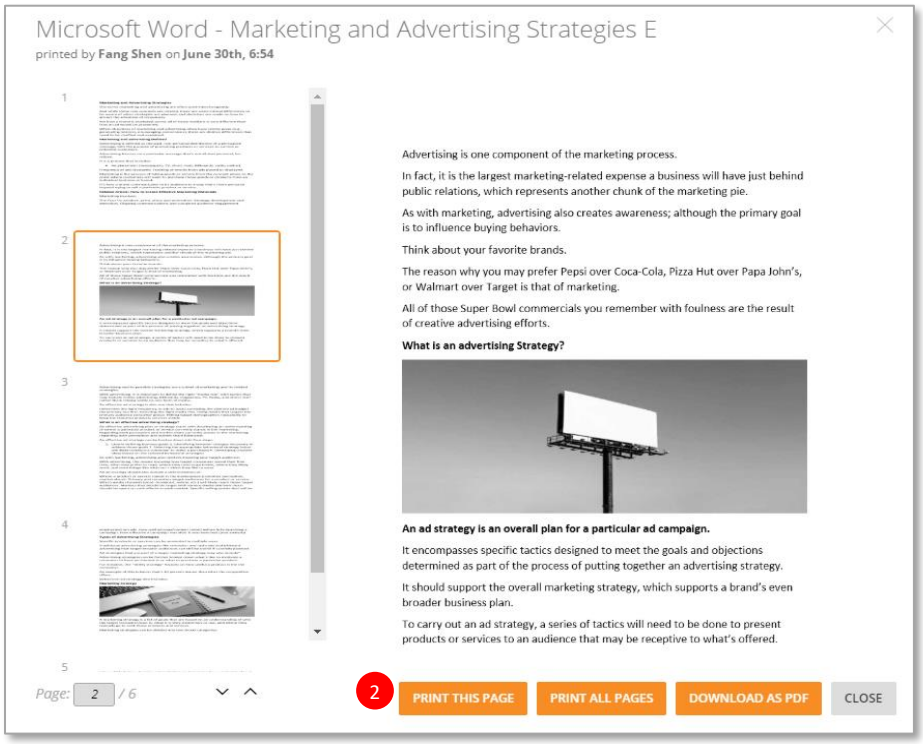
This report shows statistics on documents sent to the local or network printers. The report comes with only one tab, *Basic*, that shows several *Chart Widgets*: Timeline (shows no. of print jobs, pages and copies), Top Employees (by no. of print jobs) and an Hourly heatmap of the print jobs. There is also a *Grid Widget* (table) that shows all printing activity by Timestamp, Employee, Printer Name, Document Name, Pages, Copies etc.



2.4.10.1 Viewing / Saving Copies of a Printed Document



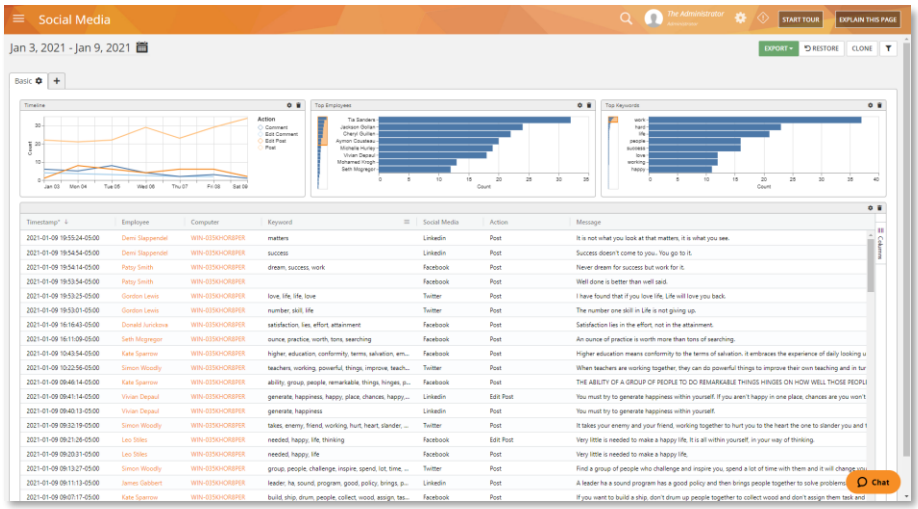
1. Right click on a row on the *Grid Widget* and select the **View Document** option from the pop-up menu. A pop-up window will open that will show the printed document:



2. Click one of the buttons at the bottom to print the document or download it as a PDF.

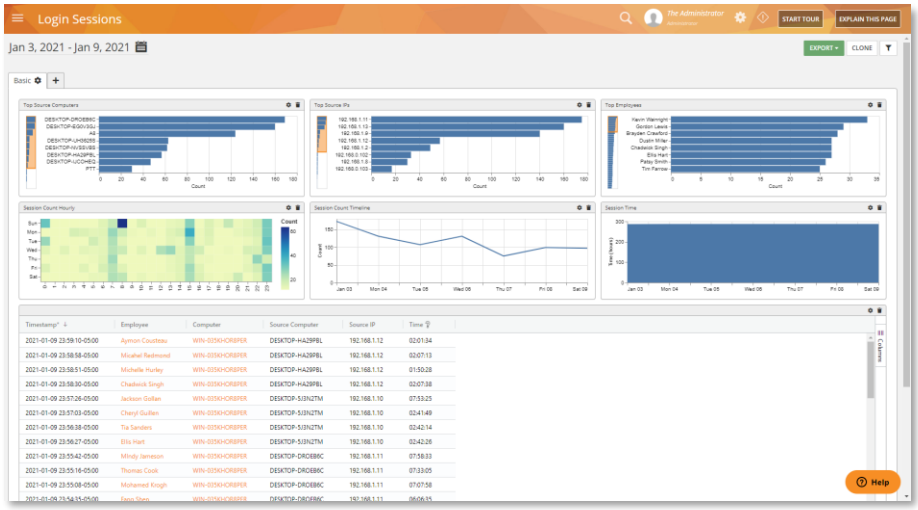
2.4.11 Social Media

This report shows statistics of employee social media activities for popular platforms such as Facebook, Twitter, LinkedIn etc. The report comes with only one tab, *Basic*, that shows several *Chart Widgets*: Timeline (shows no. actions for post, comment, edit post etc.), Top Employees (by no. of social media activities) and Top keywords. There is also a *Grid Widget* (table) that shows all social media activity by Timestamp, Employee, Computer, Keyword, Platform, the actual Message etc.

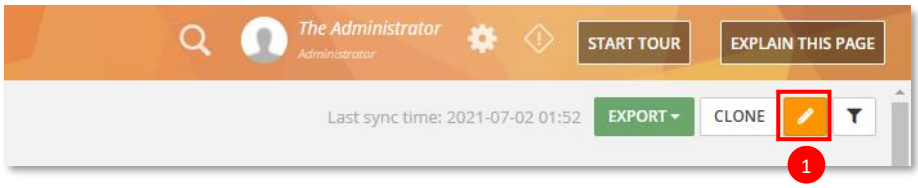


2.4.12 Login Sessions

This report shows an immutable logs of user sessions. The report comes with only one tab, *Basic*, that shows several *Chart Widgets* for session counts by Top Source Computer, Top Source IPs, Top Employees, Session Count by Hour, Session Count by Timeline and Session Time. There is also a *Grid Widget* (table) that shows all sessions by Timestamp, Employee, Computer, Source IP, Time (total logged in time including any locked sessions) etc.



2.5 Enabling / Disabling the Report Edit Mode



1. Click the **Pencil** icon near the top-right corner of a BI report to toggle its edit mode.

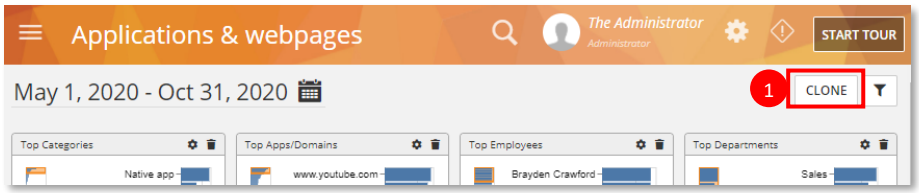
When the edit mode is enabled, you will be able to clone the report (see the Custom BI Reports section below), add/remove widgets and tabs, change widget settings and tab settings, etc.

This feature will help you keep your reports, especially the custom reports from changes by accident or by other users who have access to the reports.

2.6 Custom BI Reports

In addition to the pre-built BI reports, you can create your own custom BI reports by 'cloning' an existing report (a pre-built report or another custom report). You can also share these custom reports with your team.

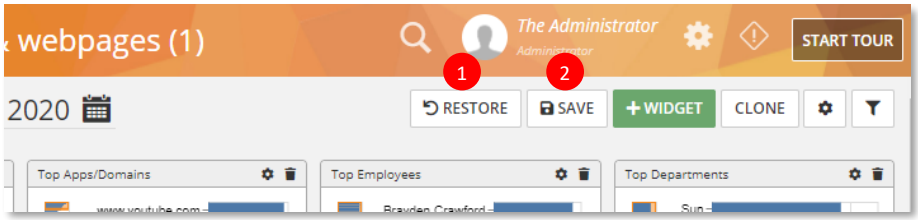
2.6.1 Creating a Custom BI Report



1. Click the **CLONE** button near the top-right corner of a report to create a copy/clone of it. You will be automatically switched to the newly created report screen. You can create multiple clones of a report. Each cloned report will have a default name and a number in the bracket, for example: *Applications & webpages (1)*, *Emails (2)* etc. Once create, you will be able to rename the report later (see the Renaming / Sharing / Deleting a Custom Report section below).

2.6.2 Saving/Restoring a Custom BI Report

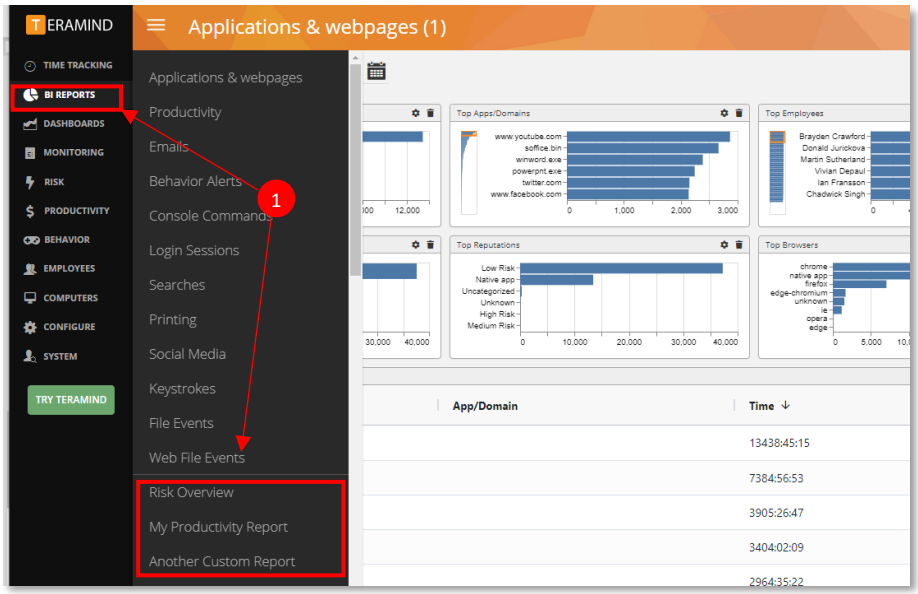
Any newly created custom report is automatically saved. However, if you change it (e.g. add/change a widget), you can save or restore it:



1. Click the **RESTORE** button to discard any changes you made to the report. If you made multiple changes, clicking the **RESTORE** button each time will undo the last change.
2. Click the **SAVE** button to save any changes.

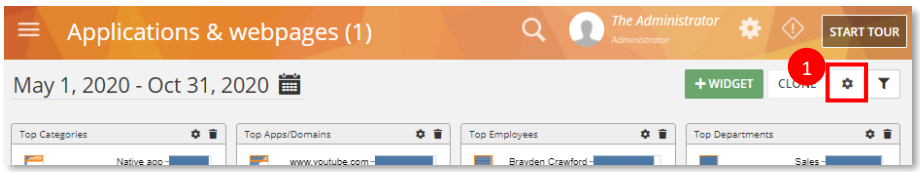
2.6.3 Accessing a Saved Custom BI Report

Any custom report you create is automatically saved. You can access them from the **BI REPORTS** menu:

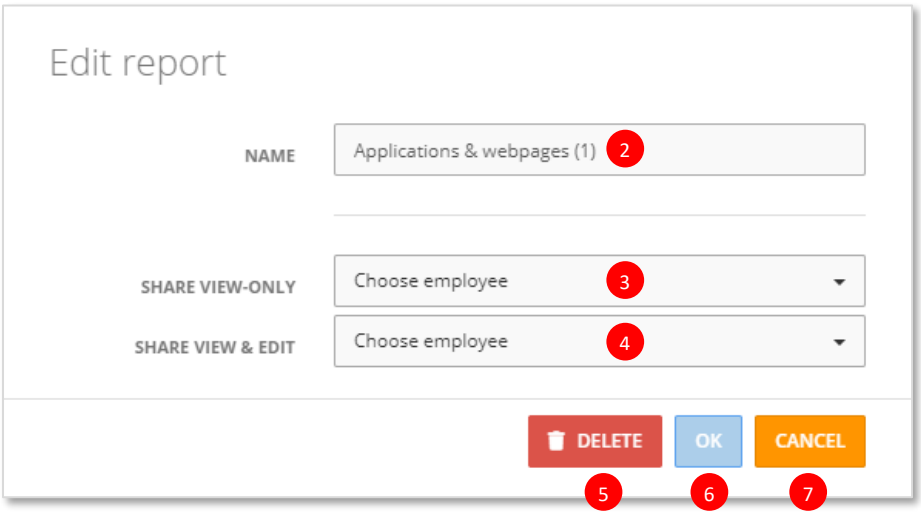


1. The custom reports will show up under the **BI REPORTS** menu, below the pre-built reports. Click a report to open it.

2.6.4 Renaming / Sharing / Deleting a Custom BI Report



1. Click the small **Gear** icon near to top-right corner of a custom BI report. An *Edit report* window will pop up:

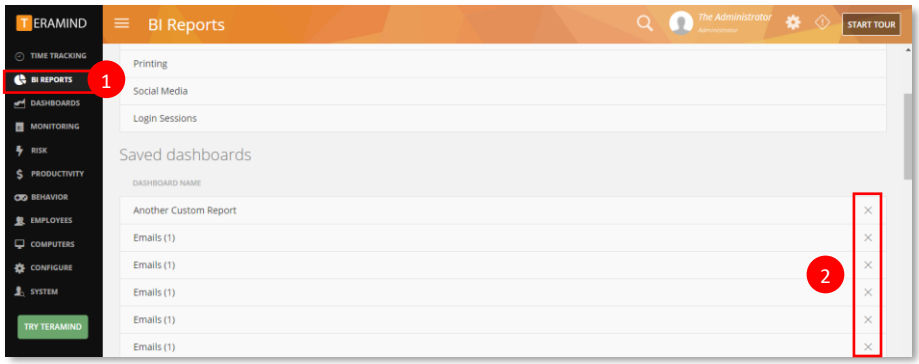


2. Enter a new name in the **NAME** field to rename it.

3. Select employees from the **SHARE VIEW-ONLY** drop-down list to share the report in view-only mode.
4. Select employees from the **SHARE VIEW & EDIT** drop-down list to share the report in view and edit mode. Selected employees will be able to edit the report.
5. Click the **DELETE** button to delete the report.
6. Click the **OK** button to save any changes.
7. Click the **CANCEL** button to cancel the changes.

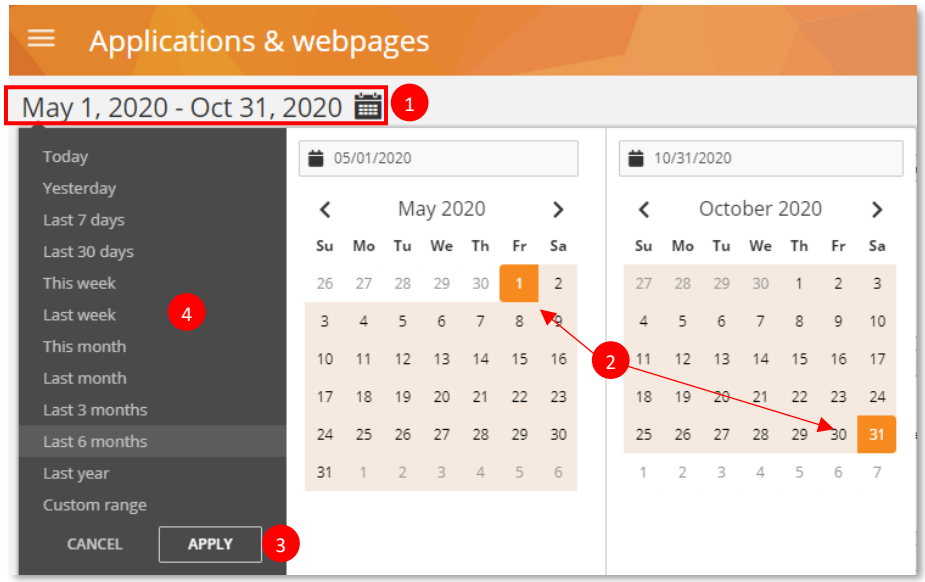
2.6.5 Deleting a Custom BI Report from the BI Report Menu

You can delete a custom BI Report from the *Edit report* panel (see the above section). You can also delete a custom BI Report from the BI REPORTS menu itself:



1. Click the **BI REPORTS** menu.
2. On the sub-menu, scroll down until you can see the *Saved dashboards* section. Under this section you will see all your custom reports. Click the **X** button next to a report to delete it.

2.7 Setting a Date Range for the BI Reports



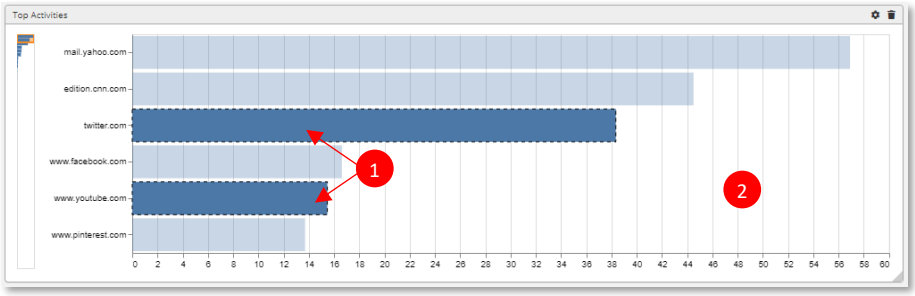
1. Each BI Report screen has a dates selector at the top-left corner. Click the **Dates Selector** button.
2. Select a start date (left) and an end date (right) from the dates-selector window.
3. Click the **APPLY** button.
4. You can also select one of the pre-defined date sets (i.e. Today, Yesterday, Last 7 Days etc.) from the left of the dates selector window without having to select the start/end dates.

> The data displayed on the BI widgets is not real-time. It can take up to 4 hours for it to refresh.

2.8 Drilling-Down / Filtering a BI Report

2.8.1 Using the Quick Drill-Down Feature

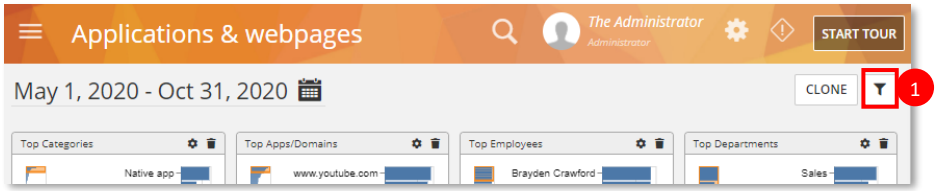
You can quickly drill-down/filter a Bar or Column chart to view the report for the select data point(s):



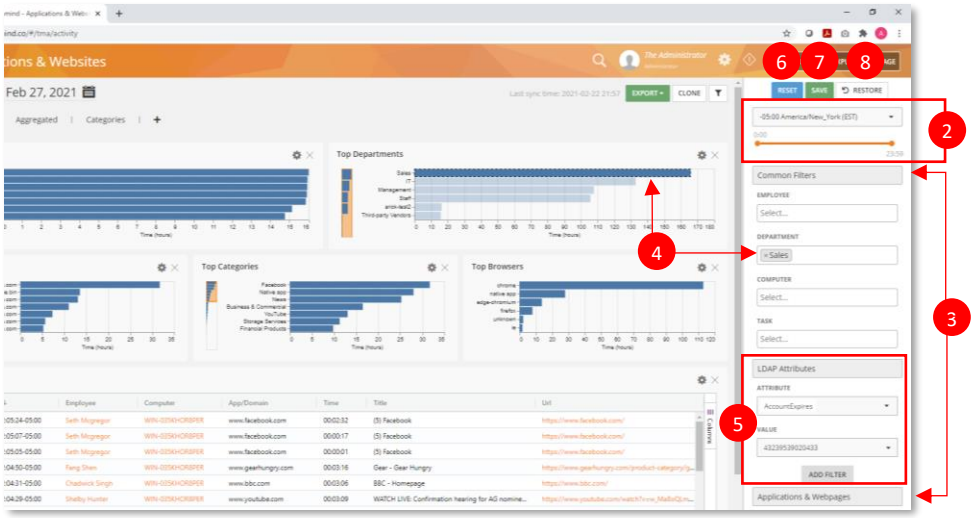
1. Click on a **bar/column** on a Bar or Column *Chart Widget* to drill-down. **SHIFT** + **Click** to select/deselect multiple bars or columns. All the other widgets (and the Filter Panel) will update to show data for the selected bar's/column's data point.
2. Click on an **empty area** inside the chart canvas to deselect and return to the original chart.

2.8.2 Using the Filter Panel

The Filter Panel allows you to configure all filters available for a report. Each BI report has a time-range filter and a set of common filters that let you narrow down the number of items displayed. You can filter by employees, departments, computers, tasks etc. Additionally, each report also has its own content-specific filters. For example, the Emails BI Report has filters for subject, body, mail directions, email clients, attachments etc. To use the Filter Panel:



1. Click the **Filter** icon near the top-right corner of a report to open/close its filter panel:



2. Use the **Time Zone** drop-down menu to select a time zone for the report. You can also drag the **Timeslot Sliders** ● to set a time range.
3. Click the **Filters** buttons (such as *Common Filters, Applications & Webpages, Behavior Alerts* etc.) to expand/collapse the filter.

> *Common Filters* such as EMPLOYEES, DEPARTMENTS etc. are available to all BI Report. Other filters may be available depending on what widgets are displayed on the report. For example, if you use a widget that displays data sources from the emails, then you will see an *Emails* filter on the list. Check out the BI Widgets section below to learn more about widgets.

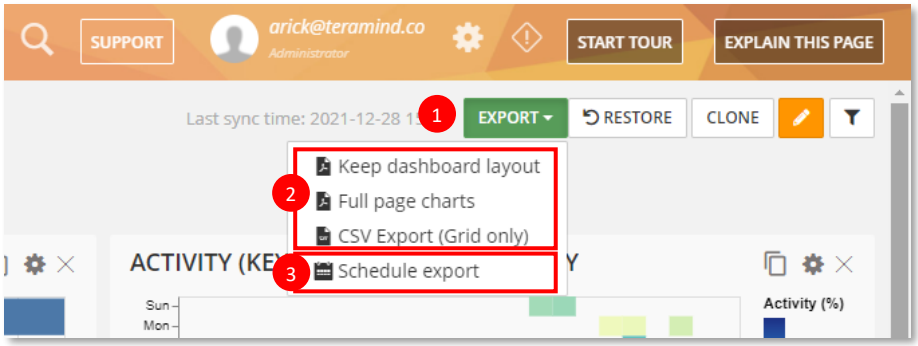
4. When you expand a filter, you will see fields to set the filter's criteria. For example, you can select specific employee(s) or department(s) under the *Common Filters*. You can also click on a chart data element (such as a bar on a bar chart). The clicked element will then highlight, and rest of the chart will become semi-transparent. The Filter panel will automatically update with the selected field.
5. If you have Active Directory integration setup, you will see an additional filtering option: *LDAP Attributes*. Click the filter to expand it. You can then select ATTRIBUTE and VALUE pairs to filter the report. You can add as many attributes as you need by clicking the **ADD FILTER** button.

> Note that Active Directory *attributes* are not available as data points and cannot be displayed on the BI reports. However, you can still use them to filter any report.

6. Click the **RESET** button on top of the panel to reset any changes you made on the Filter Panel.
7. Click the **SAVE** button to save the filter. Note that, this option is available for custom reports only.
8. Click the **RESTORE** button to restore the filter to its latest saved version. Note that, this option is available for custom reports only.

2.9 Exporting a BI Report

A BI report can be exported as a CSV and/or PDF file or scheduled for auto-delivery to email address(es). Follow the instructions below to export/schedule a report:

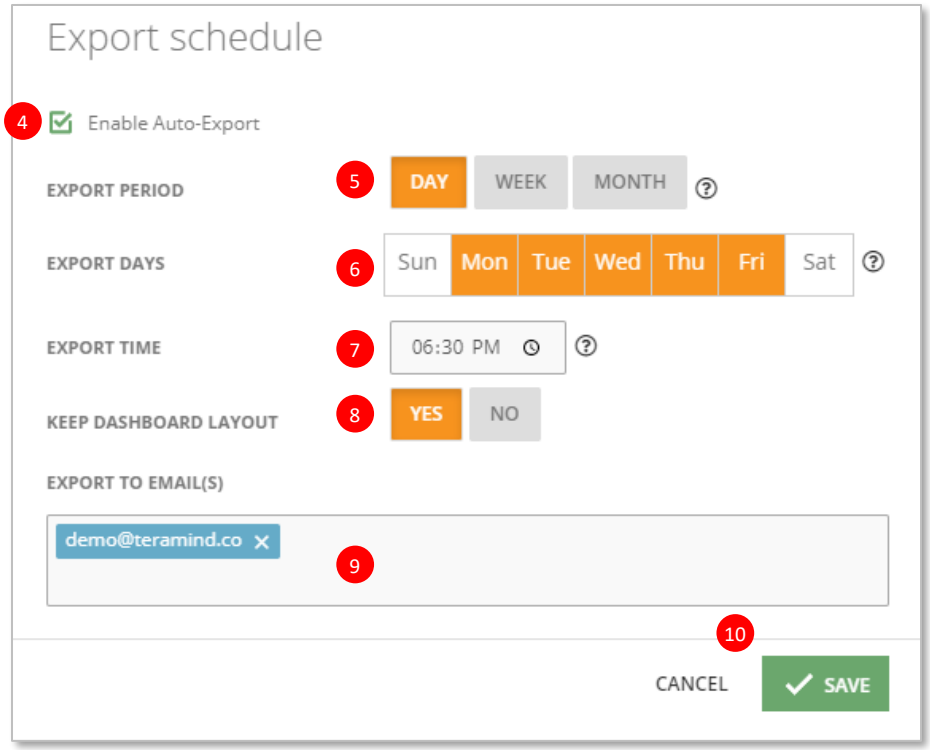


1. Click the green **EXPORT** button near the top right corner. A pull-down menu will open.
2. Select the **Keep dashboard layout** option to export the charts in the original dashboard layout. Select the **Full page charts** option to export each chart on its own page. Click the **CSV Export (Grid only)** option to export only the Grid Widgets on the report. Once you click either of these options, you will see a message that the report is queued for export. Once the report is ready you will see a download message like below. Click it to download the report:

> You can also download the exported reports from the [System > Report export] screen.

> In case of the first two export options (*Keep dashboard layout* and *Full page charts*), if the report contains only Chart Widgets, it will be exported as a PDF file. If the report has a mix of charts or more than one Grid Widget, it will create a ZIP containing both PDF (for the Charts) and CSV (for the Grids) files.

3. Select the **Schedule export** option to schedule automated delivery of the report over emails. When you click this option, a pop-up window will open where you can configure the export options:



4. Click the **Enable Auto-Export** check box to turn auto-export on/off.
5. Select an **EXPORT PERIOD**. You can choose from **DAY/WEEK/MONTH**.
6. You can specify the **EXPORT DAYS** (for daily/weekly period) or **EXPORT DAY OF MONTH** (monthly period). This option essentially lets you define how long exported data will be. Daily reports will be sent every day with single day only. Weekly reports will contain last 7 days and sent on everyday basis too. Note that, for the daily/weekly reports, auto export will happen only on the selected days of the week (Sun-Sat). For the monthly reports, you can specify exact day when auto export should happen. For this type of report, it will contain data from same day (including) in previous month to export day (exclusive).
7. Enter or select the **EXPORT TIME** you want to receive the exported report. Note that, the exported data will not contain the selected export day.
8. If you enable the **KEEP DASHBOARD LAYOUT** option, the PDF containing the charts will be kept in their original dashboard layout. Otherwise, each chart will be exported in their own page.
9. You can specify who will receive the reports in the **EXPORT TO EMAIL(S)** field. You can specify multiple email recipients.
10. Click the **SAVE** button to save and schedule the export or the **CANCEL** button to discard any changes.

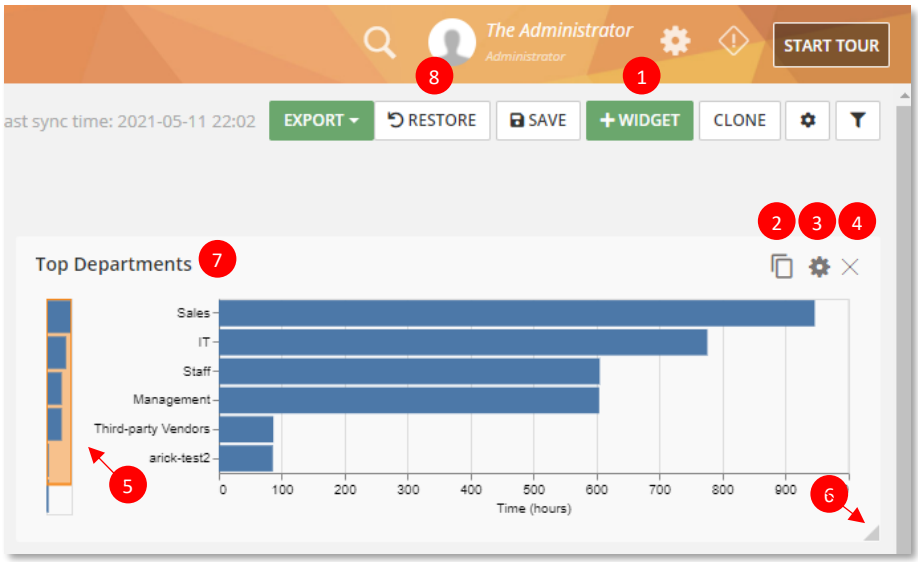
2.10 BI Widgets

Widgets are the main components of a BI report. Widgets are dynamic tiles that displays snippets of information on selected data point(s) or KPIs. Teramind has many BI widgets you can place on your BI reports according to your needs.

The widgets are placed on a virtual grid. They can be moved around or resized. When you move or resize a widget, other widgets around it will reposition themselves to make room for it.

> The data displayed on the BI widgets is not real-time. It can take up to 4 hours for it to refresh.

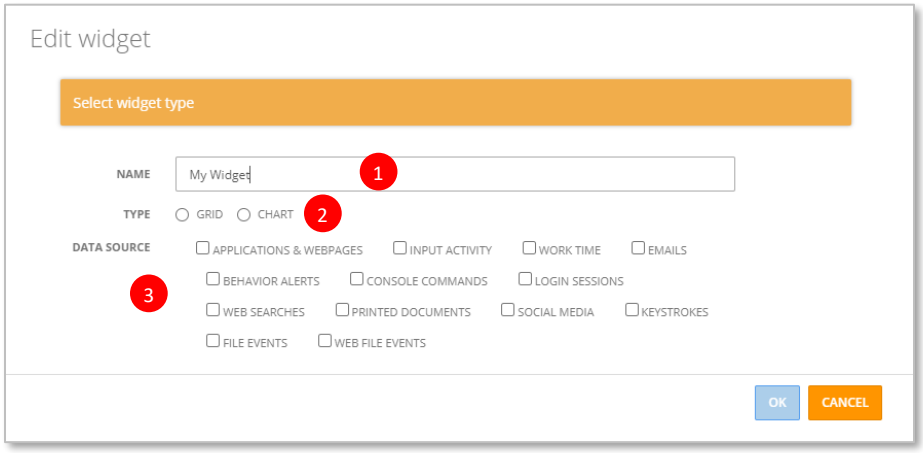
2.10.1 Managing (Add/Copy/Edit/Remove/Arrange) the BI Widgets



1. To add a new widget: Click the green **+WIDGET** button. Note that you can only add widgets to a custom report (see the Editing / Configuring a BI Widget section below to learn how to edit a newly created widget).
2. To copy/clone/duplicate a widget: Click the **Copy** icon near the top-right corner of a widget. You can then edit the duplicated widget (see below).
3. To edit a widget: Click the **Gear** icon (see the Editing / Configuring a BI Widget section below to learn how to edit a widget).
4. To delete/remove a widget: Click the × icon.
5. To move a widget: Click and drag the widget's title bar to move it around.
6. To resize a widget: Click and drag the widget's bottom-right corner, bottom or left-side.
7. To navigate/scroll in a widget: If a (large) chart has a *minimap*, you can drag the small **yellow rectangle** to scroll through the chart.
8. To restore a widget: Click the **RESTORE** button to discard any changes you made to the report. If you made multiple changes, clicking the **RESTORE** button each time will undo the last change.

2.10.2 Editing / Configuring a BI Widget

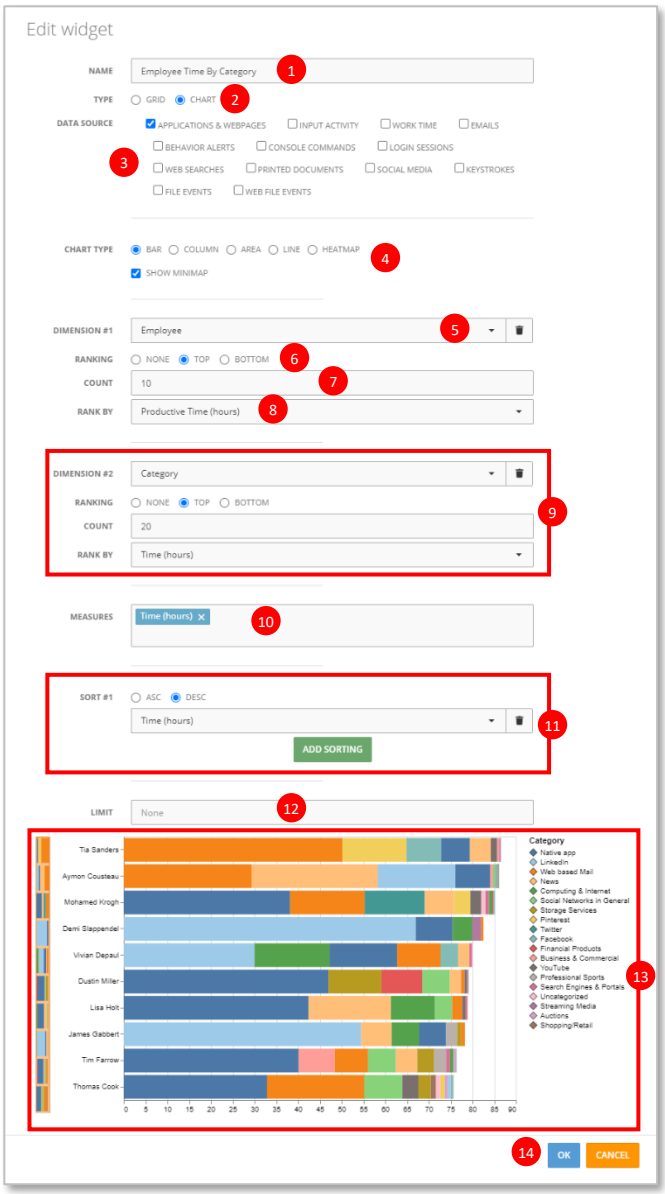
Clicking the green **+WIDGET** button (new widget) or the **Gear**/**Edit** icon (edit widget) next to a widget, will launch the *Edit widget* pop-up window:



1. Enter a **NAME** for the widget.
2. Select a widget **TYPE** such as GRID or CHART.
3. Select one or more **DATA SOURCE** for the widget such as, APPLICATIONS & WEBPAGES, INPUT ACTIVITY, WORK TIME etc.

2.10.2.1 Editing / Configuring a Chart Widget

If you select the **CHART** as the widget TYPE, the *Edit widget* window will expand to show more options:

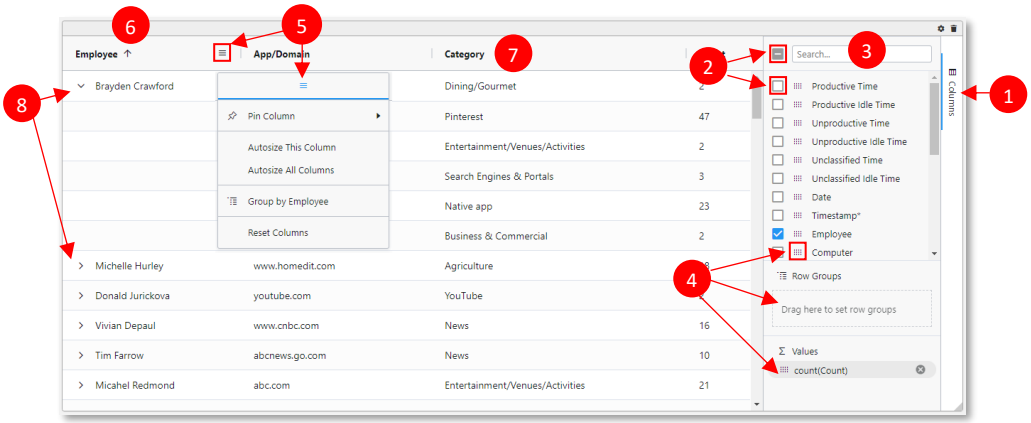


1. Enter a **NAME** for the widget.
2. Select **CHART** from the TYPE options.
3. Select one or more **DATA SOURCE** for the widget such as, APPLICATIONS & WEBPAGES, INPUT ACTIVITY, INPUT TIME etc.
4. Select a **CHART** TYPE such as BAR, COLUMN, AREA etc. For some chart types, you might see a **SHOW MINIMAP** option. This is useful for large charts. You can drag the yellow area of the minimap to scroll through the chart.
5. Select a data point for a chart's axis from the **DIMENSION #1** pull-down menu. Note that, if you have chosen multiple data sources in *Step 3*, then only dimensions common to all the selected data sources will be shown on this list. You can delete a DIMENSION by clicking the small **Trash Can** icon next to it.
6. You can optionally select a ranking order for the data sources under the **RANKING** option.
7. You can optionally enter how many of the data sources are shown at a time on the **COUNT** field.
8. If you have chosen a RANKING option, you can select the **RANKING BY** option and choose a data source.
9. You can optionally select a second set of data points to be displayed on the chart from the **DIMENSION #2** menu. The options are similar to DIMENSION #1 (*Step 5*).
10. You can optionally enter what values the chart will display in the **MEASURES** field.
11. You can optionally add one or more sorting orders for the data under the **SORT** option. Chose either **ASC**-ending or **DESC**-ending option and then select a data point the sort will apply to. You can click the green **ADD SORTING**

	button to add multiple sort orders. You can delete a SORT by clicking the small **Trash Can** icon. 12. You can optionally limit the number of items displayed on the chart by entering it in the **LIMIT** field. 13. You will be able to see a preview of the chart near the bottom of the *Edit widget* window. 14. Click the **OK** button to save or the **CANCEL** button to discard any changes.

2.10.2.2 Editing / Configuring a Grid Widget

The GRID widget does not have any settings other than NAME and DATA SOURCE on the *Edit widget* window. However, you can change its options from the widget's panel:



1. Click the **Columns** tab on the right side of the widget to open/close it.
2. Click on the **small checkbox** in front of a data point to add/remove it as a column on the grid. Use the top checkbox to select/deselect all data points.
3. You can search for a data point using the **Search…** field.
4. You can group multiple rows by dragging one or more data point(s) and dropping them under the **Row Groups** section. For example, create group by *Employees*, *Departments* etc. You can also create sums for some of the data points by dragging them to the **Σ Values** section. Use the **small grid** icon to drag the data point(s) you need. Note that, you cannot drag and drop certain data points to the Row Groups. For example, *Productive/Unproductive* time cannot be grouped. Similarly, you cannot drag and drop data points which cannot be summed up. For example, *Employee*, *Date* etc. If a data point cannot be dropped to a Row Group/ Σ Values section, you will see a small **no** symbol as you drag it.

> You can also create **Row Groups** or **Σ Values** quickly from a column's menu (see *Step 5* below).

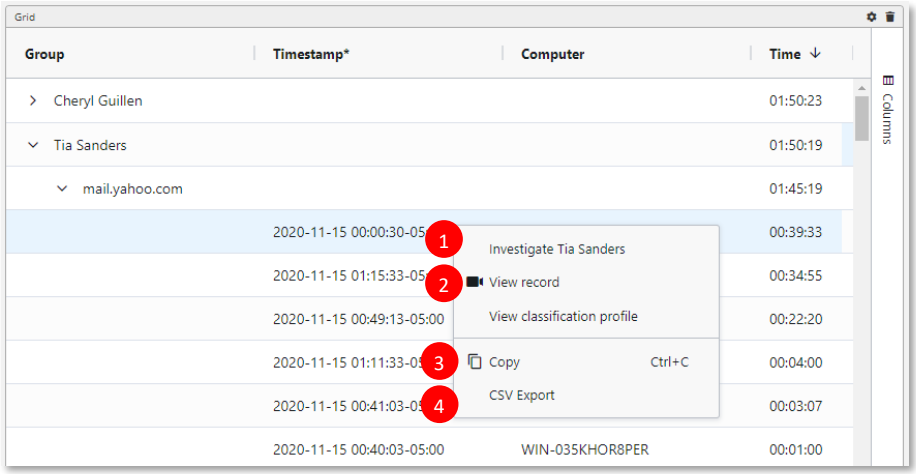
5. If you hover over a column, you will see a small **column menu** icon. Clicking it will display a small pop-up menu. From this menu you can pin columns, auto-size them or reset the changes. You can also create a **Row Group** or **Σ Values** for the selected column.
6. Click a **column title** to sort it. Click again to change the sort order (between ascending or descending). Note that, you cannot sort a *Group* column.
7. You can also click and drag a column name to move it left/right.
8. You can click a Group row's **right arrow** icon to expand it and the **bottom arrow** icon to collapse it.

2.10.2.3 Using the Grid Widget's Context Menu

Right clicking on the Grid widget will open its context menu.

Single Select Options:

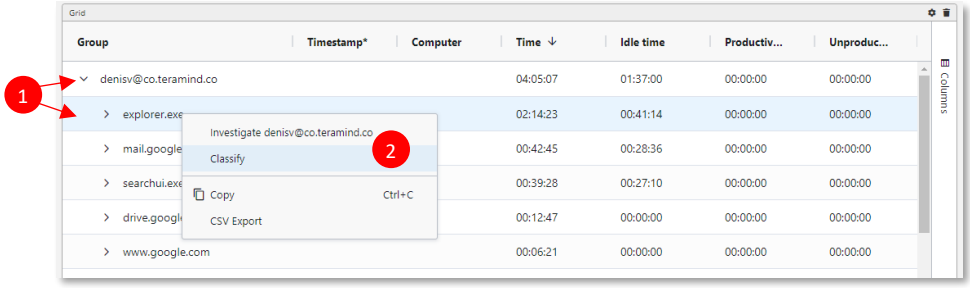
If you right-click on a single cell, depending on the BI report and the type of information being displayed on the grid, the context menu will show different options:



1. The **Investigate** option is available if the *Group* column is expanded to show the *Timestamps*. Selecting this option will take you to the Employee's Activity Monitoring Report page.
2. View record option is available if the *Group* column is expanded to show the *Timestamps*. Selecting this option will take you to the Session Player and display the recording at the selected timestamp.
3. Use the **Copy** option to copy the selected cell's data to the clipboard.
4. Use the **CSV Export** option to download the entire grid's data as a CSV file.

Other Options: You might see other options on the context menu depending on which BI report you are on. For example, there might be a **View Document** (on the Printing BI report), **View Email**, **Download attachment** (on the Emails BI report) etc. option(s).

Viewing / Changing Productivity Classifications:



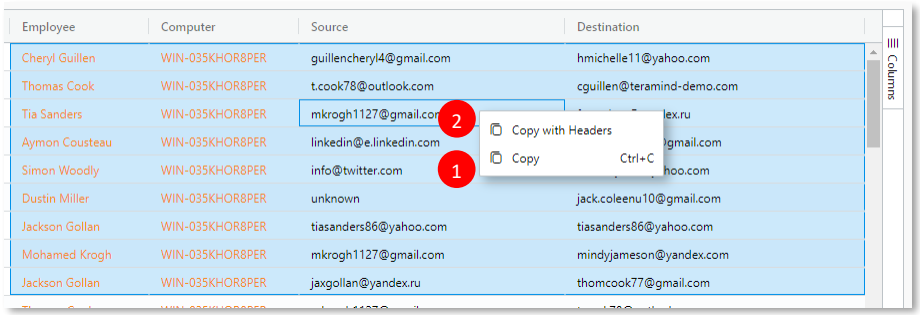
1. On the *Grid Widget* of the Applications & Webpages report, click on the **right arrow** > icon on the first column to expand it until you can see the app/domains (e.g. `explorer.exe`, `www.yahoo.com` etc.).
2. Right click on any of the expanded row. You will see a **Classify** option. Select this option to be able to change/edit the Productivity Profiles for that particular site/app.

> You can classify any app or website from your custom reports too. As long as a Grid Widget has an expanded *App/Domain* column, you can right-click on it to classify the app/website.

> To learn more about app/web classifications or to change them in groups, check out the Productivity Profiles section.

Multi-Select Options:

If you select multiple rows/columns (**SHIFT+Click** or **Click+Drag**) and then right-click on them, you will see a different context menu:



1. The **Copy with Headers** option will let you copy the selected cells along with the column headers to the clipboard.
2. The **Copy** option is similar to the *Copy with Headers* option but will not copy the column headers.

3 Dashboards

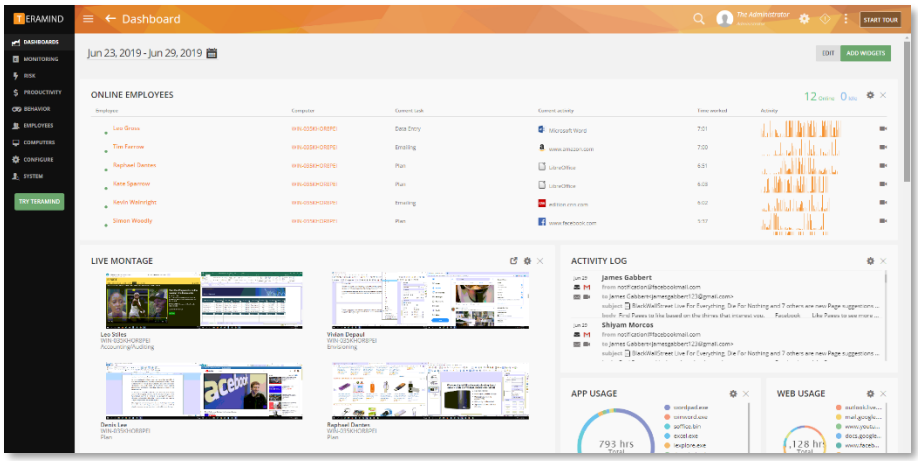
3.1 Introduction to Dashboards

The dashboard is the place where the manager or administrator can have a quick snapshot of what's happening in the company. The dashboards are easy to configure using drag-and-drop widgets. You can also create your own custom dashboards. Each user's dashboards are specific to their own login account and of them can have their own set of dashboards.

Teramind comes with two default dashboards:

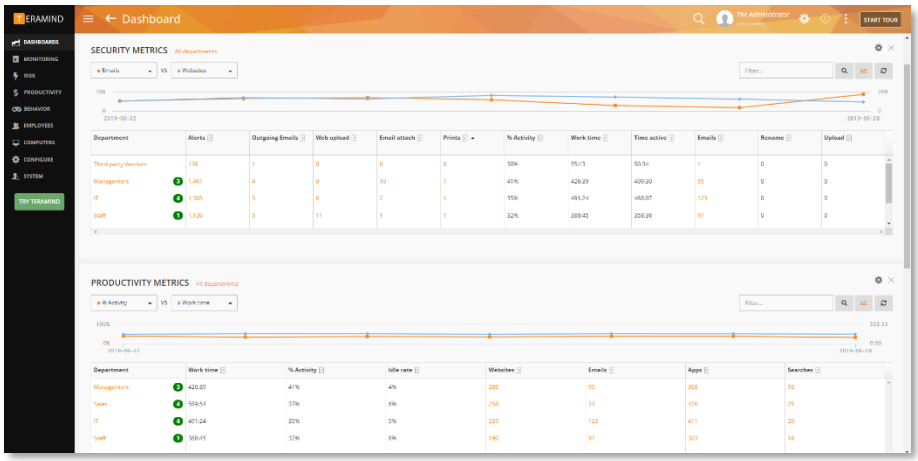
3.1.1 Focused Dashboard

The Focus dashboard is designed for department managers, security analysts and administrators who might want to view detailed information on online employees, user activities or a live montage of online users.

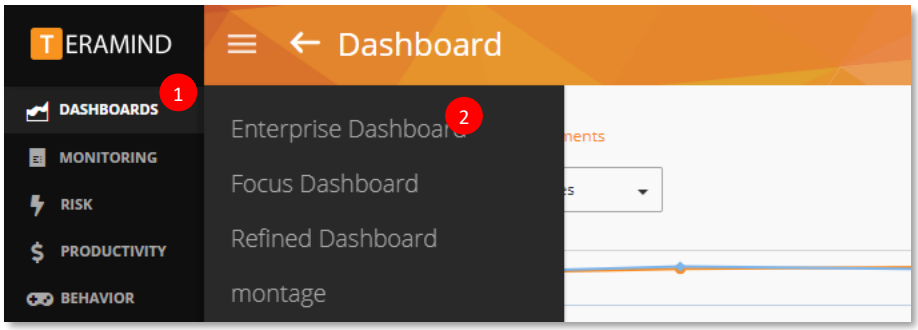


3.1.2 Enterprise Dashboard

Enterprise dashboard is primarily useful for business owners, executives, senior management, HR management and CSOs who might want to keep an eye on the organization's overall security and productivity health. As such, this dashboard focuses on Enterprise KPIs.

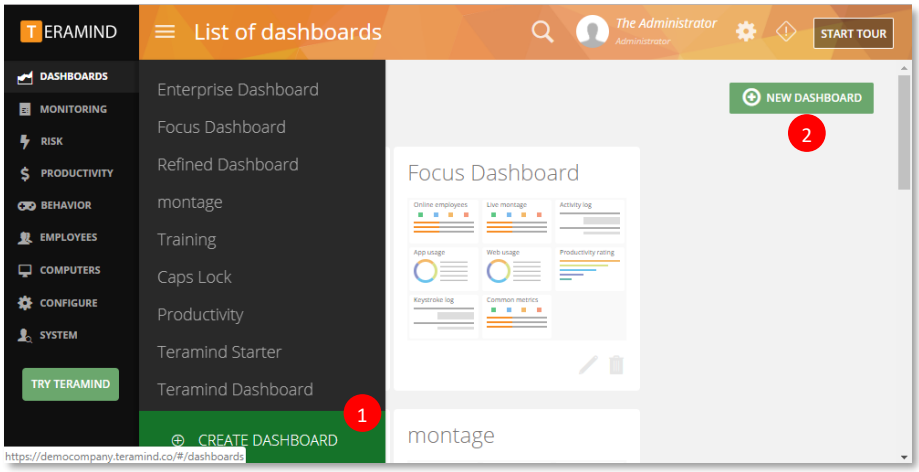


3.2 Accessing the Dashboards Menu



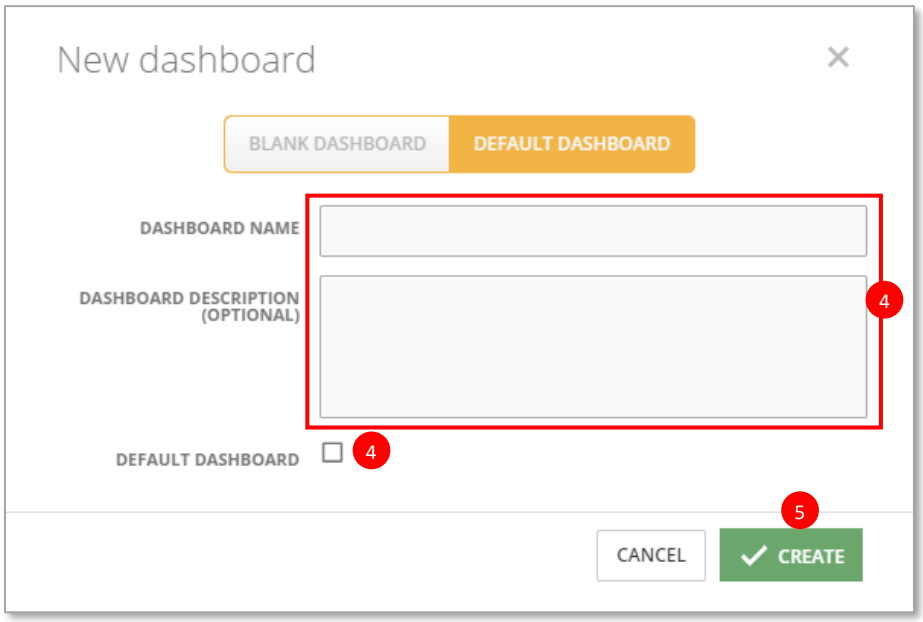
1. To switch among dashboards, hover your mouse over the **DASHBOARD** menu, then
2. Select a dashboard from the sub-menu.

3.3 Creating a New Dashboard



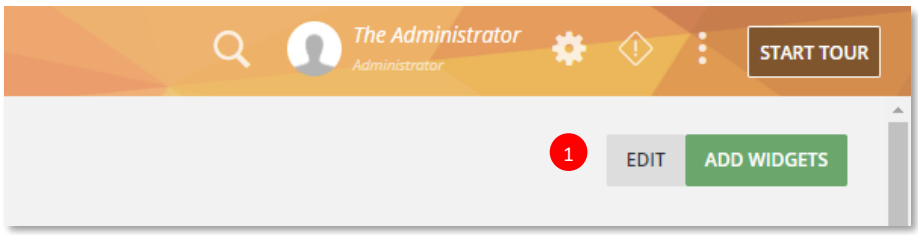
There are two ways you can create a new dashboard:

1. Hover your mouse over the **DASHBOARD** menu, then click the Green **CREATE DASHBOARD** at the bottom of the sub-menu.
2. Or, click the DASHBOARD menu, which will take you to a screen titled, *List of dashboards*. Click the Green **NEW DASHBOARD** button on this screen.

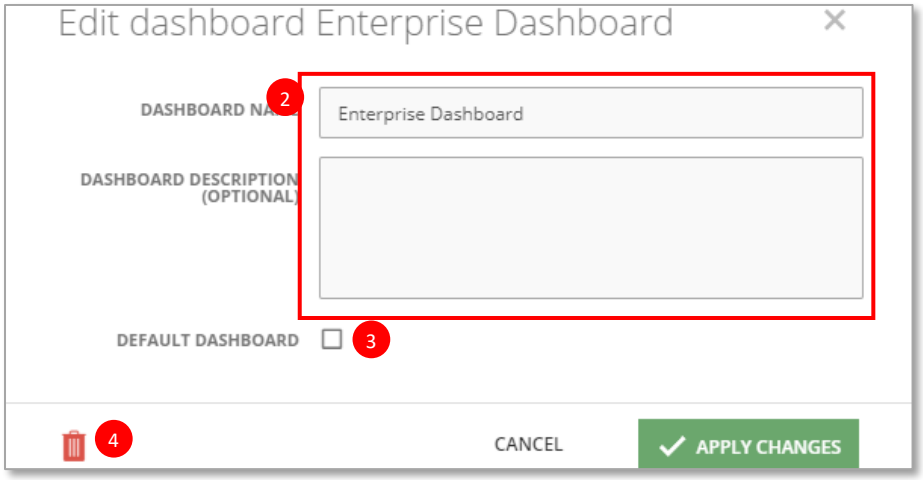


3. On the pop-up window, give your dashboard a unique name and optionally, a description.
4. You can also make it the default dashboard by enabling the **DEFAULT DASHBOARD** checkbox.
5. Click **CREATE** to save the dashboard.

3.4 Editing / Deleting a Dashboard



1. Click the **EDIT** button on the top right corner.



2. On the pop-up window, you can change the name and description of the dashboard.
3. You can also make it the default dashboard by enabling the **DEFAULT DASHBOARD** checkbox.
4. To delete the dashboard, click the **Trach Can** icon. Note that, if you have only one dashboard, it cannot be deleted.

3.5 Introduction to Widgets

Widgets are tiles that displays snippets of information on a particular activity or KPI. Teramind has many widgets you can place on your dashboard according to your need.

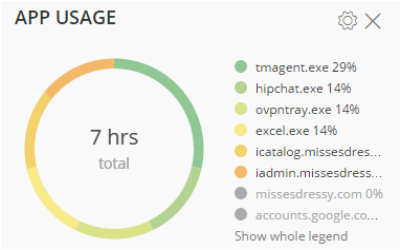
The widgets are placed on a virtual grid. They can be moved around on it. When you move or resize a widget, other widgets around it will reposition themselves to make room for it.

Good to know: If you set the Dashboard's date to current date (Today), the data of all the widgets will refresh automatically every 5 minutes.

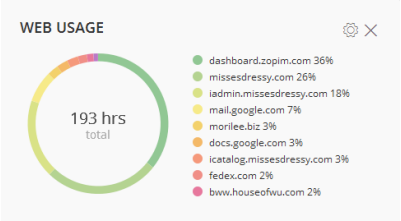
3.6 Widget Types and Usage

There are three different types of widgets you can choose from:

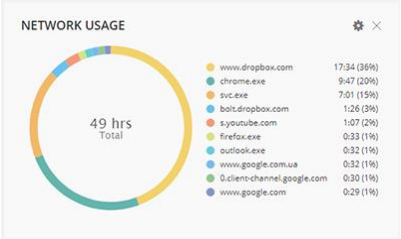
3.6.1 Monitoring Widgets



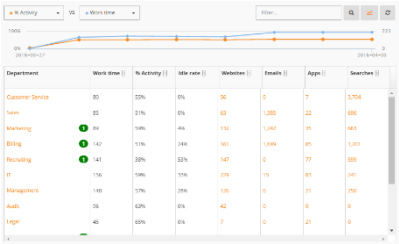
App Usage
Shows the time spent on each application.



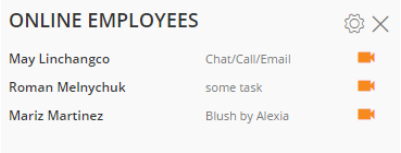
Web Usage
Shows the time spent on each web page.



Network Usage
Shows network usage by time, bytes or connections count.

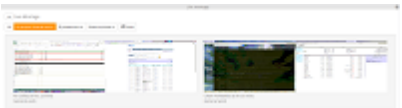


Combined Report
Shows behavioral and productivity data in a combined table format with trend graphs comparing select metrics.

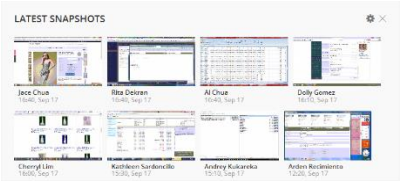


Online Employees
Shows the data of all the currently online employees.

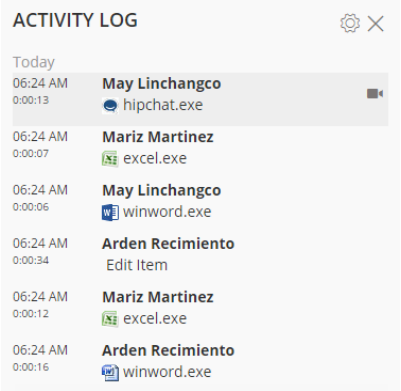
State of Employees
Shows no of employees online, idle, late, absent etc.



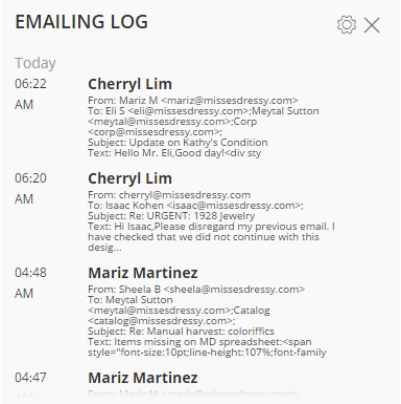
Live Montage
Shows a live montage of the desktops of online employees.



Latest Snapshots
Shows the latest snapshots of the employees' screens.

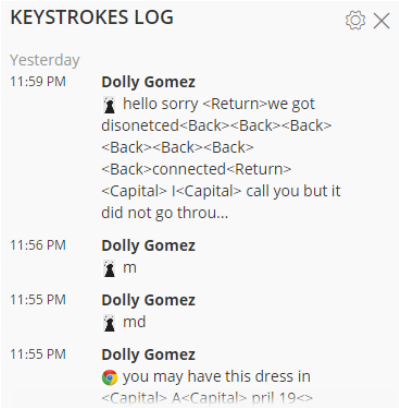


Activity Log
Shows a list of employee activates for the given time range.



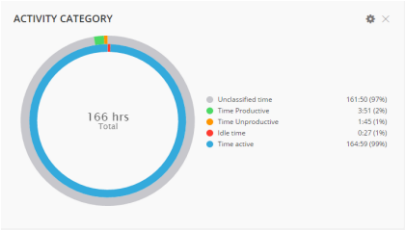
Email Log
Similar to Activity log, but for emailing only.

Commands Log
Shows a log of all commands run on the command prompt.

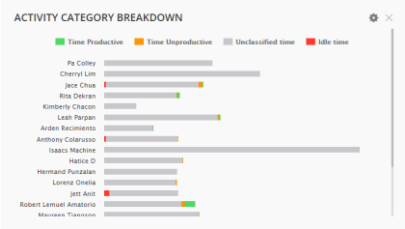


Keystroke Log
Shows a log of all keystrokes pressed by the users.

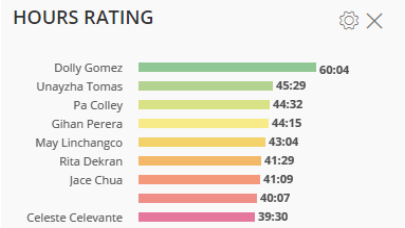
3.6.2 Productivity Widgets



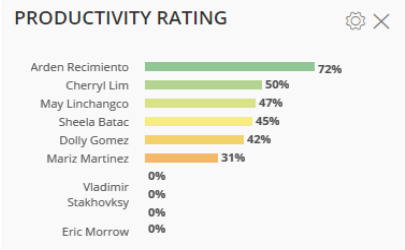
Activity Category
Activity category by active, idle, productive, unproductive time.



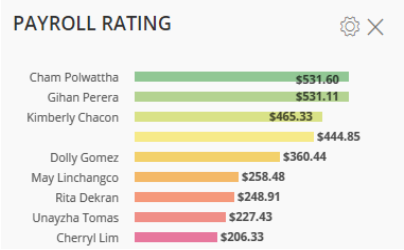
Activity Category Breakdown
Activity category breakdown in a bar graph format.



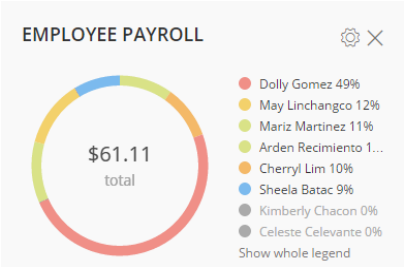
Time Worked
Rates the employees by the hours they have worked.



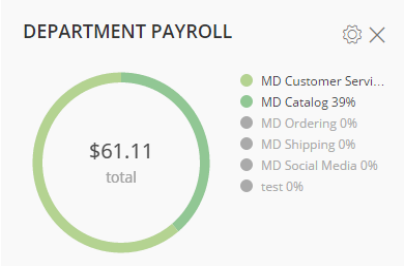
Activity Rating
Rates the employees by their productivity.



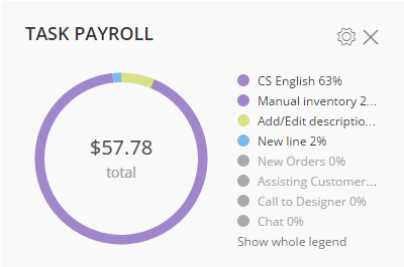
Payroll Rating
Rates the employees by their payroll.



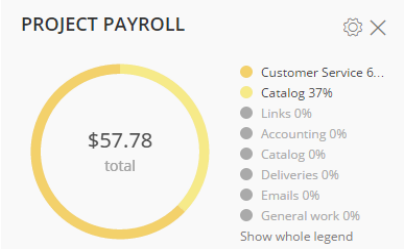
Employee Payroll
Shows the money spent on each employee.



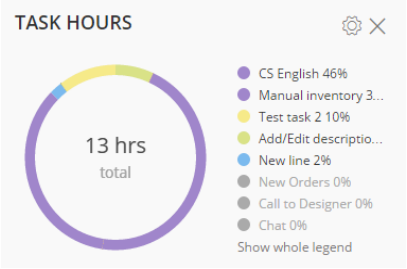
Department Payroll
Shows the money spent on each department.



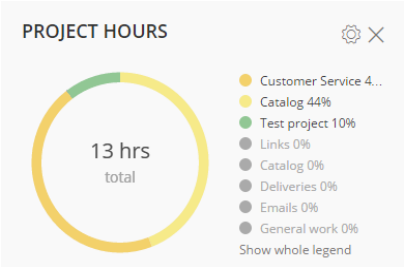
Task Payroll
Shows the wage/salary spent on each task.



Project Payroll
Shows the wage/salary spent on each project.

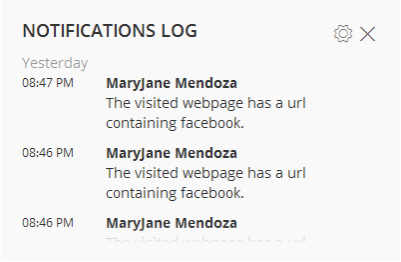


Task Hours
Shows the time spent on each task.

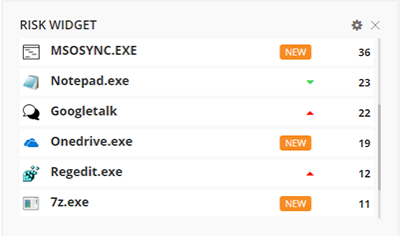


Project Hours
Shows the time spent on each project.

3.6.3 Security and Risk Widgets

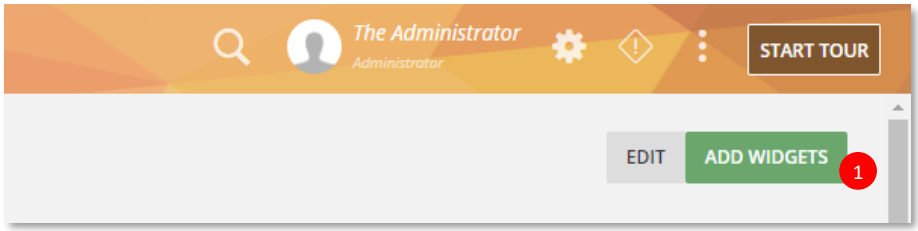


Alerts Log
Shows a log of all alerts and notifications.

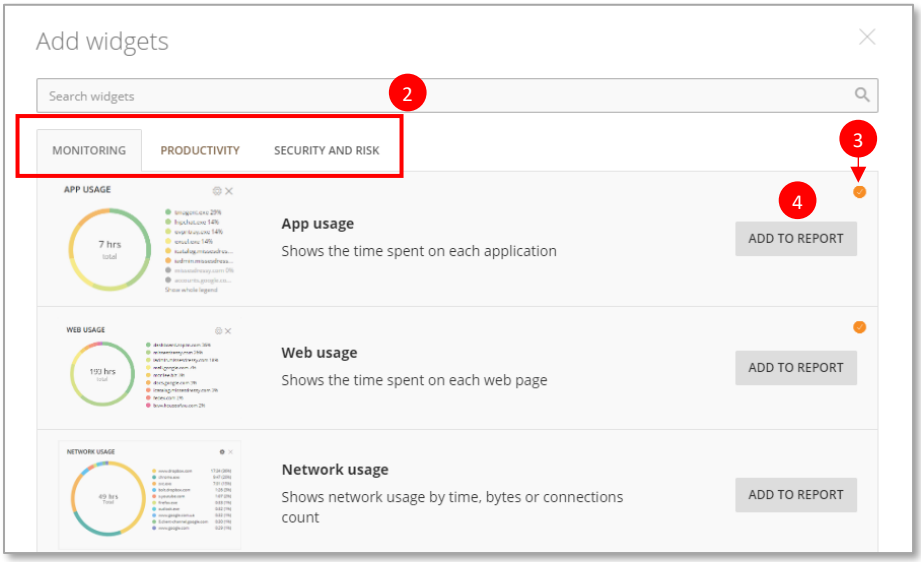


Risk Widget
Shows risky users, rules or activities.

3.7 Adding Widgets to the Dashboard

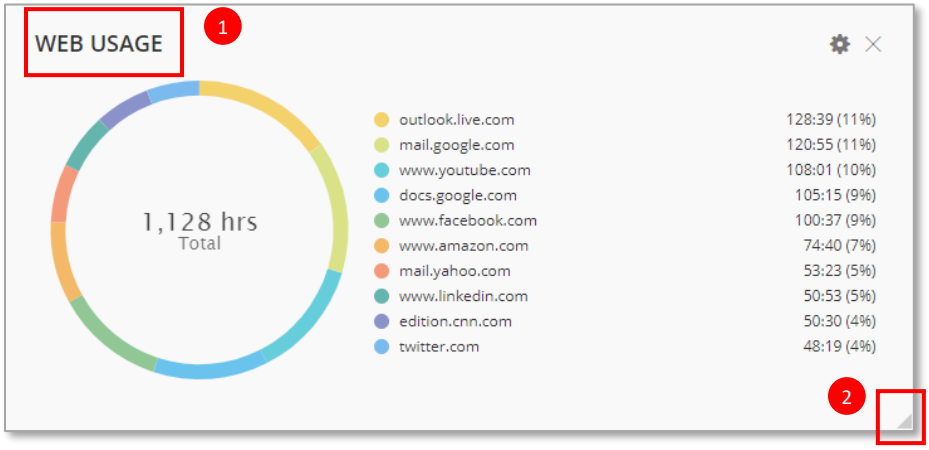


1. Click the **ADD WIDGETS** button on the top right corner of a dashboard.



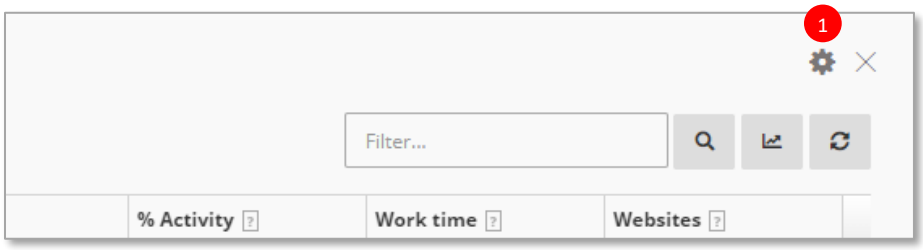
2. On the *Add widgets* pop-up window, click on the **MONITORING**, **PRODUCTIVITY** or the **SECURITY AND RISK** tab.
3. A small Orange Circle in the corner indicates that the widget is already used on the dashboard.
4. To add a widget to the dashboard, click the **ADD TO REPORT** button. You can add multiple copies of a widget. You can then configure each widget to show the same type of information (such as App Usage) but for different employees, departments or other criteria. This way, you can compare between them.

3.8 Moving and Resizing the Widgets

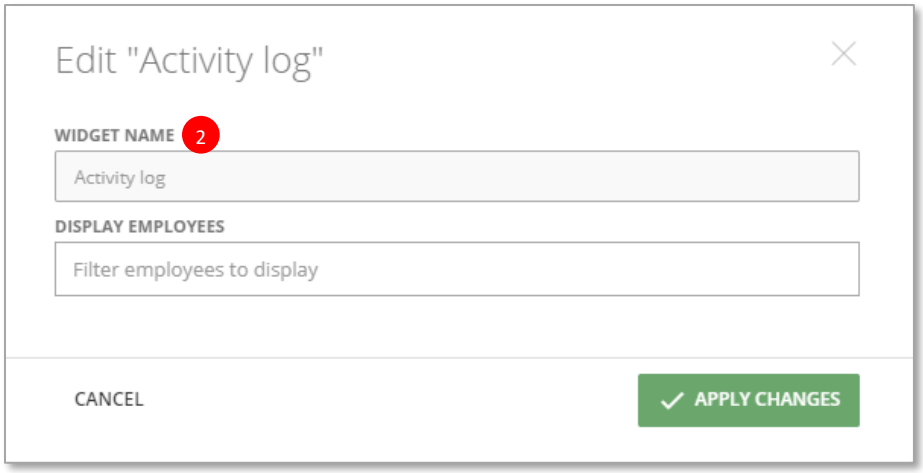


1. To move a widget, click and drag its **title/header**. As you move the widget around, other widgets will rearrange themselves to make space for it automatically.
2. To resize a widget, hover over the bottom-right corner of the widget. A small triangle will appear. Click and drag the **triangle** to resize the widget. As you resize the widget, other widgets will rearrange themselves to make space for it automatically.

3.9 Configuring / Editing a Widget

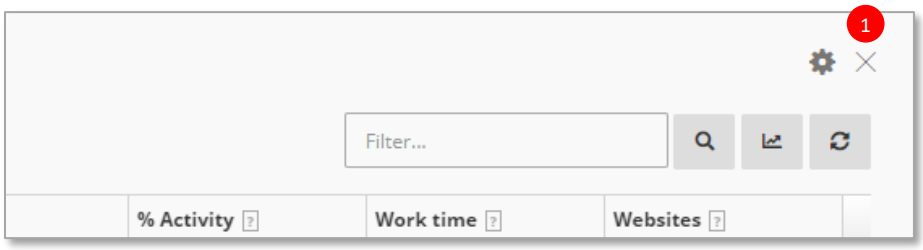


1. Click the **Cog Wheel** button on the top right corner of a widget to access its settings window.



2. On the pop-up window, you can assign the widget a name and filter the employees you want to display on the widget. Note that, some widgets may have additional settings and filters you can use to further fine tune what information is displayed on the widget.

3.10 Removing Widgets from the Dashboard



1. Click the "**X**" button on the top right corner of a widget to remove it from the dashboard. The widgets around it will automatically rearrange to fill up the empty space. Note that, any changed you made to the widget's settings or filters will be lost when you remove it from the dashboard.

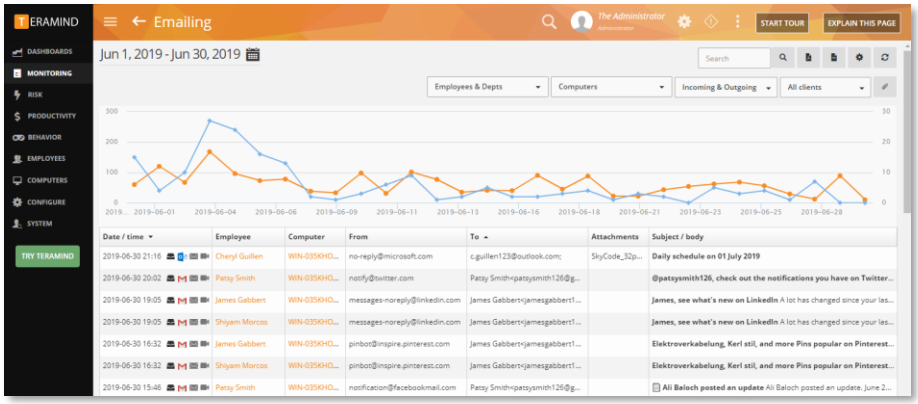
4 Monitoring Reports [deprecated]

DEPRECATED FEATURE

The Monitoring Reports are deprecated. Please use the new Business Intelligence (BI) Reports which offers more information, drill-down capabilities, enhanced export, and faster load time. Please contact Teramind support if you have any questions.

4.1 Introduction to Monitoring Reports

Monitoring reports are individual activity reports for all the system objects (i.e. Websites, Apps, Network) tracked by Teramind. The data is usually displayed in a tabular format, but some reports may also have a trend graph near the top of the report. The reports can be viewed for a select date range. They can be searched; filtered by employees, departments or computers; exported as PDF/CSV files or scheduled to be delivered to email accounts at regular intervals. Each report screen also has its own setting you can use to configure if for your needs.



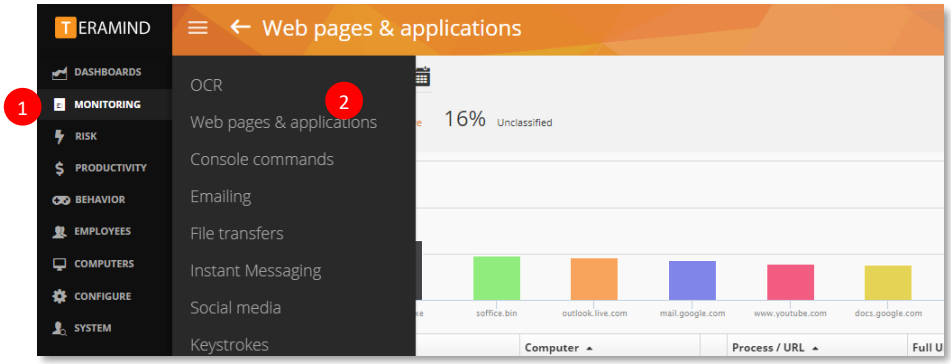
To change what and how Teramind monitors user activity, check out the Monitoring Settings section.

Note that, not all reports are available in all Teramind offerings. The table below shows which reports are available on what product:

Monitoring Report	Teramind Starter	Teramind UAM	Teramind DLP
OCR	✗	✓	✓
Web Pages & Applications	✓	✓	✓
Emailing	✗	✓	✓
Console Commands	✗	✓	✓
File Transfers	✗	✓	✓

Instant Messaging	✓	✓	✓
Social Media	✓	✓	✓
Keystrokes	✗	✓	✓
Searches	✓	✓	✓
Printing	✗	✓	✓
Screen Snapshots	✓	✓	✓
Sessions	✓	✓	✓
Network Monitoring	✗	✓	✓
Video Export	✓	✓	✓

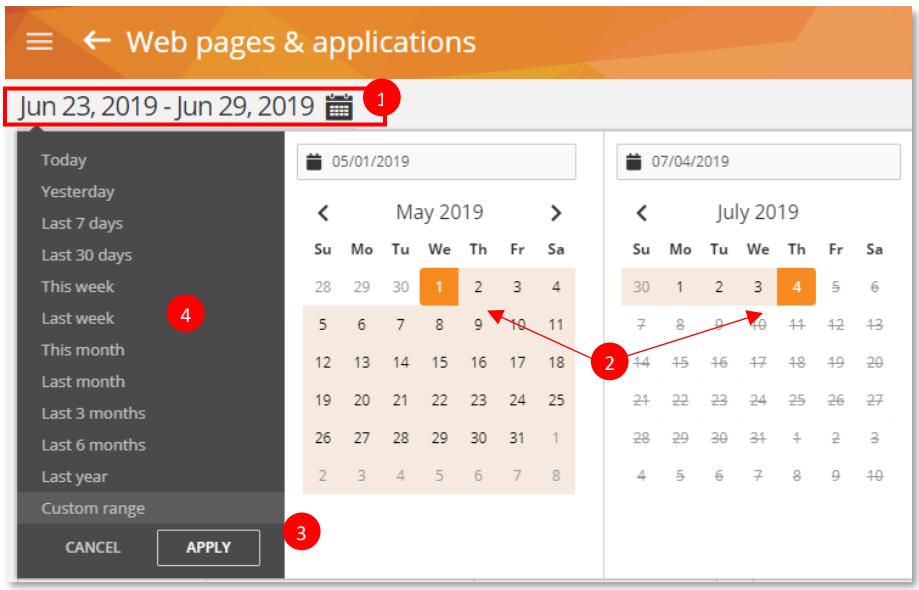
4.2 Accessing the Monitoring Report Menus



5. To access a monitoring report, hover your mouse over the **MONITORING** menu, then
6. Select a report from the sub-menu.

4.3 Performing Common Reporting Tasks

4.3.1 Setting a Data Range

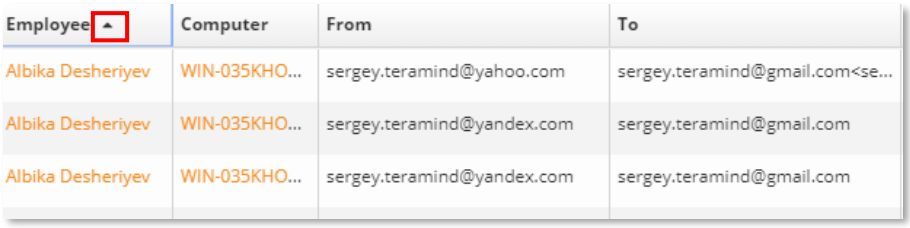


5. Each monitoring report screen has a dates-selector at the top-left corner. Click the **dates-selector** 📅.
6. Select a start date and an end date from the dates-selector window.
7. Click the **APPLY** button.
8. You can also select one of the pre-defined date-sets (i.e. Today, Yesterday, Last 7 Days etc.) from the left of the dates-selector window without having to select the start/end dates.

> **Good to know:** If you set the date to current date (Today), the data on the report will refresh automatically every 5 minutes.

4.3.2 Sorting the Report Columns

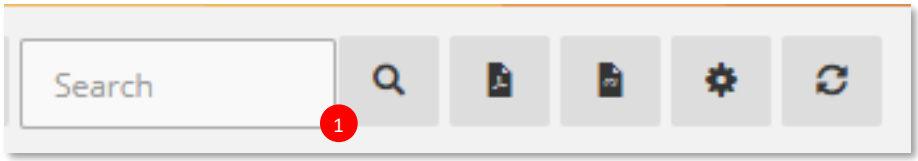
Some of the report columns are sortable (i.e. Date/time, Employee etc.). Click on such a column's title/header to toggle it's sorting by Ascending ▲ or Descending ▼ order.



Employee	Computer	From	To
Albika Desheriyev	WIN-035KHO...	sergey.teramind@yahoo.com	sergey.teramind@gmail.com<se...
Albika Desheriyev	WIN-035KHO...	sergey.teramind@yandex.com	sergey.teramind@gmail.com
Albika Desheriyev	WIN-035KHO...	sergey.teramind@yandex.com	sergey.teramind@gmail.com

4.3.3 Searching in a Report

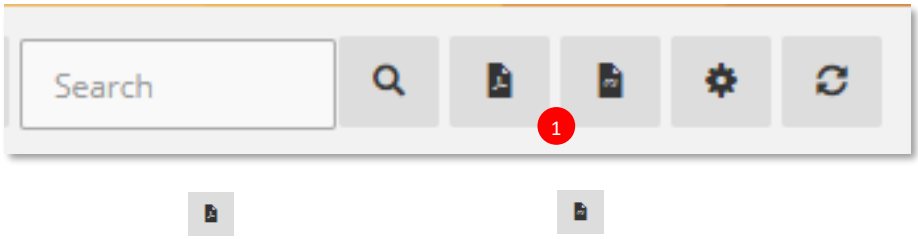
You can search for an item (i.e. activity, application name, website, document) in the monitoring reports. Note that, some reports (i.e. Screen Snapshots) do not have any Search option.



1. Each report screen has a Search bar near the top-right corner. Type your text and click the **Search** button or press **Enter**.

4.3.4 Exporting Reports

You can export a monitoring report in PDF or CSV format. Note that, some reports (i.e. Screen Snapshots) do not have any export option.



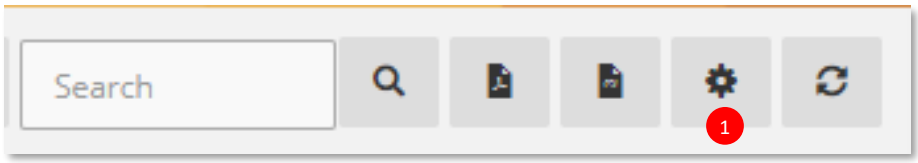
1. Click the **PDF export** button or the **CSV export** button near the Search bar at the top-right corner to export the report in those formats. You will see a message that the report is queued for export. Once the report is ready you will see a download message like below:

2. Click the message to download the report.

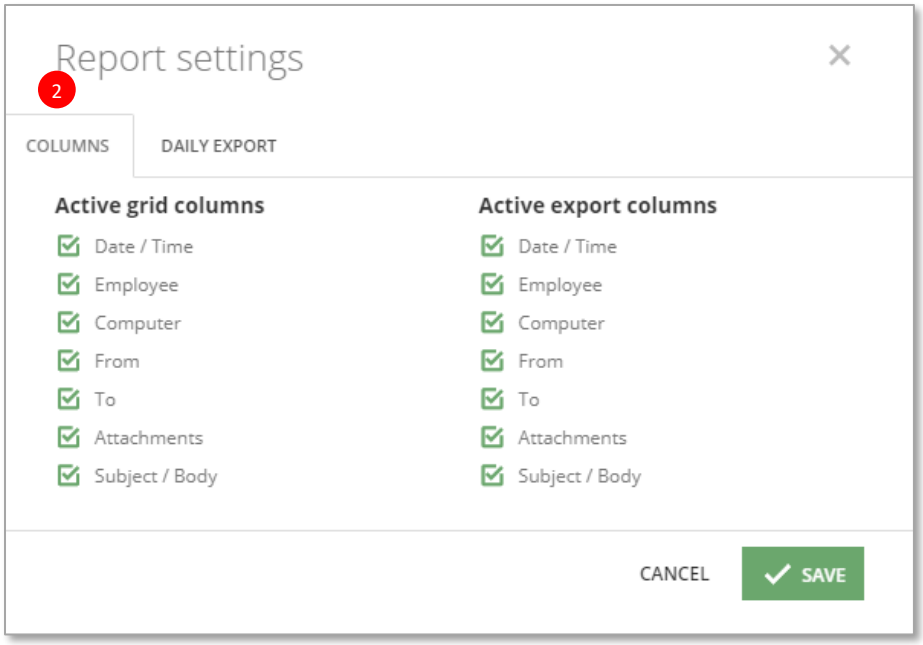
> You can later view and download all the exported reports from the **System > Report export** menu.

4.3.5 Changing the Report Settings

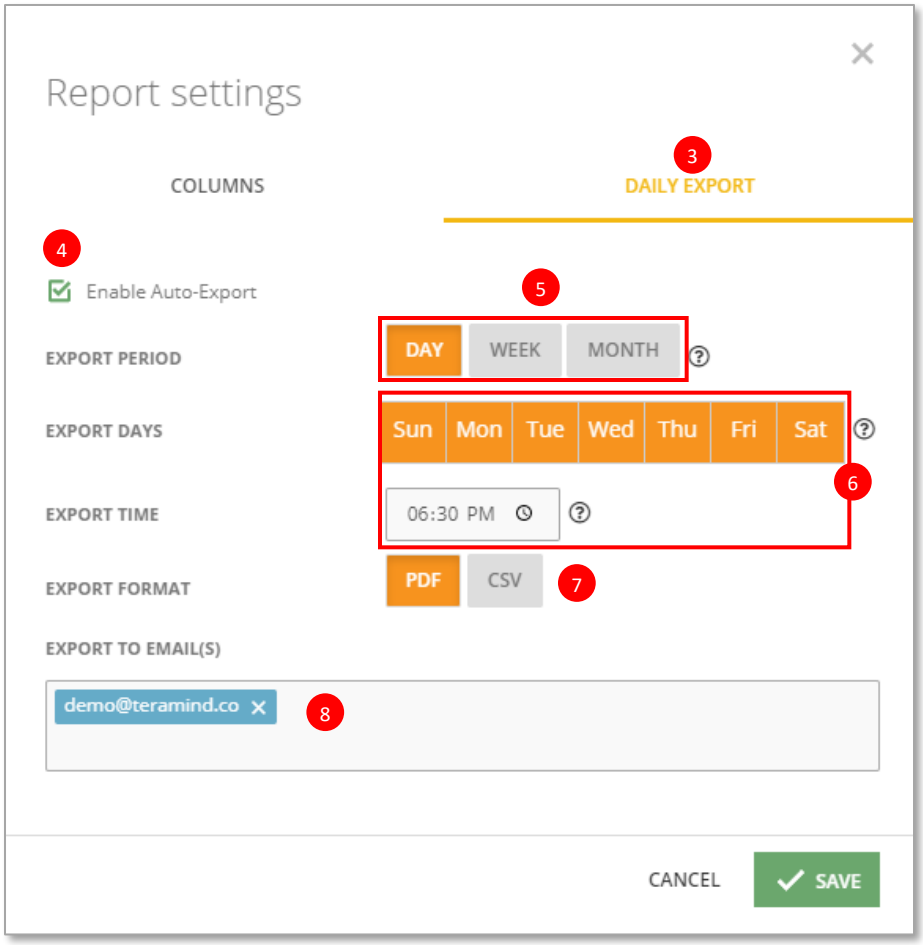
You can change which columns to Show/Export and the Daily Export settings for each monitoring report independently. Note that, some reports (i.e. Screen Snapshots) do not have any Settings/Export options.



1. Click the **Cog Wheel** button to access the report's settings window.



2. Click the **COLUMNS** tab to change which columns are displayed (*Active grid columns*) and which of them are exported (*Active export columns*).

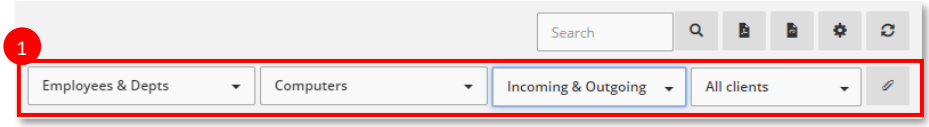


3. Click the **DAILY EXPORT** tab to change which columns will be exported.
4. You can also turn on the **Enable Auto-Export** feature for a scheduled delivery of the report.
5. EXPORT PERIOD will let you define how long exported data will be. Daily reports will be sent every day with single day only. Weekly reports will contain last 7 days and sent on everyday basis too.
6. You can specify the **EXPORT DAYS** (daily/weekly reports) or **EXPORT DAY OF MONTH** (monthly reports). Note that, for daily/weekly reports, auto export will happen only on the selected days of the week (Sun-Sat). For monthly reports, you can specify exact day when auto export should happen. For this type of report, it will contain data from same day (including) in previous month to export day (exclusive).
7. You can select PDF or CSV from the **EXPORT FORMAT** option.
8. You can specify who will receive the reports in the **EXPORT TO EMAIL(S)** field. You can specify multiple email recipients.

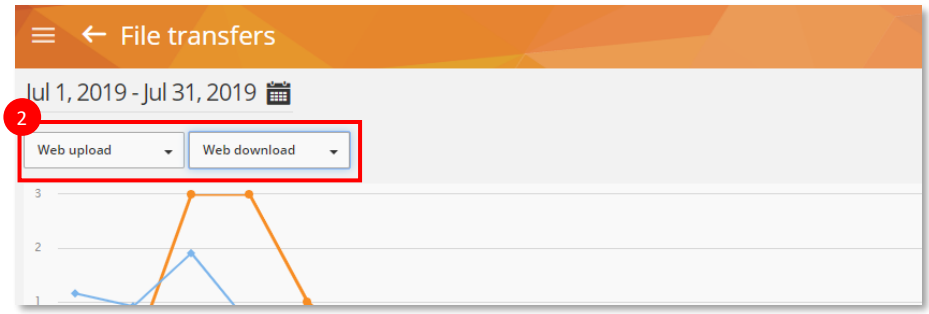
You can later view and download all the exported reports from the **System > Report export** menu.

4.3.6 Using the Report Filters

Most of the monitoring reports have a set of common filters that let you narrow down the number of items displayed. You can filter by employees, departments, computers etc. Additionally, each report also has its own content-specific filters. For example, the Emailing Monitoring Report has filters for mail directions, email clients, presence of attachments etc.



1. Report filters are usually located on the second row of the screen, at the top-right corner.



2. Reports which have a graph/chart may also have additional filters. These are usually located on top of the chart, at the top-left corner. For example, the File Transfers Monitoring Report has filters for the chart to compare two different file activities.

4.3.7 Viewing Session Records

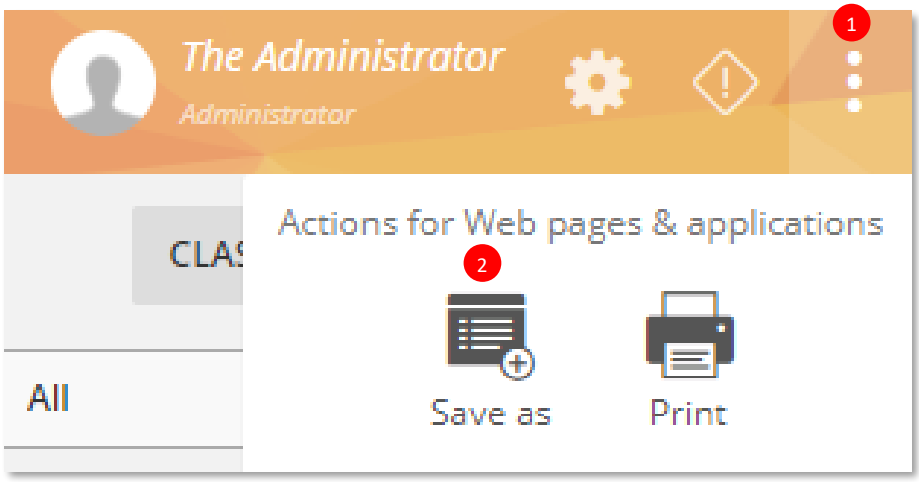
You can access a user's desktop session live or view records of their past sessions.

1. Wherever you see the **Movie Camera** icon, click it to access the Session Player. Usually, the icon is displayed on the *Date/time* column of a report or on a dashboard widget.

For more information about session recordings and playback check out the Session Player section.

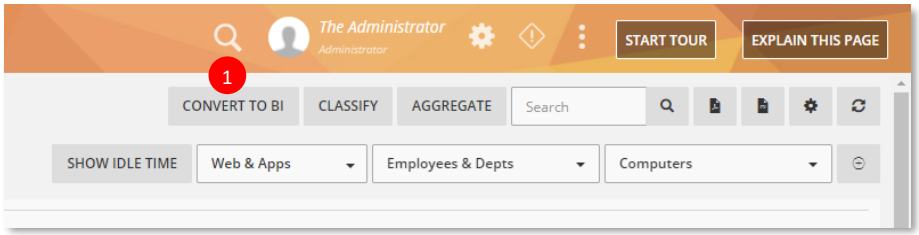
4.3.8 Creating / Saving a Custom Report

You can create and save your own custom report. To do so, go to a Monitoring Report. Configure the filters or settings the way you want it, then do the following:



1. Click the **Dot Menu** near the top-right corner of the Dashboard. A pop-up menu will appear.
2. Click the **Save as** button to save the report. The report will show up on the main MONITORING menu under *Saved reports*.

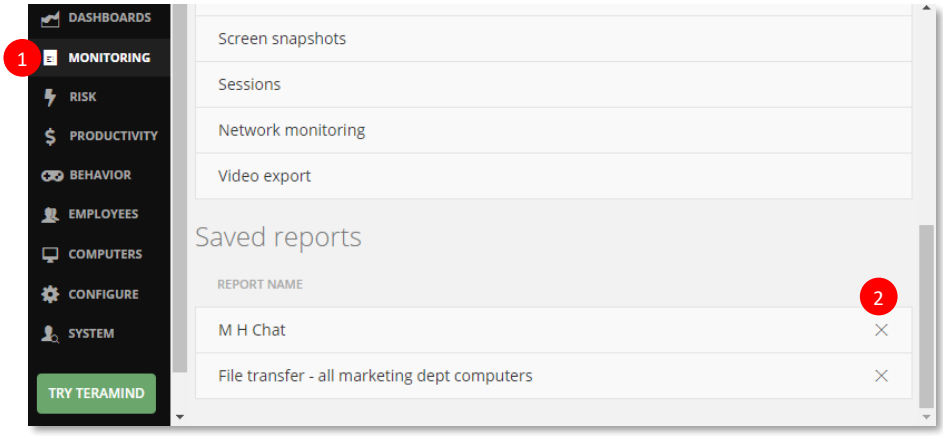
4.3.9 Converting a Saved Monitoring Report to a BI Custom Report



1. Open your custom/saved Monitoring Report. Click the **CONVERT TO BI** button at the top. This will create a custom BI Report with widgets that show the same data as your Monitoring Report. Any filters you applied to your Monitoring Report will be preserved on the BI Report. See the Custom BI Reports section for more information.

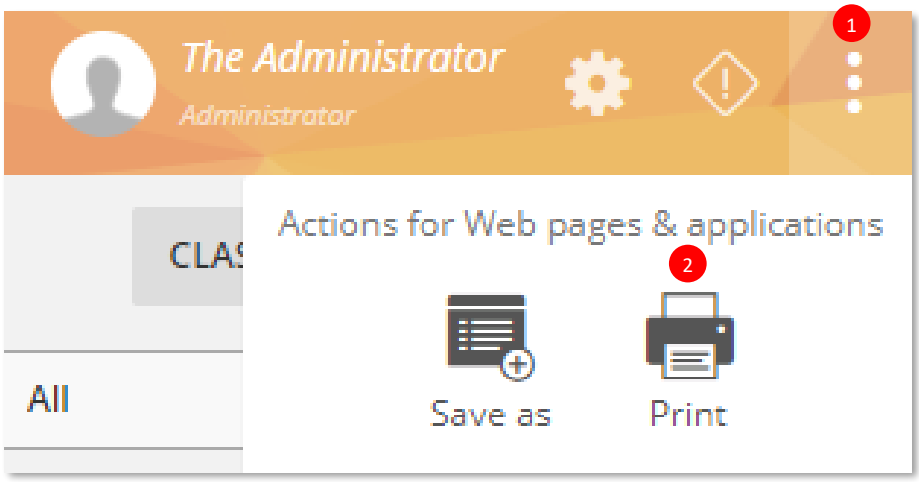
Note that, at the moment not all of your saved monitoring reports can be converted. Only Monitoring Reports which have equivalent BI Report types can be converted.

4.3.10 Deleting a Saved Report



1. Click the **MONITORING** menu. A list of monitoring reports will appear.
2. Scroll down until you see *Saved reports*. Under it, you will see all your saved reports. Click the small **X** button at the right side of a saved report to delete it.

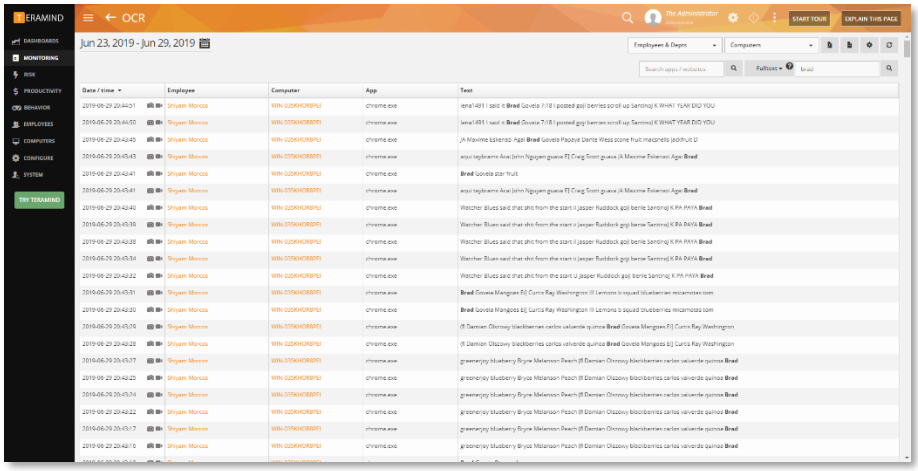
4.3.11 Printing a Report



1. Click the **Dot Menu** near the top-right corner of the Dashboard. A pop-up menu will appear.
2. Click the **Print** button to print the report.

4.4 OCR (Optical Character Recognition)

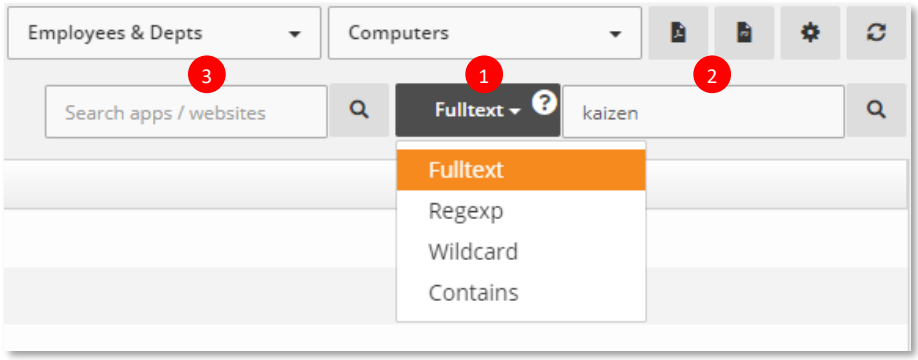
Teramind's advanced OCR feature allows you to discover onscreen text in real-time. The OCR engine continuously captures, indexes and analyses a user's desktop using machine learning and sophisticated pattern recognition algorithms. With OCR, you can quickly search for textual information even inside images or videos, build powerful content-rules or conduct forensic investigation easily.



The OCR works with multi-monitor setups and virtual desktops, including the ones from the Terminal Servers.

4.4.1 Using the OCR Search Feature

To conduct an OCR search, do the following:



1. Click the **pull-down menu** in-front of the search bar near the top-right corner of the screen (or at center of the screen if you are using the OCR report for the first time). Select a search type from the list.

   You can conduct four types of OCR search:

   - **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**.

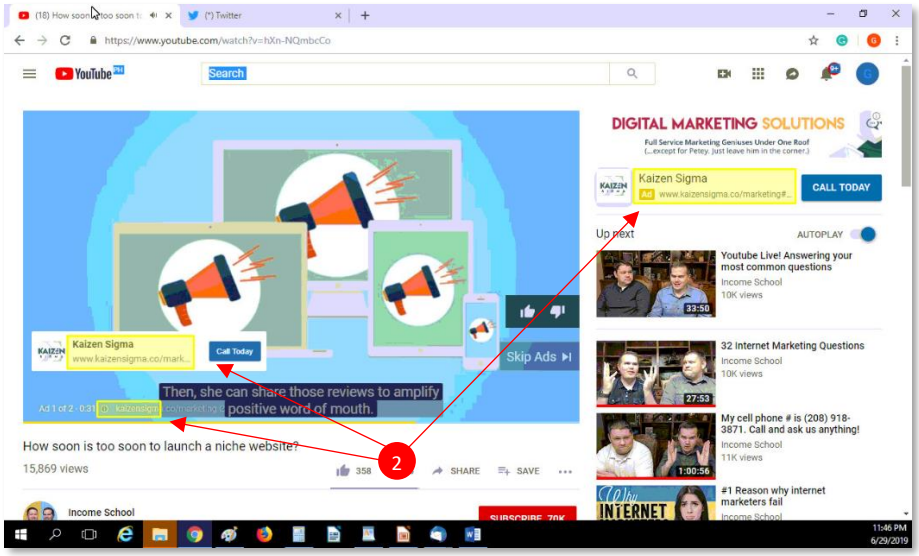
2. Enter your search criteria and press **Enter** or click the **Search** button:
3. Optionally, you can use the second search box (*Search apps/websites*) to further narrow down the results.

4.4.2 Viewing the OCR Snapshots

OCR snapshots show a still picture of the screen where OCR located a search term. To access the snapshot, do the following:

Date / time	Employee	Computer
2019-06-29 19:54:21	Gordon Lewis	WIN-035KHOR8PEI
2019-06-29 19:54:20	Gordon Lewis	WIN-035KHOR8PEI
2019-06-29 19:54:19	Gordon Lewis	WIN-035KHOR8PEI
2019-06-29 19:54:18	Gordon Lewis	WIN-035KHOR8PEI
2019-06-29 19:54:16	Gordon Lewis	WIN-035KHOR8PEI
2019-06-29 19:54:15	Gordon Lewis	WIN-035KHOR8PEI

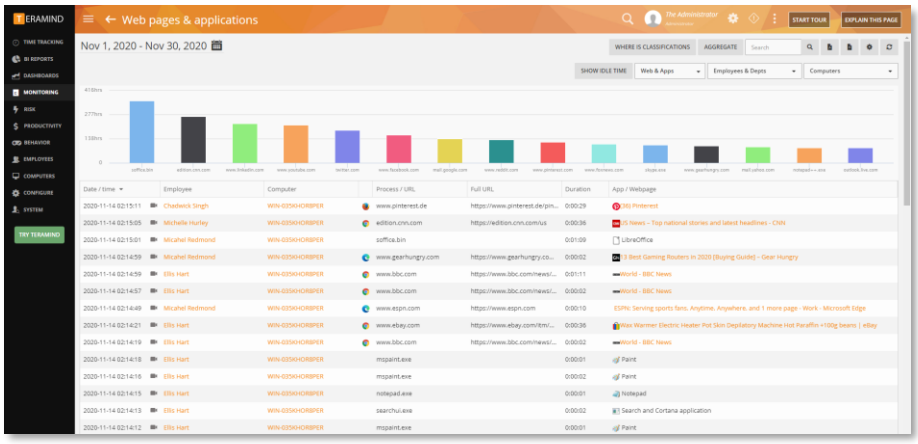
1. Click the **Still Camera** icon on the *Date / time* column to view the OCR snapshot for the searched item at a specific date and time. The OCR snapshot window will pop-up.



2. On the OCR snapshot window, you will be able to see the user's desktop with the areas highlighted in semi-transparent Yellow color where the OCR text were detected.

4.5 Web Pages & Applications

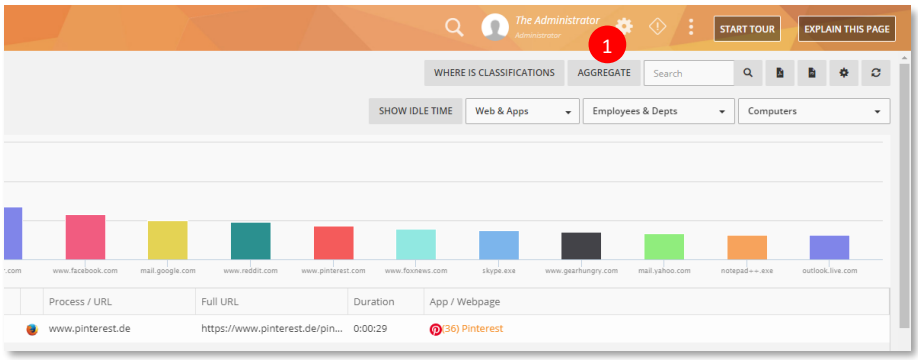
Web Pages & Applications report shows all the application processes run by the users and the webpages they have visited. In addition to the common report filters, you can view the report by individual website/app or aggregate the items by similar apps/websites.



Classifying Web Pages & Applications as Productive/Unproductive

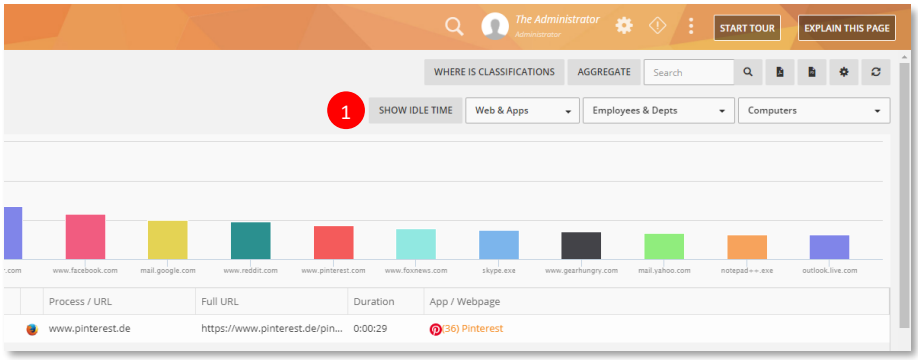
We have enhanced the web pages & applications classification feature and moved it under the Configure > Productivity profiles menu. We have also moved all the productive, unproductive and unclassified time reporting from the monitoring reports to the BI Reports (e.g. Applications & Webpages and Productivity reports). These changes will give you more control and options for classifying employee productivity and reporting.

4.5.1 Aggregating Similar Items



1. Click the **AGGREGATE** button near the top-right corner of the screen to turn it on or off. When aggregation is turned on, the report will aggregate similar web pages and apps together and the report columns will change to Process/URL, Duration, Agents (users) and Applications.

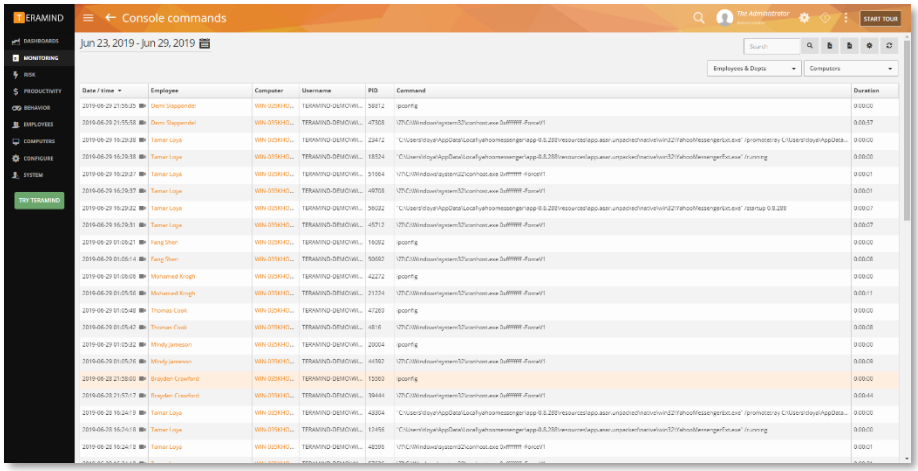
4.5.2 Showing Idle Time



1. Click the **SHOW IDLE TIME** button to see idle times on the applications/websites.

4.6 Console Commands

Console Commands monitoring report tracks any console/terminal commands executed by a user or an application from the command line. The report shows: Date time, employee, computer, username, PID (program ID), the executed command and how long the program had been running.

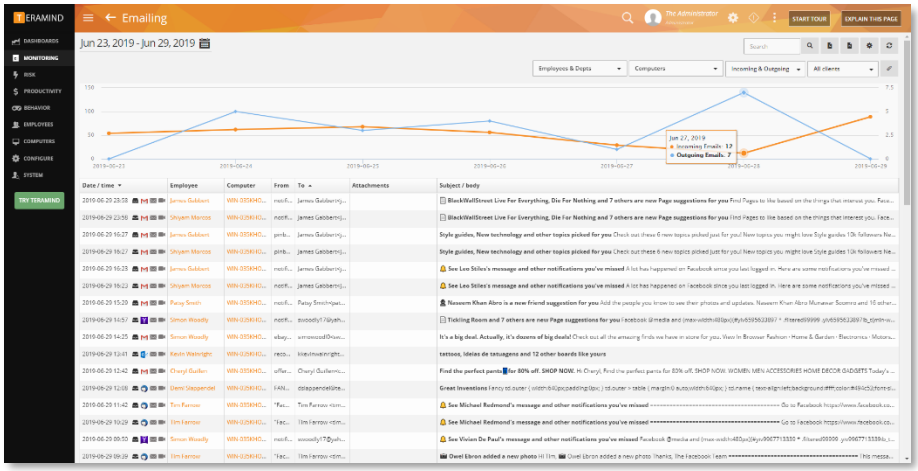


Console Commands can be useful to keep an eye on privileged users (system admins, power users etc.) as these commands are often used to execute system-level applications and scripts. In the wrong hands, such commands can be dangerous and need overseeing.

4.7 Emailing

The Email monitoring report tracks all emails being sent or received including information about the senders, recipients, email subject and body. The system can also save a copy of outgoing attachments (see the note below). All the email records are indexed so you can search for information related to the email actions, preventing security compromises and sensitive data from being transferred out of a system.

The report has a chart you can use to compare between the volumes of incoming and outgoing emails.

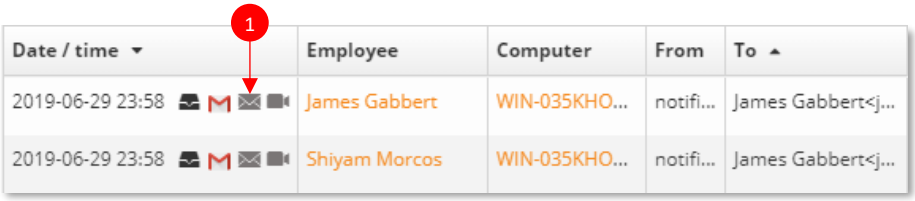


The software covers all email platforms, such as Outlook (web & desktop), Gmail, Yahoo, Yandex, and more.

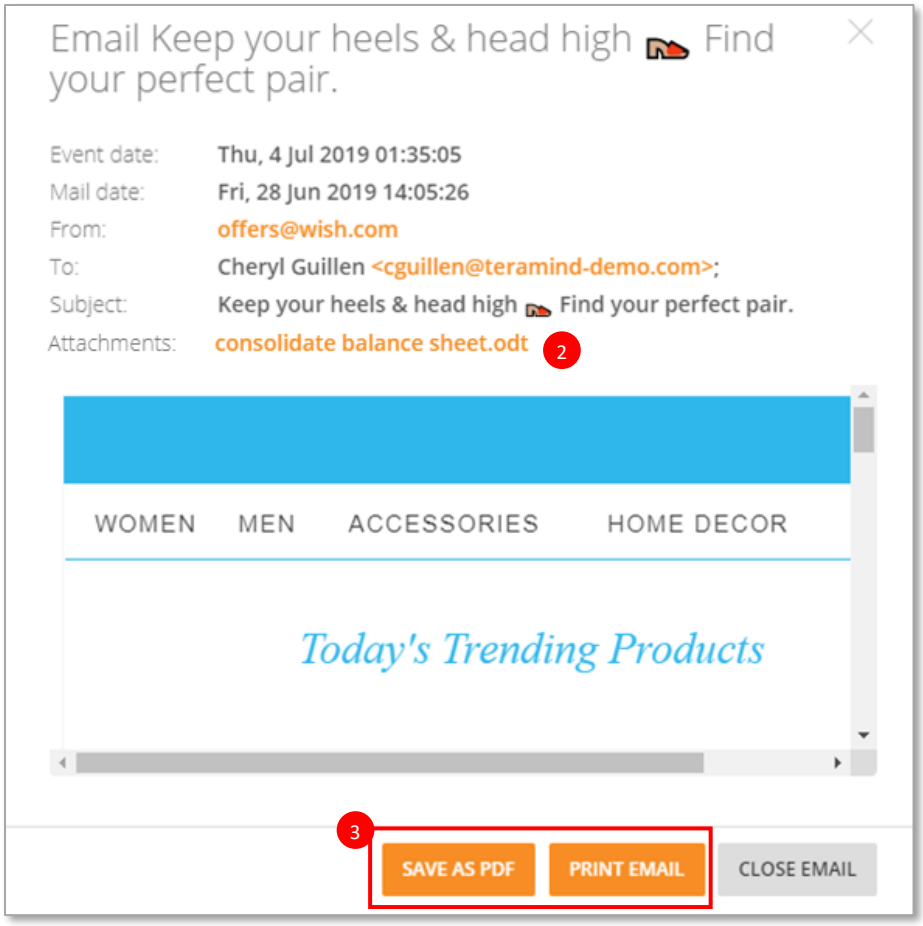
4.7.1 Identifying the Email Origin

1. The first icon on the *Date/time* column shows if it's an incoming or outgoing mail.
2. The second icon on the *Date/time* column shows what email client was used, for example Outlook, Gmail, Yahoo Mail etc.

4.7.2 Viewing / Saving / Printing Email Contents



1. To view the email content, click the **Envelope** icon. A pop-up window will open.



2. If there are any attachments (and you have enabled attachment captures on the Email Monitoring Settings) then, you can click on the attachment(s) to download them.
3. You can save a copy of the email by clicking the **SAVE AS PDF** button or print it with the **PRINT EMAIL** button.

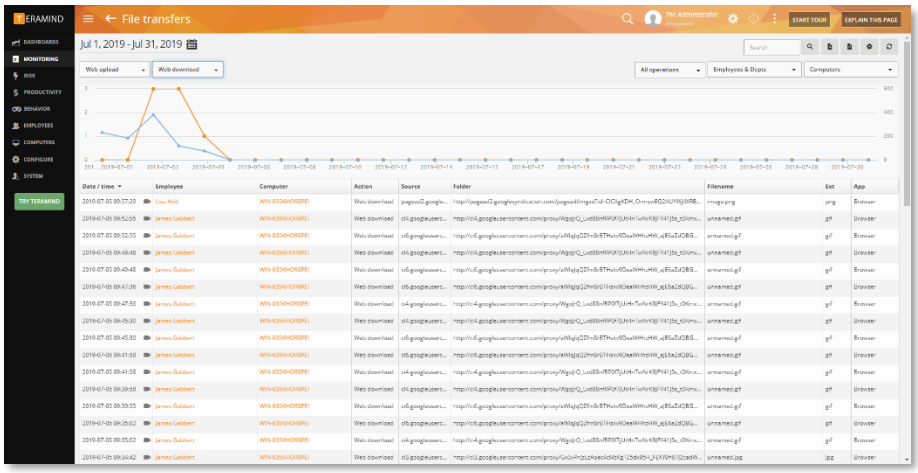
4.7.3 Saving Email Attachments

1. If there are any attachments (and you have enabled attachment captures on the Email Monitoring Settings) then, you can click on an attachment to download from the *Attachments* column. Note: you can also save an attachment from the email view window.

4.8 File Transfers

Use the File Transfers report to monitor all file transfer activity on the local drives, external drives (such as USB drives), network and even Cloud files. The report shows file action (access, write, upload/download etc.), the source (i.e. local disk, network), the full path of the file, file name, extension and what app initiated the file operation. File transfer monitoring helps prevent unauthorized access to sensitive files.

The report also has a chart you can use to compare between two file activities such as Upload vs. Download.

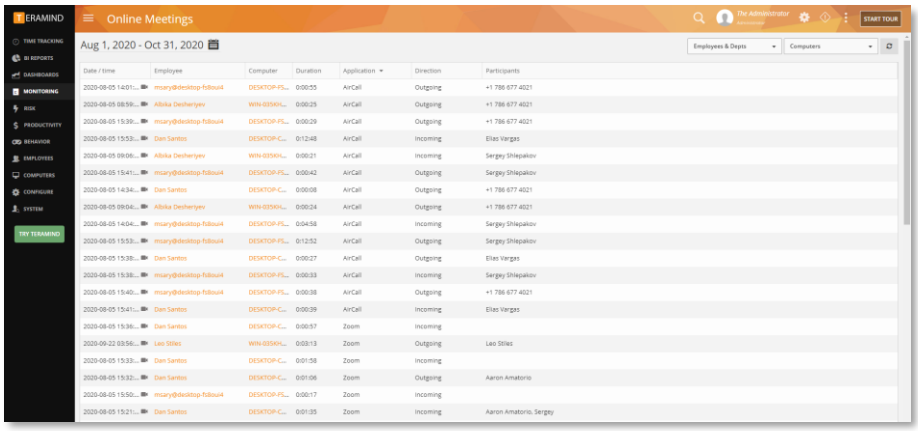


Note that Teramind cannot track the copy operation for a file from one network server to the same network server (e.g. source and destination is the same). For example, copying of a file from `\\103.247.55.101\source_folder` to `\\103.247.55.101\destination_folder` cannot be tracked. Copy to and from same local drives is detected as usual.

Also copying of an empty file cannot be tracked since it will be impossible for the system to distinguish between the file *create* and *copy* operations due to the zero size of the file.

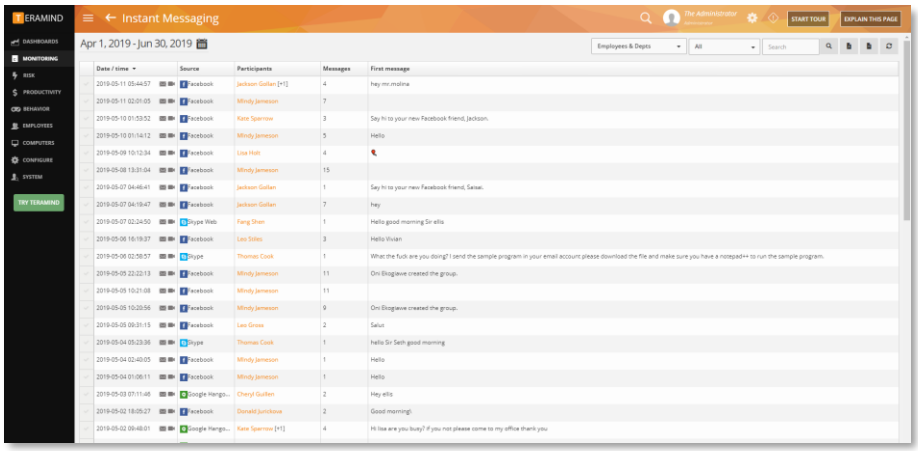
4.9 Online Meetings

You can use the Online Meetings report to monitor online meeting activities for apps such as Zoom, Webex, AirCall, Microsoft Teams, BlueJeans, 8x8, RingCentral etc. The report shows employee, computer, when the meeting took place, duration, app, direction (incoming/outgoing) and participants. If you have enabled screen recording and/or audio recording from the monitoring settings, you will be able to view and/or hear the meetings by clicking the session player icon.



4.10 Instant Messaging (IM)

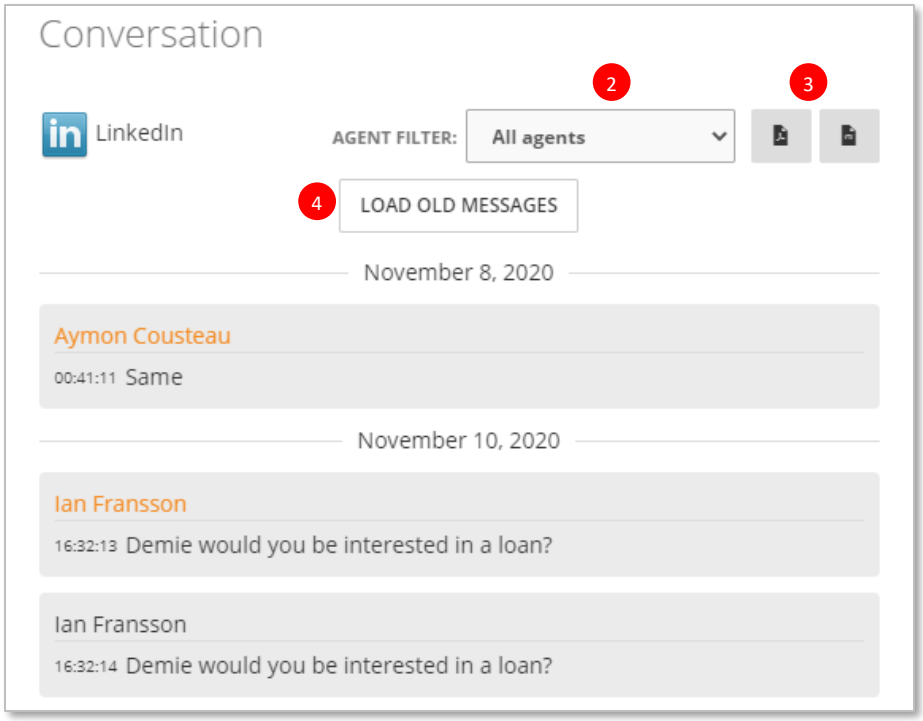
Instant Messaging monitoring report helps you track any chat conversation, whether on the web or in-app. It can track Google Hangout, Skype Web, Skype Desktop, Slack, Facebook Messenger etc. You can monitor incoming and outgoing messages and group chats.



The report shows the source, participants, no. of messages and the first line of the message. You can view a full copy of the conversation and export it as a PDF or CSV file.

4.10.1 Viewing / Saving IM Messaging Contents

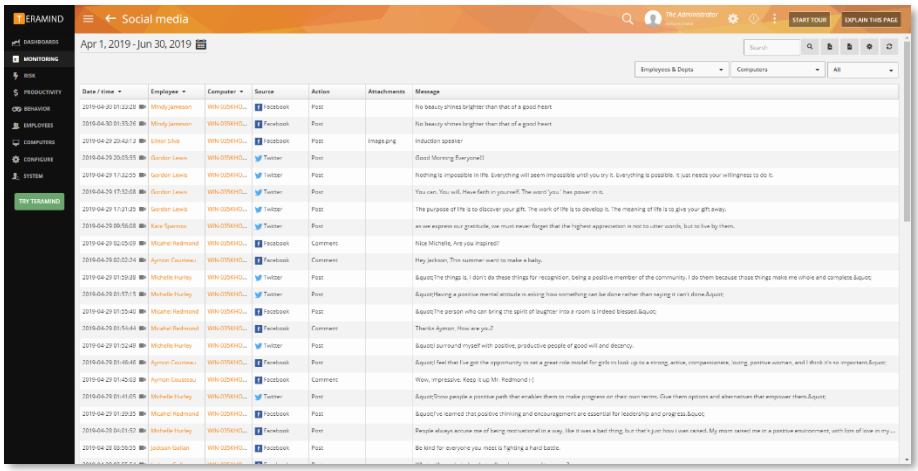
1. To view the messaging content or conversations, click the **Envelope** icon. A pop-up window will open:



1. If more than one agent participated in the conversation, you can use the **AGENT FILTER** drop-down list to view a selected agent's conversation only.
2. Click the **PDF/CSV** download buttons to save the whole conversation as a PDF/CSV file.
3. Click the **LOAD OLD MESSAGES** button to view older messages.

4.11 Social Media

Social Media monitoring report lets you track popular social media platforms such as Facebook, Twitter and LinkedIn. You can track new comments, edit comments, new posts and edit posts activities.

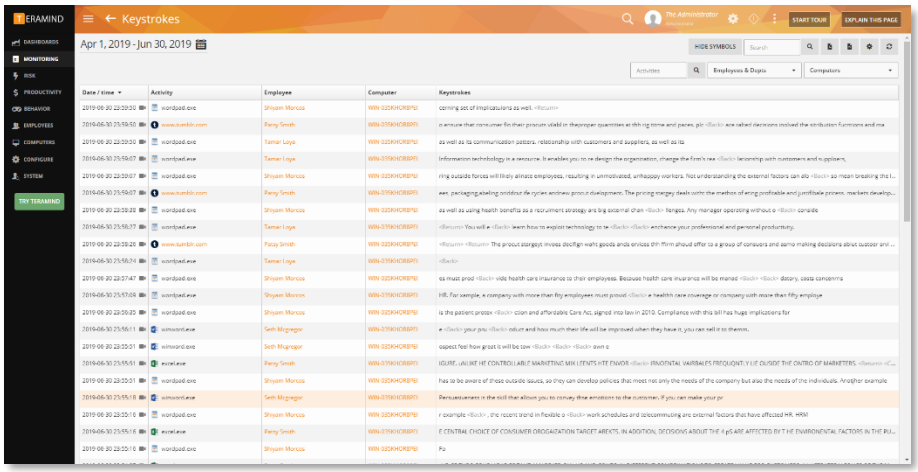


The report shows the source, action (post, comment etc.), name of any attachments being shared and the actual message.

> Note that, you can only see the name of the files being shared on the *Attachment* columns. At the moment, you cannot download them.

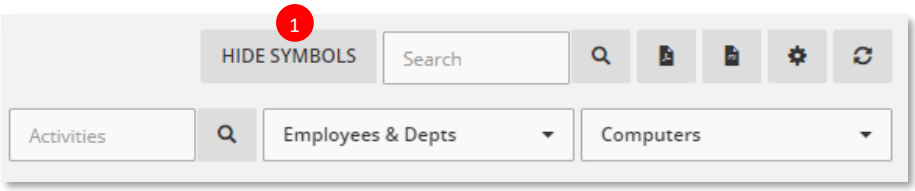
4.12 Keystrokes

Keystrokes monitoring report shows all the keystrokes enter by the users. In addition to regular keys, you can monitor the clipboard operations (copy/paste), use of special keys such as the Print Screen button, hidden symbols (i.e. Space, Delete) etc. All the keys are captured, regardless of the user's selected language.



Keylogging provides a wide range of insight into a user's behavior. For example, you can detect if an employee is using unprofessional language with a customer; if someone is taking screenshots of an important document (with the likely intention of stealing information); a user repeating easy to guess passwords (hence, creating a security risk) etc.

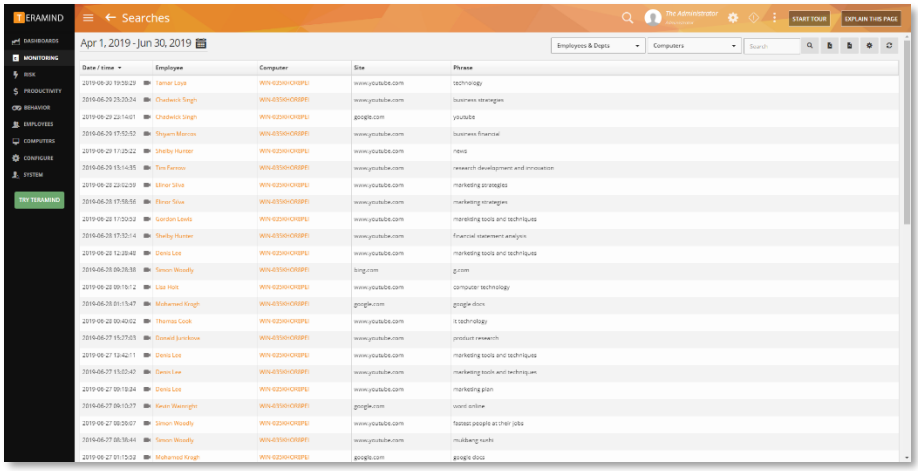
4.12.1 Showing / Hiding Special Symbols



1. Click the **HIDE SYMBOLS** button on the top right corner to show/hide symbols like the <Space>, <Control+C>, function keys etc.

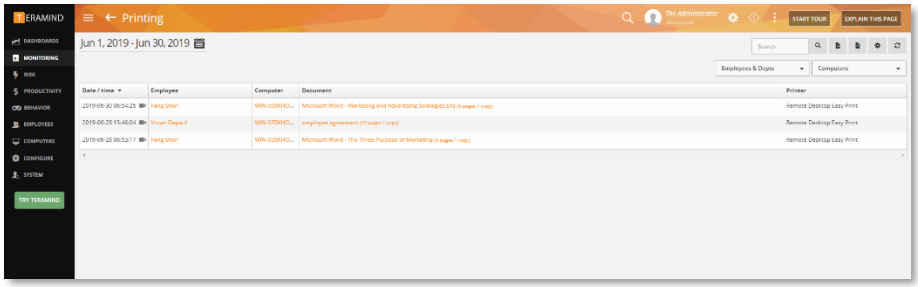
4.13 Searches

Searches monitoring report lets you track what the users are searching for on sites like Google, Bing, YouTube etc.



4.14 Printing

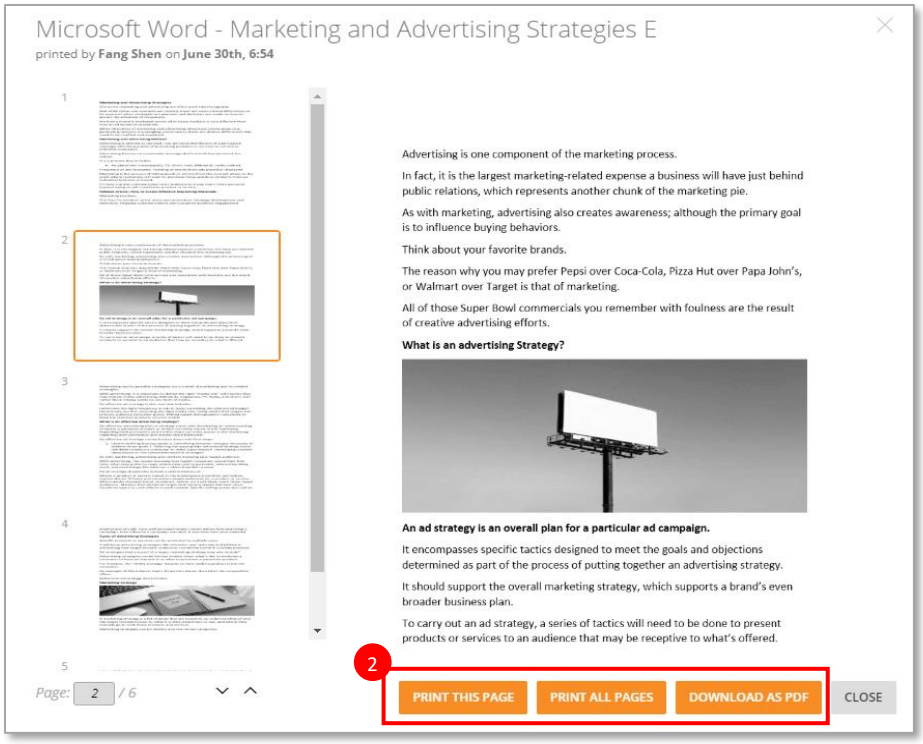
The Printing monitoring report tracks all documents sent to the local or network printers. You can view or print a copy of the document or save it as a PDF file. The report shows the name of the document, printer, computer and user.



Monitoring employee print logs helps you reduce printing waste. It's also prevents data leaks over hardcopies.

4.14.1 Viewing / Saving / Printing Copies of the Document

1. Click the **document link** under the *Document* column. A window will pop-up.

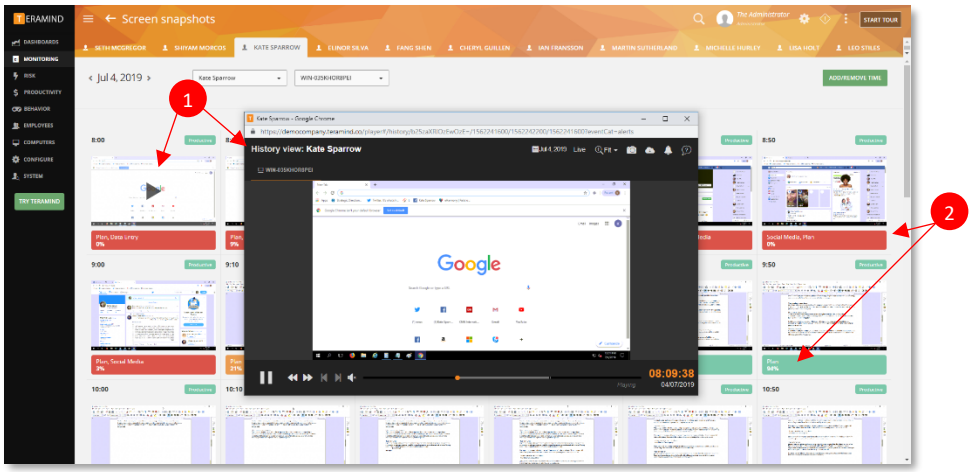


2. From the pop-up window, you can print a selected page, all pages or save the document as a PDF file.

4.15 Screen Snapshots

The Screen Snapshots monitoring report allows you to have a quick glance over users' desktops. You can choose multiple users or computers to view.

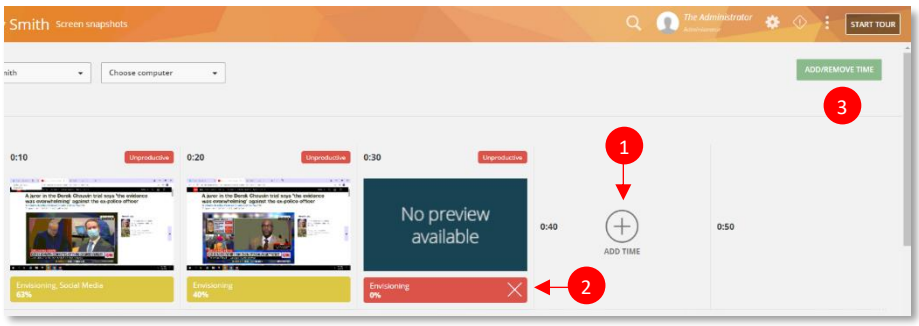
> The snapshots are taken at 10-minute interval.



1. By clicking a snapshot image, you can view a session recording of the user's desktop. Check out the Session Player section for more information about session recordings and playback.
2. Under each snapshot, you will see the Task the user's working on and their activity level (in percentage). You can also quickly identify how a user is performing by taking a look at the color of this area:

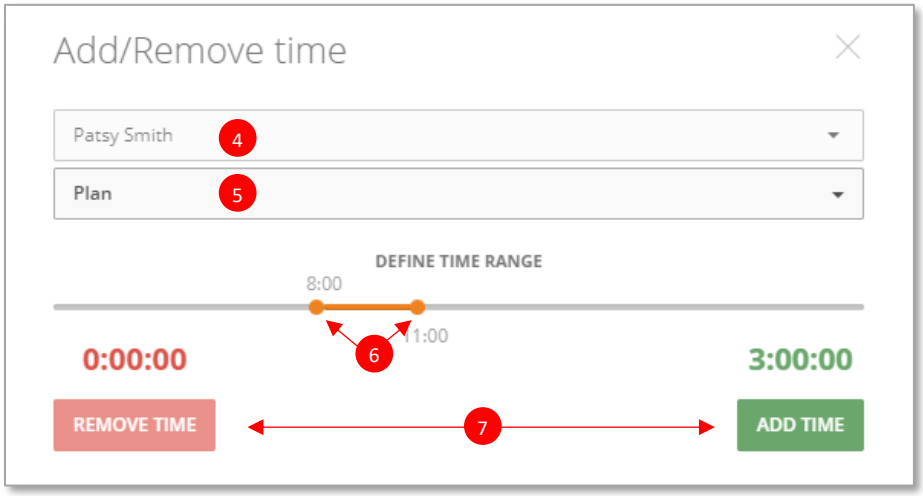
   - Green = 71% - 100% activity
   - Yellow = 41% - 70% activity
   - Orange = 21% - 40% activity
   - Red = 0% - 20% activity.

4.15.1 Adding/Deleting Time



Note that removing a timeslot removes it from the Screen Snapshots reports only. The screen recordings are still accessible from the Session Player.

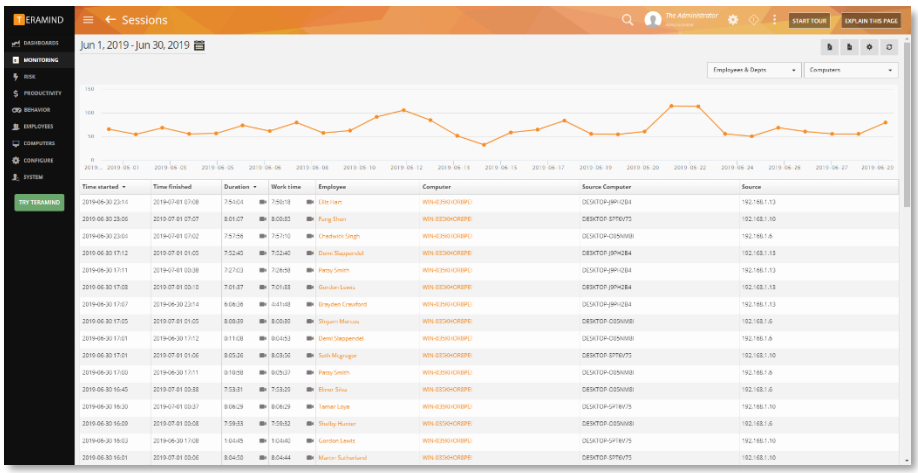
1. You can quickly add time to an empty slot by hovering over it and clicking the **+ ADD TIME** button.
2. You can quickly remove a time slot by hovering over it and clicking the **X** button.
3. You can also click the **ADD/REMOVE TIME** button located near the top-right corner of the report to add/remove time. If you click this button, a pop-up screen will appear:



4. Select a **user** (you need to select a user if you are viewing the screenshots for a computer which has multiple users).
5. Select a **task** (you need to select this only if you are *adding* time).
6. Drag the **two sliders** to set the start and end time.
7. Click the **REMOVE TIME** button to remove or **ADD TIME** button to add the selected time.

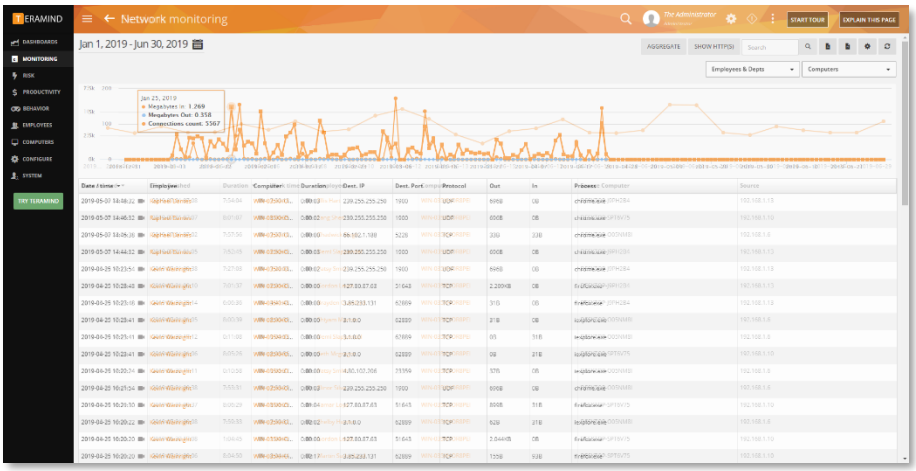
4.16 Sessions

Sessions monitoring report shows an immutable log of all user sessions including: Time Started, Time Finished, Duration, Work Time, Employee, Computer (to which a remote user is connected to), Source Computer (from which a remote user connected from) and the IP. You can also view a trend graph for the sessions.



4.17 Network Monitoring

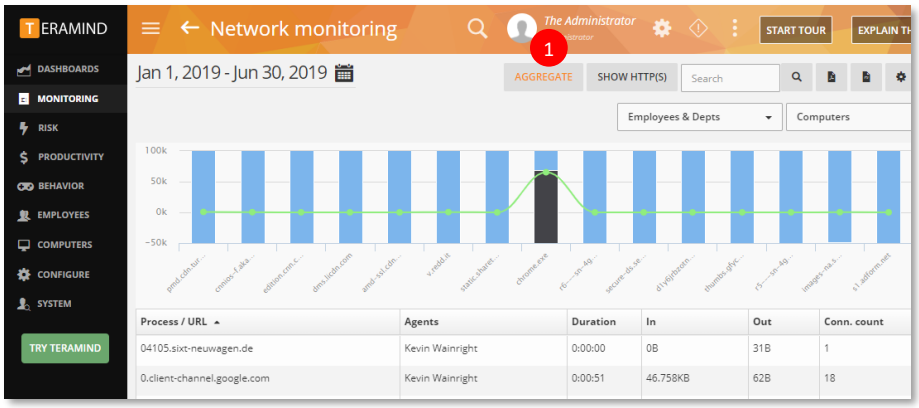
Network Monitoring report allows you to monitor network traffic from all applications and users connected to the internet, identify their locations, time and the exact IPs and ports used for the connections. Additionally, administrators can measure the amount of bandwidth used by employees and the specific computers used to establish the network connections.



The report shows detailed information for each network activity such as, the application processes/URLs, agents (users), duration of a network session, amount of information sent or received, number of connections, ports and the protocols used (i.e. TCP, UDP, HTTPS).

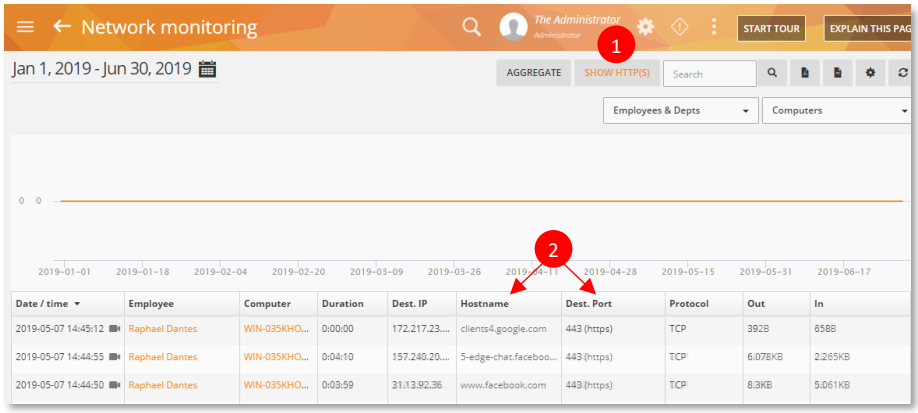
Monitoring your company's networks can give you insights into your network and detect potential signs of danger or abuse. For example, you can detect sudden spike in network usage indicating potential intrusion attempts. Or, you can discourage unproductive activities such as online shopping or social media browsing. Or, you can monitor video streaming sites to reduce unnecessary use of network traffic or bandwidth.

4.17.1 Aggregating Similar Items



1. Click the **AGGREGATE** button near the top-right corner of the screen to turn it on or off. When aggregation is turned on, the report will group similar application processes/URLs together and the report columns will change to: Process/URL, Agents, Duration, In, Out and Connection count.

4.17.2 Showing / Hiding HTTPS Connections

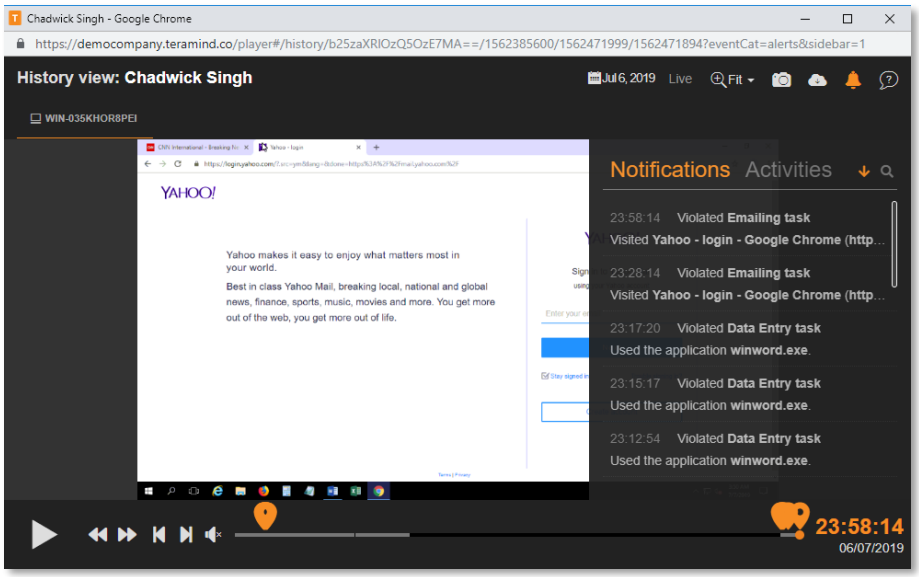


1. By default, HTTPS (SSL) connections aren't shown on the report. To show/hide HTTPS connections, click the **SHOW HTTPS** button near the top-right corner of the screen.
2. An extra column named '*Hostname*' will be added to the table. The *Dest. Port* will also change to indicate if a connection is on HTTPS port.

5 Session Player

5.1 Introduction to the Session Player

Teramind visually captures every action that a user makes while on a machine in real-time. Teramind also saves this information complete with meta-data and indexes for later processing. Hence, the Session Player supports both Live View and History Playback features.

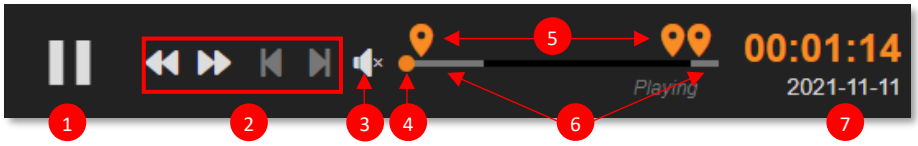


- **Live Mode:**
  With the Live Mode, the Session Player turns into a fully functional remote desktop client. You can view a real-time stream of the user's desktop, take remote control of it, freeze input or lock out the user.
  Note that, the Live Mode is available only when a user is online. You will see the 'Live' indicator on top of the player turns Orange when the session player is in Live Mode.

- **History Playback Mode:**
  With the History Playback Mode, you can use the Session Player to view previous desktop session recordings of the user.

Both modes allow you to see detailed list of Notifications (Alerts) and Activities related to the user. If Audio recording is enabled, you can also hear recordings of both sound outputs and inputs (speakers/line-out, microphone/line-in). Finally, you can forward the recordings to select email addresses or download them as MP4 files.

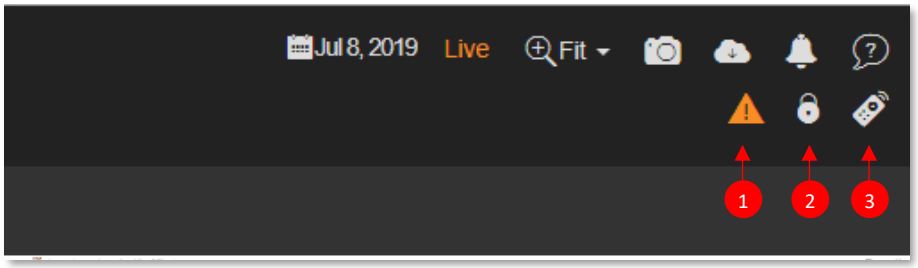
5.2 Basic Navigation



1. Use the **Play/Pause** buttons to play/pause the video.
2. Use the **Rewind**, **Fast Forward**, **Beginning/End** buttons to control the playback. Note that, these controls aren't available on the Live View mode.
3. Use the **Audio** button to turn sound on/off.
4. You can also drag the **Play Head** to move back and forth on the recording timeline.
5. When Notifications is turned on (the **Bell Icon** on top of the player turns Orange), you can click a **Notification Indicator** to jump to a time where a rule violation incident occurred.
6. If the **Timeline** is *grey*, it means video recording is available for that time. If it's *black*, it means video recording is missing. There might be several reasons for missing recordings for a period of time. For example, the user was logged out, the agent was disabled, screen recording turned off, locked session recording is turned off, etc. Check out this Knowledge Base article to learn about troubleshooting video recording issues.
7. You can see the **Time** and **Date** of the recording. Click on either the **Time** or **Date** to enter a new time/date.

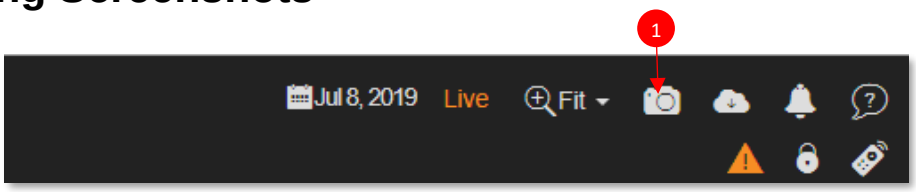
5.3 Live Mode Controls

There are three special buttons available on the Live Mode, using which you can control the user's desktop.



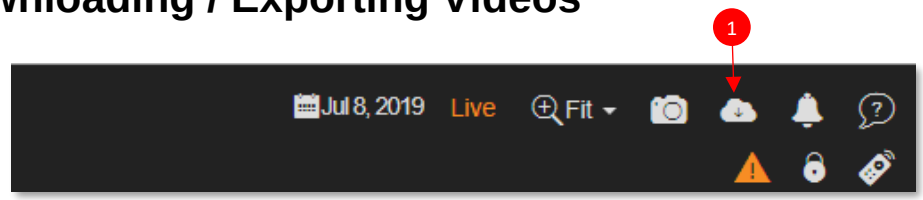
1. **Invoking the Task Manager (Windows):**
   Use the **Warning** button to send CTL+ALT+DEL command to the user's computer. This will bring up the Windows Task Manager screen, where you can access options to change the account password, switch a user etc.
2. **Freezing User Input:**
   Use the **Padlock** button to freeze/unfreeze user's input. When input is frozen the user won't be able to use their keyboard or mouse.
3. **Remote Control:**
   Use the **Remote-Control** button to take full control of the user computer.

5.4 Taking Screenshots

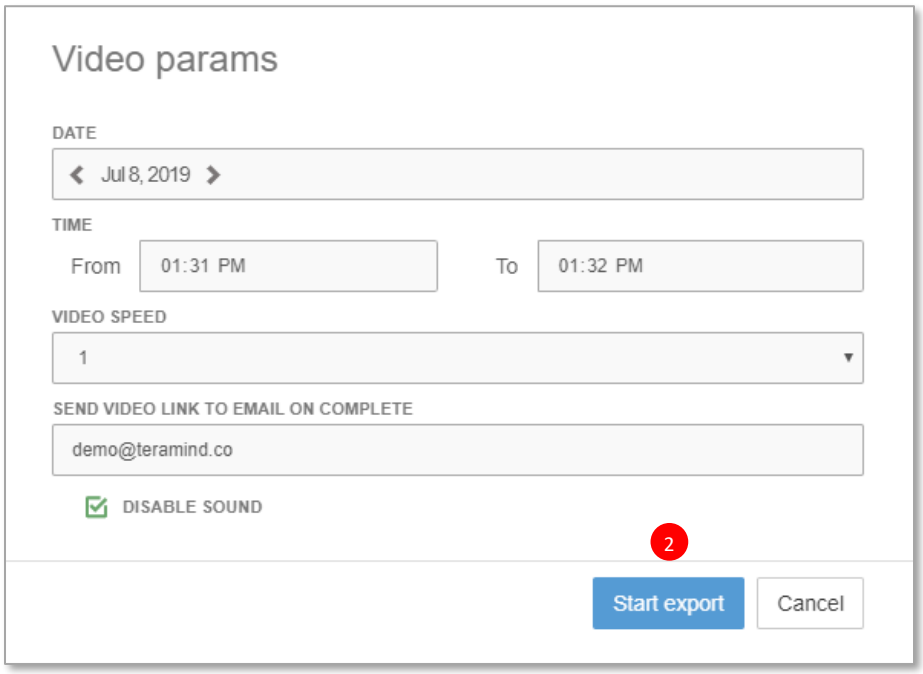


1. Use the **Camera** button to take a screenshot of the desktop and save it as a PNG file.

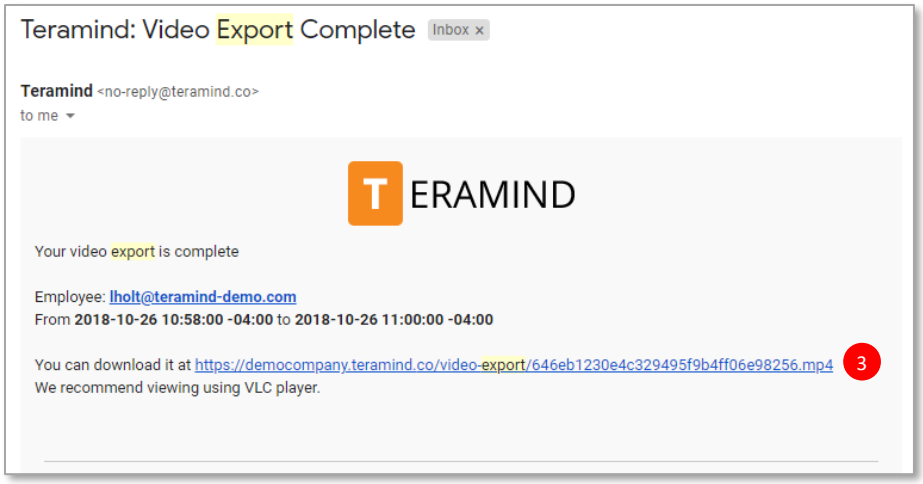
5.5 Downloading / Exporting Videos



1. Click the **Cloud Download** button. A pop-up window will open.



2. On the *Video params* pop-up window, select a date and specify time range, video speed and an email address. You can also disable audio if wanted. Click the **Start export** button.

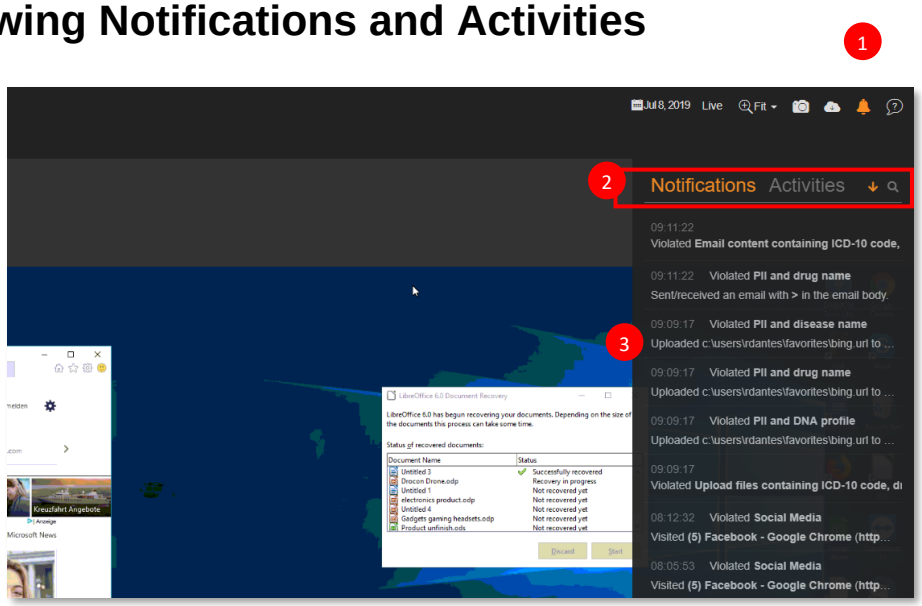


3. Once the video is ready, an email will be sent to the specified email address(es) with a link to the video for download.

You can view a list of all the exported videos and download them from the **System** > **Video Export** screen. Note, some restrictions apply. See the Video Export section for more information.

Note that, if domain restriction is enabled for exporting data, then you can only send export emails within that domain. If it's left blank, then any email addresses can be used. Check out the Outgoing Exported Data section for more information.

5.6 Viewing Notifications and Activities

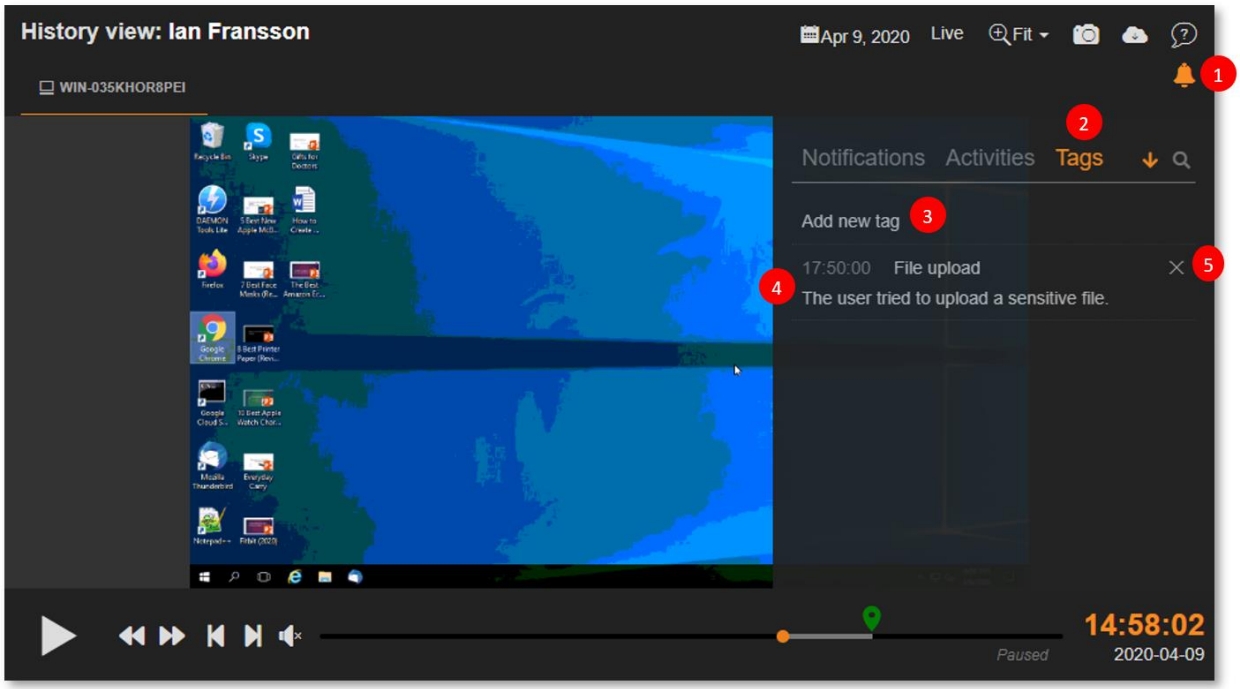


1. Click the **Notification** button.

2. You will see a list where you can switch between **Notifications** and **Activities**. You can also search for an activity using the **search** button.
3. Click on any notification/activity to move the Player Head to the time when the notification/activity occurred.

5.7 Viewing / Adding / Removing Tags

You can add custom tags to the video for auditing, tracking or other purposes. Tags let you mark a time on the video and add a label to it. You can also add notes.

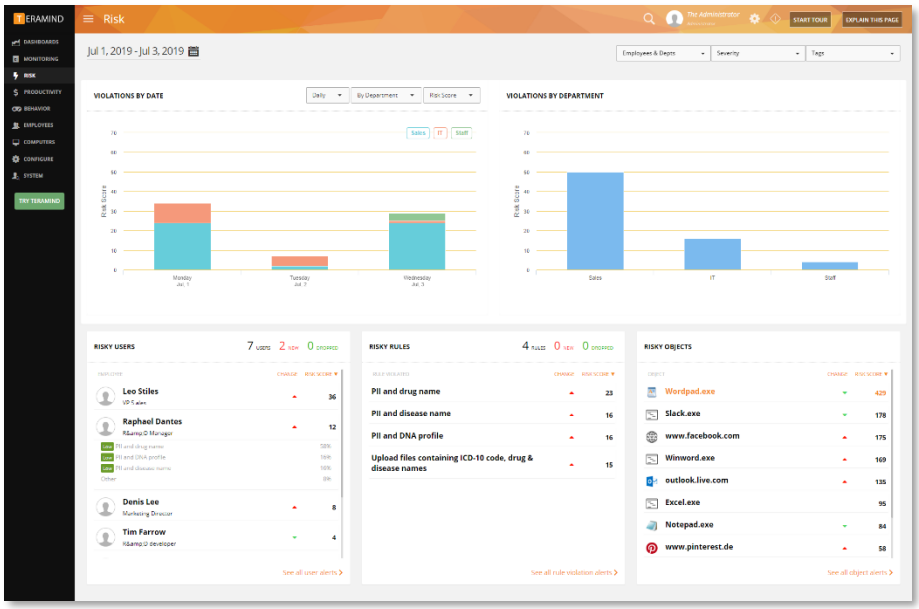


1. Click on the **Notifications** icon
2. Select the **Tags** tab. You will see a list of existing tags (if any).
3. Click the **Add new tag** link to create a tag. This will open a pop-up window where you can specify the tag details such as tag name, date, time and notes.
4. Click on a **Tag** to move the player head to the time the tag was created.
5. Click the **X** button to delete a tag.

6 Risk

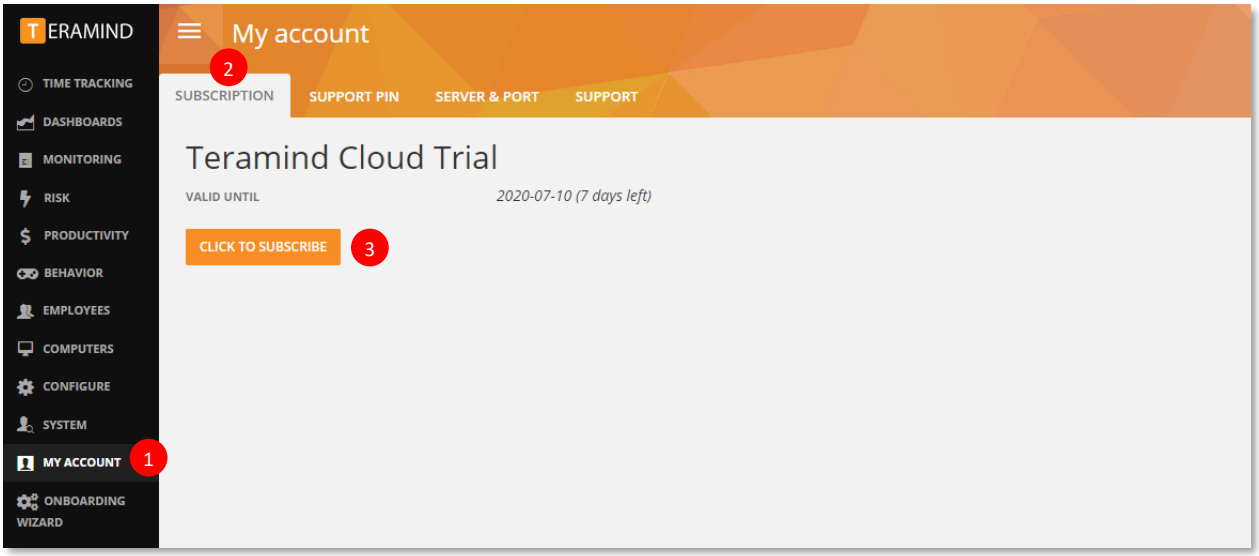
6.1 Introduction to Risk

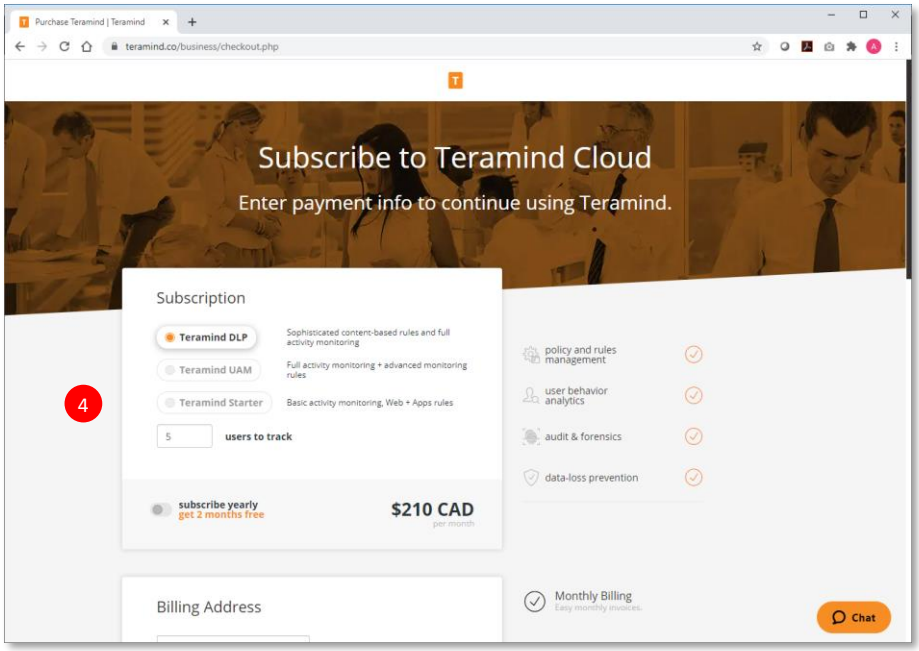
The Risk report allows you to conduct organization-wide risk assessment. The report shows top risky users, rules and objects (applications and websites). The report also lets you plot risk trend by department, severity, number of violations, tags (tags are used to identify a rule) etc. Unique risk score helps you identify high-risk users or policies so that plans can be developed for treating the risks. You can filter the report by employee, department, severity and tag.

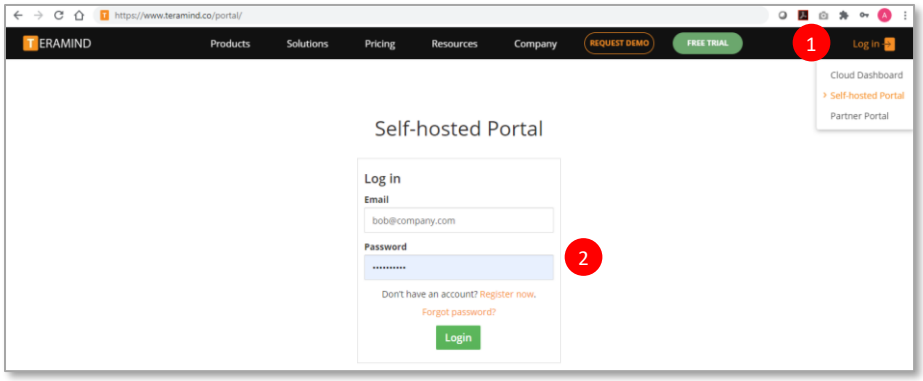


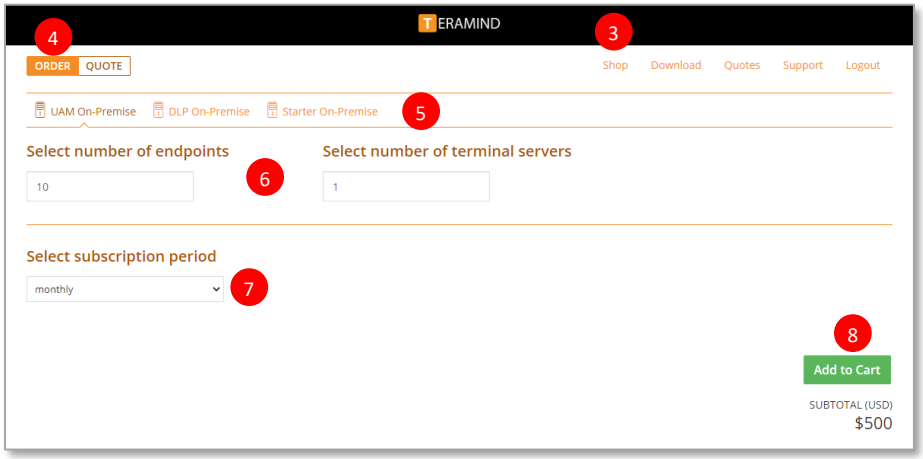
Teramind uses a combination of inputs derived from the Rules (Advanced Mode), Anomaly Rules and proprietary algorithms that analyze user behavior to calculate a risk score.

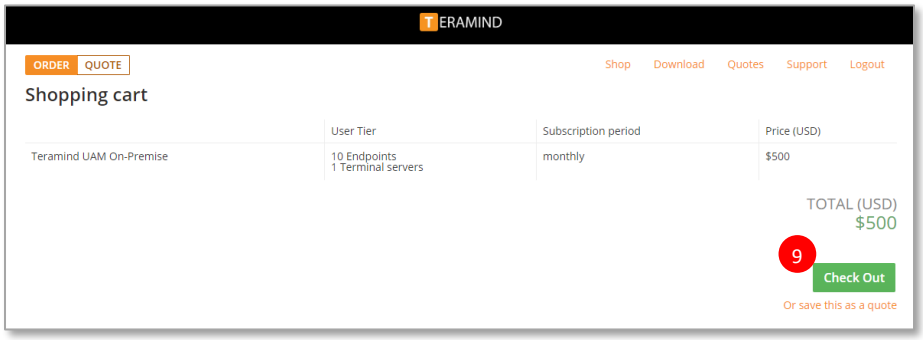
6.2 Accessing the Risk Menu



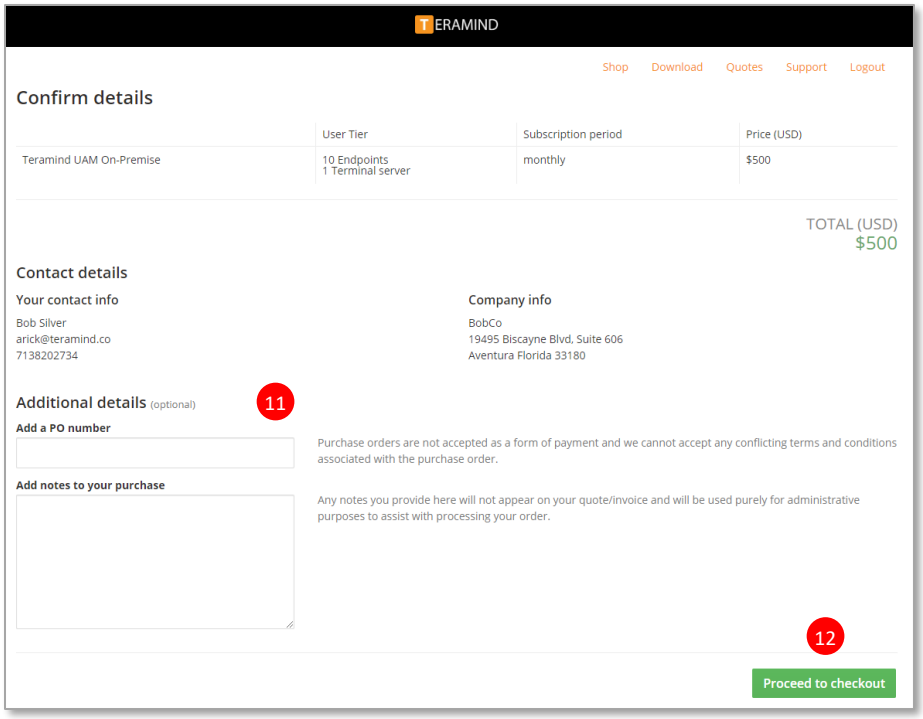



https://www.teramind.co/portal/
TERAMIND
Products
Solutions
Pricing
Resources
Company
REQUEST DEMO
FREE TRIAL
1
Log in
Cloud Dashboard
Self-hosted Portal
Partner Portal
Self-hosted Portal
Log in
Email
bob@company.com
Password
Don't have an account? Register now.
Forgot password?
Login
2


TERAMIND
4
3
ORDER
QUOTE
Shop
Download
Quotes
Support
Logout
UAM On-Premise
DLP On-Premise
Starter On-Premise
5
Select number of endpoints
10
6
Select number of terminal servers
1
Select subscription period
monthly
7
8
Add to Cart
SUBTOTAL (USD)
$500

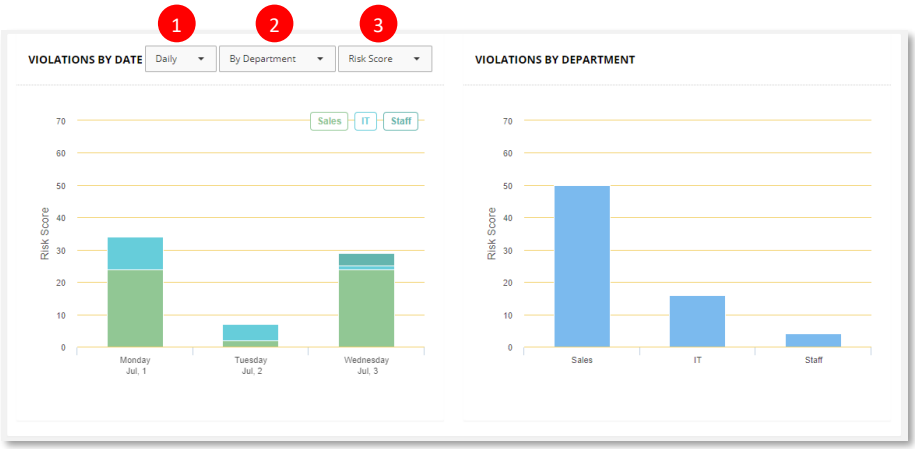

TERAMIND
ORDER
QUOTE
Shop
Download
Quotes
Support
Logout
Shopping cart
User Tier
Subscription period
Price (USD)
Teramind UAM On-Premise
10 Endpoints
1 Terminal servers
monthly
$500
TOTAL (USD)
$500
9
Check Out
Or save this as a quote


TERAMIND
Shop
Download
Quotes
Support
Logout
Your contact info
Email
bob@boco.com
First Name
Bob
Last Name
Silver
Phone
7138202734
10
Your company
Comany Name
BobCo



1. You can access the Risk report by clicking the **RISK** menu.

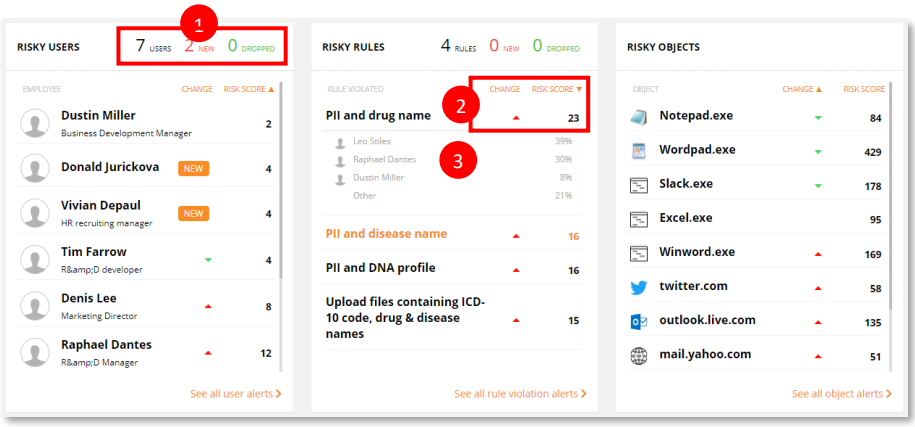
6.3 Plotting the Risk Trend



You can control what the top two graphs on the Risk report will show through their three pull-down menus:

1. The first menu lets you choose the frequency of the data being plotted. You can choose from *Daily*, *Weekly* or *Monthly* options.
2. The second menu lets you choose the X-axis (horizontal) categories for the graphs. You can choose from *Tags*, *Departments* and *Severity*.
3. The third menu lets you choose the Y-axis (vertical) values for the graphs. You can choose between *Violations* or *Risk Scores*.

6.4 Identifying High Risk Users, Rules and Objects



The bottom part of the Risk report has three panels that show the top risky users, rules and objects.

1. At the top-right corner of the users and rules panels, you can see how many users/rules are identified as the top risk, how many of them are new, and how many risk items were dropped (based on the time period you have selected for the report).
2. The third column of the risk items shows the up ▲ , down ▼ or no change (no indicator icon) trend for each risk.
3. You can click on any risk item to expand it. When expanded, it shows the top risky items causing the risk. For example, if you click a Rule item, it will show the three top users who are associated with the risk and a break down of their risk contribution (in percentage).

7 Productivity [deprecated]

DEPRECATED FEATURE

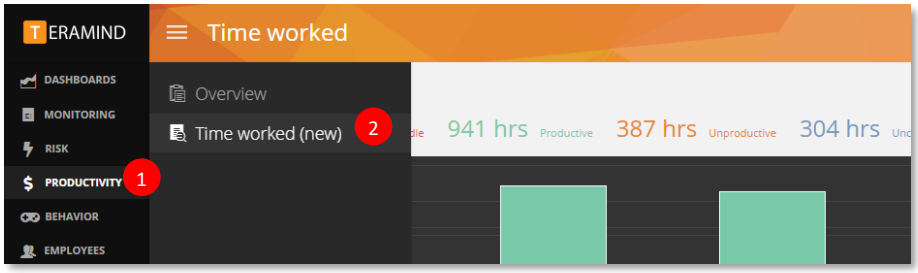
These Productivity Reports are deprecated. Please use the new BI Reports > Productivity report which offers more information, drill-down capabilities, enhanced export, and faster load time. Please contact Teramind support if you have any questions.

7.1 Introduction to the Productivity Report

The Productivity report lets you track employee productivity and performance. It shows productive, unproductive, active and idle time and how much you are spending on employee wages/salary.

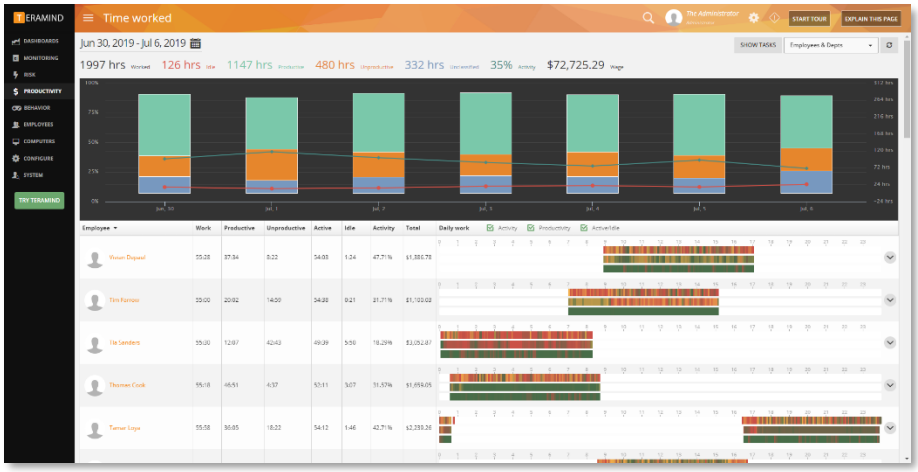
Productivity report aggregates data from the activity monitoring, employee profiles, productivity profiles and other configuration settings such as departments, schedules, user input from the Revealed Agent etc.

7.2 Accessing the Productivity Report



1. Hover over the **PRODUCTIVITY** menu, then
2. Click the **Overview** or the **Time Worked** sub-menu.

7.3 Productivity Report Explained



The report comes with the following special columns:

7.3.1 Session Time

Total time which user had been being logged into windows.

Why Session time is 0 for current date?

Session time, as well as Productive / Unproductive time and some others time values may be calculated with some delay, up to several hours, especially on the Cloud.

Why Session time is > 24 hours for a single day in selected date range?

Because user could be logged into several machines and we show total time on all machines.

7.3.2 Work Time:

Work represents the gross amount of time which your employees logged as user sessions (excluding any locked sessions). With this column, you can see if your employees were present or absent from work; and how many hours they have clocked in for a selected date range.

Why Work time is greater than Session time?

It can happen when the Agent is offline for some time (Teramind server was inaccessible due to network connection or other issues). In offline mode. Teramind continues recording all activity and Work time, but not the Session time.

Why Work time reported on Productivity Report is different thant the Dashboard Widgets?

The Online employees widget on the Dashboard shows Work time only on current computer on which user works at the moment. Productivity Reports summarize time on all computers on which user has been working at the day.

Please note that, for Work time to work properly, the Agent should have a task assigned. Especially, if it's a Hidden Agent. You can change the Default Task from the Agent Default Settings. It's configured by default, but sometimes you may have reset it, so Work times may stop counting. The Agent should be reconnected to apply new default task. Restart machine for that.

7.3.3 Productive Time:

Represents time spent on productive websites and applications; based on the classification you made in the Web Pages and Application report. Check out Productivity Profiles section for more information on activity classification.

Why Productive/Unproductive/Unclassified time can be greater than 'work time'?

That is possible because Work time does not take into account the time when the session was locked and if there is no task set for the user, work time won't be counted. Same is possible for Session time in case of offline mode.

7.3.4 Productive (no idle) Time:

Similar to Productive time, only difference is, this time measures time the user is actually active (moving the mouse, typing on the keyboard) on the websites/applications.

7.3.5 Unproductive Time:

Any time NOT spent on Productive web pages/applications are classified as unproductive.

7.3.6 Active Time:

Represents time spent engaging the keyboard or mouse.

7.3.7 Idle Time:

Idle time represents the absence of activity on keyboard and mouse.

This is calculated in conjunction with the Idle Time Threshold set on the Applications settings page. For example, if the idle time threshold is set to 10 minutes, and someone didn't use their mouse/keyboard for 15 minutes, then the idle time will be 5 minutes. So, basically, the system will not start counting the idle time until the threshold is reached.

7.3.8 Activity (%):

Represents the average activity percentage for the selected date range. This value is an average of the activity level in 5-minute intervals during which the employee was logged into a session. The score of each five-minute interval is calculated based on the user's keyboard and mouse activity. If the user types

at or above 40 words-per-minute or is active on the mouse with relatively few breaks, score will be 100%. If the user is completely idle, their score will be 0%.

Color guide:

The color table below shows the activity %:

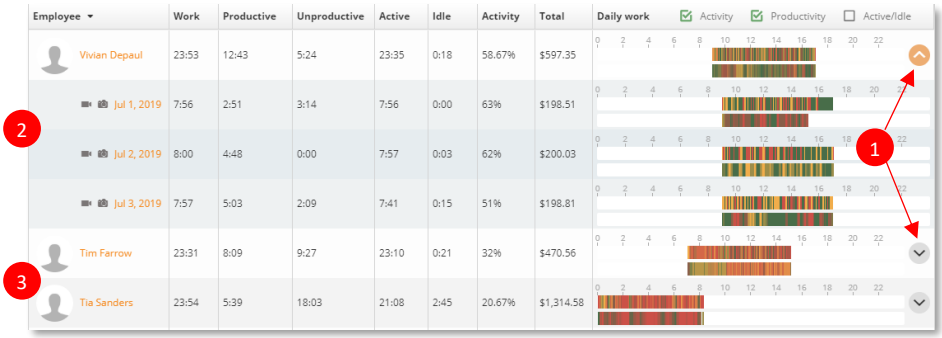
	Green = 70% – 100% activity
	Yellow = 11% – 69% activity
	Red = 0% – 10% activity

7.3.9 Total Time:

Represents the total wages earned by the user during this time frame and is based on salary/wage rate you may have designated to the user. Check out [Entering / Editing Employee Profile] to learn how to assign salary/wage to an employee.

7.4 Summary vs. Detailed View

When viewing the report for multiple days, you can expand a row to view details for each day in addition to a summary of all days.



1. Click the **up/down arrow button** at the right side of a user's row to expand/collapse it.
2. When expanded (Detailed View), each date is shown in separate rows in addition to a summary for all days.
3. When collapsed (Summary View), the dates are aggregated into a single row for each employee.

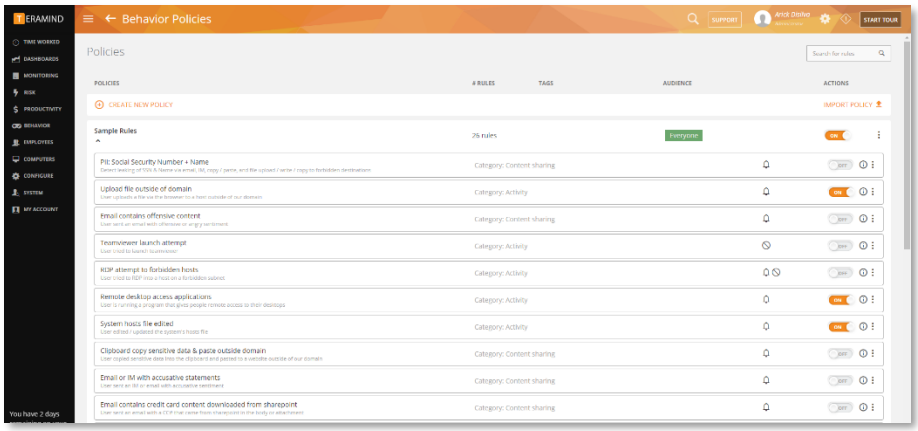
8 Behavior

8.1 Introduction to the Behavior

The Behavior menu consists of the Polices, Alerts and Anomaly Rules. These features utilize Teramind's core Behavioral Engine. With the Policy & Rules Editor, you can set up conditions to detect any unproductive, harmful or dangerous activity in real-time, while having Teramind act on your behalf. When a rule is violated, you can be notified about incident and optionally, the system can take actions automatically in different ways (such as warning the user, blocking the activity etc.). You can see the rule violations report from the Alerts screen. Teramind also lets you create Anomaly Rules. These special types of rules use behavioral baselines to detect and prevent behavioral anomalies that's harder to implement with the regular policies and rules.

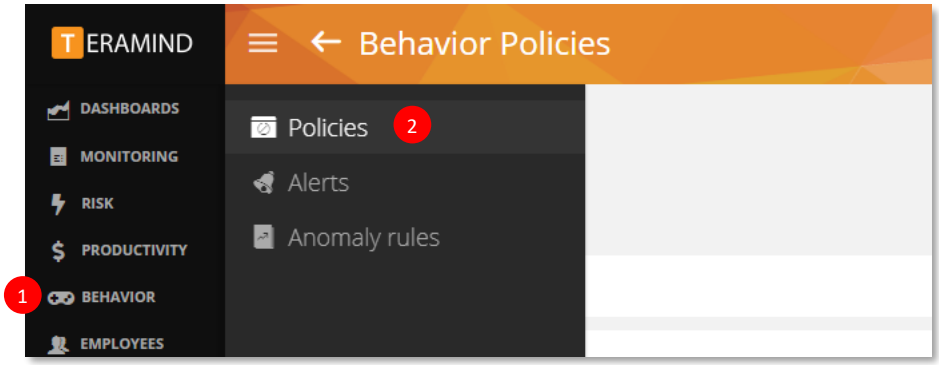
8.2 Policies

Policy helps you organize similar rules together. In a sense, policies are like folders where you keep your rules. For example, you can have all your PCI related rules under a policy called 'PCI compliance'. Or, keep all your HR specific rules such as 'Preventing email harassment', 'Limiting social media use' etc. under the 'Business Etiquette' policy.



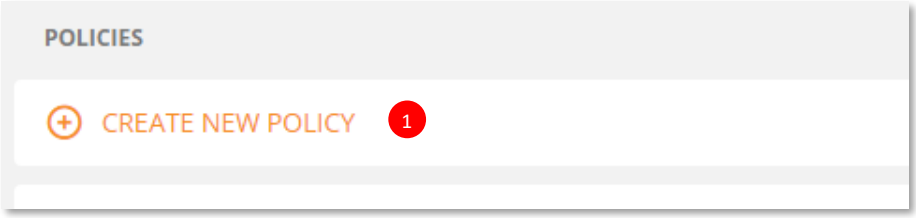
Each Teramind solution comes with a sample policy containing several sample rules. You can experiment with the sample rules to learn how the rules work. Once you are comfortable, you can create your own rules with the intuitive yet easy to use Rules Editor.

8.3 Accessing the Policies Menu

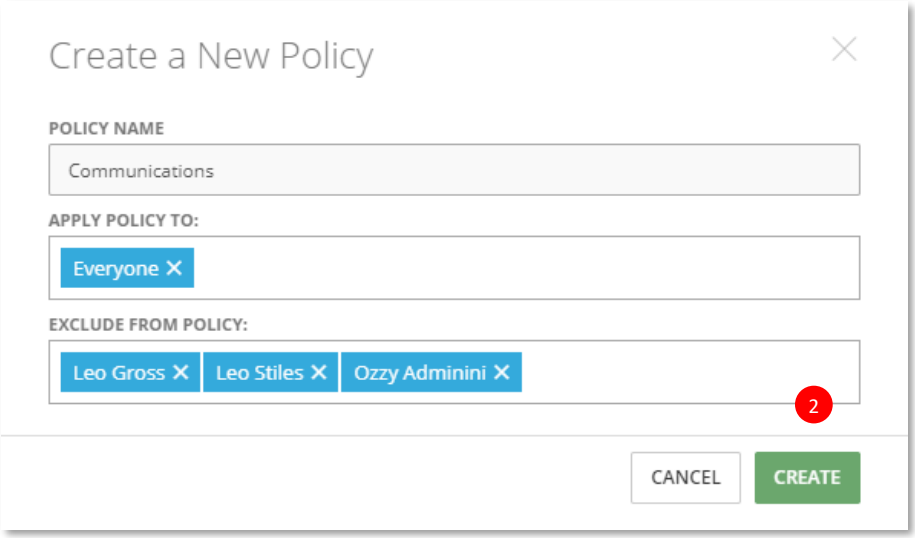


3. Hover your mouse over the **BEHAVIOR** menu, then
4. Select **Policies** from the sub-menu.

8.4 Creating a New Policy



1. Click the **CREATE NEW POLICY** button. A pop-up window will appear.

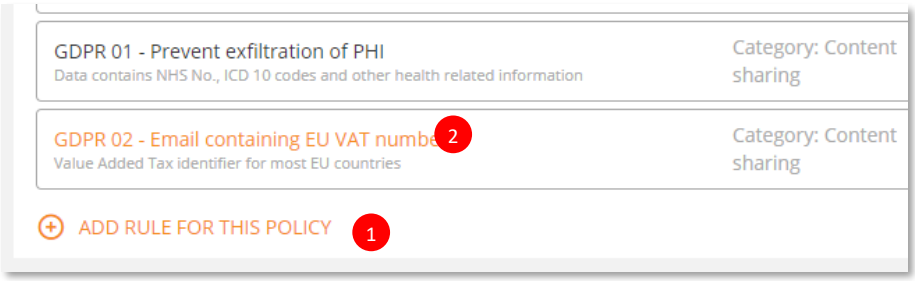


2. On the *Create a New Policy* window, enter a name for the policy. Select the users the policy will apply to and optionally, select any users you want to exclude from the policy. Click the **CREATE** button to create the policy.

8.5 Moving / Exporting / Editing / Deleting Policies

1. Click the **Dotted menu** at the top-right corner of the policy. A pop-up menu will open.
2. To move a policy up on the list, click the **Move Policy up** button.
3. To move a policy down on the list, click the **Move Policy down** button.
4. To export a policy, click the **Export Policy** button. The policy will be saved as a .TM file.
5. To edit a policy, click the **Edit Policy** button. An *Edit Policy* window will pop-up where you can edit the policy.
6. To delete/remove a policy, click the **Delete Policy** button.

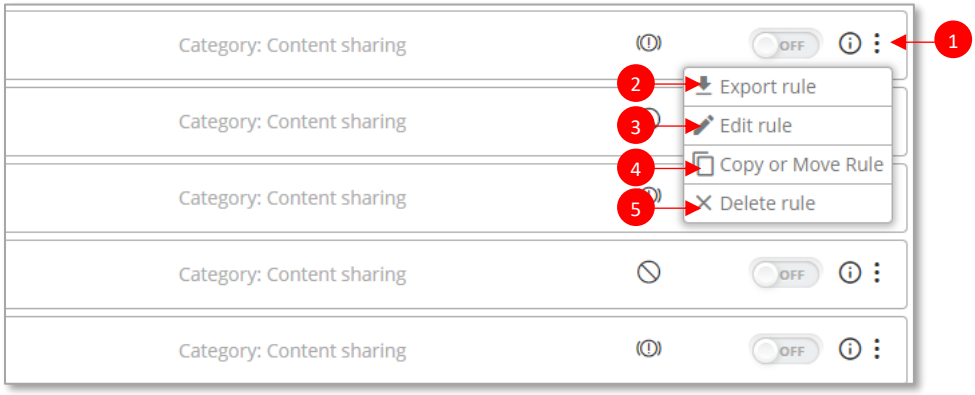
8.6 Creating / Editing Rules



1. Click the **ADD RULE FOR THIS POLICY** button near the bottom of the policy to add a rule to the policy.
2. Click a rule's **name** to edit it.

In both cases, you will be taken to the Rules Editor where you can edit the rule. Check out the [Rules Editor] for more information on how to create or edit rules.

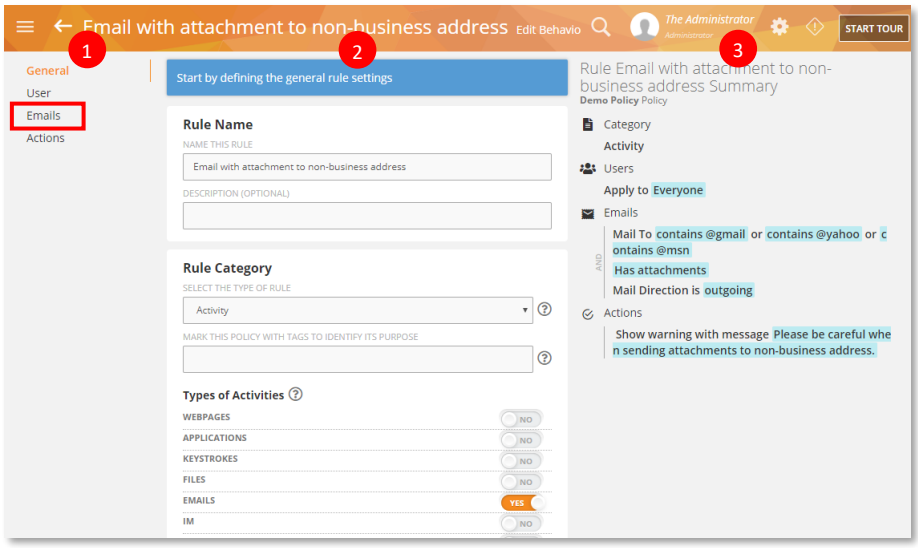
8.7 Moving / Exporting / Editing / Deleting Rules



1. Click the **Dotted menu** at the top-right corner of the rule. A pop-up menu will open.
2. To export a policy, click the **Export rule** button. The rule will be saved as a .TM file.
3. To edit a rule, click the **Edit rule** button. Note that, you can also click the rule's name to edit it. In both cases, you will be taken to the Rules Editor where you can edit the rule. Check out the Rules Editor for more information on how to create or edit rules.
4. To duplicate a rule or to move it to another policy, click the **Copy or Move Rule** button. A pop-up window will open where you can choose to copy or move the rule.
3. To delete/remove a policy, click the **Delete Policy** button.

8.8 Rules Editor

The Rules Editor is an intuitive, visual editor where you can create sophisticated behavioral rules easily without going through multiple screens or coding. Here are the main parts of the editor:



1. The left-most part of the editor is where the main tabs/steps of a rule are displayed. A basic rule has at least three tabs: General, User, *Category* and Action. Note that, the exact name for the

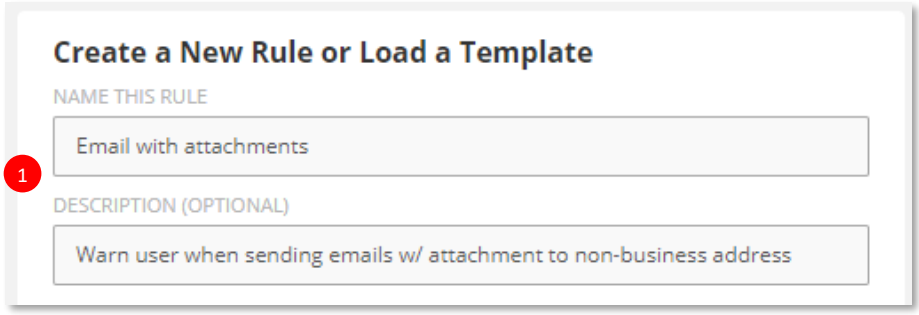
Category will change based on which rule category you select on the General tab. For example, on the screenshot above, the *Category* is 'Emails'.

2. The middle part of the editor is where you specify the actual rule parameters.
3. The right-most part of the editor displays a summary of the rule in easy to follow language.

8.8.1 General Tab – Setting the Rule Basics

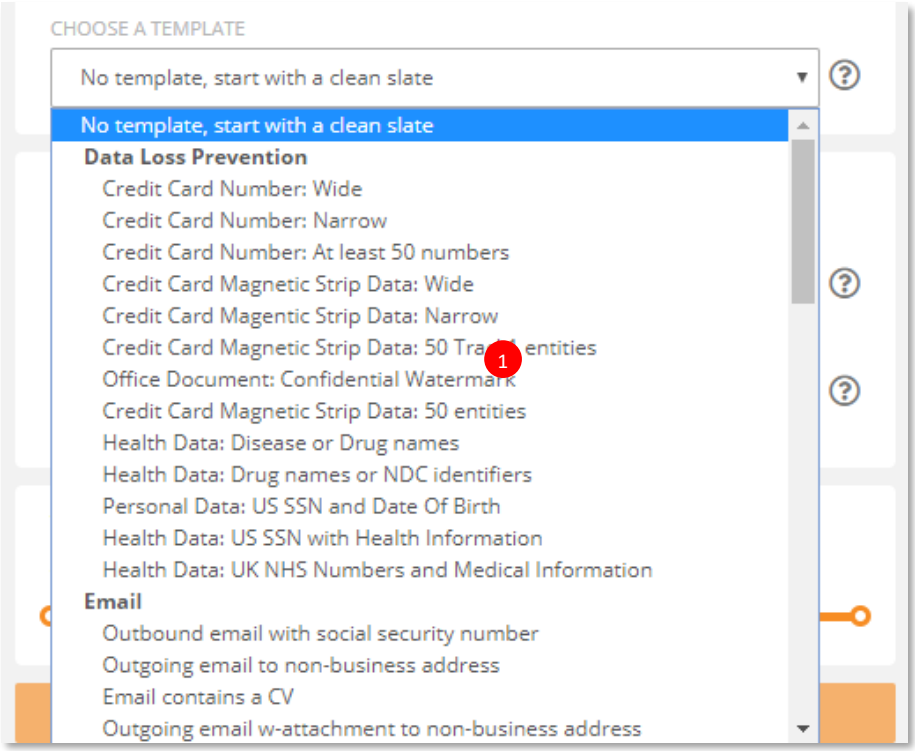
In the first tab, General, you specify the basic settings for the rule. You also select which activity or content the rule will detect.

8.8.1.1 Rule Name and Description



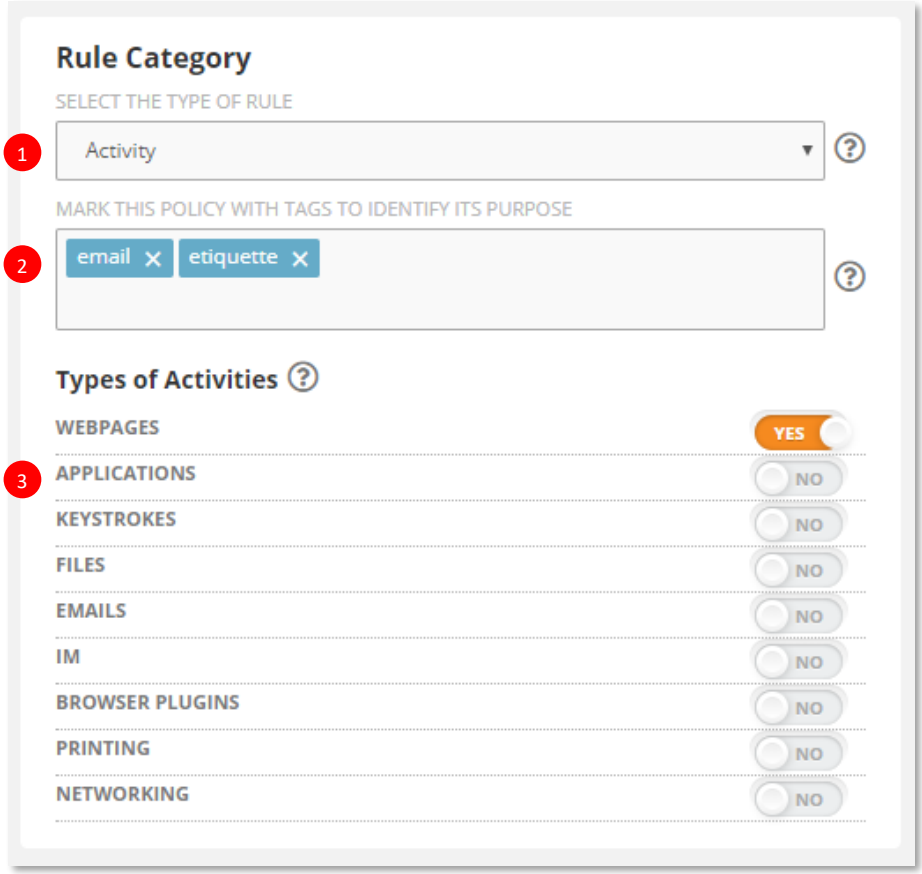
1. On the top fields, you can specify a name and optionally, a description for the rule.

8.8.1.2 Rule Template



1. When creating a new rule, you can choose from a list of pre-built templates. Click the **CHOOSE A TEMPLATE** field to choose a template on the General tab. Teramind has many templates for Data Loss Prevention, Email, Applications, Websites, File Operations etc. Once you select a template, the rest of the rule's tabs will be automatically populated with pre-configured settings and sample data. You can, of course, change the settings.

8.8.1.3 Rule Category and Type



1. There are three categories of rules you can select from the **SELECT THE TYPE OF RULE** drop-down menu on the General tab:
   - **Agent schedule:** This is the most basic rule type. It's based on an agent/user's schedule such as when an employee started work, if they are late at work, if a user is idle etc. The rule takes input from the Schedules you create for employees to determine when a user/agent is supposed to start/finish.
   - **Activity:** Activity-based rules apply to majority of the monitored objects. With this type of rules, you can detect user and application activities. For example, warn a user when they visit a gambling site, Or, stop them from copying a sensitive file to an external drive.
   - **Content sharing:** These rules are used to detect content or text inside an object. The object can be a file, a web page, text in an email or IM chat etc. These powerful rules can be used to prevent data exfiltration attempts such as, block transferring of a file

when it contains credit card numbers; warn a user when they attempt to send emails containing sensitive keywords etc.

> Note that Content sharing rule is available on Teramind DLP only.

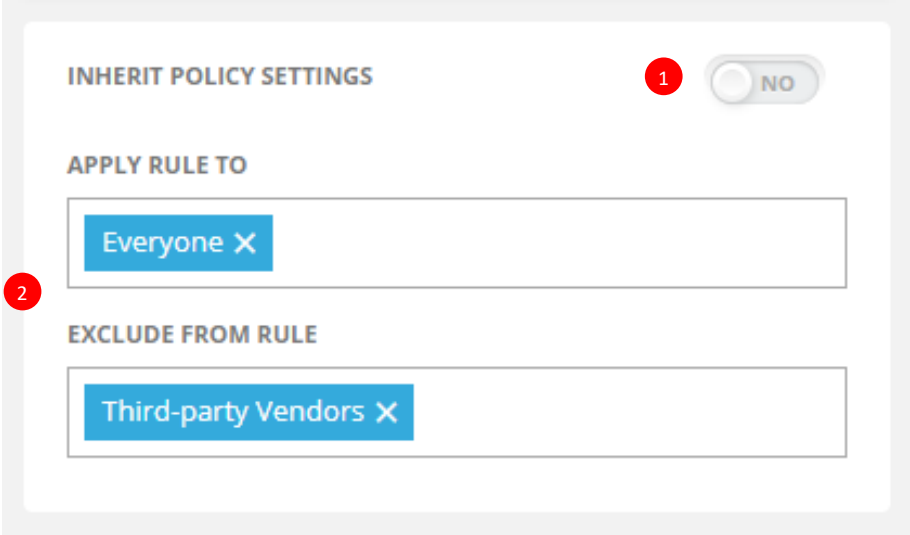
2. Optionally, you can assign tags to a rule to easily identify it or use them as filters (i.e. on the Risk or Alerts report).
3. Once you select a rule type, you can then select the *Types of Activity* (for Activity-based rules) or *Types of Content* (for Content-based rules). You can select multiple activity or contents. If you select multiple activities/contents, the rule will trigger separately for each of the activity/content. Note that, rules based on the *Agent schedules* do not have this section.

8.8.1.4 Rule Schedule

1. By default, the rule stays active for 24 hours. However, you can change the time. For example, you can have the rule active during work hours but disable it during the employee lunch breaks. To change when the rule is active, drag the two **Circles** to adjust the time. You can click the **Plus** + and **Minus** — buttons to add/remove additional time slots.

8.8.2 User Tab – Specifying Users and Groups

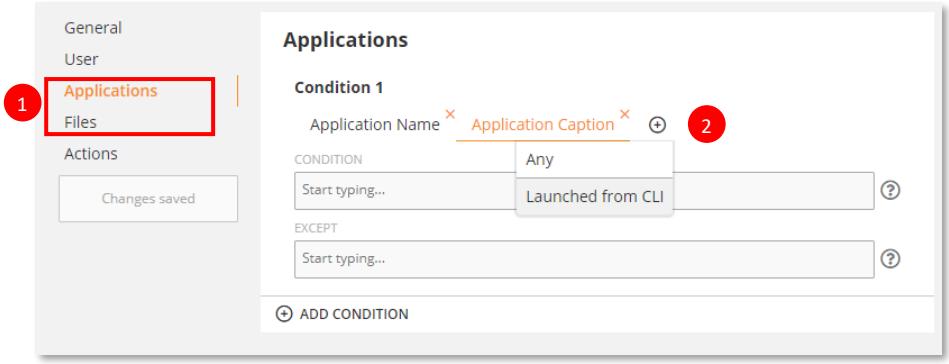
Here you specify which users, groups or departments the rule will apply to.



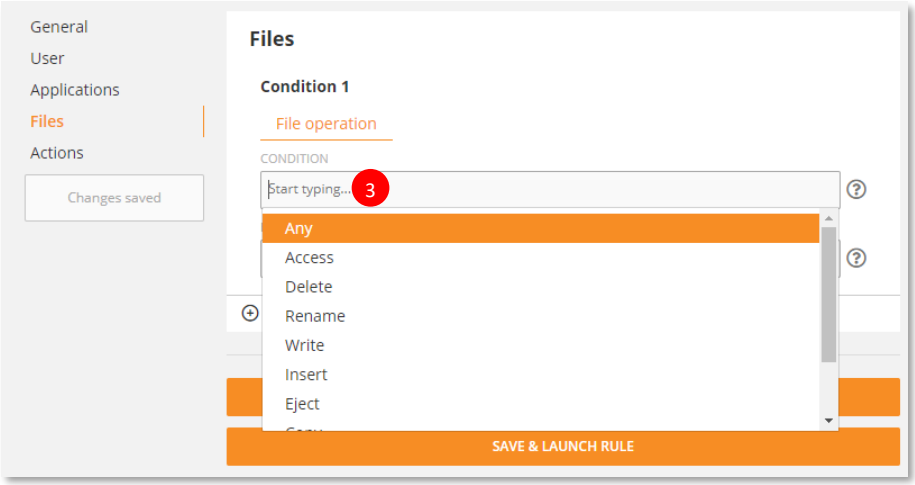
1. By default, the rule will inherit the user settings from the policy. However, you can turn it off to select users manually.
2. You can specify who the rule will apply to and optionally, exclude anyone you don't want to be included using the EXCULUDE FROM RULE field.

8.8.3 Categories Tab – Setting Rules Conditions

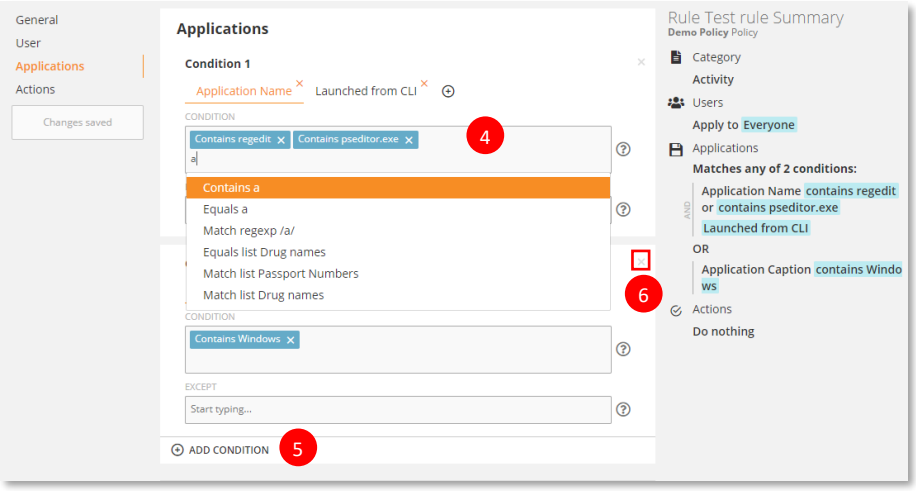
Categories is where you define the conditions for the rules.



1. The Categories tab will change depending on what *Types of activities* / *Types of content* you choose from the General tab. So, for example, if you choose Applications and Files, you will have two tabs named **Applications** and **Files** here.
2. **Condition Parameters – Option 1:** For categories that support it, click the ⊕ button to add parameters to a condition. A small pop-up menu will appear where you can select a parameter. You can select multiple parameters for a condition. In such cases, the conditions will show up as separate tabs. Condition parameters are different for each category. For example, the Application category might have parameter such as 'Application Name', 'Application Caption' etc. while the Emails category might have 'Mail Body', 'Mail Subject' etc.
   You can delete a condition parameter by clicking the small ✕ button next to its name.



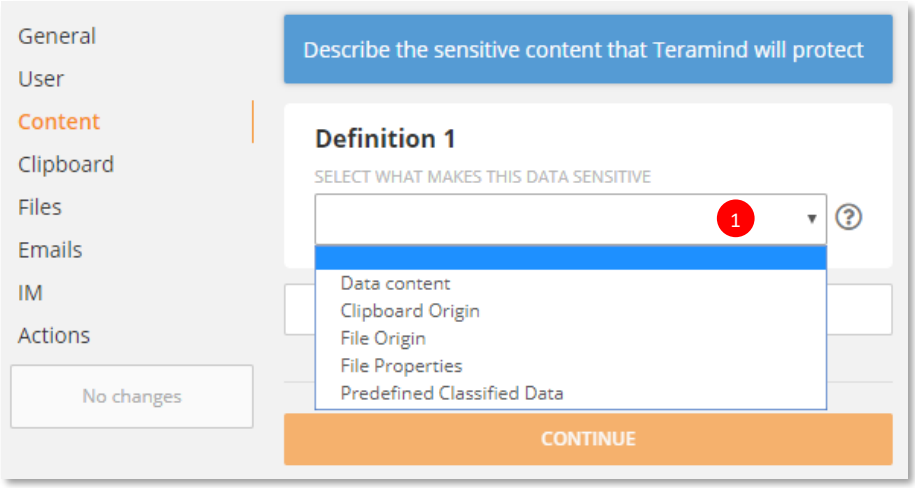
3. **Condition Parameters – Option 2:** For categories (i.e. Files) that do not have a ⊕ button, the **CONDITION** filed is used to set its rule parameters.



4. **Conditions Values:** For categories that support it, you use the **CONDITION** field to specify what values to compare the rule parameters with. Start typing, then select an option from the pop-up to tell Teramind what type of value it is. There are may ways you can use the conditions. For example, to block certain applications from running, you can type them in the **CONDITION** field and choose the *Contains* or *Equals* from the list. Or, you can create a *Shared List* containing all the names (see Shared Lists section for more information on how to create shared lists). For complex matches, such as Credit Card Numbers, Social Security Numbers etc., you can use the *RegEx* option.
   Each value is considered as an 'OR' clause. So, in the above example, the rule will trigger if the 'Application Name' matches with '`regedit`' *or* '`pseditor.exe`'. Each condition parameter is considered as an 'AND' clause. So, in the above example, the rule will trigger if the 'Application Name' *and* the 'Launch from CLI' parameters meets the condition.
5. **Addition Conditional Blocks:** To add additional condition blocks, click the **ADD CONDITION** button. Each new condition is considered as an 'OR' clause. So, if either of the conditions meets the criteria, the rule will be triggered.
6. **Deleting Conditional Blocks:** To remove a condition block, click the small X button at the top-right corner of the condition block.

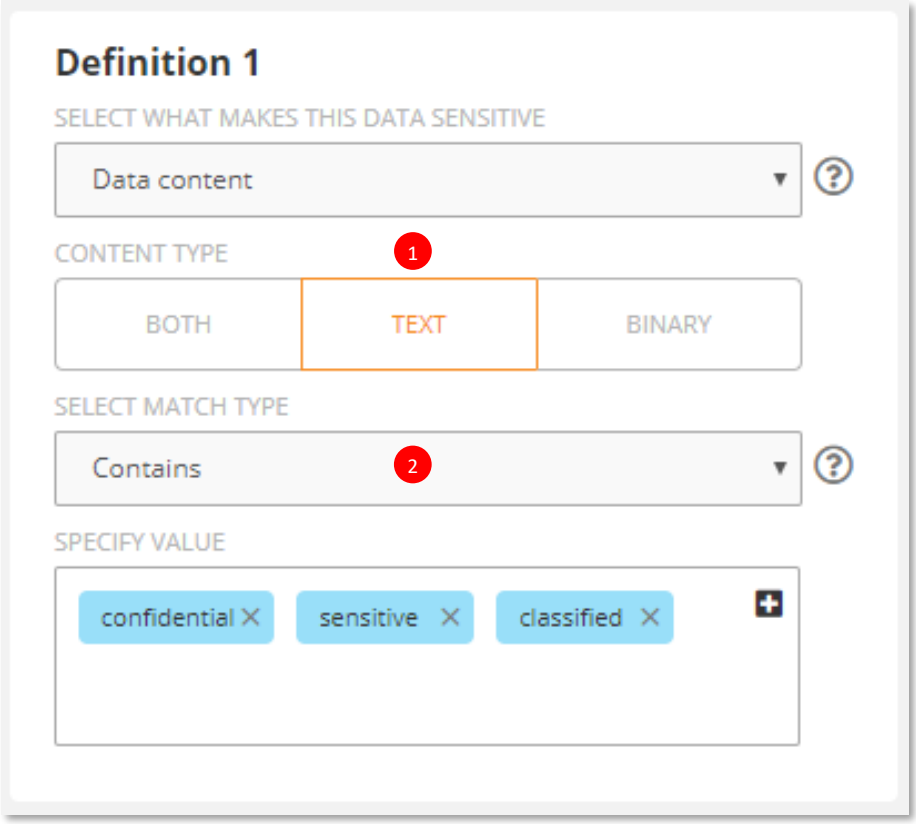
8.8.4 Content Tab – Defining Sensitive Data Types

This tab allows you to define what makes the content sensitive and specify values to look for. Note that, Content tab is available only on Teramind DLP and is shown only when you select the *Content sharing* rule type.



1. You can specify several content types depending on what *Types of activities* / *Types of content* you have selected in the General tab (i.e. Clipboard, Files, Emails, IM).

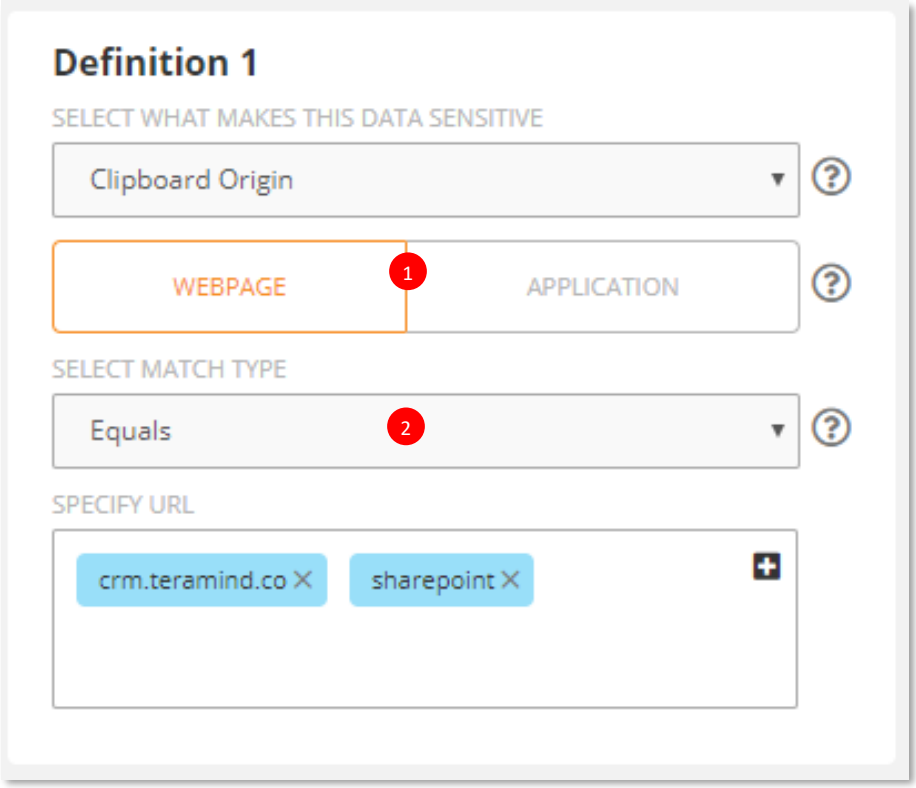
8.8.4.1 Data Content



1. Data content can be used to look for text or binary data for any of the content types. You usually use the Data content rule where you are looking for information in all the supported objects. For example, by using it with the Clipboard, you can detect anything copied on the clipboard.

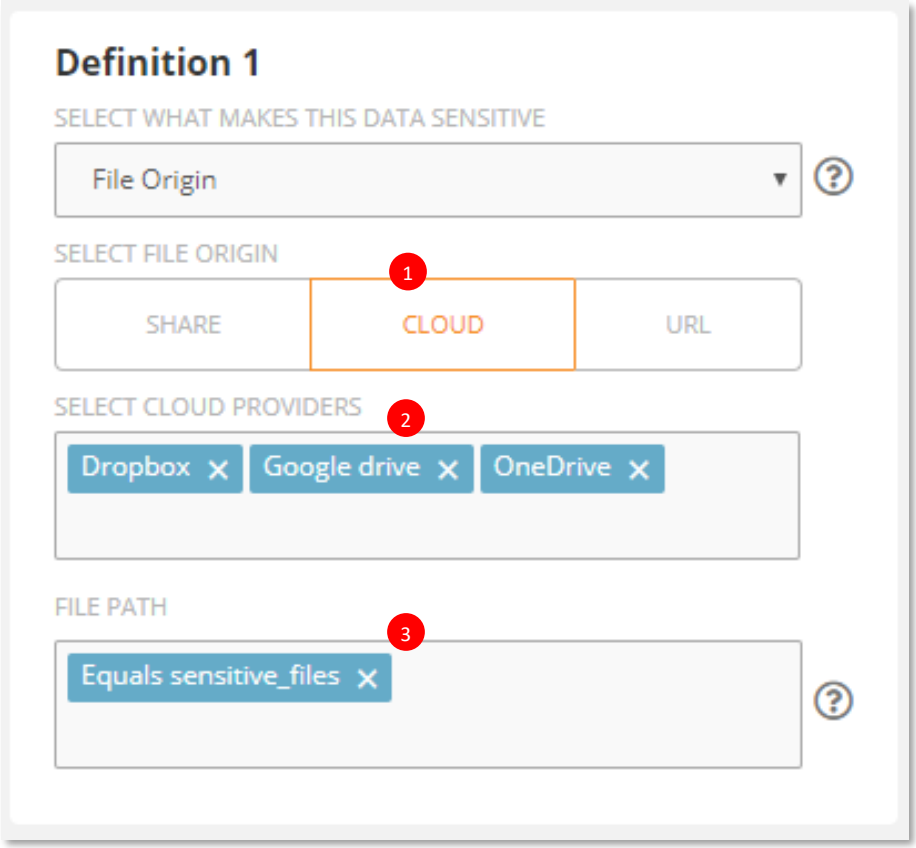
2. You can use Contains, Equals, Regular Expression match, List match etc. from the SELECT MATCH TYPE pull-down menu.

8.8.4.2 Clipboard Origin



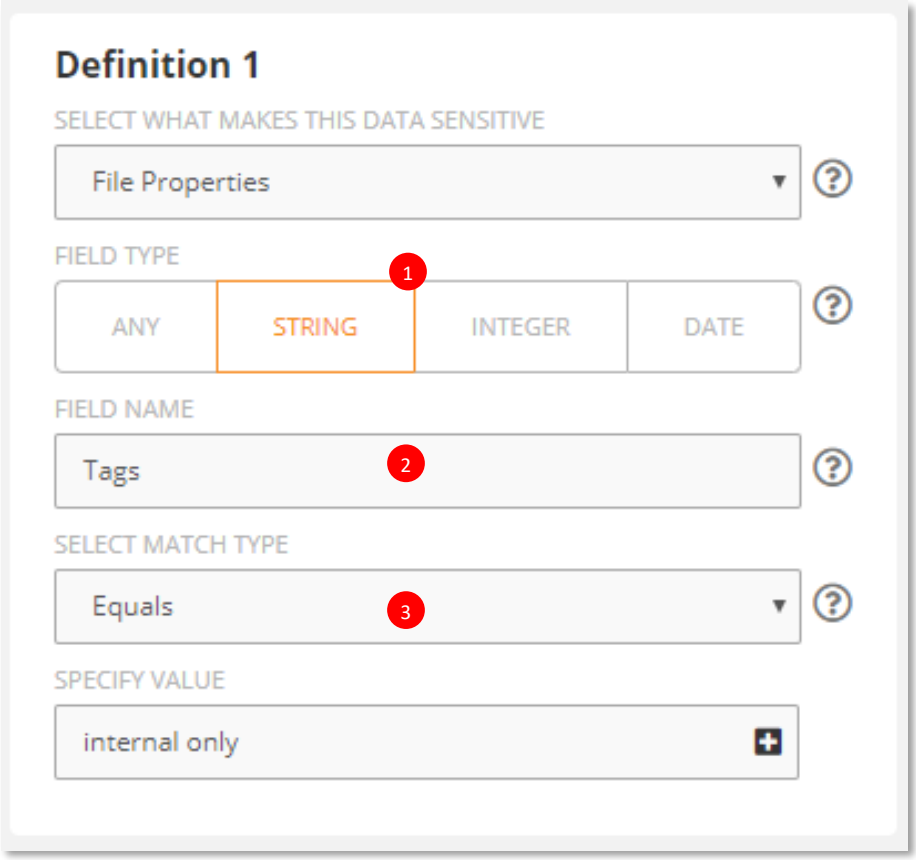
1. Clipboard Origin detects data that's pasted into the clipboard from a specific webpage or application. By using it you can, for example, build a rule that prevents copy pasting customer data from your CRM site.
2. You can use Contains, Equals, Regular Expression match, List match etc. from the SELECT MATCH TYPE pull-down menu.

8.8.4.3 File Origin



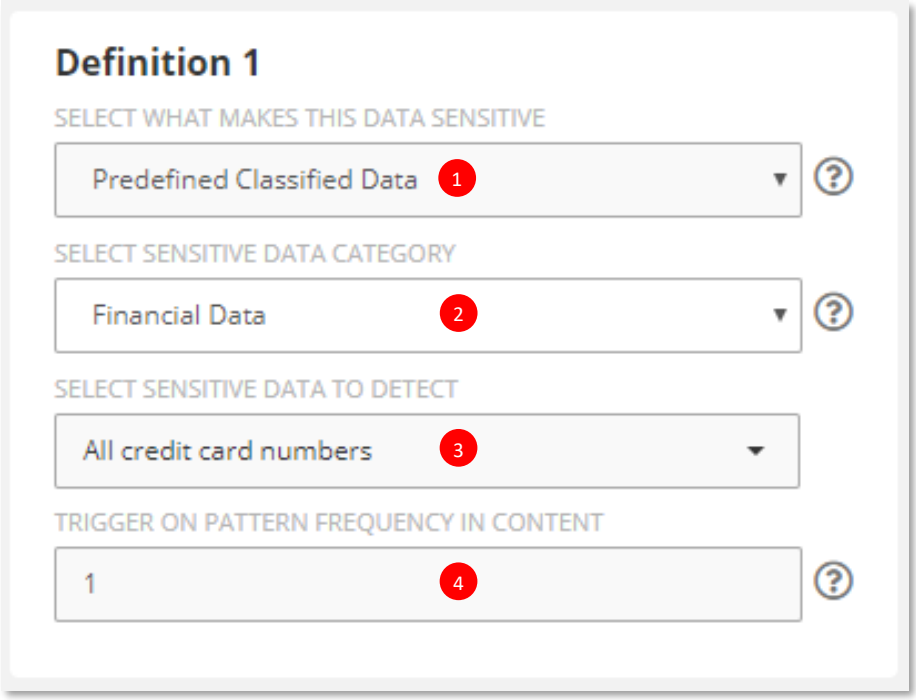
1. File Origin detects file sharing based on their origin or source. It supports local, Cloud and web file sharing. By using it you can, for example, build a rule that prevents sharing of files residing in certain PATH (or folder) to Cloud drives.
2. You can select from a list of Cloud providers if you choose the CLOUD option.
3. You can use Contains, Equals, Regular Expression match, List match etc. for the FILE PATH field.

8.8.4.4 File Properties



1. File Properties detect files based on their meta-tags. By using it you can, for example, build a rule that prevents sharing of any Microsoft Word documents outside your company that has a *Tags* property containing the string value of 'internal only'. You can create such tags/fields/properties from an application (such as Microsoft Word) or from the Windows Explorer.
2. You can use Contains, Equals, Regular Expression match, List match etc. from the SELECT MATCH TYPE pull-down menu.

8.8.4.5 Classified Data



1. Classified Data detects content based on pre-defined data categories, such as, credit cards, Personally Identifiable Information (PII), Protected Health Information (PHI) etc. By using it you can, for example, build a rule that warns a user when they share credit card numbers over the emails or IM chats.
2. There are several types of data categories you can choose from: Financial Data, Health Data, Personally Identifiable Data and Code Snippets.
3. The SENSITIVE DATA TO DETECT will have different menu options depending on what you choose in the SELECT SENSITIVE DATA CATEGORY field. For example, if you choose Financial Data in the previous field, you can choose from 'All credit card numbers', 'Magnetic data', 'SWIFT code' etc. Similarly, if you choose the Health Data, you can choose from 'Common drug names', 'Common disease names', 'DNA profile' etc.
4. Finally, you can specify how often a data pattern can appear in the content before the rule is triggered. As an example, you might not care if a single credit card number is detected in an email, but if more than 5 such numbers are detected then you would like to warn the user.

8.8.5 Actions Tab – Responding to Rule Violation Incidents

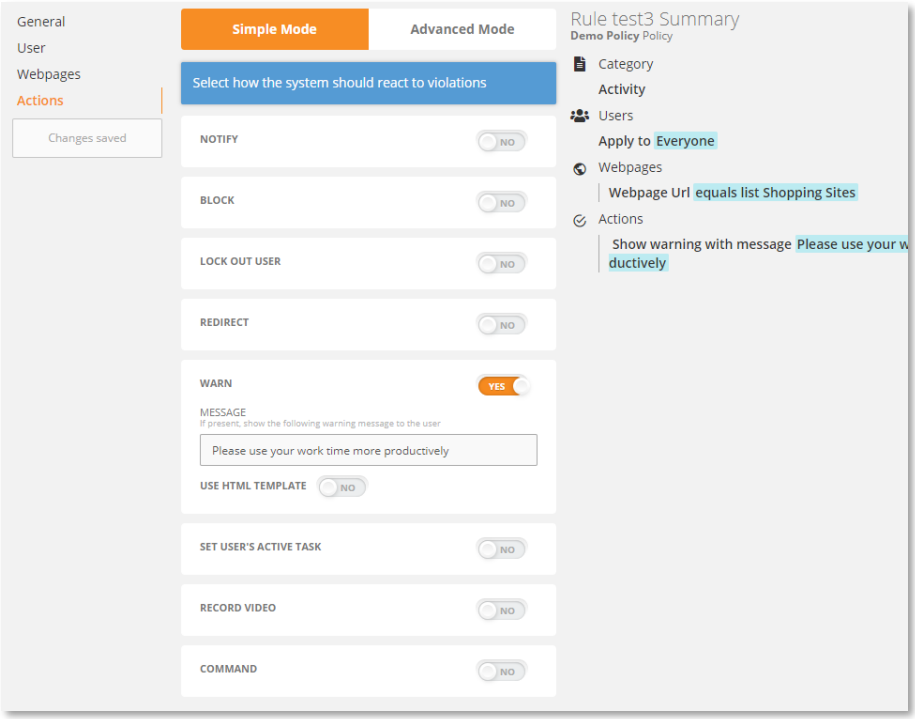
Actions tab is where you specify what the system will do when a rule is violated. You can warn a user or block them, receive notification, record a video of the desktop etc. Note that, not all rule categories support all actions. For example, most of the Agent Schedule-based rules only support the NOTIFY action (except for the *Login* and *Idle* schedules). Same way, different Activity Type or Content Type may also have their own special actions. For example, Webpages have an action called REDIRECT which is not available for other activity types. Also, not all actions are available on all the operation systems. For example, the LOCK OUT USER action does not work on the macOS at the moment.

In some cases, you can use multiple actions as long as they do not conflict with each other. For example, you can use the NOTIFY and BLOCK actions together as they do different things. But you cannot use the BLOCK and LOCK OUT USER actions together because they both prevent the user from doing something. The Rule Editor will automatically grey-out/disable actions that conflict with the currently selected action(s).

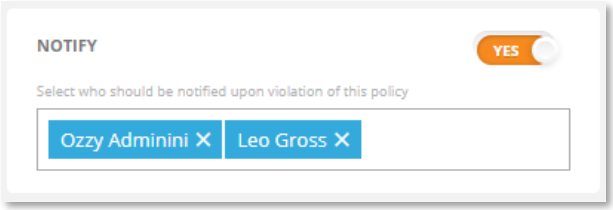
There are two ways you can setup actions: Simple Mode and Advanced Mode.

8.8.5.1 Simple Mode

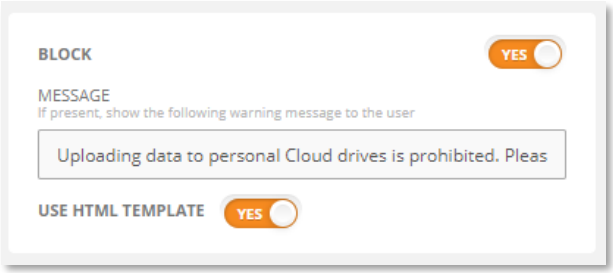
Simple Mode is the easiest way to create rules and is recommended for beginners. In the Simple Mode, you can specify actions, but you cannot set any risk thresholds.



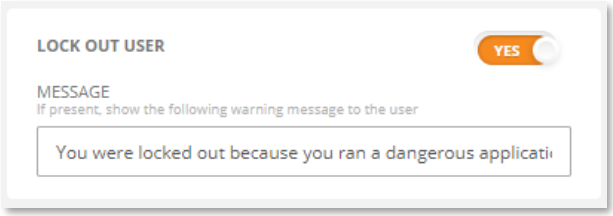
Here are some of the actions you can use:



Notify
Teramind will send an email notification to the specified admins/managers whenever any user violates the rule.

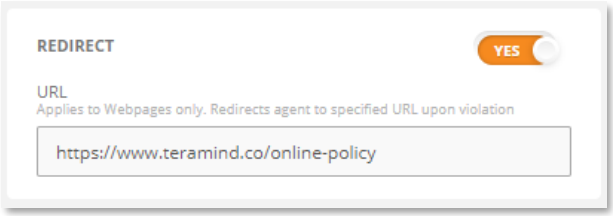


Block
Blocks the user activity and shows a message. You can use a HTML template to display the message (see Alerts section for more information on using an HTML template with your rule messages).



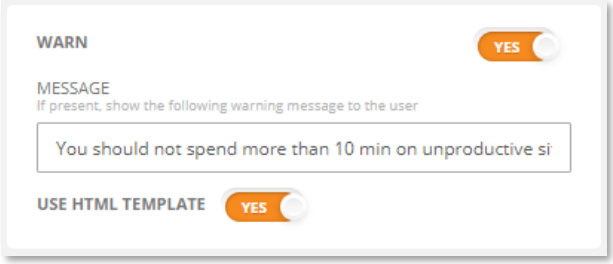
Lock Out User
Shows a warning message to the user and then when they press the OK button, they are locked out of the system. If the user logs back in, they will be logged out automatically. An administrator has to unlock the user for them to be able login again (See the Employee Action Menu section for more information on unlocking a user).

This action works on Windows only.

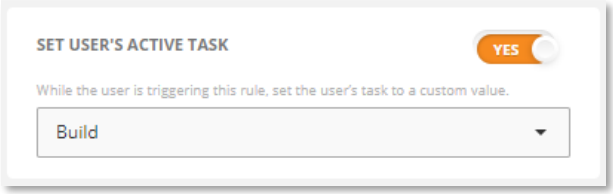


Redirect
Redirects user to a different website when they try to access certain URL(s).

This action applies to Website-based rules only.

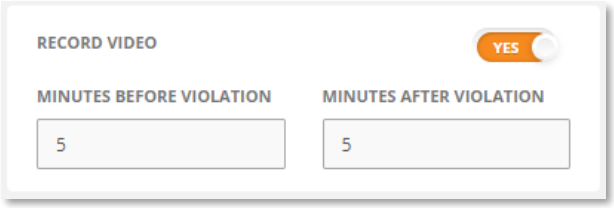


Warn
Warns a user with a message. Similar to the Block rule, but without blocking the action. You can use a HTML template to display the warning message.



Set User's Active Task
You can automatically assign the user a task based on their activities.

Applicable only if the user is using a Stealth Agent.



Record Video
If video recording is disabled in your Screen monitoring settings, you can still record a video of the rule violation incident with this action. The system will automatically record for the specified number of minutes before and after the incident.

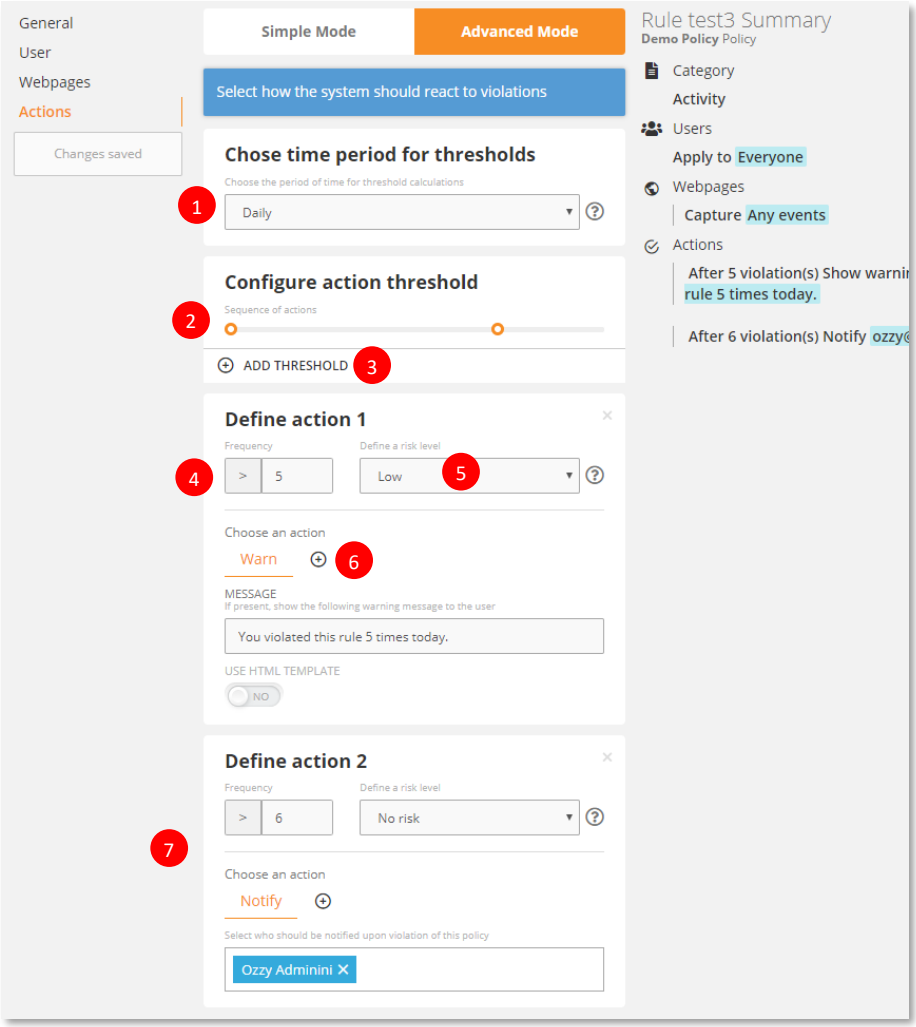
Command
With this action, you can execute a Windows command automatically when a rule is violated.

This action works on Windows only.

8.8.5.2 Advanced Mode

In the Advanced Mode, you can specify risk thresholds for a rule. 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 and a Warn action when a user sends 5 emails in a day. However, if they send more than 10 emails a day, then set a Moderate risk level and trigger a Notification action.

The risk levels that you assign in the Advanced Mode are used by Teramind to calculate risk scores (see the Risks section to learn more about risk analysis) and can also be used to filter other reports (i.e. Alerts).



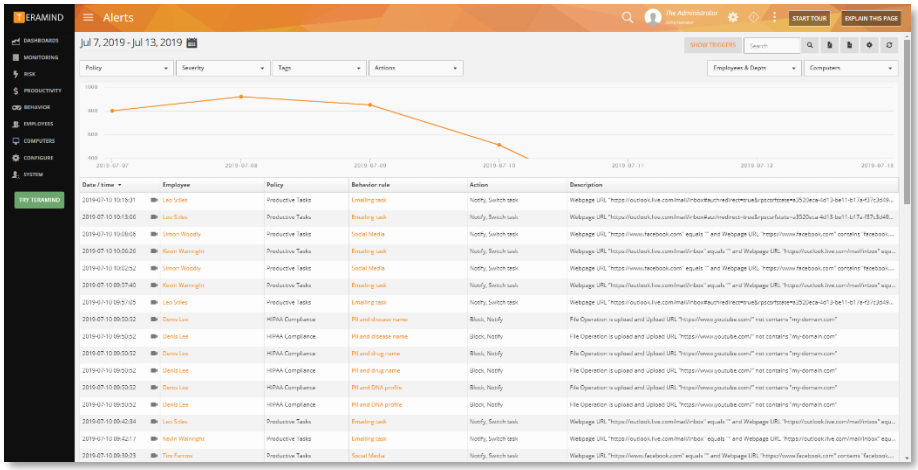
1. You can choose the time period for the thresholds such as Hourly, Daily, Monthly etc.
2. The threshold slider lets you adjust the frequency once you have added one or more thresholds.
3. Click the **ADD THRESHOLD** button to add new threshold (actions). For example, in the picture above, we added two actions (action 1 and action 2).
4. You can use the *Frequency* field to set a frequency.
5. Use the *Define a risk level* field to set a risk level. You can choose from: No Risk, Low, Moderate, High and Critical.
6. Use the small ⊕ button to add an action for the frequency/risk level.
7. You can set additional risk levels and associated action as you need.

8.9 Alerts [deprecated]

DEPRECATED FEATURE

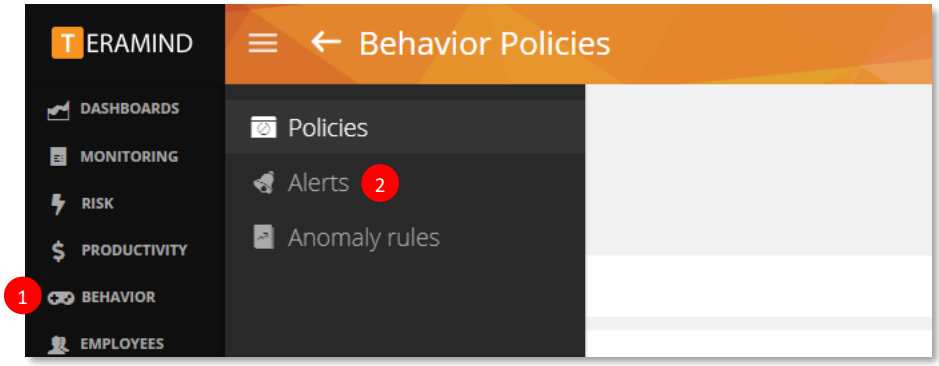
The Alerts report is deprecated. Please use the new BI Reports > Behavior Alerts report which offers more information, drill-down capabilities, enhanced export, and faster load time. Please contact Teramind support if you have any questions.

The Alerts report shows all the rule violation incidents (triggered by the regular Rules) and any anomalies (triggered by the Anomaly Rules). The report shows the date/time the incident happened, which user was involved, what policy and rule were violated, what action was taken by the system and a description of the incident (i.e. what applications the employee was using and what triggered the alert).



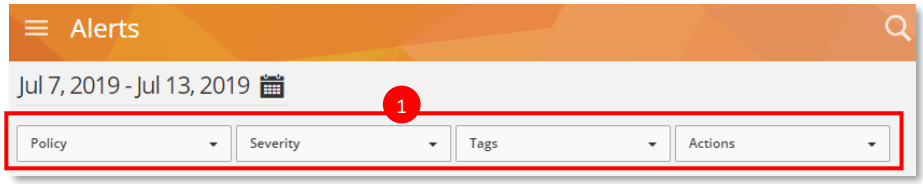
The report also shows a trend graph for the number of alerts triggered over the period. Like all other reports, you can view a session recording of an alert incident by clicking the **movie camera icon** on the *Employee* column. Same way, you can also export an alert report or schedule it for auto delivery to selected email addresses. Check out the Introduction to Monitoring Reports section to learn how to perform these common report actions.

8.9.1 Accessing the Alerts Menu



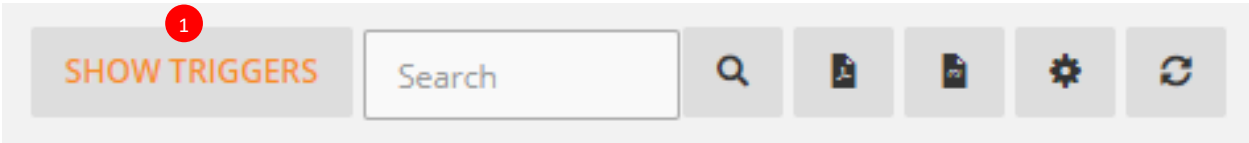
1. Hover your mouse over the **BEHAVIOR** menu, then
2. Select **Alerts** from the sub-menu.

8.9.2 Applying Alert Filters



1. There are multiple ways to filter the Alerts report. You can do so by using the drop-down menus located at the top-left corner of the report. You can filter by Policy, Severity, Tags or Actions. This is helpful if you have many alerts and wanted to narrow down the list.

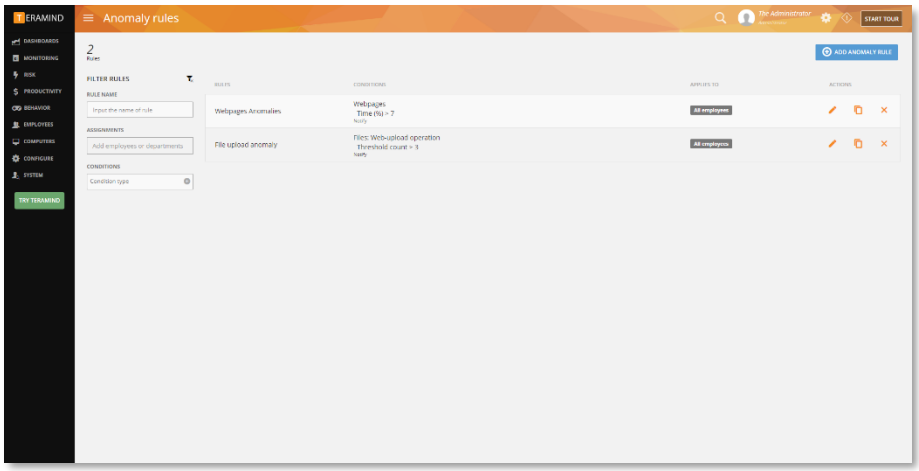
8.9.3 Showing / Hiding Rule Triggers



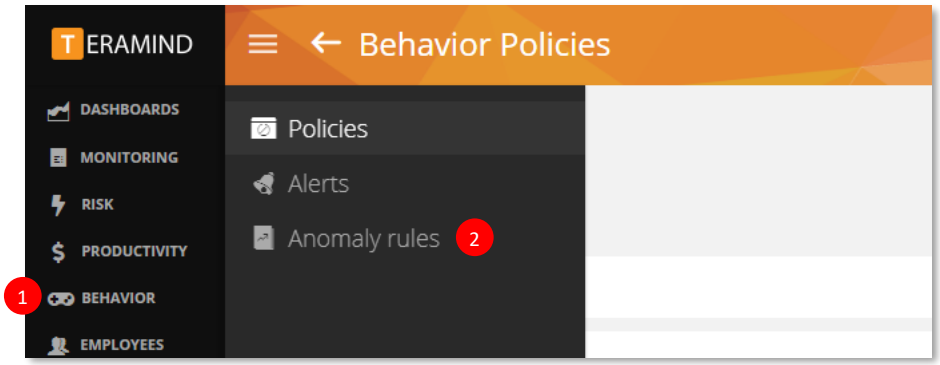
1. You can use the SHOW TRIGGERS button to toggle the display of additional information about a rule violation incident. When triggers are turned on, the *Display* column will show additional information such as what part of the rule condition was trigger and for which activity or content.

8.10 Anomaly Rules

Anomaly rules are special types of rules that allow you to identify anomalies in a user's behavior by utilizing behavioral baselines. It also allows you to assign risk levels to any anomalous behavior and a notification action to inform admins or managers about the anomaly.

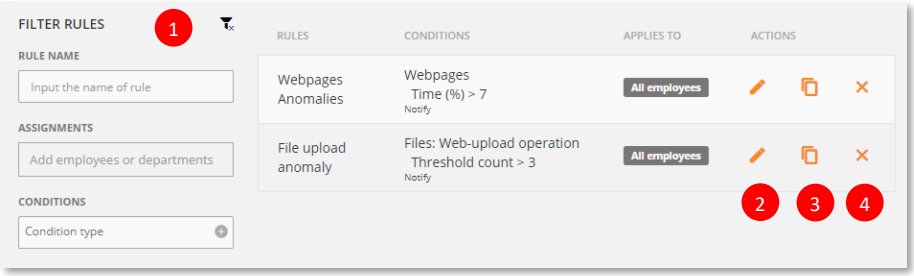


8.10.1 Accessing the Anomaly Rules Menu



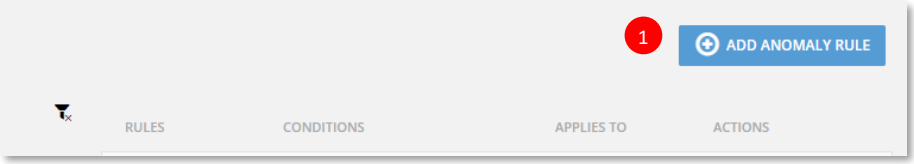
3. Hover your mouse over the **BEHAVIOR** menu, then
4. Select **Anomaly rules** from the sub-menu.

8.10.2 Filtering / Editing / Deleting / Copying Anomaly Rules

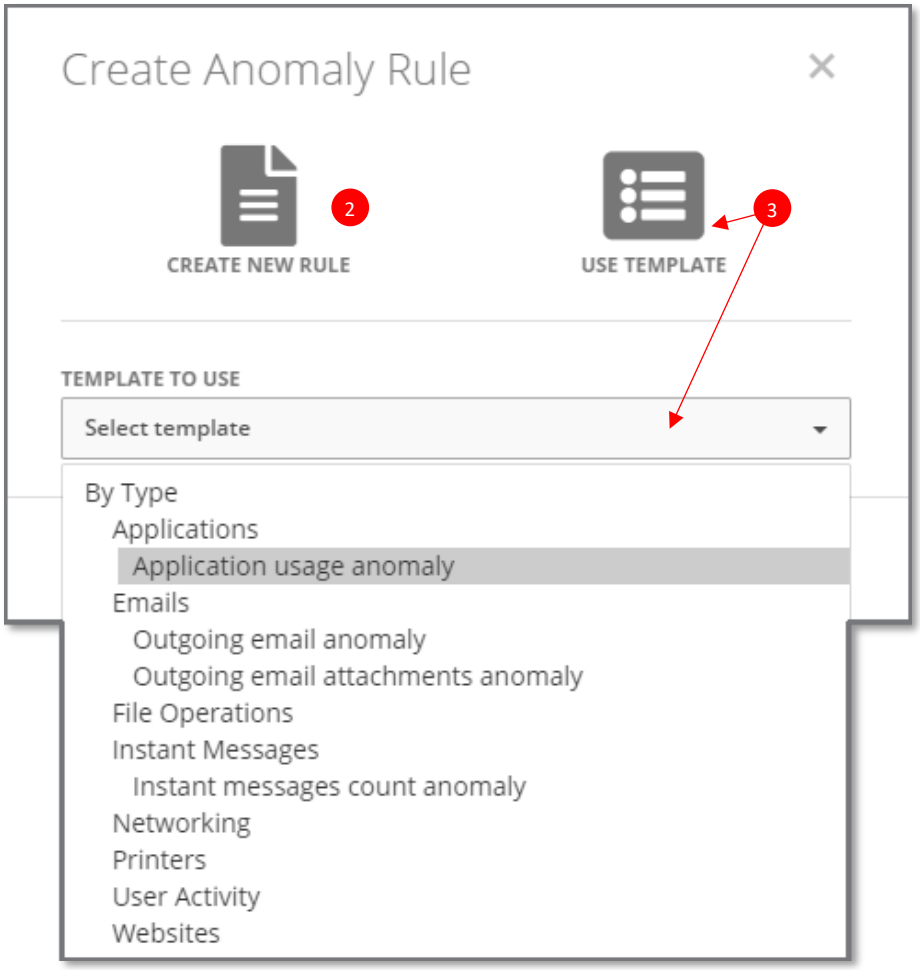


1. If you have many anomaly rules, you can decide what's displayed by using the filters on the left side of the Anomaly Rules screen. You can clear the filters by clicking the small **Funnel** icon.
2. To edit an anomaly rule, click the **Pencil** icon. You will be taken to a rule editor. Follow the Anomaly Rule Editor section to learn how to edit an anomaly rule.
3. Click the **Copy** icon to duplicate a rule.
4. Click the ✕ icon to delete a rule.

8.10.3 Creating Anomaly Rules



1. Click the **ADD ANOMALY RULE** button at the top-right corner of the screen. A pop-up window will open.



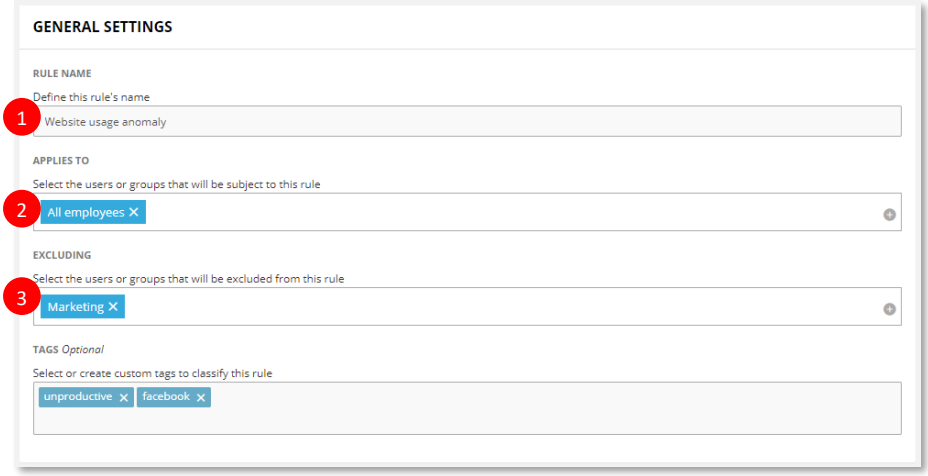
2. Click the **CREATE NEW RULE** button if you want to create a rule from the scratch. You will be taken to the Anomaly Rules Editor. Follow the Anomaly Rules Editor section to learn how to edit an anomaly rule.
3. Click the **USE TEMPLATE** button to create a rule based on a template. Teramind comes with many anomaly rules templates. You can choose from a list of types such as: Applications, Emails, File Operations etc. Click on a type to expand it. Pick a rule template and click the **LOAD TEMPLATE TO USE** button. You will be taken to the rule editor. Follow the Anomaly Rules Editor section to learn how to edit an anomaly rule.

8.10.4 Anomaly Rules Editor

The Anomaly Rules Editor is an intuitive, visual editor. The single-page interface of the editor makes it easier to view and edit the rules.

8.10.4.1 General Settings

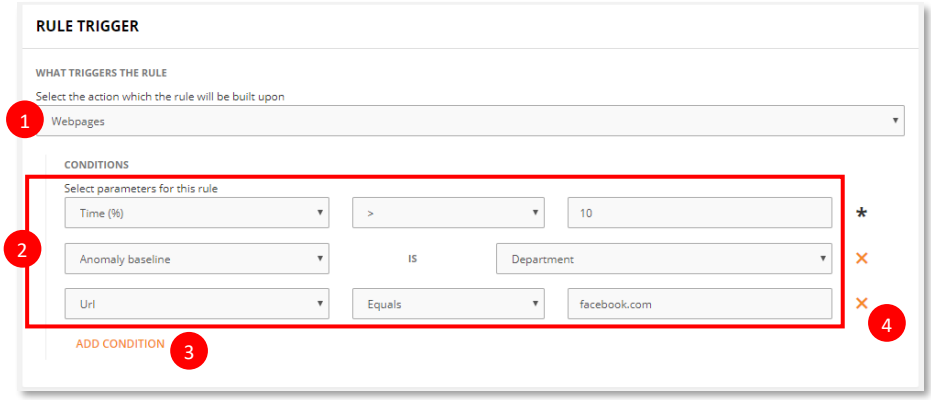
You can specify basic rule settings on the General Settings section of the Anomaly Rules Editor.



1. Give the rule a name on the **RULE NAME** field.
2. Select the users the rule will apply to on the **APPLIES TO** field.
3. Select any users that should be excluded on the **EXCLUDING** field.
4. Optionally, you can assign tags to a rule on the **TAGS** field to easily identify it.

8.10.4.2 Rule Trigger

The Rule Trigger section lets you specify which activity the rule engine will monitor and what conditions it will evaluate.



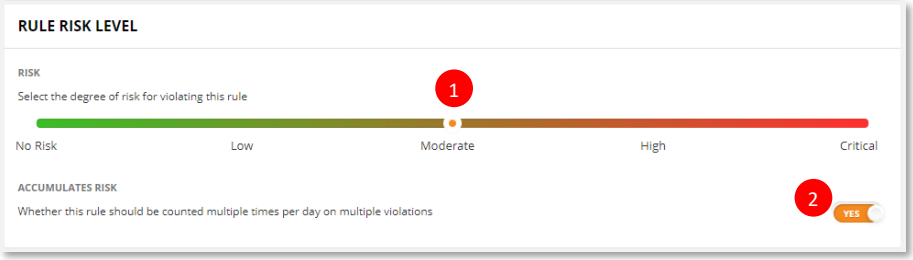
1. Select a trigger from the list. You can choose from many pre-built options such as Webpages, Applications, Emails, Productivity, Network etc.
2. Under CONDITIONS, you can choose different types of conditions such as:

- **Time (%):** with this you can create a rule for time spent on certain task. For example, you can create a rule that gets triggered if a user spends more than 10% time on a certain website.
- **Anomaly baseline:** uses algorithm to determine if certain user behavior is outside their normal behavior. This can be the user's current behavior compared to their past behavior; an employee's behavior compared to their departmental baseline; or an employee's behavior compared to baseline of the entire organization. Using a baseline lets you, for example, set an anomaly rule to notify you when a user sends an unusual number of emails than they normally do in a day-to-day basis.
- **Other Conditions:** depending on what trigger you selected, you may see additional conditions. For example, if you choose the *Webpages* trigger, you will see the *Url* condition listed as an option on the menu.

3. Click the **ADD CONDITION** button to add a new condition row.
4. Click the ✕ button next to a condition to delete it.

8.10.4.3 Rule Risk Level

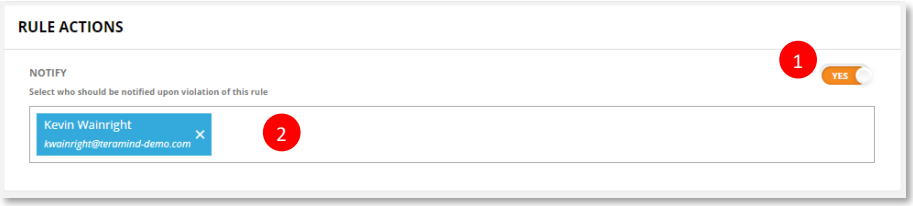
Rule Risk Level section lets you assign a risk level to the rule. The risk level is used by Teramind to calculate risk scores (see Risks section to learn more about risks) and can also be used to filter reports (i.e. Alerts).



1. Click and drag the **Circle** to adjust the risk level.
2. You can turn risk accumulation on/off. If turned on, the risk associated with this rule will be counted multiple times for multiple violations. Otherwise it will be counted once for all violations.

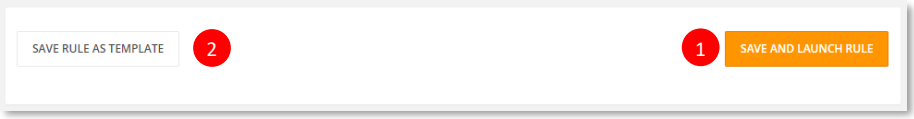
8.10.4.4 Rule Actions

Anomaly rules only support the NOTIFY action.



1. Turn the notification on/off by using the **NOTIFY** button.
2. Select the users who will get notified when the rule is violated.

8.10.4.5 Saving the Rule / Creating a Rule Template

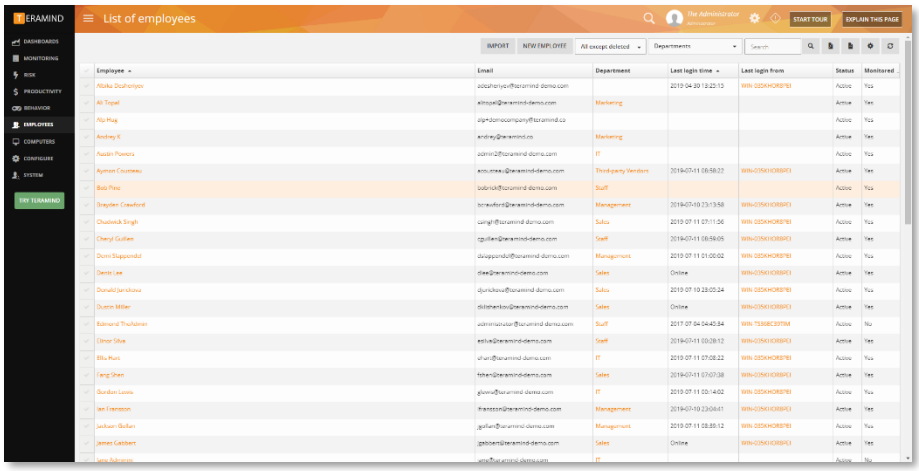


1. Click the **SAVE AND LAUNCH RULE** to save and activate it.
2. Click the **SAVE RULE AS TEMPLATE** button to save it as a template. This way, the template will be available when you are creating a new anomaly rule (see the Creating Anomaly Rules section to learn how to use an anomaly rule template).

9 Employees

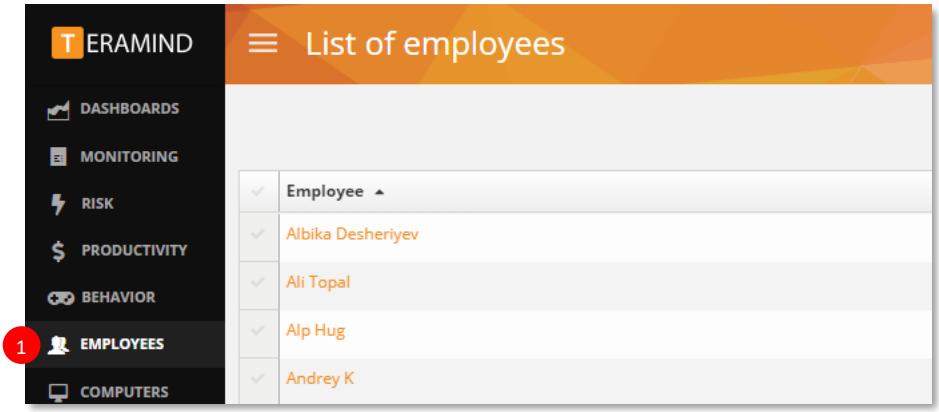
9.1 Introduction to the Employees

The Employees screen is where all your employees and other users are listed. You can see when a user logged in, which computer they logged in from, their status (i.e. active, idle, locked etc.) and if they are currently being monitored.



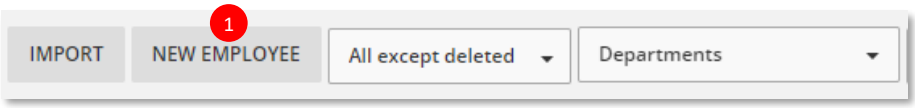
From the Employees screen, you can also perform actions such as add/import/delete/restore employees, lock/unlock their computers etc.

9.2 Accessing the Employees Menu



1. Click the **EMPLOYEES** menu to access its screen.

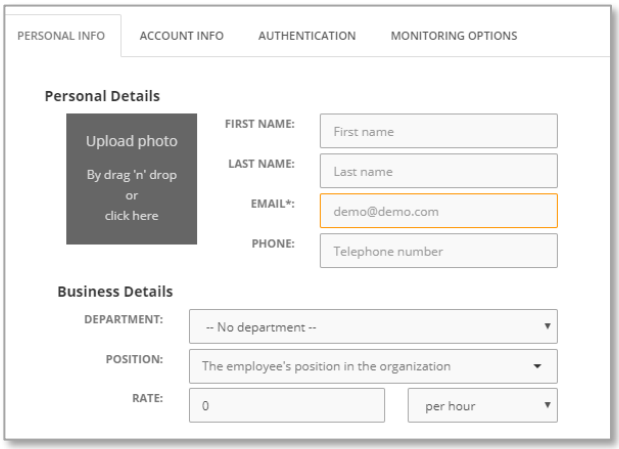
9.3 Adding a New Employee



1. Click the **NEW EMPLOYEE** button near the top of the screen. A pop-up window will open where you can edit the employee's profile details such as their personal information, account security, monitoring options etc. See the following section to learn how to enter these details for a new employee.

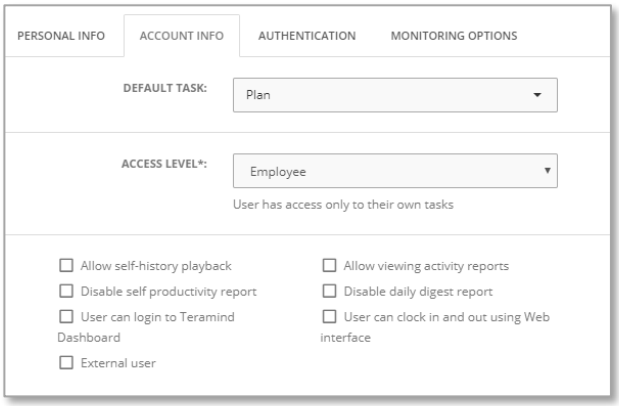
9.3.1 Entering / Editing Employee Profiles

When either creating a new employee or editing an existing employee, a pop-up window will open where you can enter/edit the employee details such as their personal information, account information, authentication and monitoring options:



Personal Info
On the first tab of the employee details window, you can enter the user's personal details such as names, contact info, department, position etc. You can also upload a photo for the employee.

If you enter any wage/salary information, you will be able to see the user's contribution on the Productivity widgets and the Productivity report.



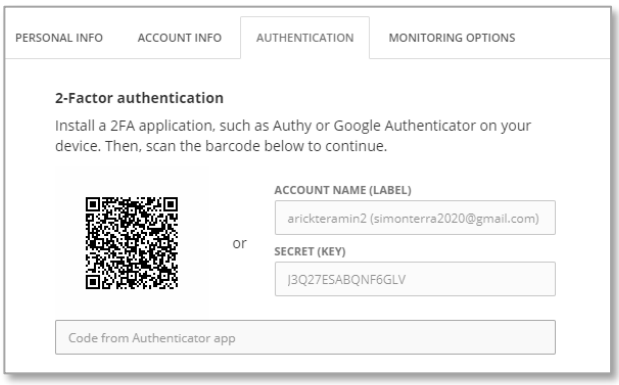
Account Information
On this tab, you can specify the user's default task (if the employee is using a Hidden Agent). You can also set their access level. There are four types of access levels you can choose from:

- *Employee* – cannot change any settings.
- *Infrastructure Admin* - has access to the system settings but cannot browse any recordings.
- *Operational Admin* - has access to the system settings, rules, computers,

other users and access control settings of other users.

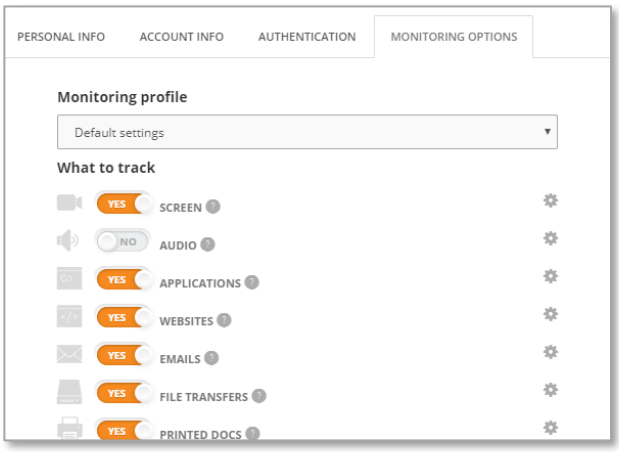
- *Administrator* – is the most powerful access level. They can monitor all employees, other admins and change any settings with no restrictions.

On this tab, you can also specify other account security settings, such as: if the employee can view their own dashboard, what reports they can access, if they are an external user etc.



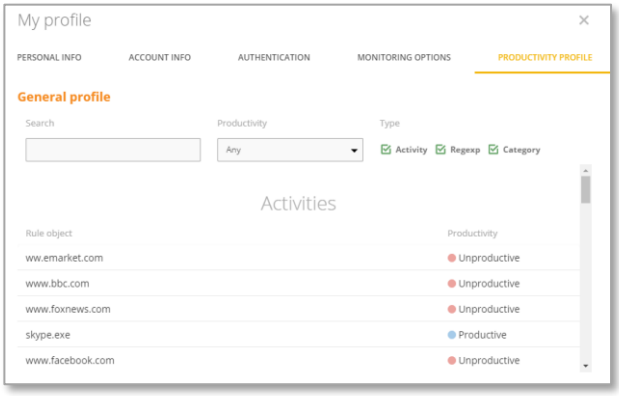
Authentication

Here you can enable/disable 2-Factor Authentication for the user. Scan the barcode in your 2FA application (such as Authy or Google Authenticator) then apply the code from the application in the *Code from Authenticator app* field.



Monitoring Option

On this tab, you can specify which monitoring profile to use for this employee and also manually control what they will be tracked for.



Productivity Profile
On this last tab, you can see which productivity profile is used for this employee. However, you cannot edit it from here. To learn how to edit a productivity profile, check out the Productivity Profiles section of the User Guide.

9.3.2 Adding Employee and Sending Invitation

After entering/editing the user details, do the following:

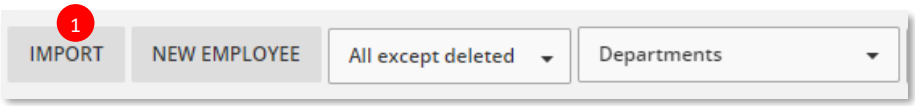
If you are adding a new employee:

1. Click the **ADD USER & SEND INVITATION** button to add the new employee and send them an invitation to install the Teramind Agent.
2. Click the **ADD USER** button to just add the user without sending an invitation.

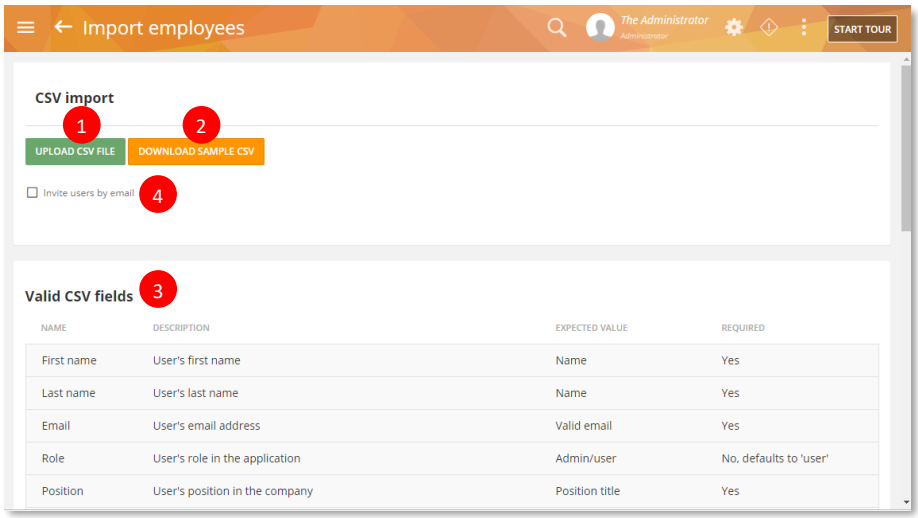
If you are editing an existing employee:

1. Click the **RESEND INVITATION** button to send the employee an invitation to install the Teramind Agent.
2. Click the **APPLY CHANGES** button to save any changes you have made to the profile.

9.4 Importing Employees



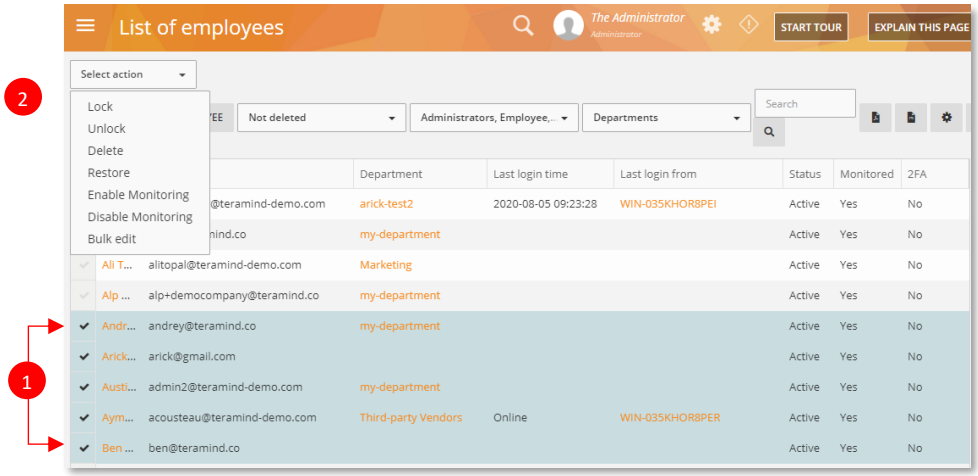
1. Click the **IMPORT** button near the top of the Employees screen. You will be taken to the *Import employee* screen.



2. Click the **UPLOAD CSV FILE** button to upload a CSV file containing employee information.
3. If you want, you can click the **DOWLOAD SAMPLE CSV** button to download a sample CSV file that shows you how the CSV file containing a list of employees should be formatted for importing into Teramind.
4. Additionally, there is a table at the lower part of the screen that shows what CSV fields Teramind can import, their expected values and which fields are mandatory.
5. Turn on the *Invite users by email* to send out invitations to install the Teramind Agent to the newly added employees.

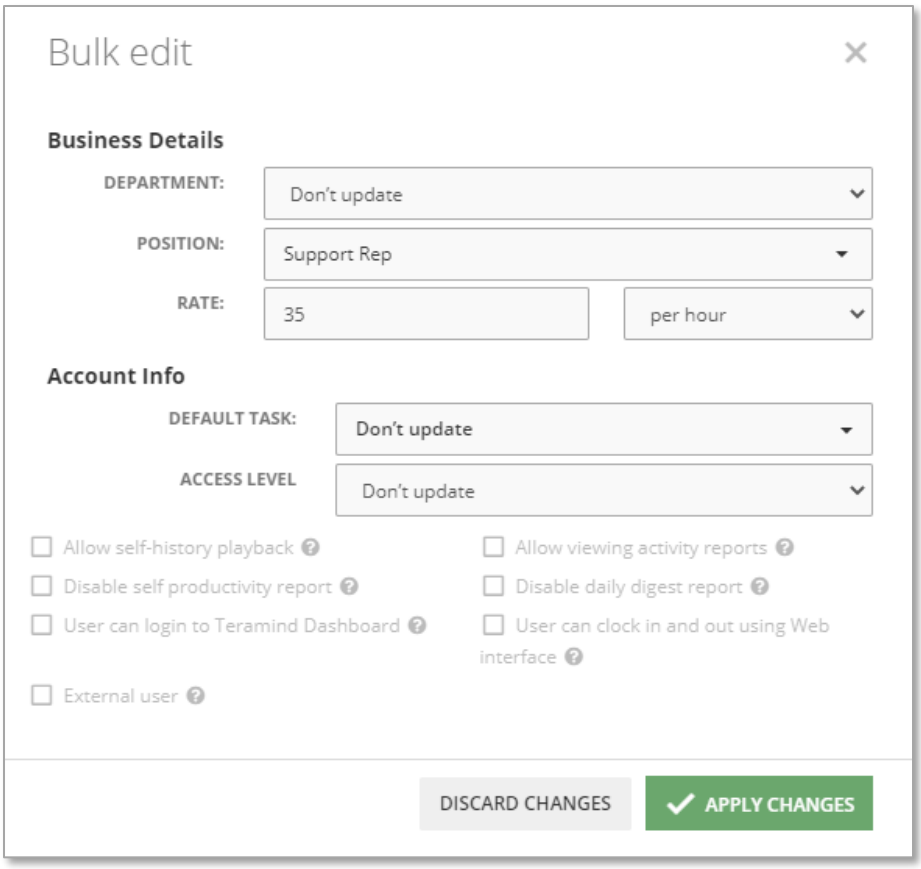
9.5 Employee Action Menu

You can perform various actions such as lock/unlock a user, delete/restore their profile or enable/disable monitoring for them.



1. Click the **check mark** in front of the employee names to select employees.
2. From the top-left corner of the screen, select the action you want to perform. Here are the actions you can perform:

- **Lock:** locks a user's computer. The *Status* column on the employees list will change to show it as locked. When a computer is locked, the user will not be able to use it.
- **Unlock:** unlocks a user's computer previously locked by the Lock menu option or by a rule's 'Lock Out User' action.
- **Delete:** deletes the selected user. Note that, when you delete a user, they are not permanently deleted, just hidden from the employee list and all monitoring reports. If you are on a Cloud deployment, deleting a user will also free up a license.
- **Restore:** restores previously deleted employee(s).
- **Enable Monitoring:** enables monitoring for a user.
- **Disable Monitoring:** disables monitoring for a user. The Monitored column will change to show the user is no longer being monitored.
- **Bulk Edit:** allows you to edit the profile information of the selected employees in bulk. Clicking the button will open the *Bulk edit* window where you can make the changes that will apply to the selected employees:

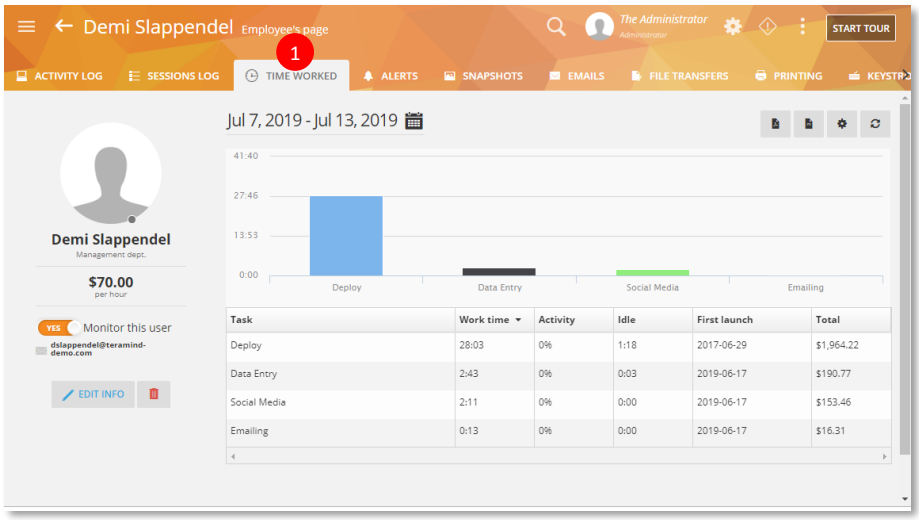


9.6 Viewing an Employee's Monitoring Reports

If you click an employee name from the list of employees, you will be taken to the *Employee's page* where you can see their detailed reports such as, Activity Log (similar to the Web Pages & Applications Report), Session Log, Time Worked, Alert Log etc.

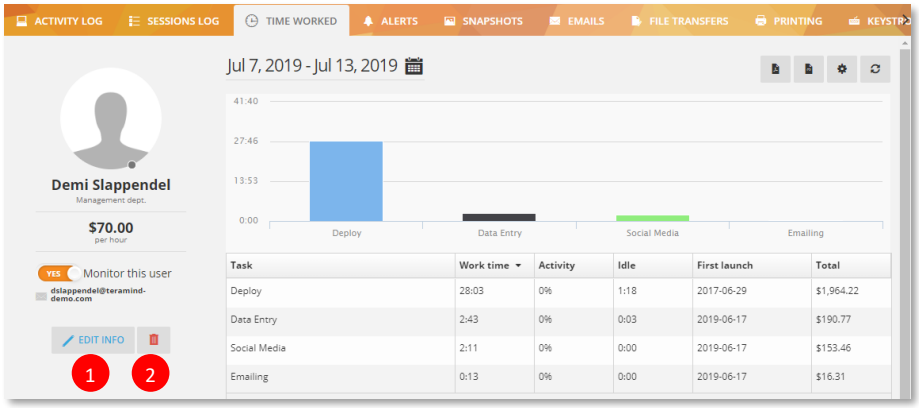
These reports are similar to the other monitoring reports except for the Time Worked screen:

> Check out the Monitoring Reports section and the individual monitoring reports for an explanation of the information they provide.



1. The Time Worked screen shows slightly different information compared to the PRODUCTIVITY report. It shows Task, Work Time, Activity, Idle, First Launch and Total salary/wage.
2. You can also edit the employee's profile or turn off their monitoring settings from this screen.

9.7 Editing / Deleting an Employee



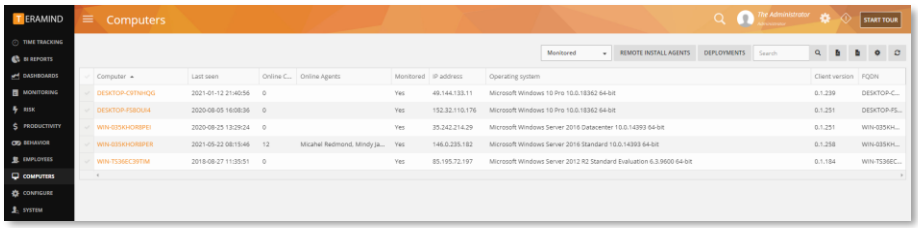
1. Click the **EDIT INFO** button from the *Employee's page*. A pop-up window will open where you can edit their profile information. Check out the Entering / Editing Employee Profiles section to learn how to edit the profile.
2. Click the small **Trash Can** icon to delete the employee. You can also delete/restore an employee from the Employee Action Menu. Note that, when you delete a user, they are not

permanently deleted, just hidden from the employee list and all monitoring reports. If you are on a Cloud deployment, deleting a user will also free up a license.

10 Computers

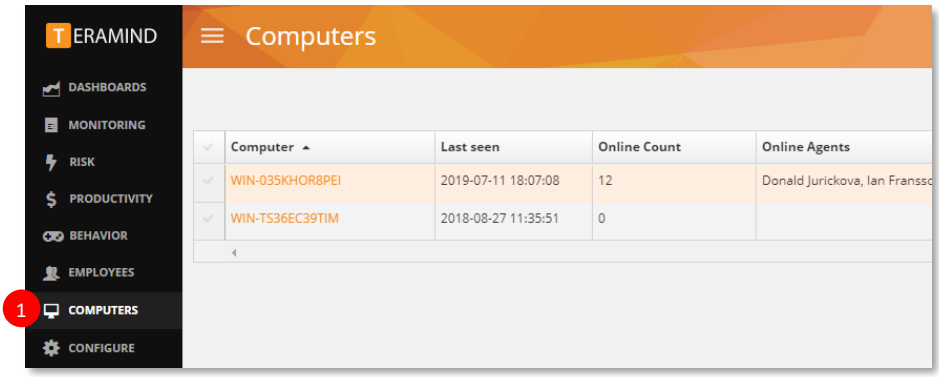
10.1 Introduction to the Computers

The Computers screen shows all the computers you have added to Teramind, when they were last seen, online counts, currently online users/agents, IP addresses, operation systems, client (Teramind Agent) versions and FQDNs (Fully Qualified Domain Names).



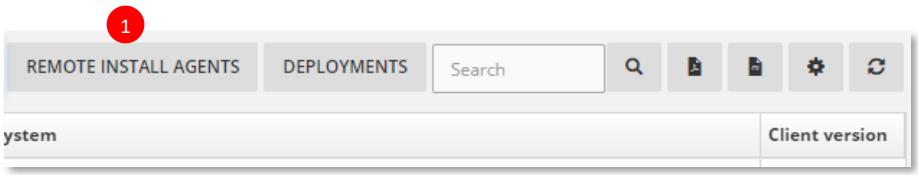
Note: if you do not see a column, click the **Settings** button near the top-right corner of the report to enable it.

10.2 Accessing the Computers Menu

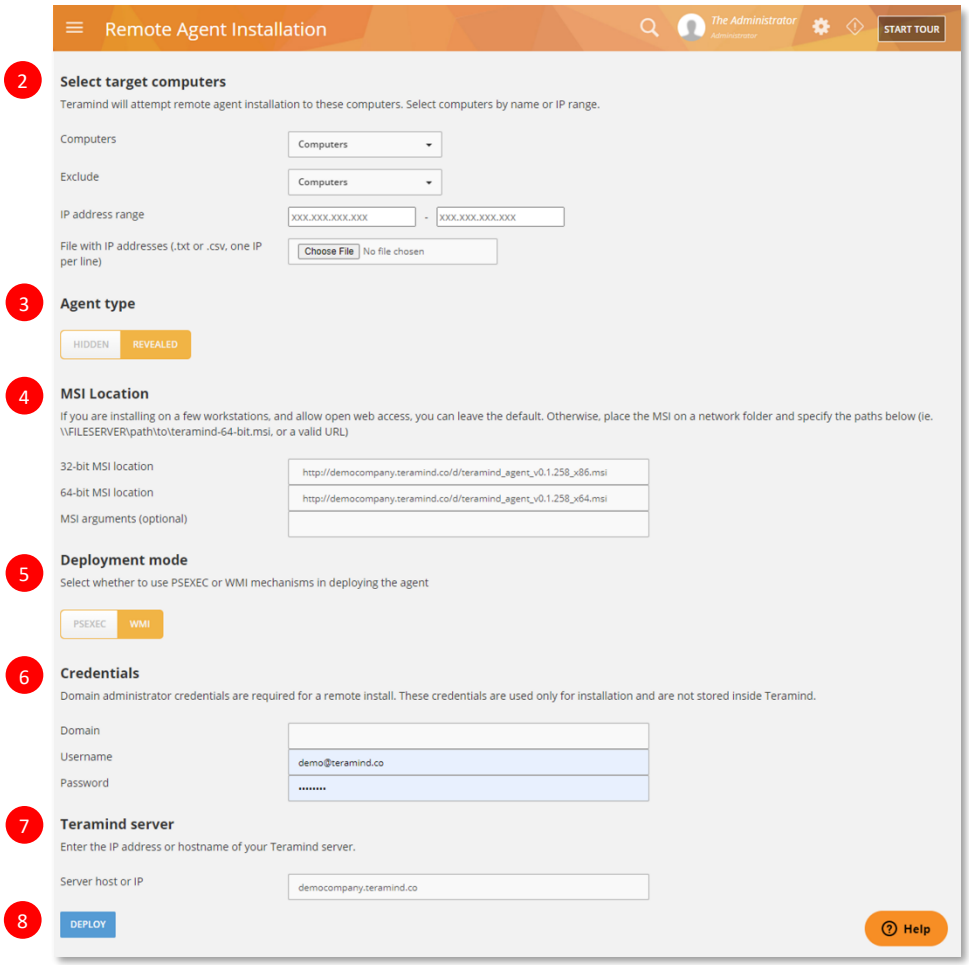


1. Click the **COMPUTERS** menu to access its screen.

10.3 Remote Installing the Teramind Agent



1. Click the **REMOTE INSTALL AGENTS** button near the top-right corner of the screen. You will be taken to the *Remote Agent Installation* screen where you can deploy the Agent remotely.



2. Under the *Select Target Computers* section, you can select the computers where you want the Agent to be installed. If you have integrated Active Directory/LDAP with Teramind, you will be able to select/exclude computers by name, groups etc. If you do not have Active Directory integration, then you can select the computers by IP range. You can also upload a .TXT or .CSV file containing IP addresses (1 per line).

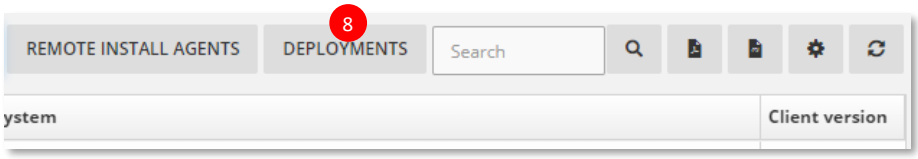
> Check out the Settings > Active Directory section to learn how to integrate Active Directory with Teramind.

3. Under *Agent type*, select HIDDEN or REVEALED agent.
4. For the *MSI Location*, if your endpoints are able to access the internet, you can leave the URLs of the Agent locations to their default values. This will fetch the Agent from your local Teramind deployment. Alternatively, you can enter local URLs or network paths where the necessary Agent files (32 bit/64 bit/MSI) are located. If you are using a web location, use HTTP if you encounter any issue using a HTTPS connection.
5. Under *Deployment Mode*, you can choose between PSEXEC or WMI mechanism to deploy the Agent.

6. Under the *Credentials* section, ensure that the domain administrator credentials, and IP address of the Teramind Server are correct.

> Note that, domain administrator privileges are mandatory for the silent install.

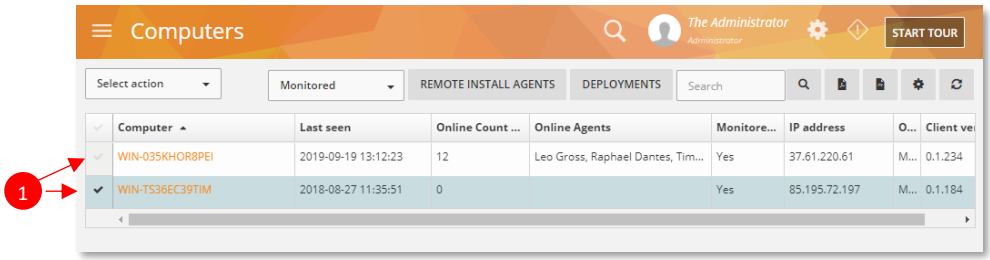
7. Under the *Teramind server*, enter host name or IP address of your Teramind server.
8. Click the **DEPLOY** button to begin the installation.



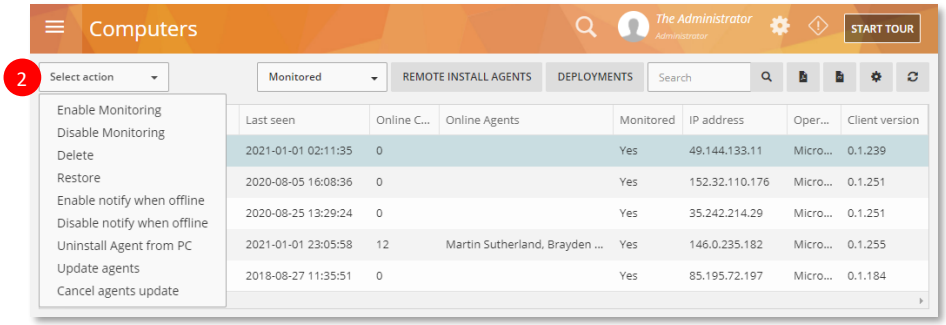
9. Back on the main *Computers* screen, you can Click the **DEPLOYMENTS** button to see the progress of all ongoing remote deployments.

10.4 Computer Action Menu

You can perform various actions such as enable/disable monitoring, enable offline notifications, update the Agent etc.



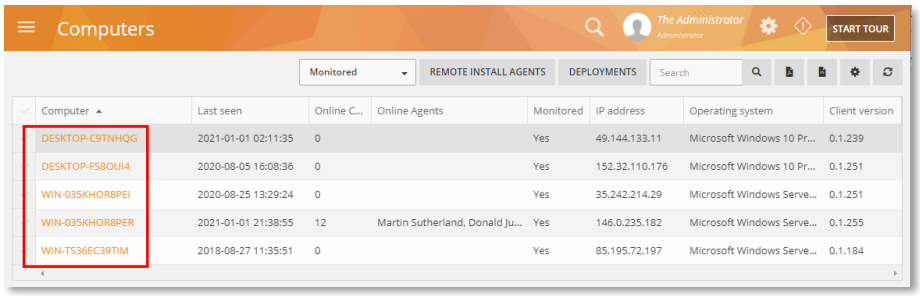
1. Click the **check marks** in front of the computer names to select computers.



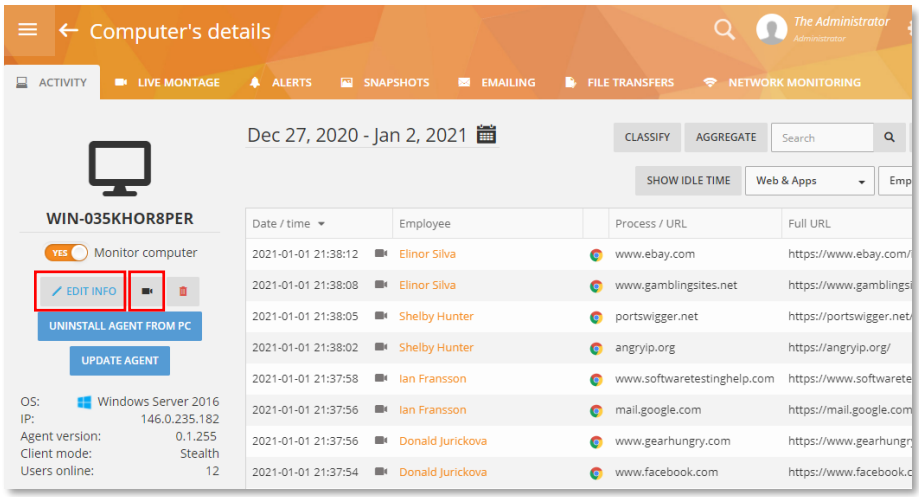
2. Click the *Select action* menu on the top-left corner of the screen, select the action you want to perform. You can choose from the following actions:
   - **Enable Monitoring:** enables monitoring for all users on the selected computers.
   - **Disable Monitoring:** disables monitoring for all users on the selected computers.

- **Delete:** Delete / remove a computer. Note that, when you delete a computer, it is not permanently deleted, just hidden from the computers list and all monitoring reports. Monitoring is also disabled when you delete a computer. If you are on a On-Premise deployment, deleting a computer will also free up a license.
- **Restore:** Restore a previously deleted computer. Note that since deleting a computer also disabled monitoring for a computer, you will need to enable monitoring after you restore it.
- **Enable notify when offline:** when you click this button, you can specify one or more email addresses which will get an email notification whenever the selected computers go offline.
- **Disable notify when offline:** disables offline notification.
- **Uninstall Agent from PC:** will uninstall/remove the agent from the computers.
- **Update agents:** updates the installed Teramind Agent on the selected computers with the latest version.
- **Cancel agents update:** cancels any pending Agent update tasks.

10.5 Accessing a Computer's Details Page



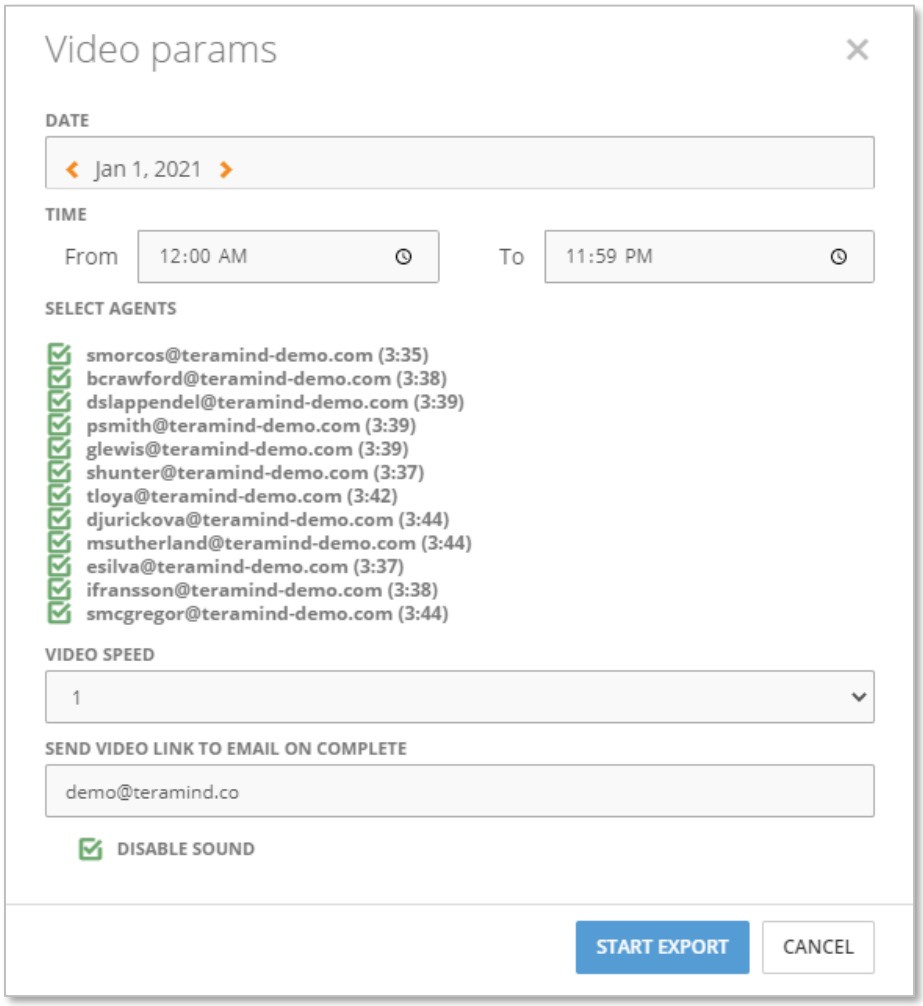
Click on a **computer** from the list of computers on the *Computers* page. You will be taken to the *Computer's details* page:



From this page you can view the computers details such as what OS is installed, the IP address, Agent version etc. You can also perform many of the same tasks found on the Computer Action Menu such as enable/disable monitoring, delete a computer, update agent etc. However, there are two new options you can access from the *Computer's details* page: viewing/editing the computer's profile and exporting session recordings. See the sections below for more information.

10.5.1 Exporting Session Recordings of Users/Agents on a Computer

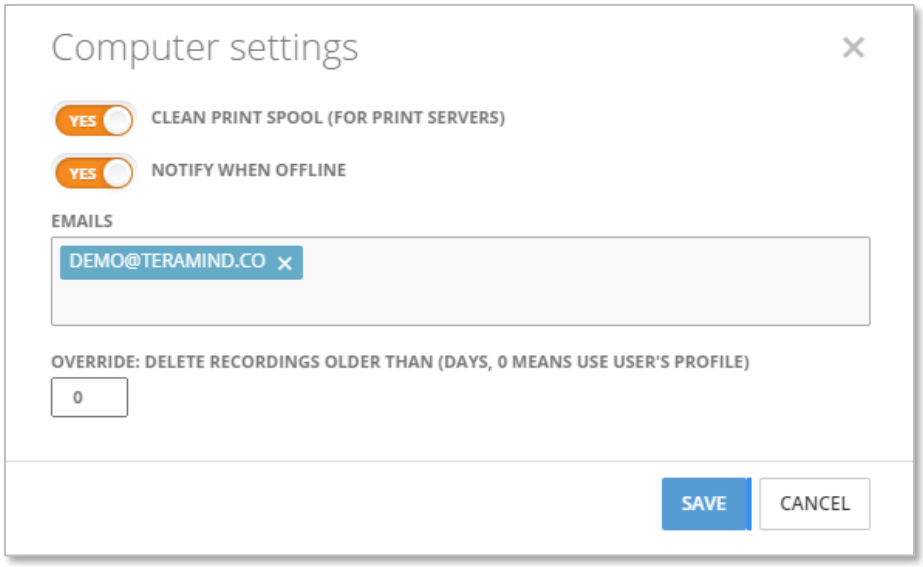
Click the **Video Camera** icon on a *Computer's details* page to export session recordings of select users/agents on the computer. Clicking this button will open a *Video params* window:



From this window you will be able to specify export date and time, select agents/users and other parameters for exporting the video/session recordings. See the Session Player section to learn more about session recordings.

10.5.2 Editing a Computer's Settings

Click the **EDIT INFO** button on a *Computer's details* page to access its settings:



You can change the following settings from the *Computer settings* window:

- **CLEAN PRINT SPOOL (FOR PRINT SERVERS):** This option is available when the Teramind Agent is installed on a print server. When Clean Print Spool is enabled, the Teramind Agent will check the print spooler every **10 minutes** and delete documents older than **6 hours**.
- **NOTIFY WHEN OFFLINE:** When you click this button, you can specify one or more email addresses which will get an email notification whenever the selected computers go offline. Note that, same option is available under the Computer Action Menu.
- **OVERRIDE: DELETE RECORDINGS OLDER THAN …:** This option lets you delete recording older than certain days. A value other than 0 will override the delete settings you have specified in the 'DELETE HISTORY AFTER…' field on the Monitoring Settings> Screen profile.

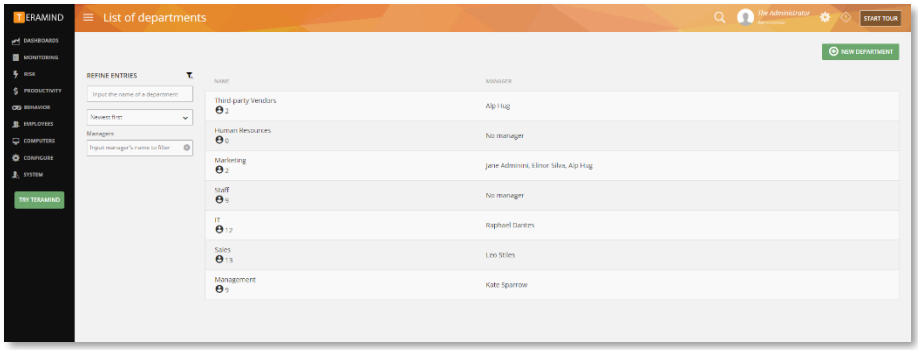
11 Configure

11.1 Introduction to the Configurations

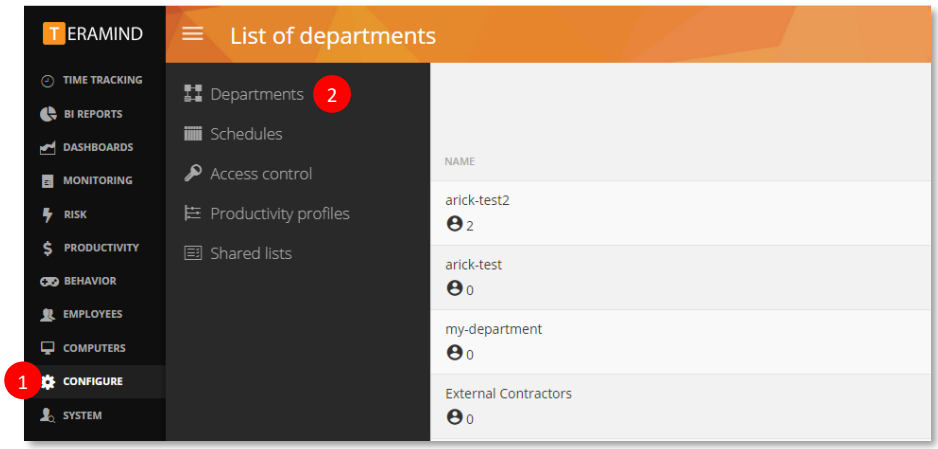
The Configure menu allows you to configure different Teramind components that are shared across the system. For example, with the Departments screen, you can create/edit departments to assign employees to; create Schedule for employees; setup Access Control and create Shared Lists for use among rules.

11.2 Departments

On the Departments screen, you can see a list of all the departments, how many employees are in each department, who the department managers are etc. You can also create/edit departments and assign managers to them.

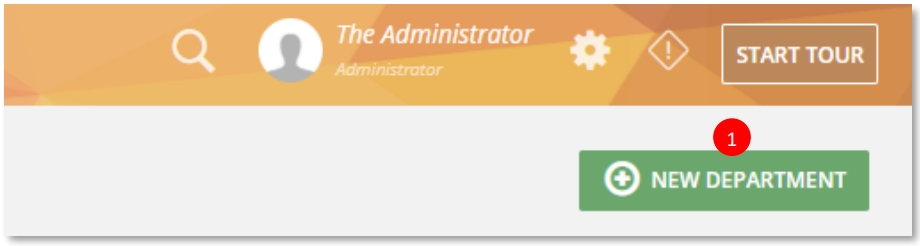


11.2.1 Accessing the Departments Menu

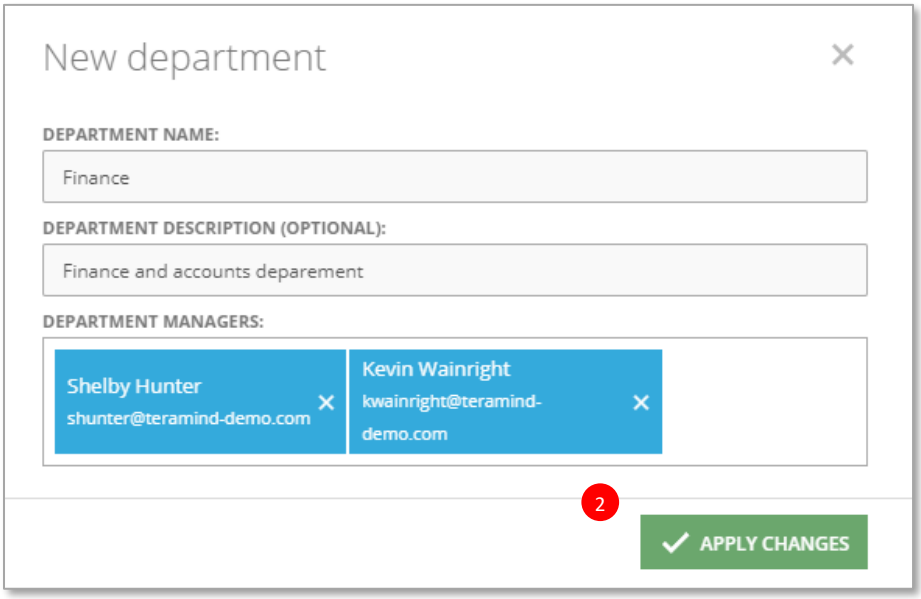


1. Hover your mouse over the **CONFIGURE** menu, then
2. Select **Departments** from the sub-menu.

11.2.2 Creating a New Department

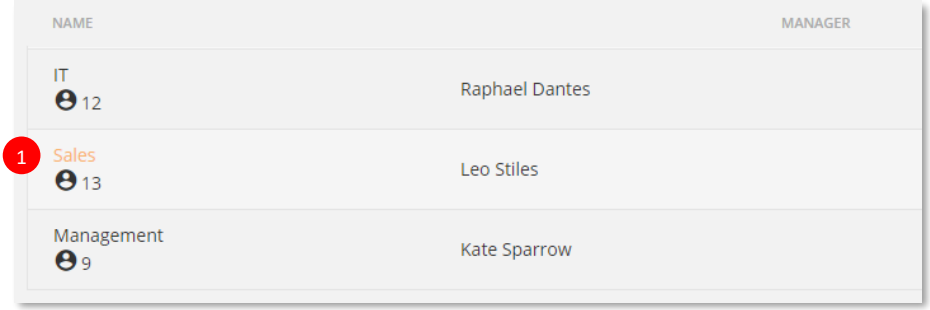


1. Click the **NEW DEPARTMENT** button. A *New department* window will pop-up.

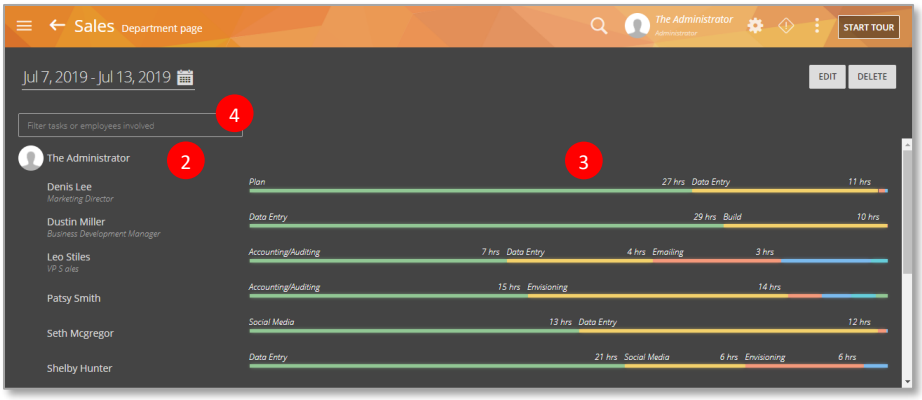


2. Specify a name and optionally, a description. Select the department managers from the list of employees. Click the **APPLY CHANGES** button to create the department.

11.2.3 Viewing the Employees in a Department



1. Click on the *name* of a department, for example, **Sales**. You will be taken to the *Department page*.



2. On the left side of the *Department page*, you will see a list of employees assigned to the department.
   Check out the Entering / Editing Employee Profiles section to learn how to assign an employee to a department.
3. On the right-side of the page, you will see a Gantt chart with a list of tasks for each employee and how much time they spent on each task.
   Check out the Rules Editor > Actions tab section, under 'Set User's Active Task' to learn how tasks can be assigned to an employee automatically by a rule when using a Steal Agent. Or, check out the Teramind Agent documentation to learn how Tasks can be created and self-assigned by users with the Revealed Agent.

11.2.4 Editing / Deleting a Department

1. While on the *Department page*, click the **EDIT** button at the top-right corner. An *Edit department* window will apprear (similar to the *New department* window) where you can change the department's name, decription and managers.
2. While on the *Department page*, click the DELETE button at the top-right corner to delete the department.

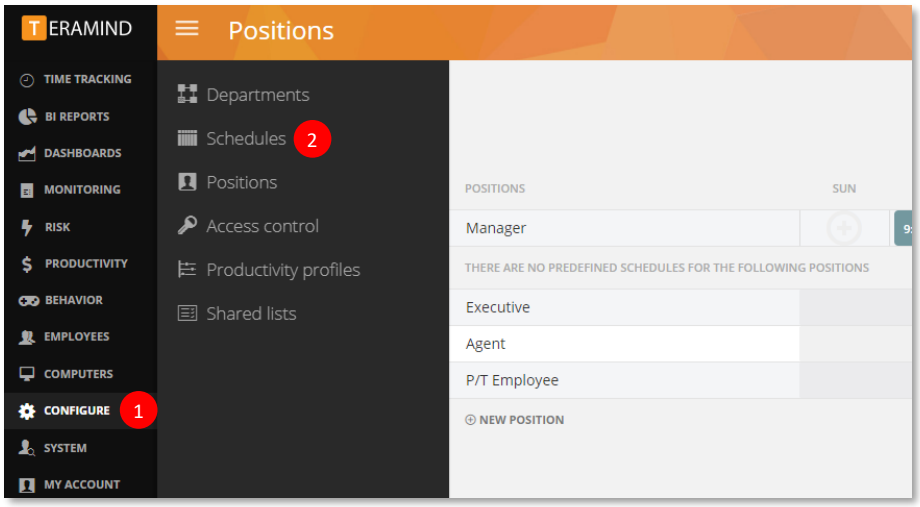
11.3 Schedules

The Schedules screen allows you to manage schedules for your employees and contractors. You can control employee work time, lunch breaks, days off etc. This information is then used by other Teramind modules. For example, in the Agent Schedule-based rules, in the Productivity Reports or for calculating payroll etc.

This screen has two tabs. The SCHEDULING tab allows you to create/edit the daily and weekly schedules for your employees. The TEMPLATES tab allows you to create/edit templates to make managing schedules for large groups easier.

> Note that you can also create schedules for various positions in your organization. Check out the Positions section for more information.

11.3.1 Accessing the Schedules Menu

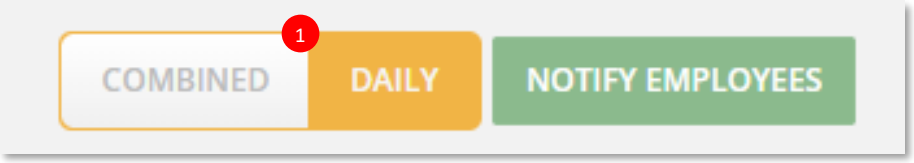


3. Hover your mouse over the **CONFIGURE** menu, then
4. Select **Schedules** from the sub-menu.

11.3.2 Adding a New Employee

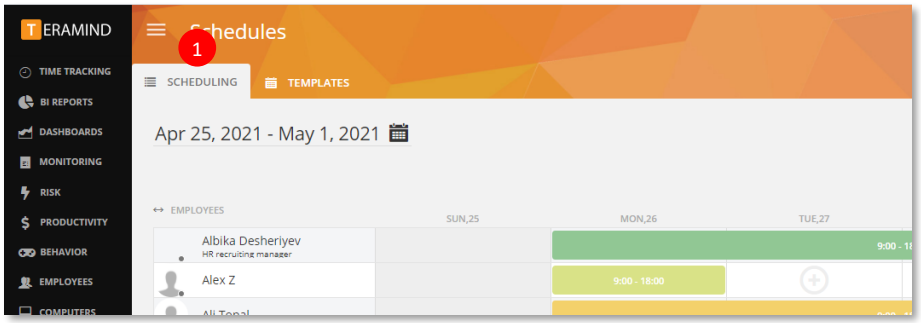
1. Click the NEW EMPLOYEE button near the bottom. This will pop-up the New employee window where you can add a new employee, configure their account details, monitoring options, etc. Check out the [entering/editing employee profiles] section for more information.

11.3.3 Switching Between Combined vs Daily Views



1. Click the COMBINED or DAILY button near the top-right corner to switch between a Combined view and a Daily view. On the Combined view, days with the same shift/timeslots are combined in a single column while in the Daily view each shift is shown as a separate column.

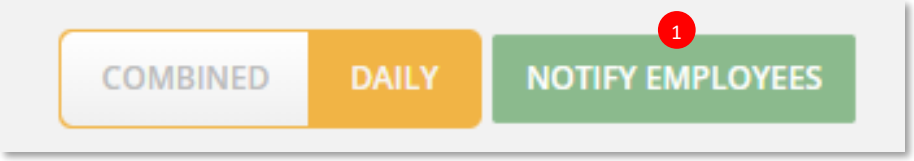
11.3.4 Managing Employee Schedule



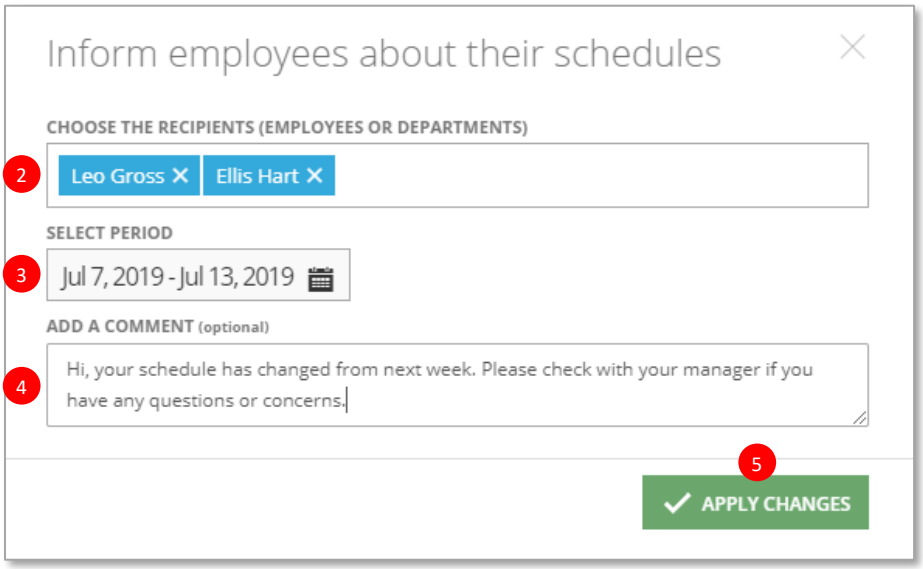
1. You can manage schedules for individual employees from the **SCHEDULING** tab.

11.3.4.1 Notifying Employees About Schedule Changes

You can send a notification to employees or departments of any schedule changes.

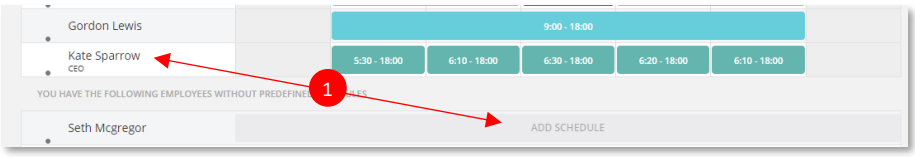


1. Click the **NOTIFY EMPLOYEES** button at the top right-corner of the SCHEDULING screen. A pop-up window will open.

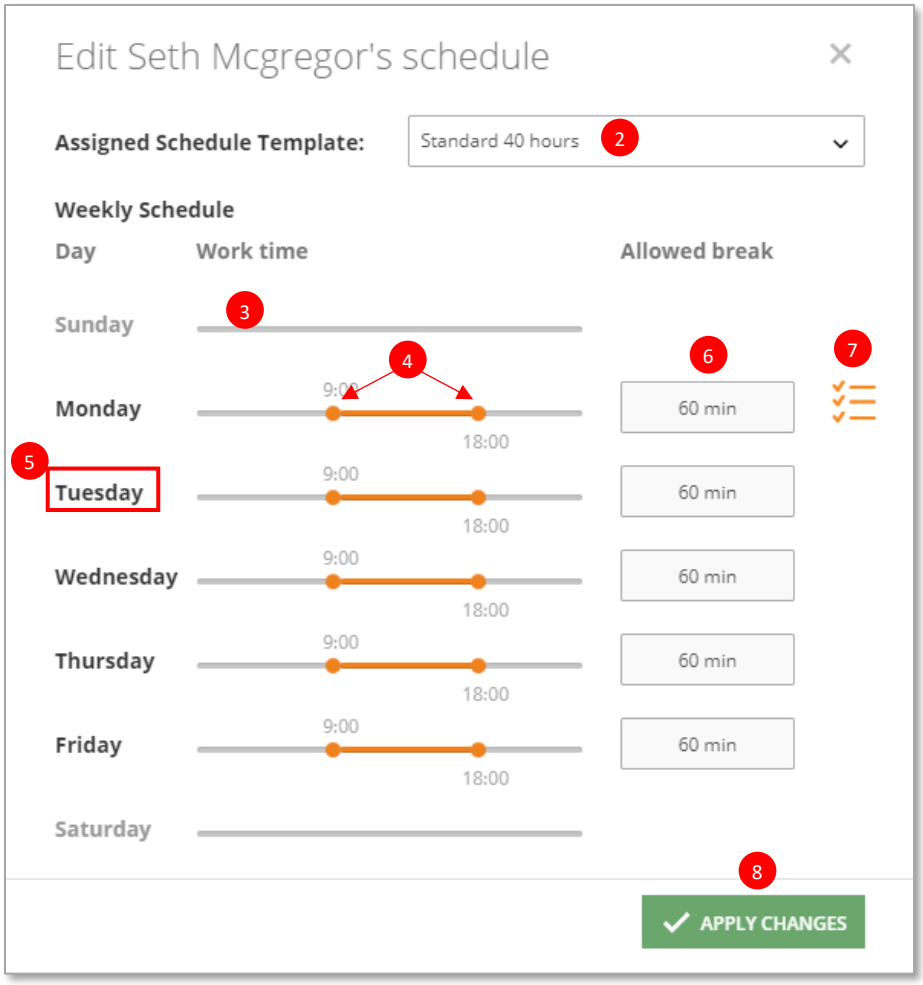


2. Select the employees you want to inform from the list of employees.
3. Select a period.
4. Optionally, add a comment.
5. Click the **APPLY CHANGES** to send the notification.

11.3.4.2 Managing Weekly Employee Schedules

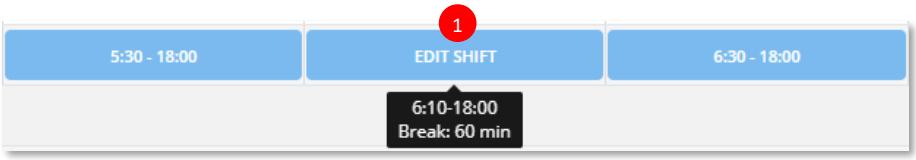


1. Click the ***name*** of an employee on the SCHEDULING screen. You can also click the **ADD SCHEDULE** button if the employee does not have a schedule already assigned. A pop-up window will be displayed:

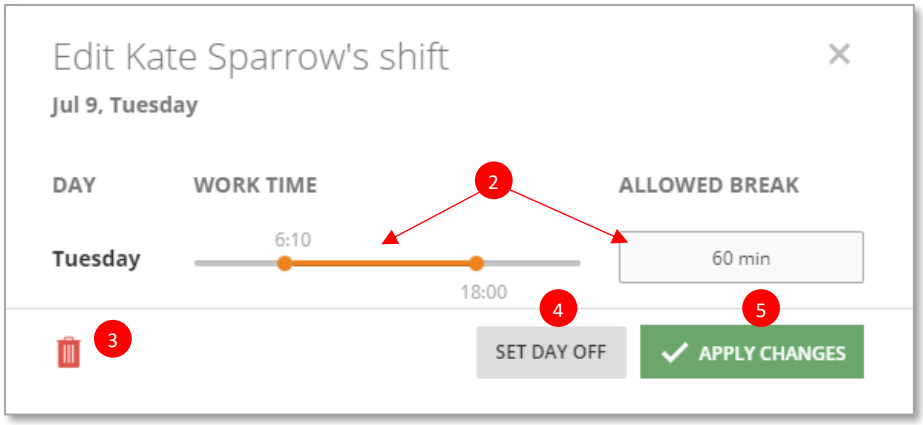


2. You can select an existing template to populate the schedules for the weekdays.
3. Click on an empty *Work time* slider to add hours to it.
4. Drag the **Circles** ● on a slider to adjust its hours.
5. Click on a day's name, for example, **Tuesday**, to turn it on/off (make it a workday/off day). If all the days are turned off for the week, the schedule will be deleted/removed from the employee.
6. Use the *Allowed break* field to assign break hours.
7. Click the **Matched List** icon to make all hours match with the first day's hour.
8. Click the **APPLY CHANGES** button to save the schedule.

11.3.4.3 Managing Daily Employee Schedules and Day Offs



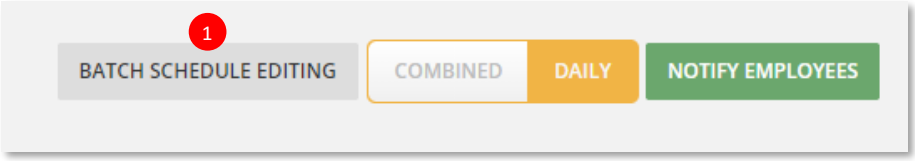
1. Click on a day's timeslot/shift or an empty day on the SCHEDULING screen. A pop-up window will appear:



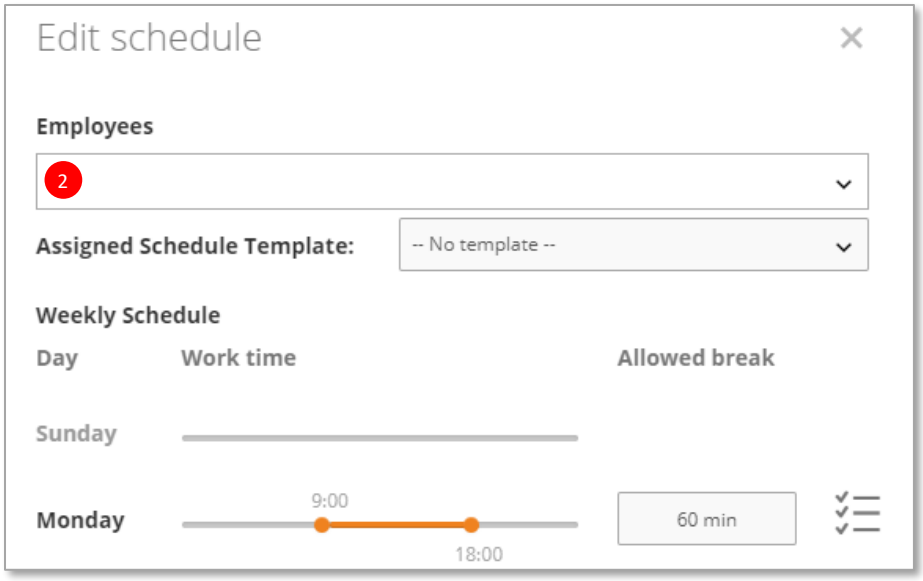
2. You can edit the worktime and breaks the same way you do for multiple days.
3. You can delete the shift (turn the day off).
4. To assign/cancel a day off, click the **SET DAY OFF** or **DEACTIVE DAY OFF**.
5. Click the **APPLY CHANGES** button to save the changes.

11.3.5 Batch Schedule Editing

This feature allows you to add a schedule to a group of employees at once instead of editing them one by one.



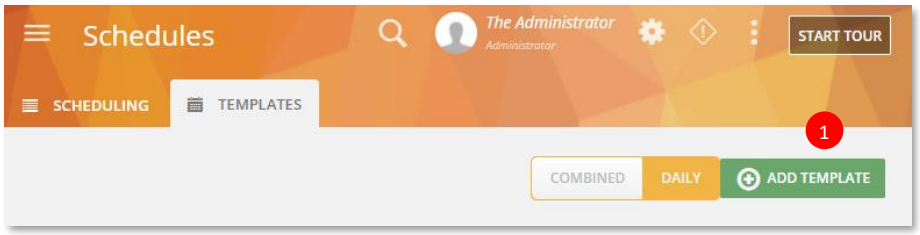
1. Click the **BATCH SCHEDULE EDITING** button near the top right-corner of the SCHEDULING screen. An *Edit schedule* pop-up window will open.



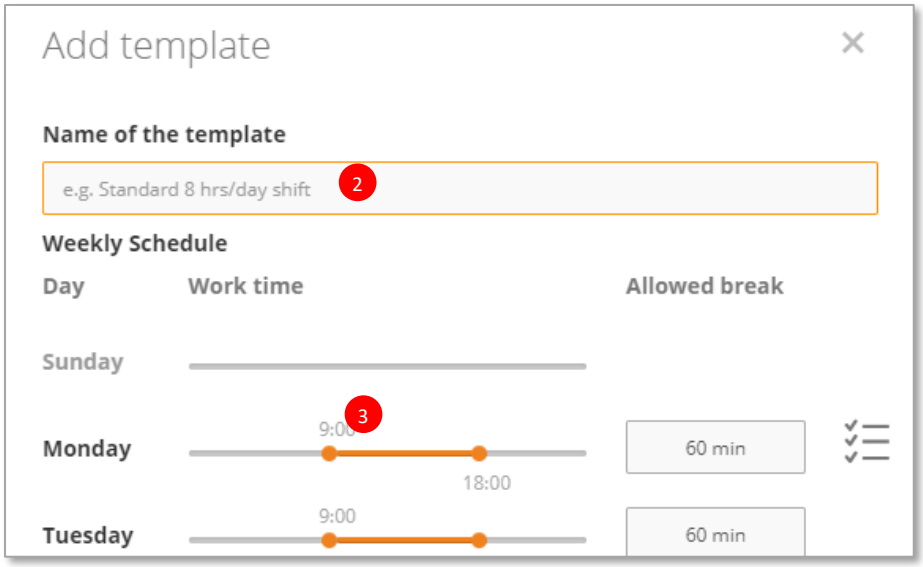
2. This is similar to editing a Weekly Employee Schedule, the only additional option is an **Employees** field where you can select and assign multiple employees to the schedule.

11.3.6 Managing Templates

11.3.6.1 Adding a New Template

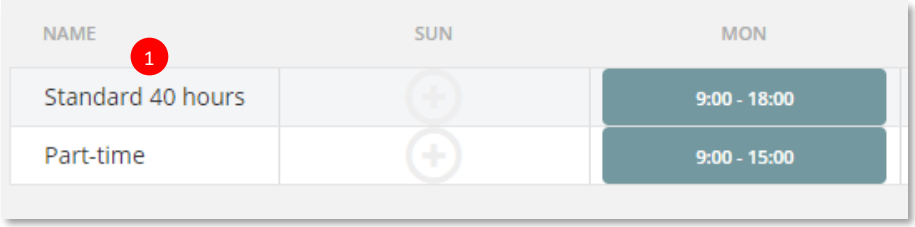


1. From the ***TEMPLATES*** tab, click the **ADD TEMPLATE** button at the top-right corner. A pop-up window will open:

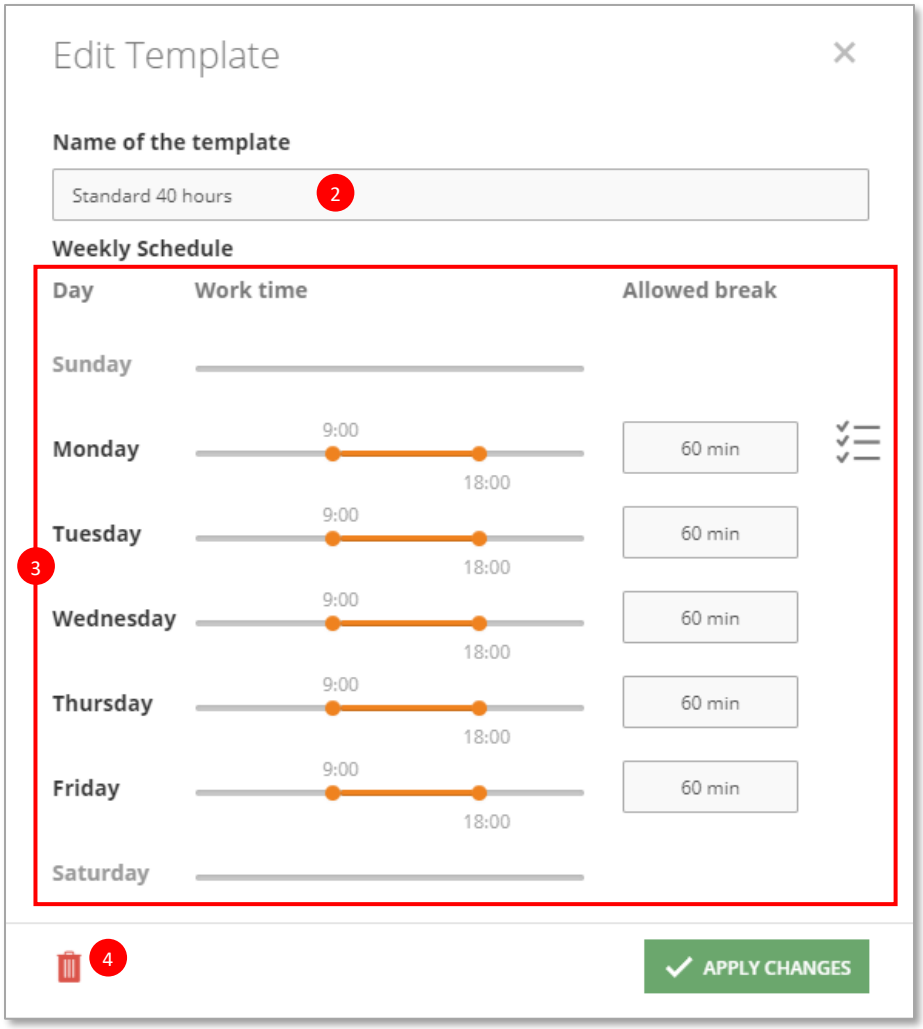


2. Give the template a name.
3. You can edit the rest of the template the same way you would edit a weekly employee schedule. Please follow the [Managing Weekly Employee Schedules]() to learn how to edit the schedule.

11.3.6.2 Editing / Deleting a Template



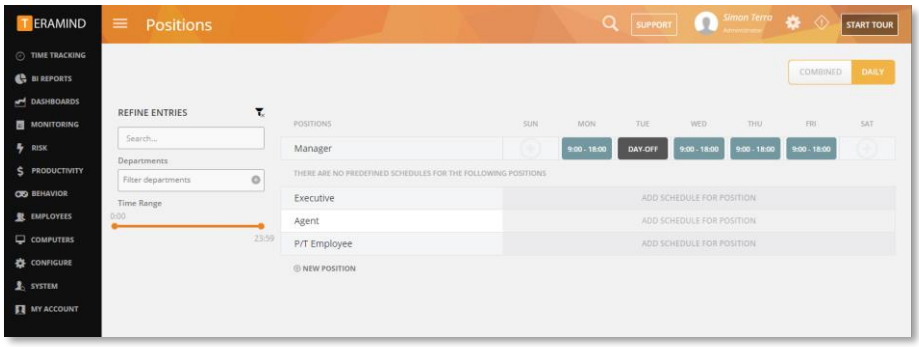
1. Click on a template name. A pop-up will open.



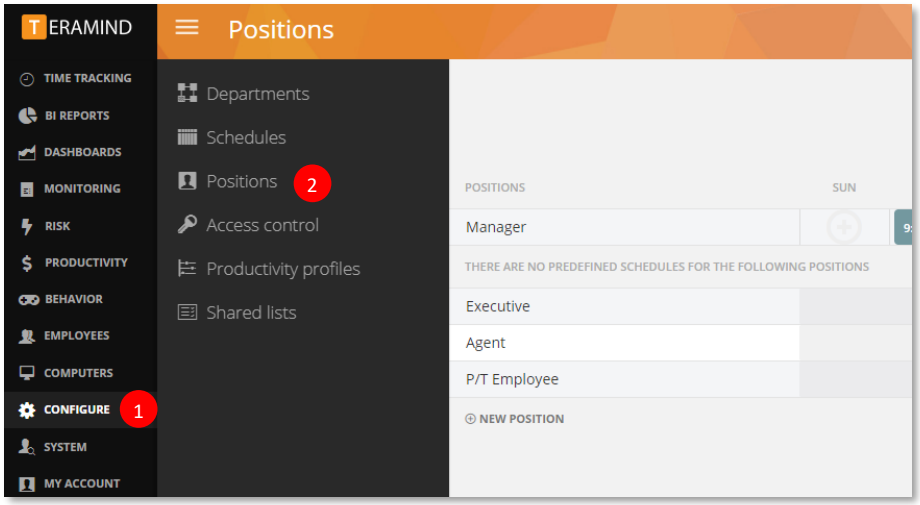
2. Change the template name if needed.
3. You can edit the template the same way you would edit a weekly employee schedule. Please follow the instructions on Managing Weekly Employee Schedules to learn how to edit a template.
4. Click the **Trash Can** icon to delete the template. You can also click on the day names (i.e. Monday, Tuesday etc.) to turn them off. If all the days are turned off for the week, the template will be deleted/removed.

11.4 Positions

The Positions screen allows you to manage schedules for positions/titles. It is very similar to the Schedules screen except that it does not have any *Notify Employee* or *Batch Update* option.

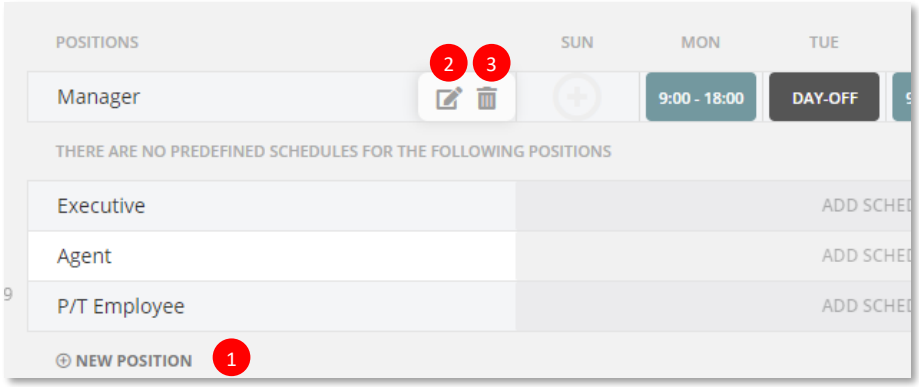


11.4.1 Accessing the Positions Menu



5. Hover your mouse over the **CONFIGURE** menu, then
6. Select **Positions** from the sub-menu.

11.4.2 Adding / Editing / Deleting a Position

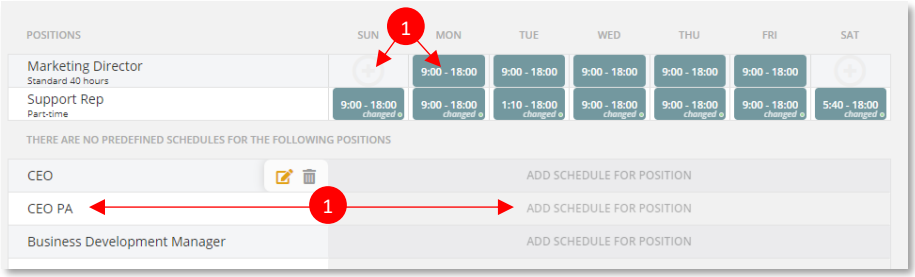


1. Click the **NEW POSITION** button to add a new position. Note that, you can also create a new position when [entering/editing employee profiles](), under PERSONAL INFO, in the *Position* field.
2. Hover over a **position name** and click the **Pencil** icon to edit the position.

3. Hover over a **position name** and click the **Trash Can** icon to delete the position.

11.4.3 Managing Position Schedules

You can manage schedules for positions the same way you manage schedules for employees. For example:



1. You can create/edit the *daily* schedule by clicking a **day** on the scheduler.
2. Similarly, you can create/edit *weekly* schedule of a position by clicking the **position name** or by clicking the **ADD SCHEDULE FOR POSITION** button.

Check out the Managing Daily Employee Schedules and Day Offs and the Managing Weekly Employee Schedules sections to learn how to edit the two types of schedules.

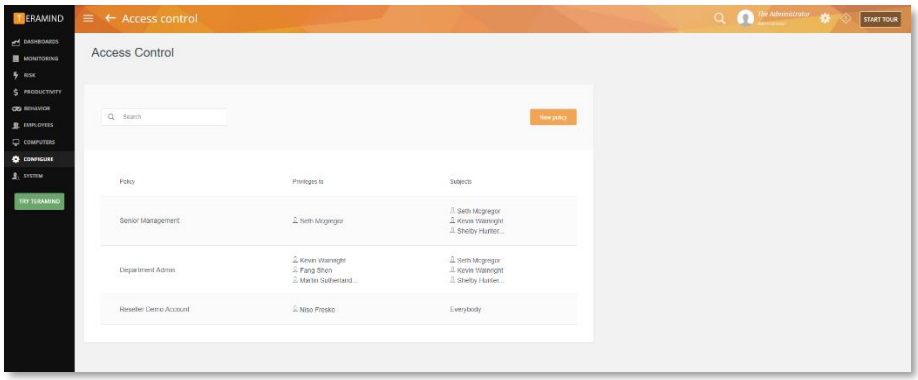
11.4.4 Using the Schedule Templates

You cannot create any schedule templates from the Position screen. However, you can use any templates created on the Schedule screen when editing a *weekly* position schedule.

11.5 Access Control

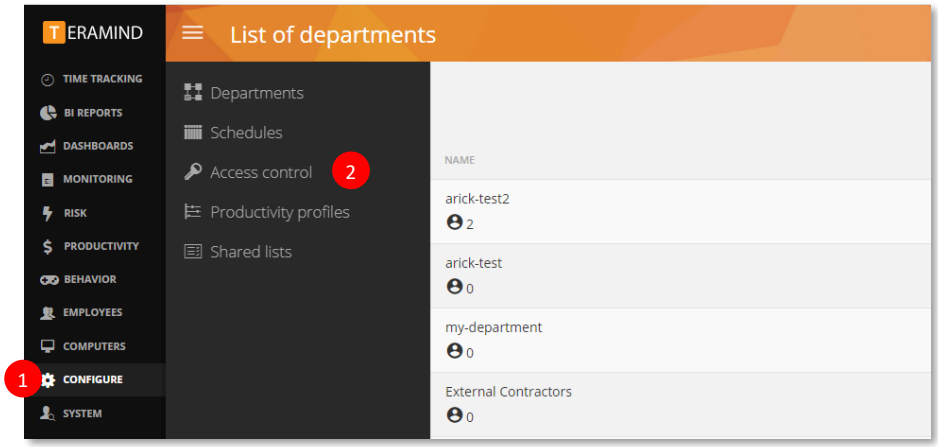
The Access Control screen allows you to control which administrators/managers have access to what information on the Teramind Dashboard and the settings they are allowed to change. On Teramind, access control is implemented through policies. A policy is composed of the following elements:

- **Privileged Users:**
  They are the admins/managers who monitor certain groups of people (Target Users/Subjects).
- **Target Users / Subjects:**
  These are the regular users monitored by the Privileged Users.
- **Permission:**
  Defines what the privileged user can do with the information of the Target Users under their responsibility. The permission is grouped into Play, View, Edit and Access Widgets categories.



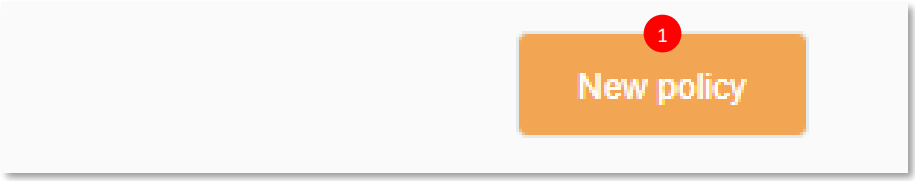
The main window of the Access Control screen shows a list of policies, privileges and the subjects they manage. You can create a new policy or edit an existing one from this window.

11.5.1 Accessing the Access Control Menu

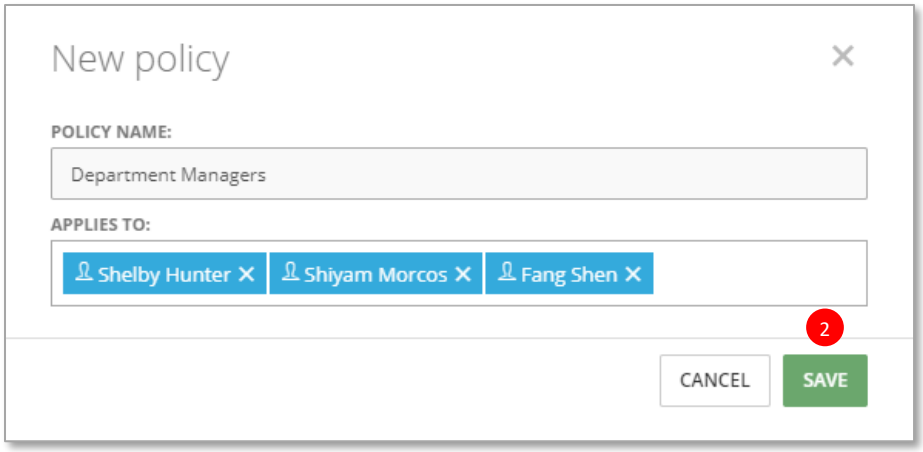


7. Hover your mouse over the **CONFIGURE** menu, then
8. Select **Access control** from the sub-menu.

11.5.2 Creating a New Access Control Policy

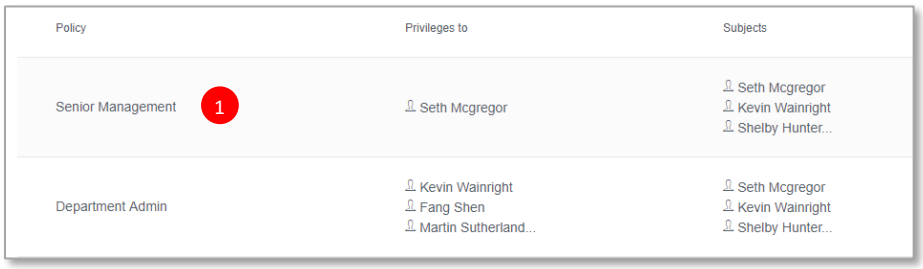


1. Click the New policy button at the top-right corner. A window will pop-up.

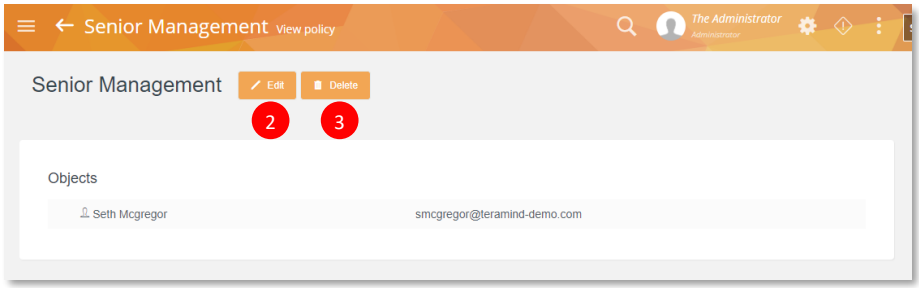


2. Enter a name for the policy, select the privileged users the policy will apply to, then click the **SAVE** button. You will be taken to the *Create policy* screen. Continue with the Access Control Policy Editor section below to learn how you can assign target users and adjust the permission settings for a policy.

11.5.3 Viewing / Editing / Deleting an Access Control Policy



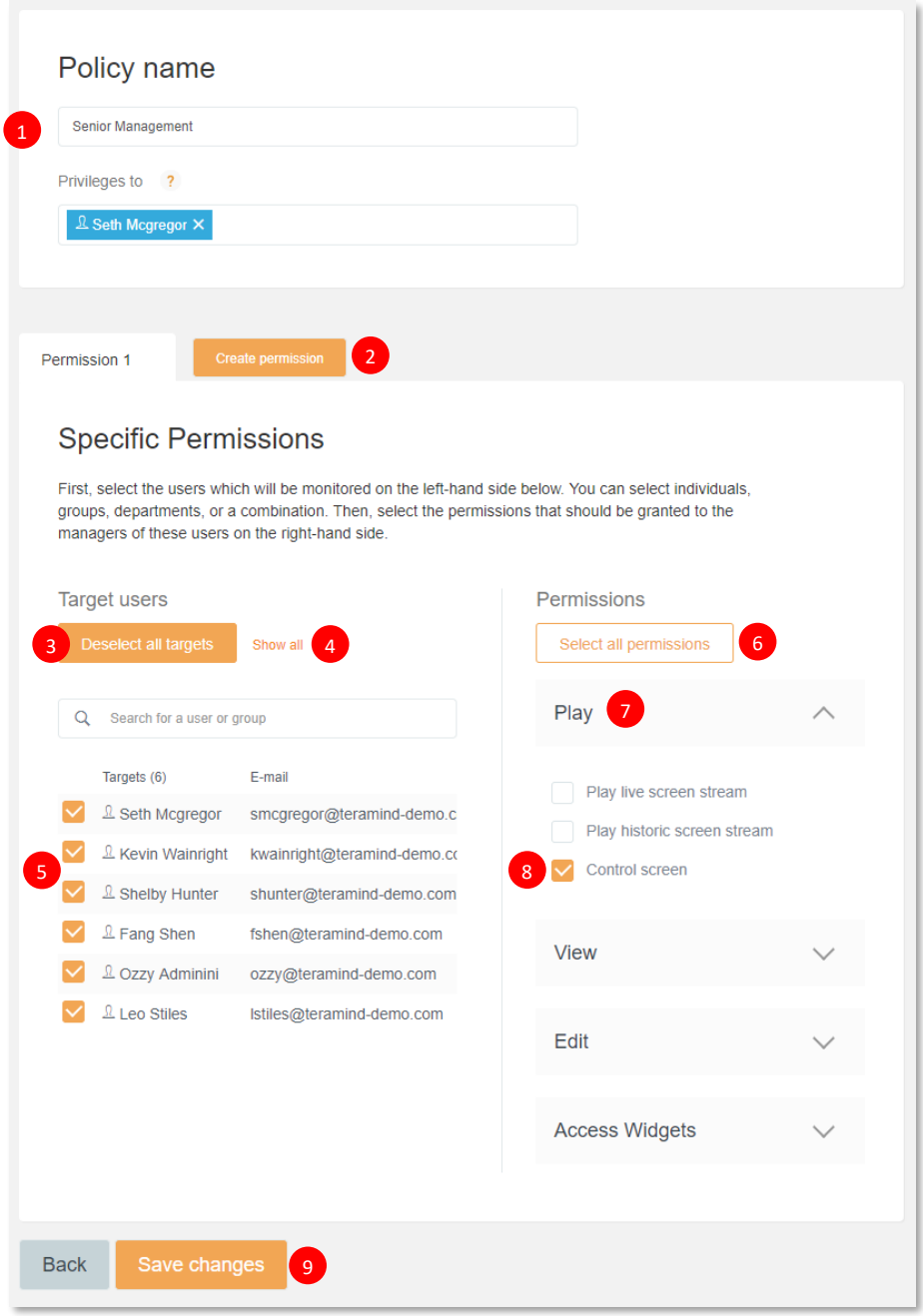
1. Click on a policy from the list of policies on the main Access Control screen. You will be taken to the *View policy* screen where you can see the details for the policy.



2. On the *View policy* screen, click the **EDIT** button to edit the policy. You will be taken to the *Edit policy* screen. Continue with the Access Control Policy Editor section below to learn how to edit the policy.
3. On the *View policy* screen, Click the **DELETE** button to delete the policy.

11.5.4 Access Control Policy Editor

The Access Control Policy Editor allows you to edit a policy. You access it through the *Create policy* / *Edit policy* screens (see the previous sections to learn how to create/edit a policy).



1. Specify a policy name and select the privileged users (admins, managers etc.) the access permission will be granted to.
2. Click the **Create permission** button to create a new permission.
3. Click the **Select all targets** button to select all target users or the **Deselect all targets** button to deselect them.

4. Click the **Show all** link to show all users or the **Show only selected** link to show only selected target users.
5. Click on a target user's name to select/deselect them.
6. Click the **Select all permissions** button to select all permissions or the **Deselect all permissions** button to deselect them.
7. Click on a **permission category** to expand or collapse it.
8. Click on a **permission item** to select/deselect it.
9. Click the **Save changes** button to save the policy.

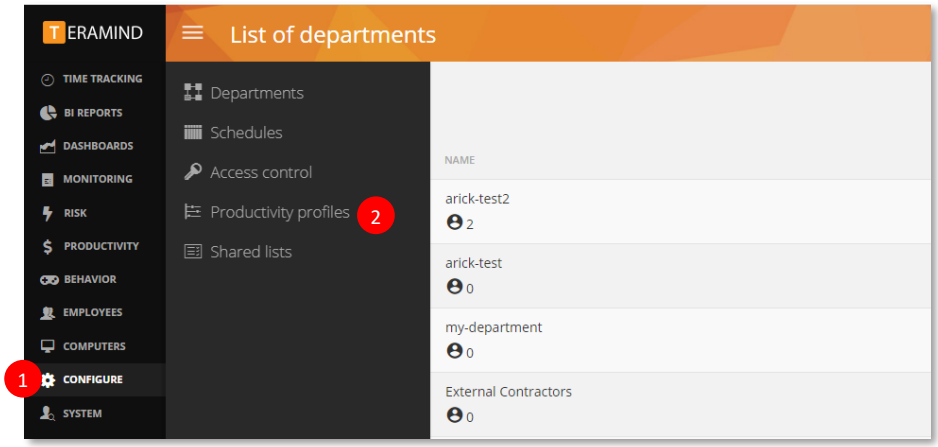
11.6 Productivity Profiles

Productivity profiles allow you to create rules to classify productive and unproductive applications and websites and assign them to individual employees, groups or departments. The profiles determine how *Productivity Classification*, *Productive Time*, *Unproductive Time*, etc. are measured and reported on the BI Reports (for example, Productivity BI Report and the Applications & Webpages BI Report).

Parent vs Child Profile and Inherited vs Owned Rule:

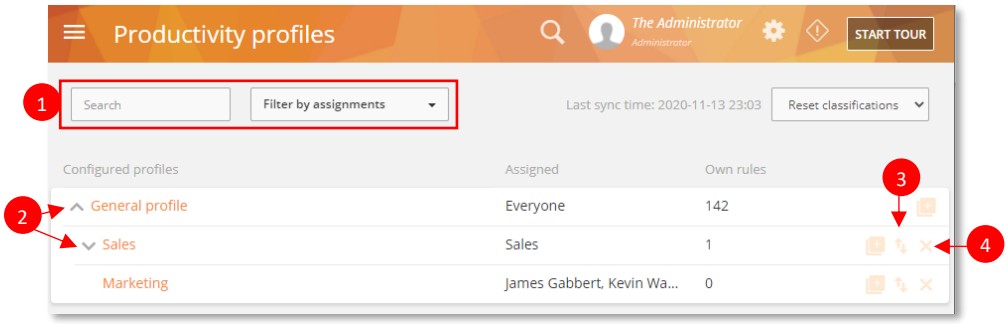
The main window of the Productivity Profiles screen shows a tree-view of all the parent and their child profiles. Child profiles will inherit all classification rules from its parent profile(s). Each profile can also 'own' its unique rules. This parent-child hierarchy and the ability to inherit/own rules allow you save time by avoiding duplicating or manually entering same rules to multiple profiles.

11.6.1 Accessing the Productivity Profiles



1. Hover your mouse over the **CONFIGURE** menu, then
2. Select **Productivity profiles** from the sub-menu.

11.6.2 Viewing and Managing Productivity Profiles

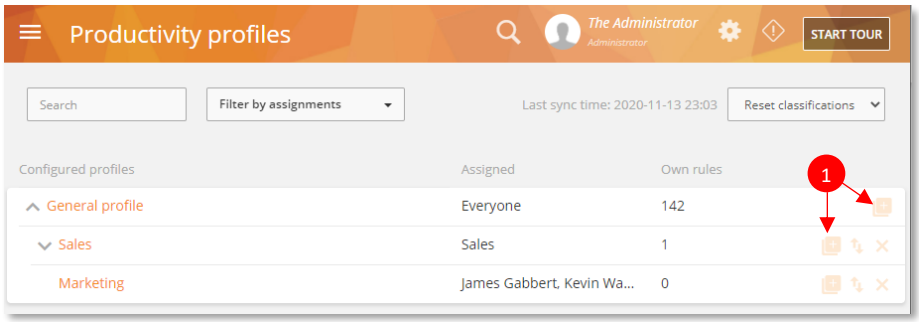


1. **To filter profiles:** You filter the list of displayed profiles using the **Search** field and/or the **Filter by assignments** list.
2. **To view all child profiles:** If a profile has any child profile(s) you can click on its **Up Arrow / Down Arrow** icons to view or hide its child profiles.
3. **To change the parent of a child profile:** Click the **Inheritance** button to change the parent of the profile.
4. **To delete a profile:** Click the **Delete** button to delete / remove a profile.

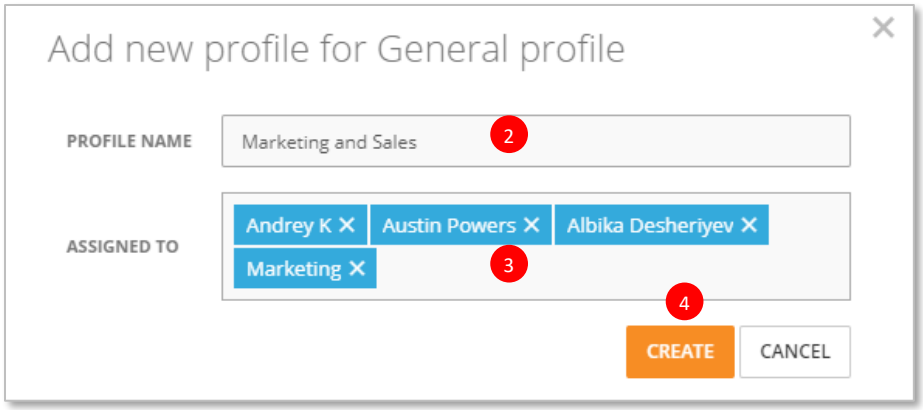
When you delete a profile, all of its child profiles and rules will be deleted too.

You can also view a user's productivity profile (but not change it) from the employee profile screen.

11.6.3 Adding a Productivity Profile



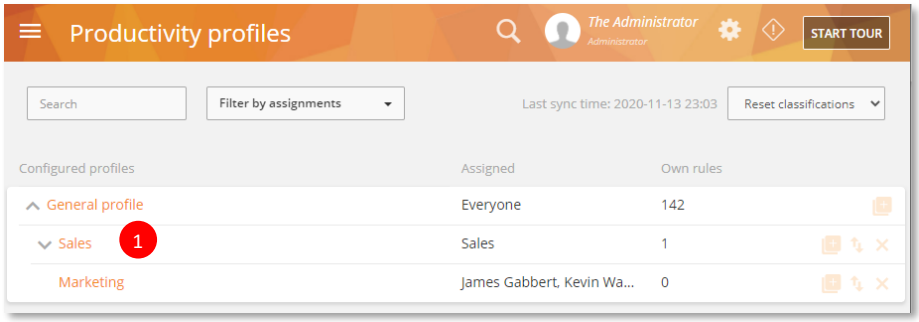
1. Click the **Add child profile** button at the right side of a profile to add a new child profile under it. A pop-up window will open:



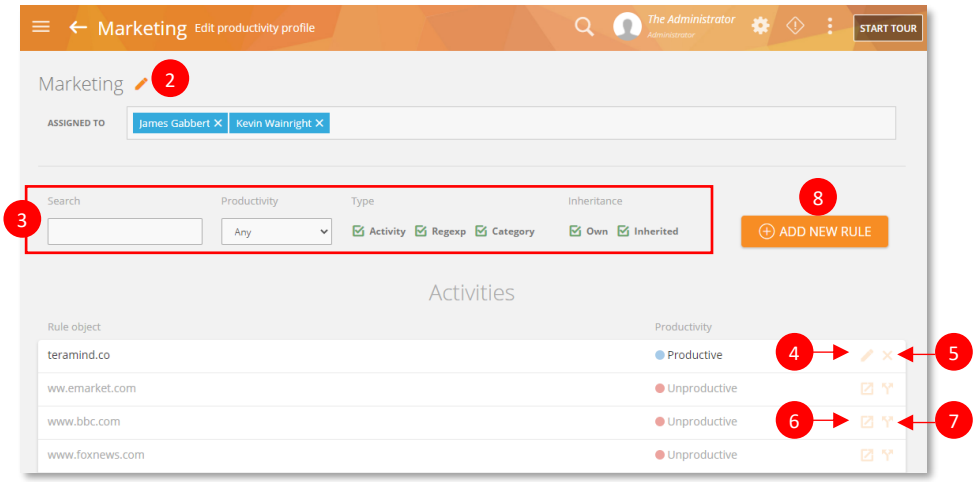
2. Enter a **PROFILE NAME**.
3. Select the employees/departments the profile will be **ASSIGNED TO**.
4. Click the **CREATE** button to create the profile. You will be taken to the Edit productivity profile screen. Check *Step 2-4* of the Editing a Productivity Profile and Classification Rules section below to learn how to configure a rule.

You can only assign one productivity profile to a user. If they are already part of a productivity profile, assigning them to a new profile will remove them from the previous profile.

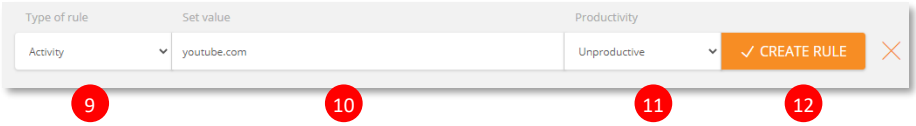
11.6.4 Editing a Productivity Profile and Classification Rules



1. Click a **profile's name** to edit it. You will be taken to the *Edit productivity profile* screen:



2. Click the **Pencil** icon next to the profile's name to edit its name and change its assignment. Note that, you can only assign one productivity profile to a user. If they are already part of a productivity profile, assigning them to a new profile will remove them from the previous profile.
3. You can change what rules are displayed by using the **Search**, **Productivity**, **Type** and **Inheritance** filter.
4. Click the **Pencil** icon next to a rule to edit it (see below for more information).
5. Click the **Delete** icon to delete a rule. You can only delete a rule 'owned' by the profile.
6. Click the **Open Parent** icon to leave the edit screen of the child profile and go to the parent profile screen.
7. Click the Click the **Override** icon to create a copy of an *inherited* rule. You can then save the inherited rule as a new *owned* rule.
8. Click the **ADD NEW RULE** button to create a new rule. The filter area will change to let you enter the details for the rule:



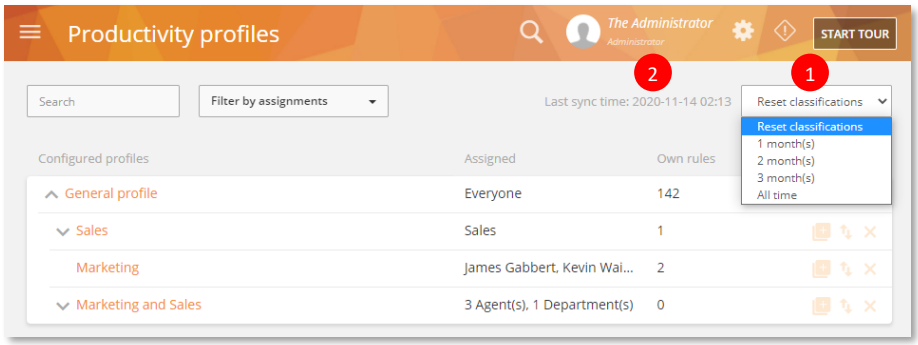
9. Select a type of rule. You can choose from **Activity**, **Regexp** and **Category**.
10. Enter a value for your chosen rule type. The value will apply to website URLs and application file names. For *Activity* type rules, you can enter any text. For example: '**`youtube.com`**', '**`word.exe`**' etc. , *Regexp* will match with a regular expression[1]. For example: **`.*tube`**. With *Category* type rules, you can select from a pre-defined list of websites categories[2]. For example: **`Entertainment`**, **`Social Media`** etc.

> [1]Teramind uses C++ standard regular expressions.
> [2]Teramind uses inCompass® NetSTAR, a comprehensive web categorization and filtering technology to automatically categorize websites.

11. Select a productivity classification such as **Productive**, **Unproductive** or **Unclassified**.
12. Click the **CREATE RULE** button to create and save the rule or **X** button to cancel.

11.6.5 Reset / Retroactive Classifications

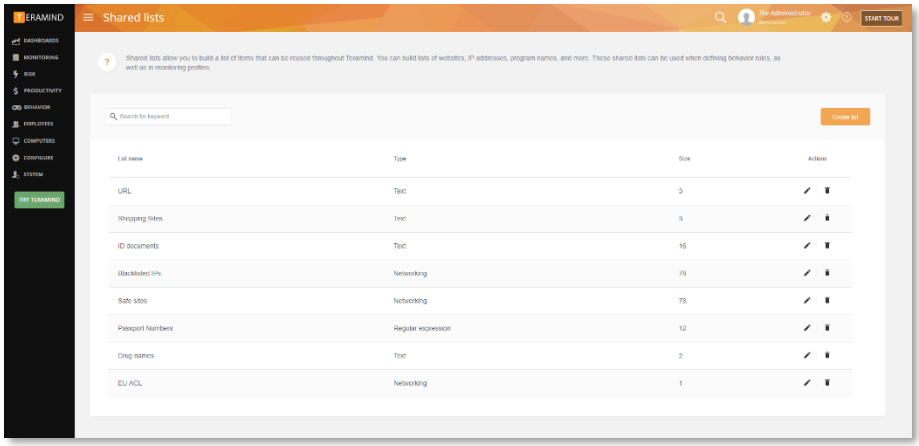
You can retroactively apply new classification profiles and rules to previous employee activities:



1. Click the **Reset classifications** menu near the top-right corner. Select a reset option from the pull-down list.
2. You can see when the profiles were last synced near the reset menu.

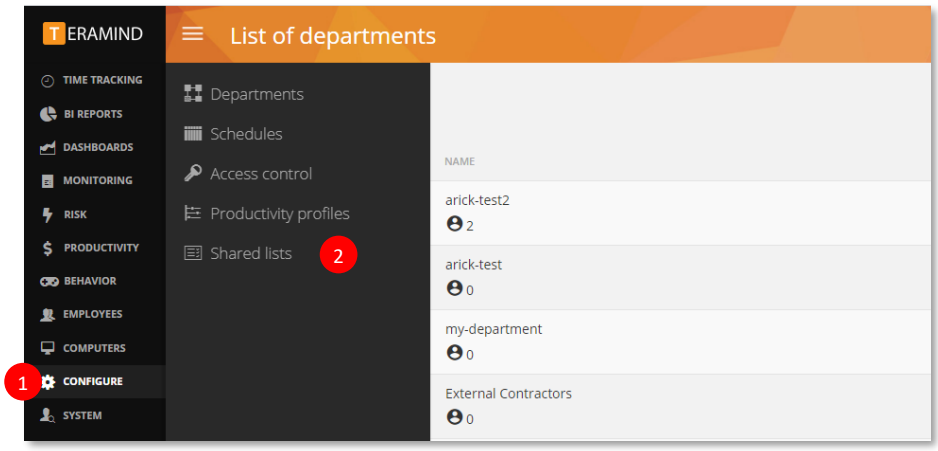
11.7 Shared Lists

The Shared Lists screen allows you to build a list of items that can be reused throughout Teramind. You can build lists of websites, IP addresses, program names, and more. These shared lists can be used when defining behavior rules, as well as in monitoring settings.



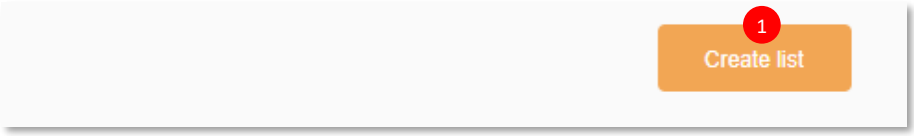
You can see all the existing lists including their name, type, number of items in the list etc. You can create, edit or delete shared lists from this screen.

11.7.1 Accessing the Shared Lists

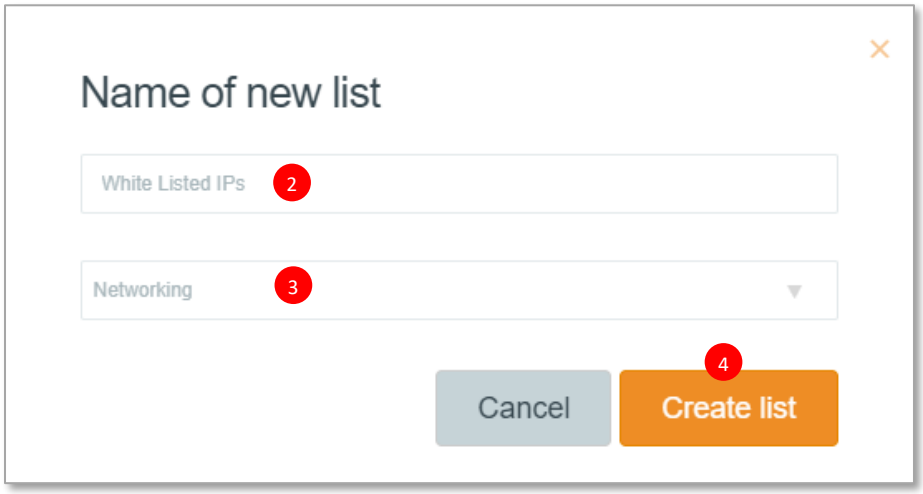


3. Hover your mouse over the **CONFIGURE** menu, then
4. Select **Shared lists** from the sub-menu.

11.7.2 Creating a New Shared List



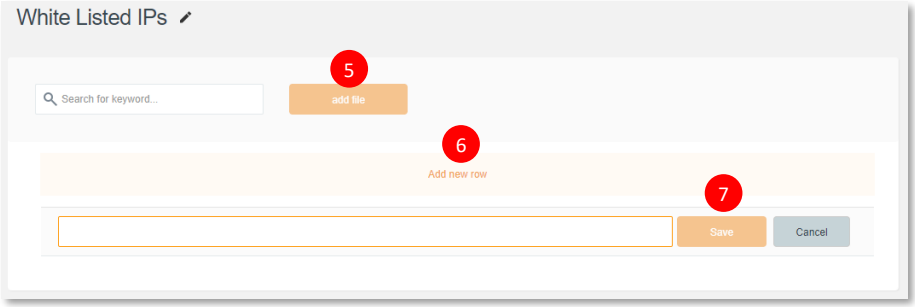
1. Click the **Create list** button near the top-right corner. A window will pop-up.



2. Enter a name for the list.
3. Select a list type. You can choose from *Text*, *Regular Expressions* and *Networking* types. Text list is useful for simple data such as names, website URLs etc. Regular Expressions is a powerful list type that can be used to detect patterns and specially formatted text such as credit card numbers, zip/postal codes etc. Networking list types are used for defining IP addresses and

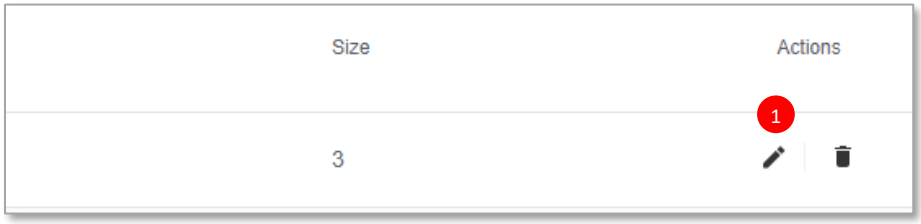
ports. Network lists can be used with the Network-based rules or to control Network monitoring settings.

4. Click the **Create List** button. You will be taken to a screen where you can add list items or upload a file.

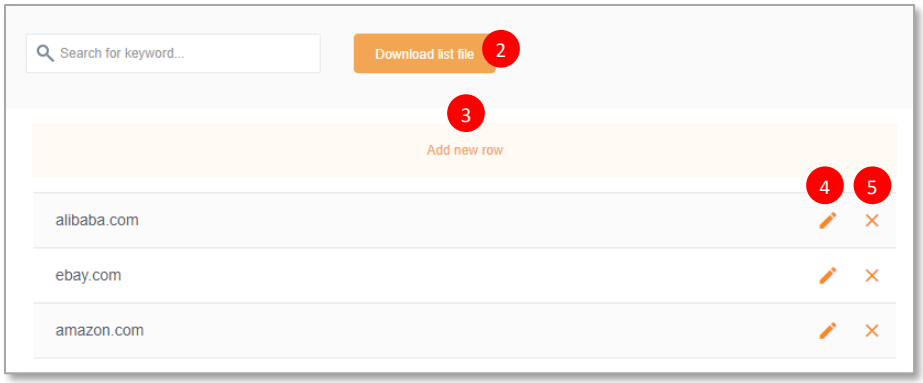


5. Click the **add file** button to upload a .CSV or .TXT file containing your list item. Each item should be in a separate line in the file for Teramind to import it correctly.
6. You can also click the **Add new row button** to enter items manually one by one.
7. If you've entered an item manually, click the **Save** button to save it.

11.7.3 Editing a Shared List



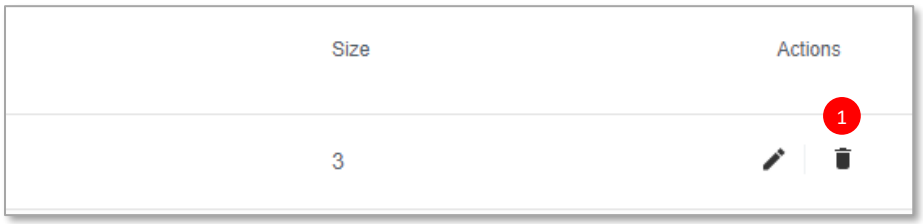
1. Click the **Pencil** button at the right side of a shared list. You will be taken to a screen where you can edit the list.



2. To download a copy of the list, replace the list or to append news items to a list from a file; click the **Download list file** button.
3. To add a new item/row, click the **Add new row** button.
4. To edit an item/row, click the **Pencil** button.

5. To delete an item/row, click the button.

11.7.4 Deleting a Shared List



6. Click the **Trash Can** button at the right side of a shared list to delete/remove it.

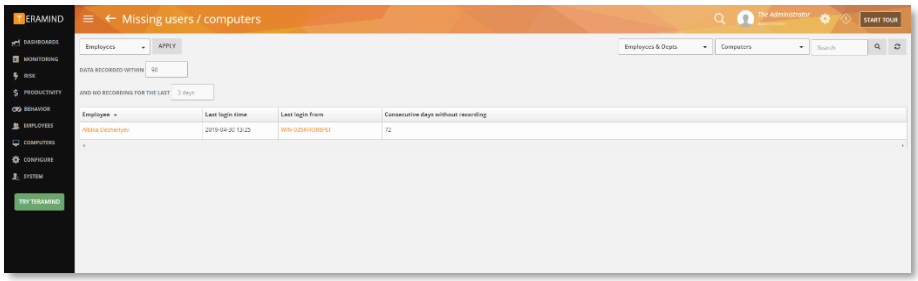
12 System

12.1 Introduction to the System

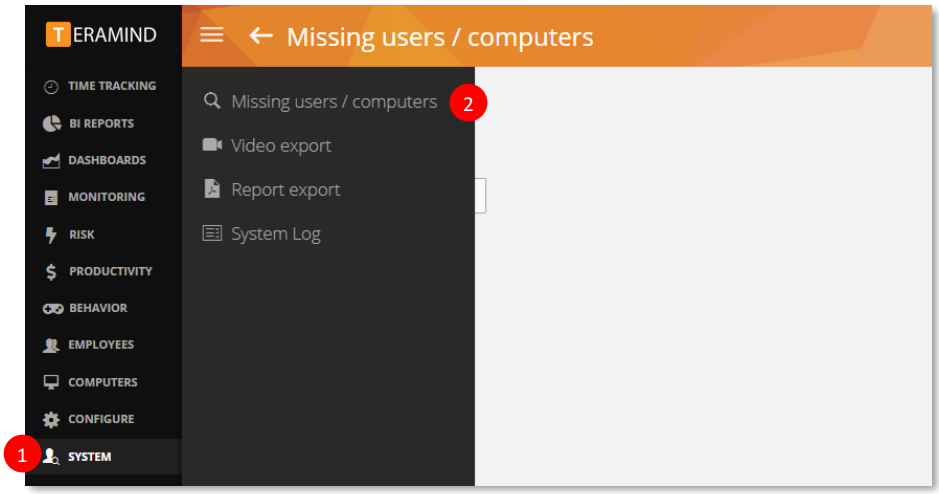
The System menu allows you to view any missing users/computers and view the system activities log.

12.2 Missing Users / Computers

The Missing Users / Computers report shows employees or computers for which Teramind didn't receive any data recording for the specified days. The report shows the following columns: Employee/computer, Last login time, Last login from and Consecutive days without recording.

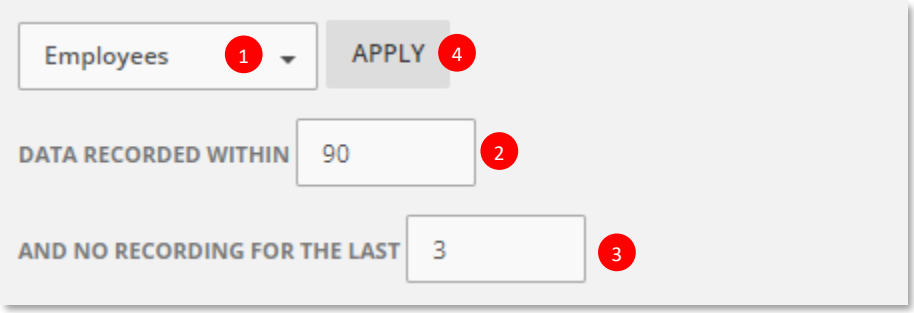


12.2.1 Accessing the Missing Users / Computers Menu



5. Hover your mouse over the **SYSTEM** menu, then
6. Select **Missing users / computers** from the sub-menu.

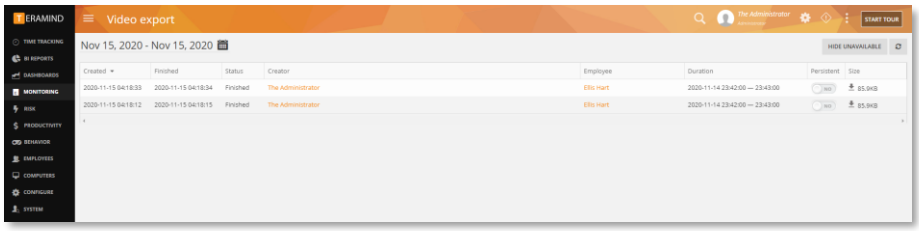
12.2.2 Searching for Missing Users / Computers



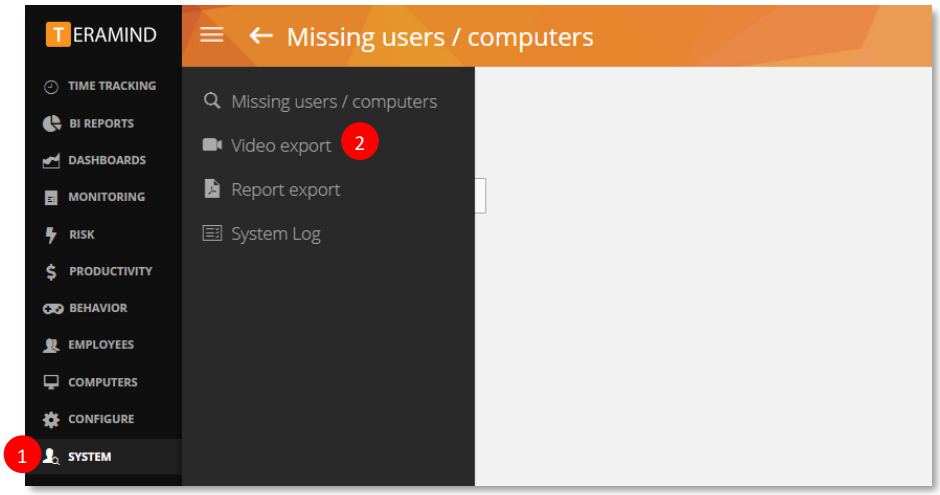
1. Select from Employees/Computers from the top-left corner of the screen.
2. Specify number of days for **DATA RECORDED WITHIN** field.
3. Specify number of days for **AND NO RECORDING FOR THE LAST** field.
4. Click the **APPLY** button to apply the filter and view the result.

12.3 Video Export

From this screen you can view a list of all videos exported from the Session Player and download them.

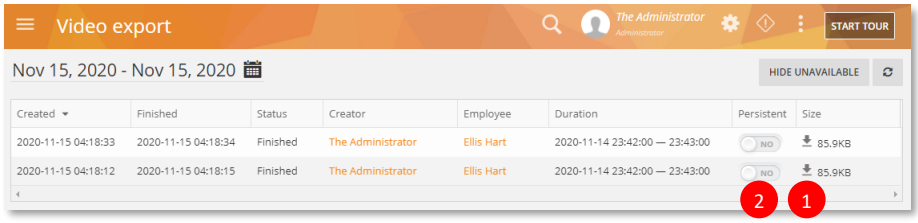


12.3.1 Accessing the Video Export Menu



7. Hover your mouse over the **SYSTEM** menu, then
8. Select **Video export** from the sub-menu.

12.3.2 Downloading Exported Videos



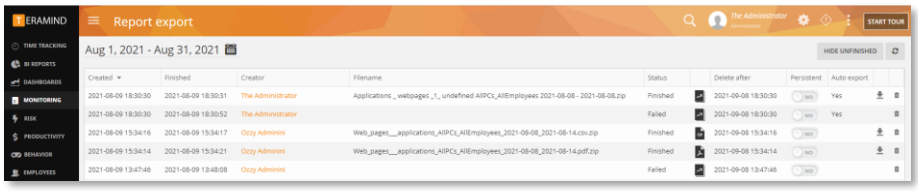
For each exported video, you can view information such as when the video was created, by whom and for which employee etc.

1. Click the **Download** icon under the *Size* column to download a MP4 file for the video.
2. If you are on an On-Premise deployment, you will also see a **Persistent** option. You can enable the Persistent option to keep a file indefinitely. Otherwise it will be deleted after 10 days automatically.

> Cloud customers will have access to the exported videos for up to 10 days. On-Premise / Private Cloud customers have the ability to make them persistent (keep for as long as they want) by enabling the *Persistent* option.

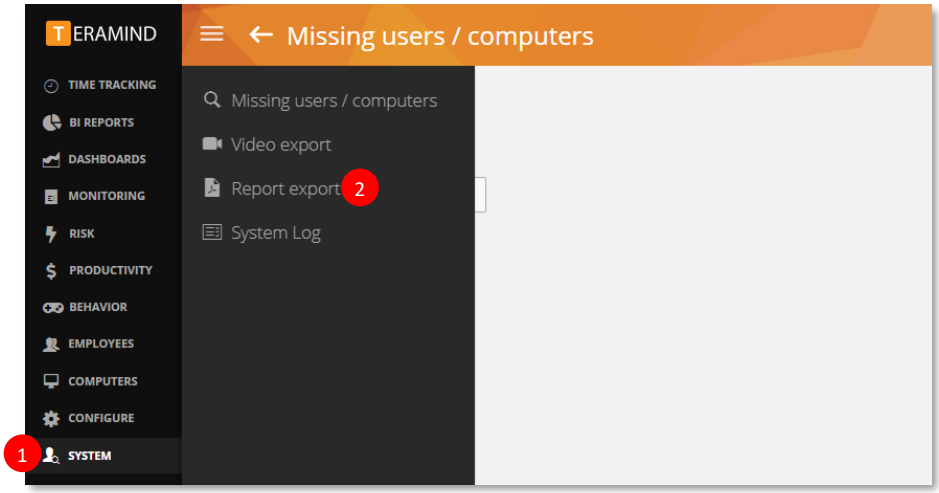
12.4 Report Export

From this screen you can view a list of all the reports exported from the Monitoring Reports and the BI Reports and download them.



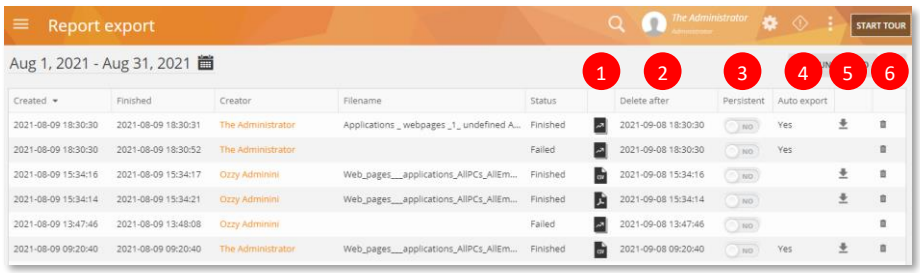
> Exported reports from the Behavior > Alerts and Productivity > Overview screens are not available for download from this Report Export screen. Exports from those screens starts immediately and are not saved for later downloads.

12.4.1 Accessing the Report Export Menu



9. Hover your mouse over the **SYSTEM** menu, then
10. Select **Report export** from the sub-menu.

12.4.2 Downloading / Deleting Exported Reports



For each exported report, you can view information such as when the report was created, filename etc.

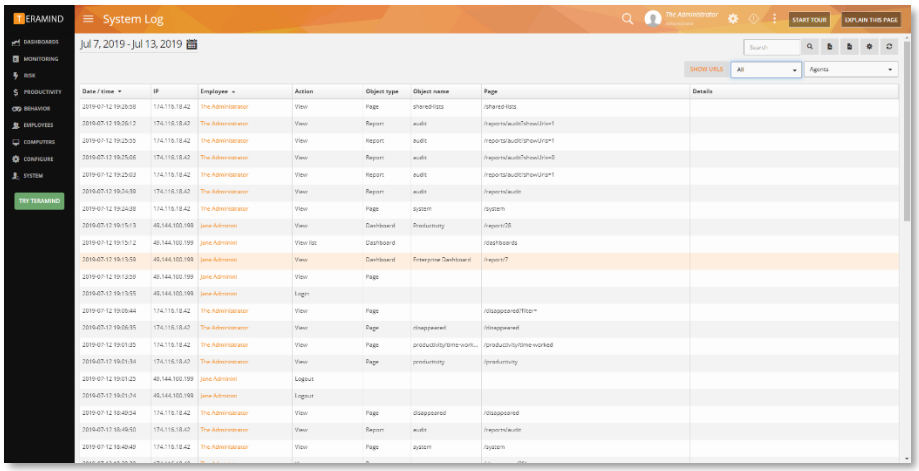
1. The **icons** column will tell you if it is an export from the *Monitoring Reports* (PDF / CSV) or *BI Reports* (BI) export.
2. Unless deleted by you, Cloud customers will have access to the exported reports for up to 30 days. The **Delete after** column shows when the report will be deleted automatically.
3. On-Premise / Private Cloud customers have the ability to make the reports persistent (keep for as long as they want) by clicking the **Yes**/**No** button on the *Persistent* column.
4. The **Auto export** column will tell you if it is part of an auto-export report.
5. Click the **Download** icon on a row to download a Zip file containing the report.
6. Click the **Trash Can** icon on a row to delete the report.

12.5 System Log

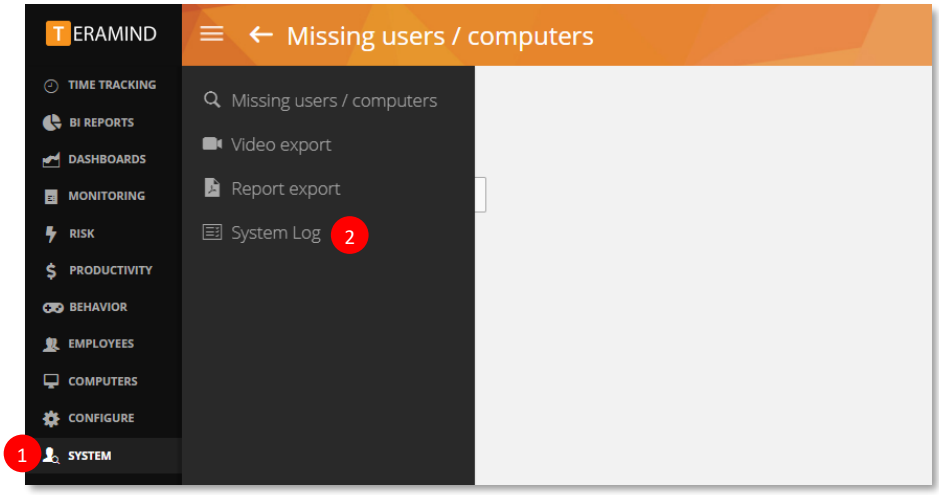
The System Log screen allows you to see all administrator/manager activities on the Teramind Dashboard. These immutable session logs are useful for monitoring privileged users' activities and identify any abuse of the system. Additionally, session logs, in conjunction with access control and other auditing and forensics features of Teramind allows you conform with compliance standards such as GDPR, HIPAA, PIC DSS etc.

The Session Log report has the following columns:

- **Date/time:** the data and time of the activity.
- **IP:** IP location of the user.
- **Employee:** name of the user/employee.
- **Action:** what action the user performed. For example, *Login*, *Logout*, *View*, *Delete* etc.
- **Object Type:** the type of object the user accessed. For example, *Report*, *Dashboard*, *Shared* etc.
- **Object Name:** internal names of the object. For example, *Productivity*, *Audit* etc.
- **Page:** the URL of the object. Only displayed when SHOW URLS filter is turned on. See the Applying System Log Filters section below for more information)
- **Details:** where applicable, displays any additional information about an activity. Such as, *Inserted an item (in a List)*, *Created a Network Shared List* etc.

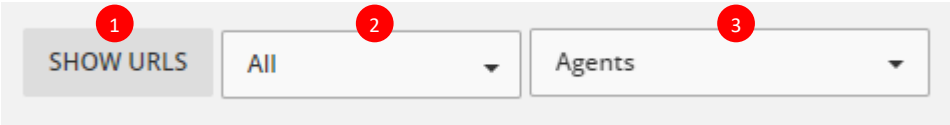


12.5.1 Accessing the System Log Menu



11. Hover your mouse over the **SYSTEM** menu, then
12. Select **System Log** from the sub-menu.

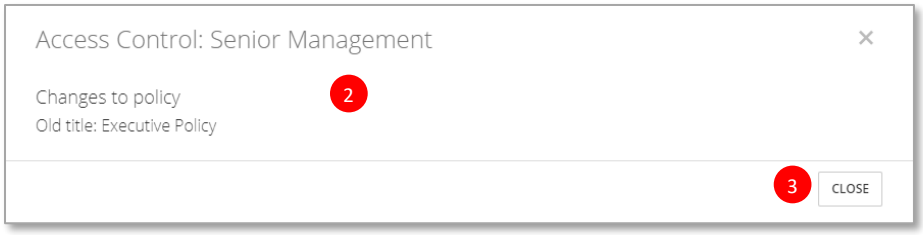
12.5.2 Applying System Log Filters



1. Click the **SHOW URLS** button near the top-right corner to turn it on/off. When on, the system log report will display an additional column, 'Page' with the exact URL of the dashboard object.
2. By default, the report displays all types of activities. However, you can use the **Activity** filter to display the logs for a single activity.
3. By default, the report displays all agents/users. However, you can use the **Agent** filter to display the logs for a single agent/user.

12.5.3 Viewing Additional Details for a Log

1. If a log object has additional details that cannot be shown in the *Details* column, you will see a **Click here to view details** link. Clicking the link will open a pop-up window.



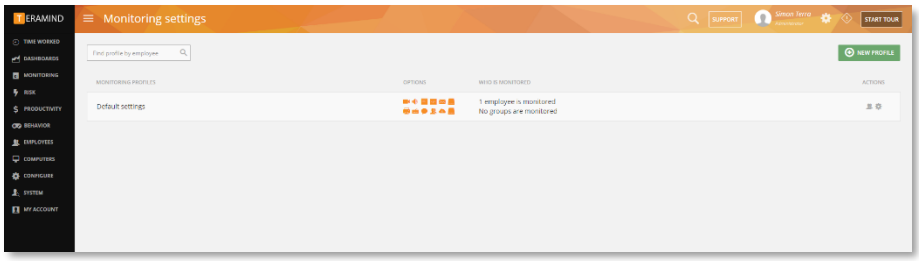
2. You can view the details on the pop-up window. For example, on the image above, it shows that and administrator changed the name of an Access Control policy from 'Executive Policy' to 'Senior Management'.
3. Click the **CLOSE** button to close the pop-up window and return to the Session Log report.

13 Dashboard Settings

The Dashboard Settings menu lets you configure various parts of Teramind, including monitoring, integrations, Agent defaults, server management, login screen etc.

13.1 Monitoring Settings

The Monitoring Settings screen lets you create/edit monitoring profiles for users, groups and departments and precisely control how much information will be collected for each monitored system (such as Websites, Apps, Emails). You can track as much or as little as you want based on your organization's needs and alleviate any privacy concerns.



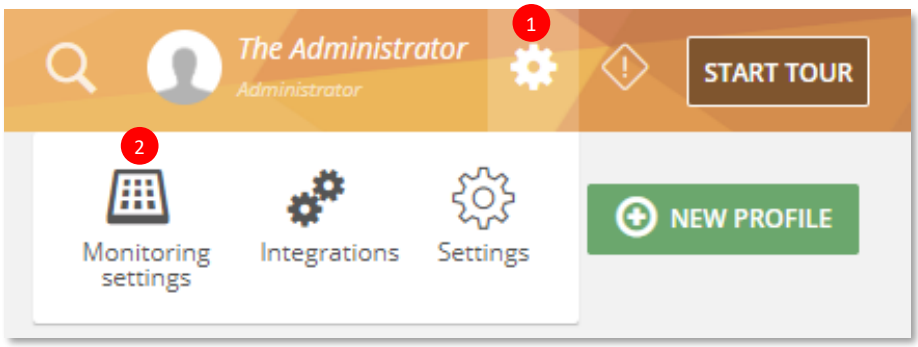
Some use cases of using Monitoring Settings are:

- Create Monitoring Profiles to enable social media monitoring for the marketing department but disable it for other departments.

- Configure the Websites so that it automatically suspends monitoring and keystrokes logging when users visit their bank's portal or opens their personal emails.
- Setup Applications monitoring in such a way that it only records activity within business applications such as QuickBooks or SAP and not record screen or keystrokes when the user is in Facebook.
- Setup a scheduled based monitoring, set up recording rule violations only, auto-delete old recordings etc. to minimize data storage requirements and comply with regulations like GDPR.

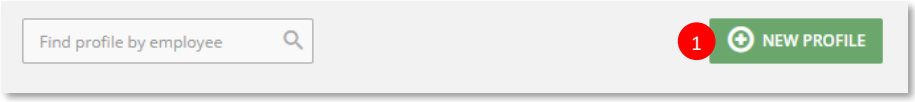
Teramind comes with a *Default settings* profile. This profile is used by default for all users and cannot be deleted.

13.2 Accessing the Monitoring Settings Menu

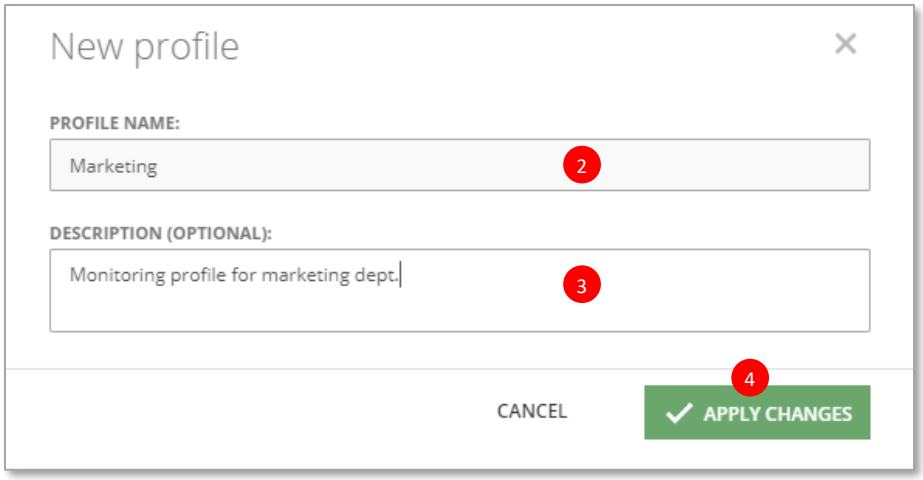


1. Click the **Gear** icon near the top-right corner of the Teramind Dashboard.
2. Click **Monitoring setting** underneath the pop-up menu.

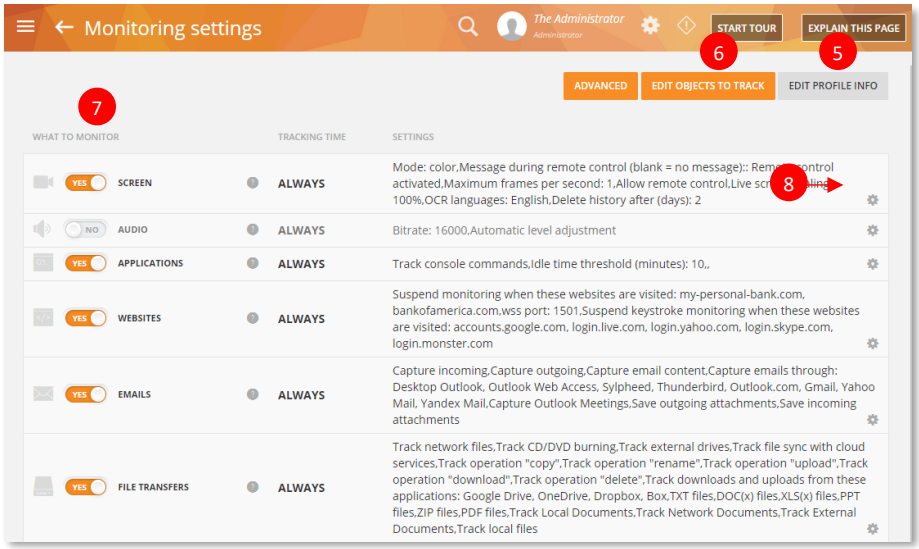
13.3 Creating a New Monitoring Profile



1. Click the **NEW PROFILE** button near the top-right corner of the main Monitoring Settings screen. A pop-up window will be displayed.



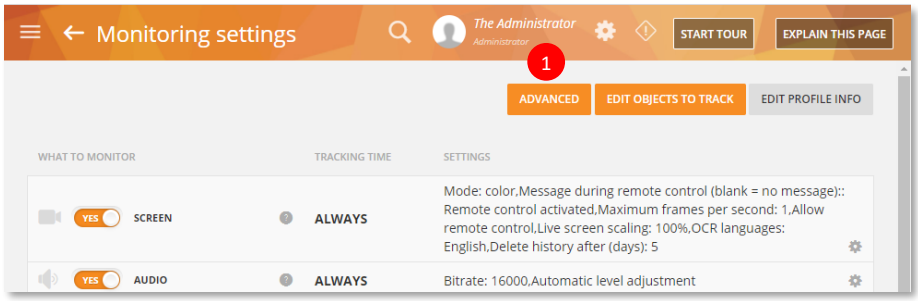
2. Give the profile a name.
3. Optionally, give it a description.
4. Click **APPLY CHANGES**. You will be taken to a different screen with a list of all monitored systems.



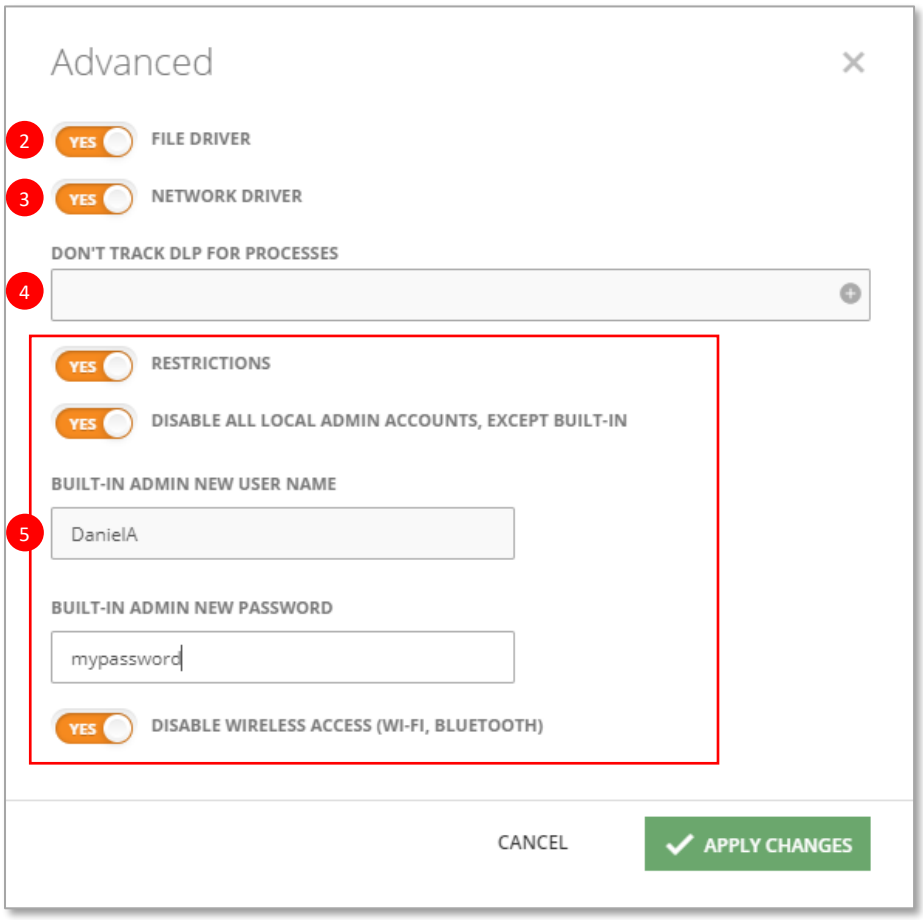
Note that, Teramind comes with some default settings for each of the monitored systems. You can change them according to your needs.

5. Click the **EDIT OBJECTS TO TRACK** button at the top-right corner to add users to the profile or remove them.
6. Click the **EDIT PROFILE INFO** button at the top-right corner to edit the profile name and description.
7. Click the **YES/NO** slider button in front of a monitored system to turn monitoring on or off for it.
8. Click the small **Gear** icon at the right side of an object to edit its settings. See the [Editing the Settings for Monitored Systems] section below to continue setting up individual monitoring objects).

13.3.1 Advanced Monitoring Settings



1. Click the **ADVANCED** button to change advanced settings (only recommended if you are troubleshooting an issue). This will pop up a window:

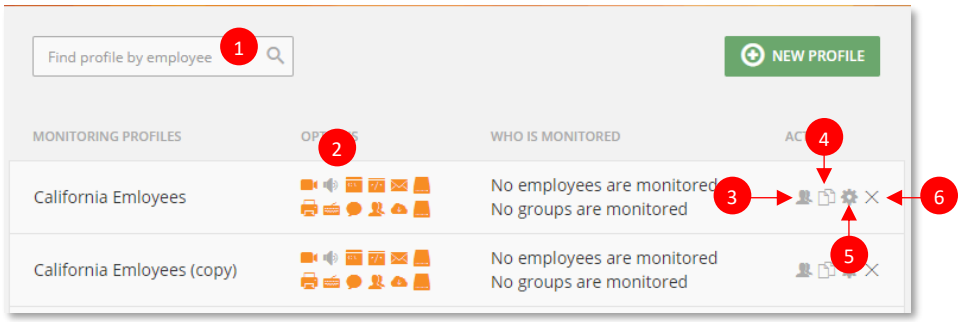


2. *FILE DRIVER*: if disabled, File Transfer report, Content Sharing Rules, Files-Based Activity etc. will not work.
3. *NETWORK DRIVER*: if disabled, Network report, IM report, Network-Based Rules, File Upload rules will not work. 'Quick web proxy' certificate will not be injected.
4. *DON'T TRACK DLP FOR PROCESSES*: allows you to exclude certain process(es) from the DLP scanning/DLP rules. For example, `svchost.exe`, `System Idle Process` etc. Note that, this is different than disabling monitoring for an application using the SUSPEND MONITORING

WHEN THESE APPLICATIONS ARE USED option on the Applications Monitoring Settings. That option disables all monitoring for a process (activity will not be captured and app will be blacked out on the session recording). On the other hand, DON'T TRACK DLP... will only disables DLP scanning for a process.

5. If you enable the *RESTRICTIONS* option, you will see two more options:
    - If you turn on the *DISABLE ALL LOCAL ADMIN ACCOUNTS, EXCEPT BUILT-IN* option, you can specify a new admin user and password. Then, when a admin logs in as a current Windows user, a new admin will be created and all existing admin accounts will be disabled.
    - If you turn on the *DISABLE WIRELESS ACCESS (WI-FI, BLUETOOTH)* then all Wi-Fi and Bluetooth network access will be disabled. Make sure the computer has an Ethernet connection before enabling!

13.4 Editing / Copying / Deleting a Monitoring Profile

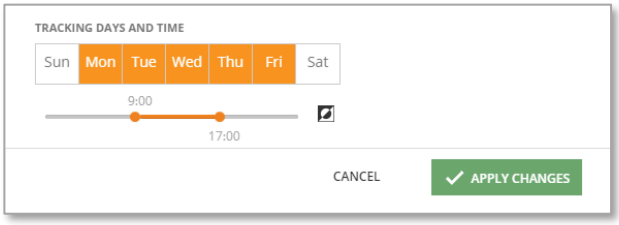


1. You can locate which profile an employee belongs to by using the **Search** box at the top-left corner of the main Monitoring Settings screen.
2. You can click the **OPTIONS** icons to turn the monitoring on/off for them.
3. Click the small **Users** icon at the top-right corner to add/remove users.
4. Click the **Copy** icon to create a duplicate copy of the profile.
5. Click the small **Gear** icon at the right site of a profile to edit it. Follow **Steps 5-6** in the Creating a New Monitoring Profile section to learn how to edit the profile.
6. Click the small × icon to delete the profile.

13.5 Editing the Settings for Monitored Systems

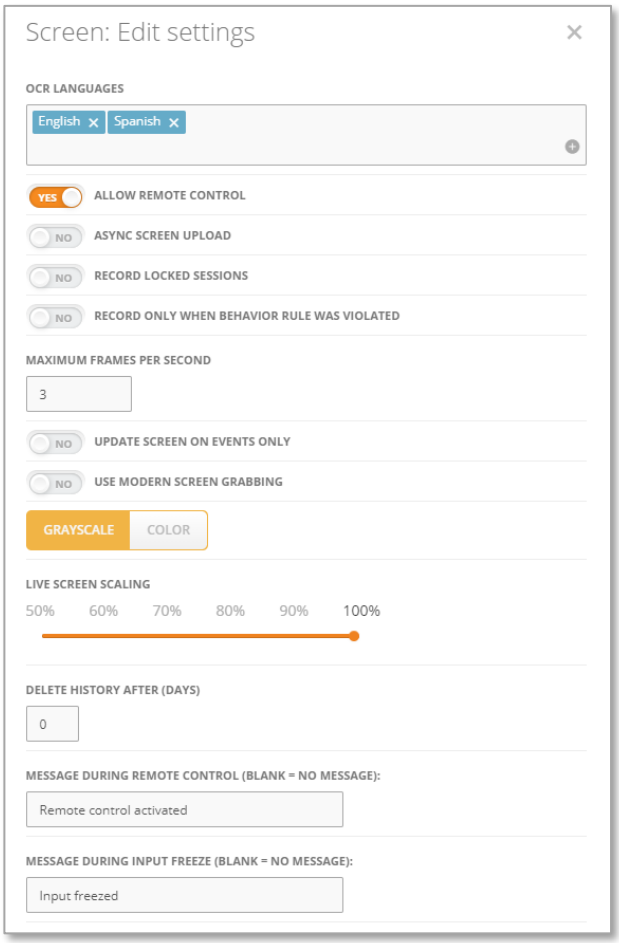
13.5.1.1 Common Settings

Each Monitored System has a simple scheduler under the TRACKING DAYS AND TIME section at the bottom of its settings panel. Using this scheduler, you can quickly specify when the tracking and recording of the Monitored System will take place.



Click on a day to enable/disable it. Drag the two **slider ends** • to adjust the time. Click the **Reverse** icon to reverse the time. Click **APPLY CHANGES** to save the settings.

13.5.1.2 Editing Screen Settings



The OCR LANGUAGES allows you to specify which language will be used for the OCR. Default is English. Teramind also supports Hebrew, Russian, Dutch, Spanish and Turkish for the OCR.

ALLOW REMOTE CONTROL option determines if Remote Control will be available on the Session Player's Live Mode Controls.

If the user is using a Hidden Agent, ASYNC SCREEN UPLOAD will force Teramind to use a queue for screen recordings instead of uploading them in real-time. It's suitable for a slower network or a busy OCR server. However, you might experience some delay between the user activity and the recording appearing on the dashboard when ASYNC is enabled.

RECORD LOCKED SESSIONS option allows you to continue recording even when the user locked their computer.

By enabling RECORD ONLY WHEN BEHAVIOR RULE WAS VIOLATED, you can reduce the storage needed for the screen recordings or alleviate privacy concern.

You can also control how many FRAMES PER SECOND is captured; if Teramind should UPDATE SCREEN ON EVENTS ONLY (i.e. something happening on the screen).

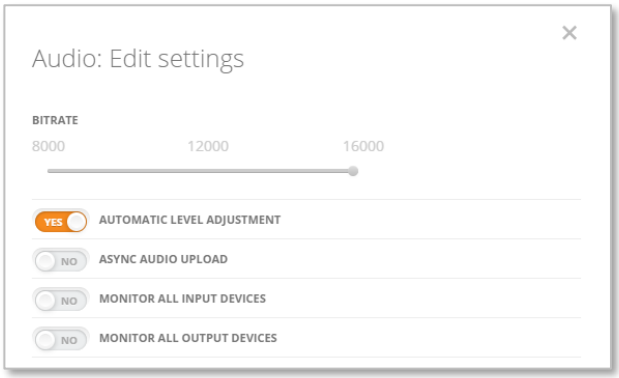
You should only enable the USE MODERN SCREEN GRABBING option on Windows 8 or above. If you are experiencing issues with screen captures, try toggling this option.

The GRAYSCALE / COLOR and LIVE SCREEN SCALING controls the quality and size of the recording.
On-Premise customers can specify when the recordings will be automatically deleted under the DELETE HISTORY AFTER. This will further reduce your storage requirements and help you comply with data retention policies.

Finally, you can specify the MESSAGE DURING REMOTE CONTROL / MESSAGE DURING INPUT FREEZE when using those features in the Session Player's Live Mode Controls.

ASYNC SCREEN UPLOAD only works with the Hidden Agent, ignore for Revealed Agents.

13.5.1.3 Editing Audio Settings



AUTOMATIC LEVEL ADJUSTMENT will automatically adjust the sound levels for higher/lower tones.

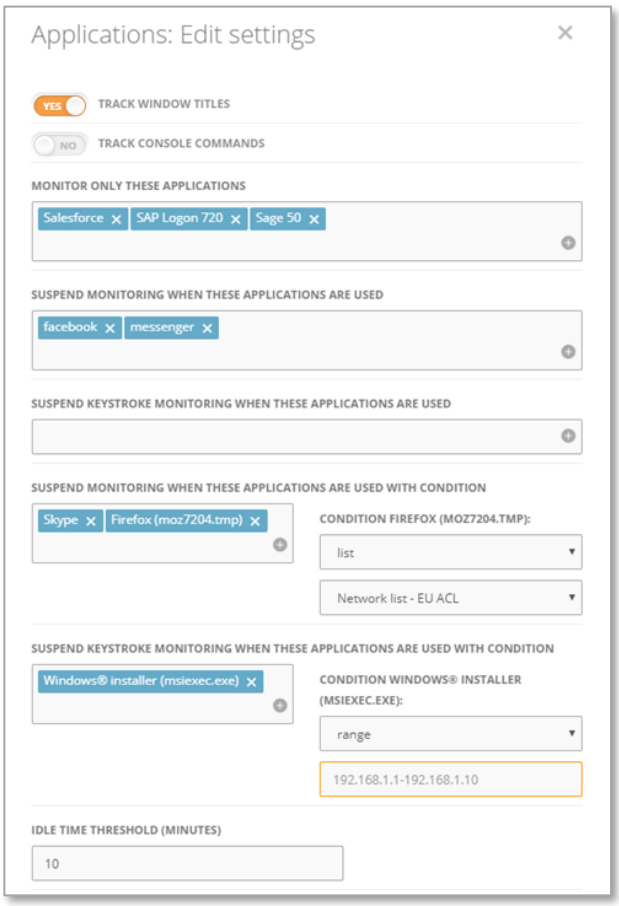
If the user is using a Hidden Agent, ASYNC AUDIO UPLOAD will force Teramind to use a queue for audio recordings instead of uploading them in real-time. It's suitable for a slower network or a busy server. However, you might experience some delay between the user activity and the recording appearing on the dashboard when ASYNC is enabled.

You can adjust the BITRATE to increase/decrease audio quality. Lower bitrate will require less CPU processing and storage.

You can toggle the MONITOR ALL INPUT DEVICES / OUTPUT DEVICES options to enable/disable recording for all microphones, speakers and line-in/out.

ASYNC AUDIO UPLOAD only works with the Hidden Agent, ignore it for the Revealed Agents.

13.5.1.4 Editing Applications Settings



You can turn monitoring on/off for the WINDOW TITLES. This gives you the ability to not track the title for apps which includes document name in their title. If you do not want Teramind to capture the document name, turning this option off can be helpful.

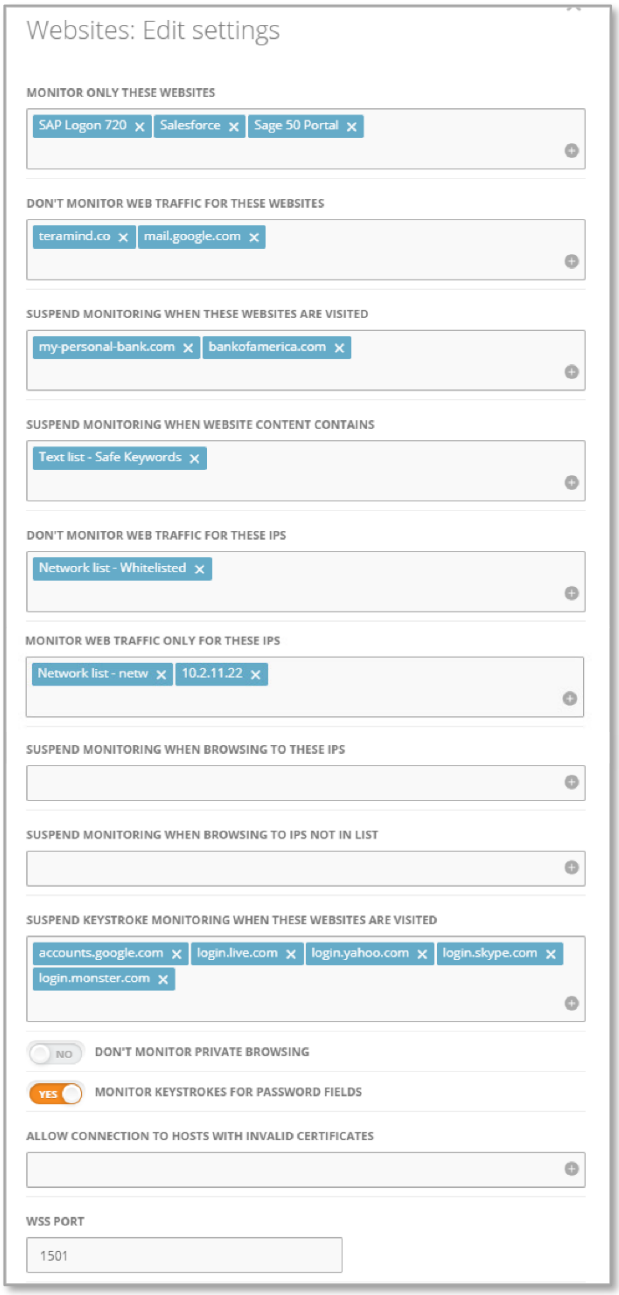
You can also turn monitoring on/off for CONSOLE COMMANDS (commands executed on the Windows Command Prompt or Terminal).

You can configure Applications settings to MONITOR only select applications; SUSPEND monitoring or SUSPEND KEYSTROKE monitoring when certain applications are used.

You can conditionally suspend monitoring/keystrokes logging using the two …WITH CONDITION options. For example, you can suspend monitoring Firefox while it's used from an IP approved by an access control *list*. Same way, you can suspend keystrokes logging of the Windows Installer when it's launched from an IP *range*. For the CONDITION, you can select from a list of *Any*, a single *IP*, an *IP range*, *list* (Network Shared Lists), and *cldr* (Classless Inter-Domain Routing).

Finally, you can define the IDLE TIME (used in the Productivity report, Agent Schedule-based rules and other places by Teramind).

13.5.1.5 Editing Websites Settings



MONITOR ONLY THESE WEBSITES field allows you to define websites or a list of websites, for which you want to record the screen and keystrokes. If you use this field, all other websites will be blacked-out in the recordings.

DON'T MONITOR WEB TRAFFIC FOR THESE WEBSITES* defines the websites for which you want to suspend recording. Screen and keystroke recording for all other sites will be enabled. *Please see notes below*.

SUSPEND MONITORING WHEN THESE WEBSITES ARE VISITED* does not capture any activity, and keystrokes when the specified websites are visited. The browser window is blacked-out in the video recording or during the live view mode of the session player.

SUSPEND MONITORING WHEN WEBSITE CONTAINS CONTENT - If the HTML of a URL contains a string listed here, that website will not be monitored, keystrokes will not be recorded, and the screen will be blacked out. A common use for this option is to determine intranet or proxy-generated websites.

The DON'T MONITOR WEB TRAFFIC FOR THESE IPS* lets you specify IPs, IPs with mask, or domain names (excluding the `http://` or `https://` prefix) that you do not want to monitor.

The MONITOR WEB TRAFFIC FOR THESE IPS is the exact opposite of the 'DON'T MONITOR WEB TRAFFIC FOR THESE IPS' option. Note

that, if you use this option, all other websites will be blacked out in the screen recordings.

Please be careful when using the two options above. You may accidentally turn monitoring on/off for other sites, as there may be several sites with the same IP.

The next three settings are the same as above, the only difference is, you use IP addresses instead of URLs. *Please see notes below*.

You can also SUSPEND KEYSTROKE … setting to suspend just the keystroke recordings.

You can suspend monitoring for all PRIVATE BROWSING (incognito) sessions.

You can turn off the MONITOR KEYSTROKES FOR PASSWORD FIELDS option to suspend capturing of keystrokes in password fields. For example, a login page containing a HTML input field such as `<input type="password">`.

ALLOW CONNECTION TO HOSTS WITH INVALID CERTIFICATES – please see notes below.

You can use the WSS PORT to specify web traffic redirection.

***SUMMARY OF WEBSITES EXCLUSION OPTIONS**

DON'T MONITOR WEB TRAFFIC FOR THESE WEBSITES

- Quick Proxy certificate IS injected
- Does NOT appear in the activity log
- Keystrokes ARE captured

SUSPEND MONITORING WHEN THESE WEBSITES ARE VISITED

- Quick Proxy certificate IS injected
- Does NOT appear in the activity log

- Keystrokes are NOT captured
- The browser window is blacked-out in the video recording or during the live view mode of the session player

DON'T MONITOR WEB TRAFFIC FOR THESE IPS

- Quick Proxy certificate is NOT injected
- DOES NOT appear in the activity log
- Keystrokes ARE captured

SUSPEND MONITORING WHEN BROWSING TO THESE IPS

- Quick Proxy cert is injected
- Appears in the activity log
- Keystrokes ARE captured

DON’T MONITOR WEBSITES / IPS

Use the DON'T MONITOR WEB TRAFFIC FOR THESE IPS / WEBSITES fields if you want to prevent the Teramind Agent from injecting the Quick Proxy SSL certificate. Use them if it looks like the agent's cert if causing an issue with a website.

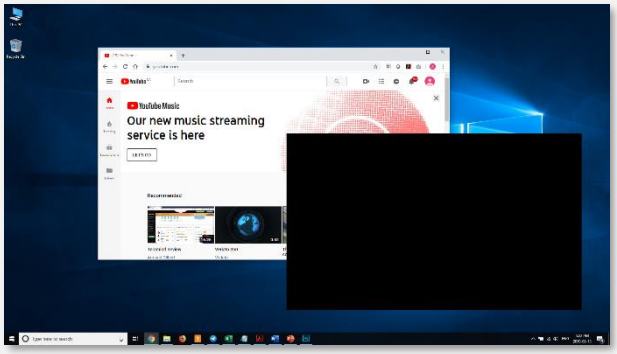
The difference between these two fields are:

- WEBSITES: if we include host name here, then Teramind will not intercept traffic from these sites. But in case of HTTPS we still inject HTTPS certificate and recode encrypted data. This may lead to network issues.
- IPS: this may contain IPs, IP with mask, or domain name of the site (excluding `http://` or `https://` prefix). For domains, it works by requesting list of IPs that corresponds to this domain. Please be careful that, when using this field, you may accidentally turn off monitoring for other sites, as there may be several sites with the same IP. If the IP is in this list, then Teramind will not recode encrypted data, and there will be no influence on the HTTPS traffic.

What sites to include in “DON’T MONITOR WEB TRAFFIC…”?

Site that resides on some domain name sometimes uses resources from other domains. To exclude all sources for the problem, you need to exclude all used resources. You can get a list of the domain names by turning off the Teramind Agent, run Chrome, Open “Developer Tools”, select “Network” tab, set “Disable cache” = true, “Preserve log” = true, right click on the header of the table with the network requests, select “Domain”, then reproduce situation that leads to an issue, and capture all domain names (from the Domain column) that were involved in the loading process.

Dynamic Blackout



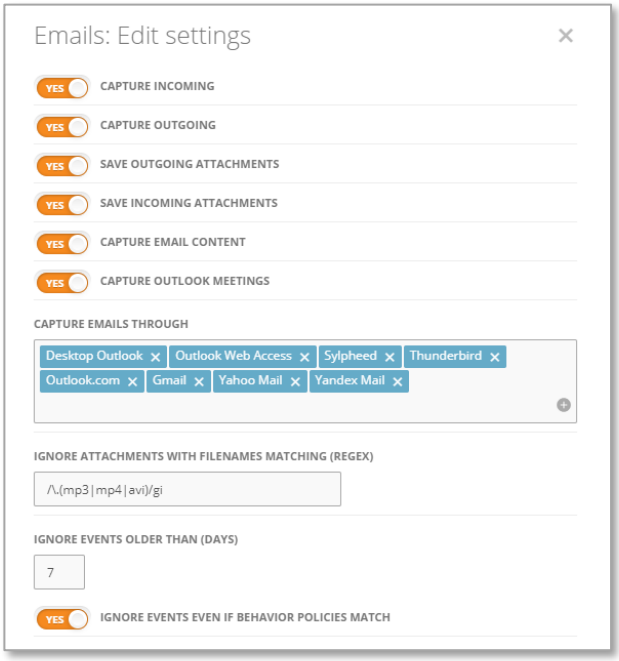
When you use any of the *SUSPEND MONITORING*… settings for any application or website, Teramind will automatically blackout the relevant application window in the video recording or during the live view mode of the session player (check out the Session Player section to learn more about session recording and live view).

The blackout feature works on both single monitor and multi-monitor setups.

ALLOW CONNECTION TO HOSTS WITH INVALID CERTIFICATES

Use the ALLOW CONNECTION TO HOSTS WITH INVALID CERTIFICATES will allow all hosts to work with invalid certificates. This is not a recommended thing to do as it may help disguise invalid certificate and allow phishing attacks. As an alternative, you can also use a Match Regular Expression condition `regexp/.*/` on any rules that require an URL/website address such as below:

13.5.1.6 Editing Email Settings



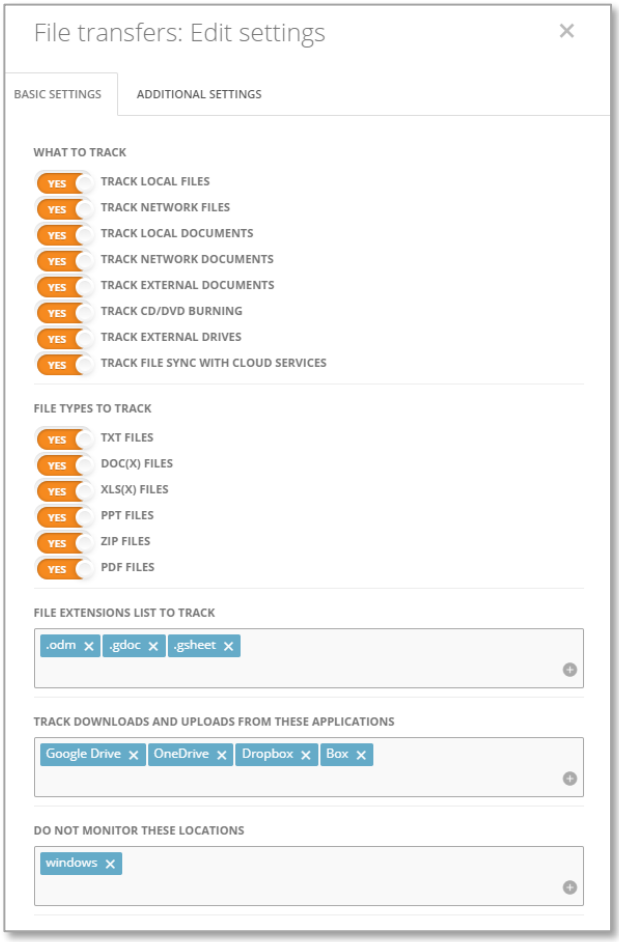
You can use the settings to CAPTURE INCOMING / OUTGOING emails, CAPTURE EMAIL CONTENT and SAVE OUTGOING / INCOMING ATTACHMENTS etc.

You can specify which email systems will be captured using the CAPTURE EMAIL THROUGH option. Teramind supports the most popular email clients such as Outlook, Gmail, Yahoo etc. - both desktop and web versions.

You can use regular expressions to ignore any attachments you do not want captured using the IGNORE ATTACHMENT... option. For example, to ignore music and video files, you can use something like this:
`/\.(mp3|mp4|avi)/gi`

The IGNORE EVENTS OLDER THAN (DAYS) option allows you to cut off monitoring and capturing of emails older than certain days. This option is sometimes useful for clients like Outlook which may scan older emails if emails are moved, or archival policies are run. In such situations, by default, the Agent will capture any emails being accessed. This setting tells the Agent to ignore scanning older emails. However, behavior policies or rules for these old emails will still get triggered which might create false positives.
To avoid that, you can enable the IGNORE EVENTS EVEN IF BEHAVIOR POLICIES MATCH option. This will prevent triggering of unexpected rule violations and false alerts by ignoring older emails.

13.5.1.7 Editing File Transfers Settings

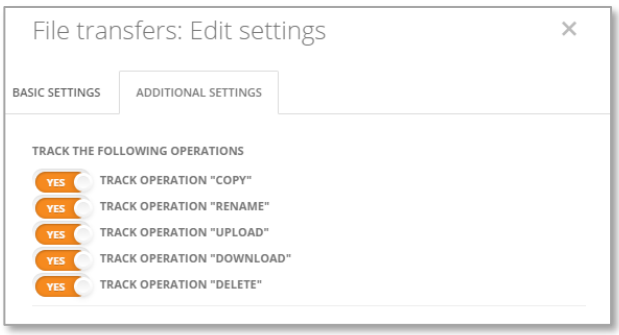


Files Transfers settings panel has two tabs. On the **BASIC SETTINGS** tab, you can specify WHAT TO TRACK such as: LOCAL FILES, NETWROK FILES, LOCAL DOCUMENTS, NETWORK DOCUMENTS, EXTERNAL DOCUMENTS, CD/DVD BURNING, EXTERNAL DRIVES (i.e. USB / pen drives) etc.

You can select which file types to track under the FILE TYPES TO TRACK section. For example, TXT, DOC, XLS, PPT etc. You can also manually enter your own extensions in the FILE EXTENSIONS LIST TO TRACK.

You can specify which applications should be monitored for upload/download activities in the TRACK DOWLOADS AND UPLOADS FROM THESE APPLICATIONS field.

Finally, if you don't want any locations (i.e. folders) to track, you can specify them in the DO NOT MONITOR THESE LOCATIONS field.

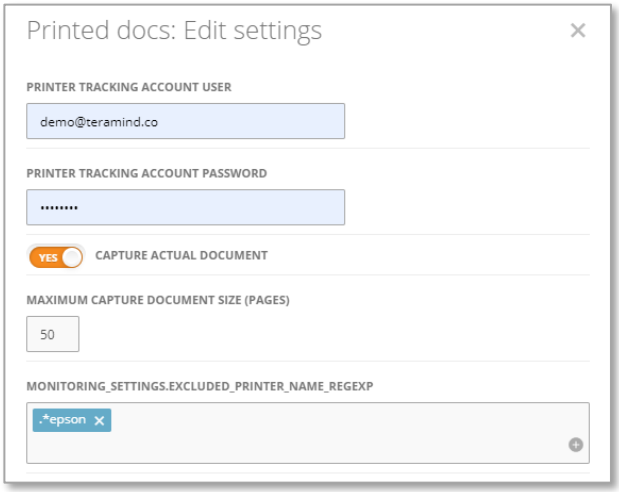


On the **ADDITIONAL SETTINGS** tab, you can specify which file operations to track such as COPY (see notes below), RENAME, UPLOAD, DOWNLOAD, DELETE etc.

Note that Teramind cannot track the copy operation for a file from one network server to the same network server (e.g. source and destination is the same). For example, copying of a file from `\\103.247.55.101\source` to `\\103.247.55.101\destination` cannot be tracked. Copy to and from same local drives is detected as usual.

Also copying of an empty file cannot be tracked since it will be impossible for the system to distinguish between the file *create* and *copy* operations due to the zero size of the file.

13.5.1.8 Editing Printed Doc / Printer Settings



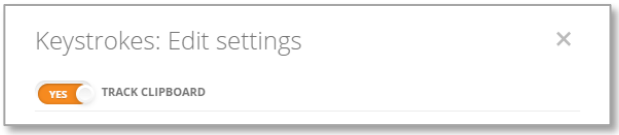
If you use a printer that requires login permission, use the PRINTER TRACKING ACCOUNT USER and the TRACKING ACCOUNT PASSWORD to specify the credentials. Otherwise, Teramind will not be able to monitor it.

You can turn CAPTURE ACTUAL DOCUMENT on/off and specify MAXIMUM CAPTURE DOCUMENET SIZE (no. of pages) too.

With the MONITORING_SETTINGS_EXCLUDED… option , you can add regular expressions to exclude any printers matching the name.

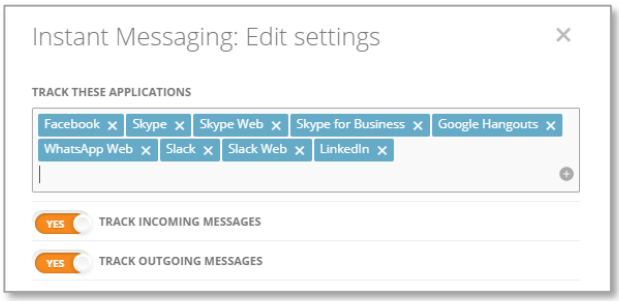
You can automatically clean the print spooler for a print server from the [Computer's details > Computer settings]screen.

13.5.1.9 Editing Keystrokes / Key Logging Settings



You can turn CLIPBOARD tracking on/off from the Keystrokes settings panel.

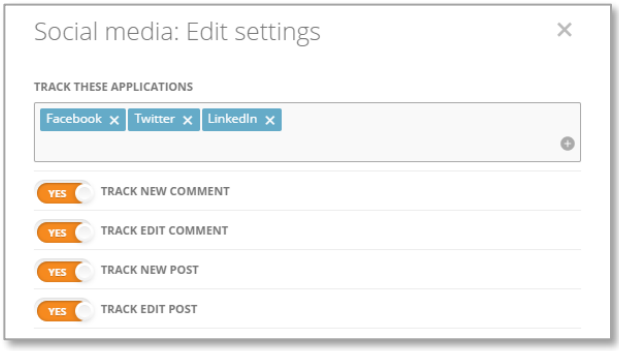
13.5.1.10 Editing Instant Messaging / IM Settings



You can specify which messaging APPLICATIONS to track. Teramind supports the popular IMs such as Facebook, Skype, Slack etc.

You can TRACK INCOMING MESSAGES only or TRACK OUTGOING MESSAGES only or both.

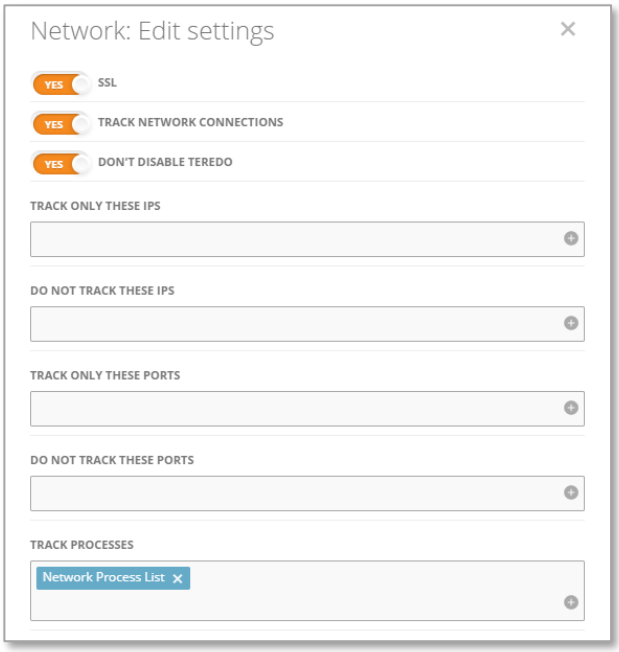
13.5.1.11 Editing Social Media Settings



You can specify which messaging APPLICATIONS to track. Teramind supports the popular social media platforms such as Facebook, Twitter, LinkedIn etc.

You can track NEW COMMENT, EDIT COMMENT, NEW POST, EDIT POST activities in those applications.

13.5.1.12 Editing Network Settings



You can turn SSL on to monitor secure connections (i.e. HTTPS).

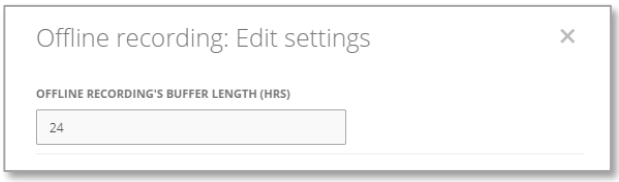
TRACK NETWORK CONNECTIONS option allows you turn network monitoring on/off.

DON'T DISABLE TEREDO prevents Teramind from disabling Teredo. It's used for secure communication over IPv6. If you encounter any problem with IP tracking, try toggling this setting.

The next four TRACK… options let you specify which IPs and ports will be tracked or not.

TRACK PROCESSES field allows you to specify which network processes to track. You can use names (i.e. *svchost.exe*), regular expressions, Network Shared Lists etc.

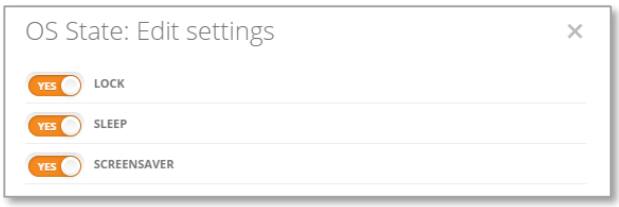
13.5.1.13 Editing Offline Recording Settings



The offline recording buffer specifies how long the Teramind Agent will continue to record user actions while the user is disconnected from the internet or Teramind server. By default, the buffer is set to 24 hours, but you can increase or decrease the time as needed.

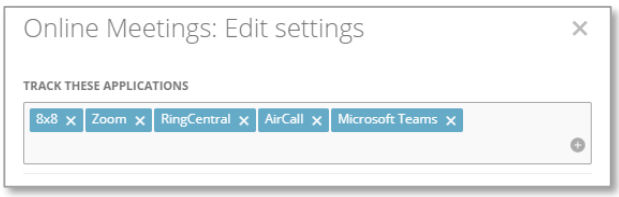
Note that, currently only the Hidden Agent on Windows supports offline recording.

13.5.1.14 Editing OS State Settings



These settings will enable event notifications for operating system states such as Lock, Sleep and Screen Saver to any SIEM integration (syslog event) you might have. These settings do not affect the monitoring of these event.

13.5.1.15 Editing Online Meetings Settings

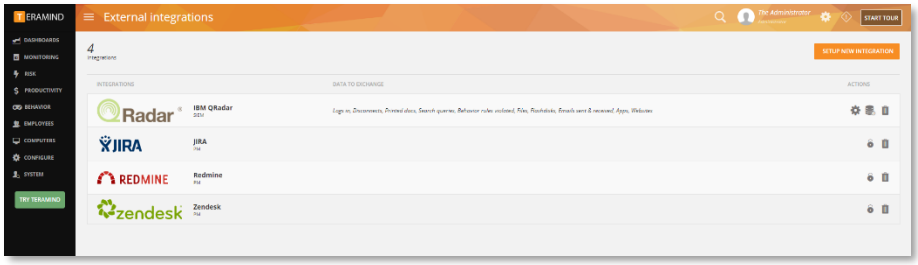


With these settings, you can specify which online meeting apps to track. Teramind supports monitoring of AirCall, Microsoft Teams, RingCentral, Zoom, 8x8.

13.6 Integrations

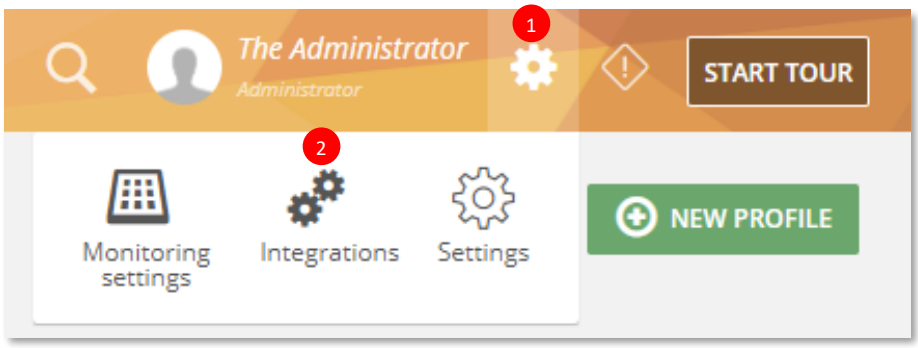
Integrations menu allows you to set up an integration with external Security Information and Event Management (SIEM) and Project Management (PM) software such as HP ArcSight, Splunk, IBM QRadar, LogRhythm, Jira, Redmine, Zendesk etc. You can then send user details and event triggers from Teramind to the integrated software.

.



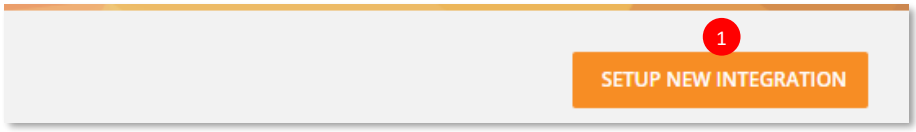
The main Integrations screen shows you a list of current integrations. From here you can also create a new integration, change the settings of an integration or remove an integration when no longer needed.

13.6.1 Accessing the Integrations Menu

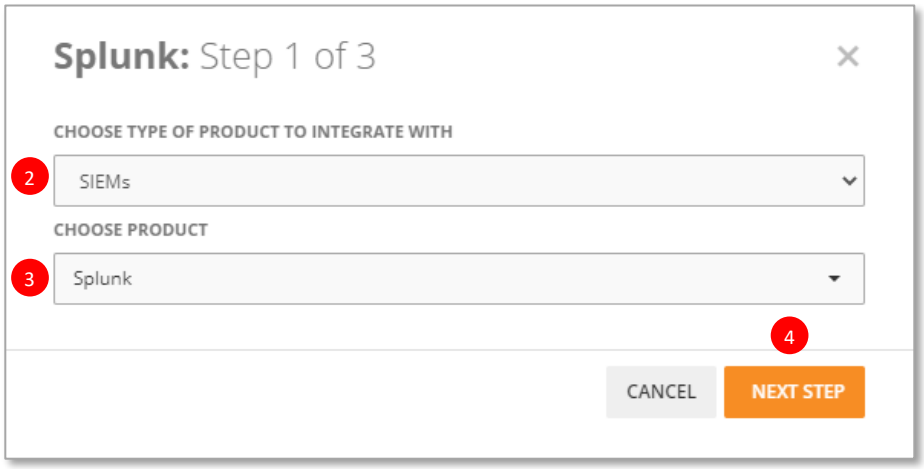


3. Click the **Gear** icon near the top-right corner of the Teramind Dashboard.
4. Click **Integrations** underneath the pop-up menu.

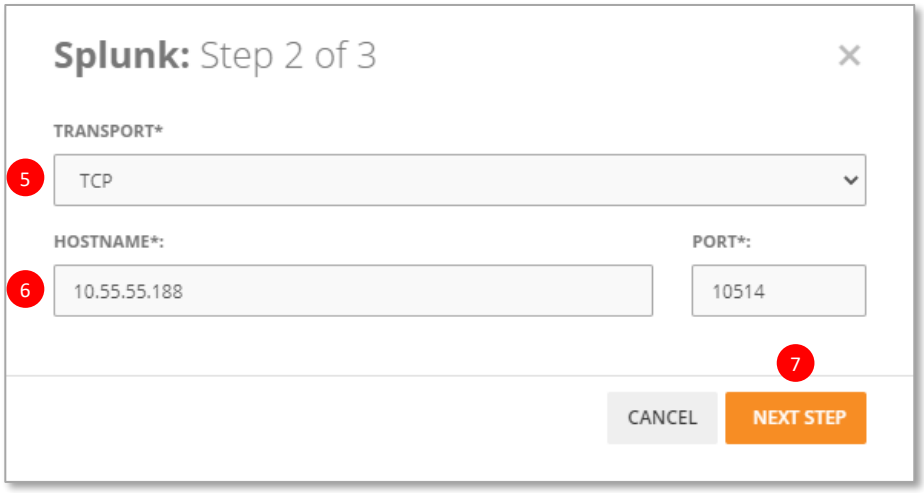
13.6.2 Setting Up a New SIEM Integration with Splunk



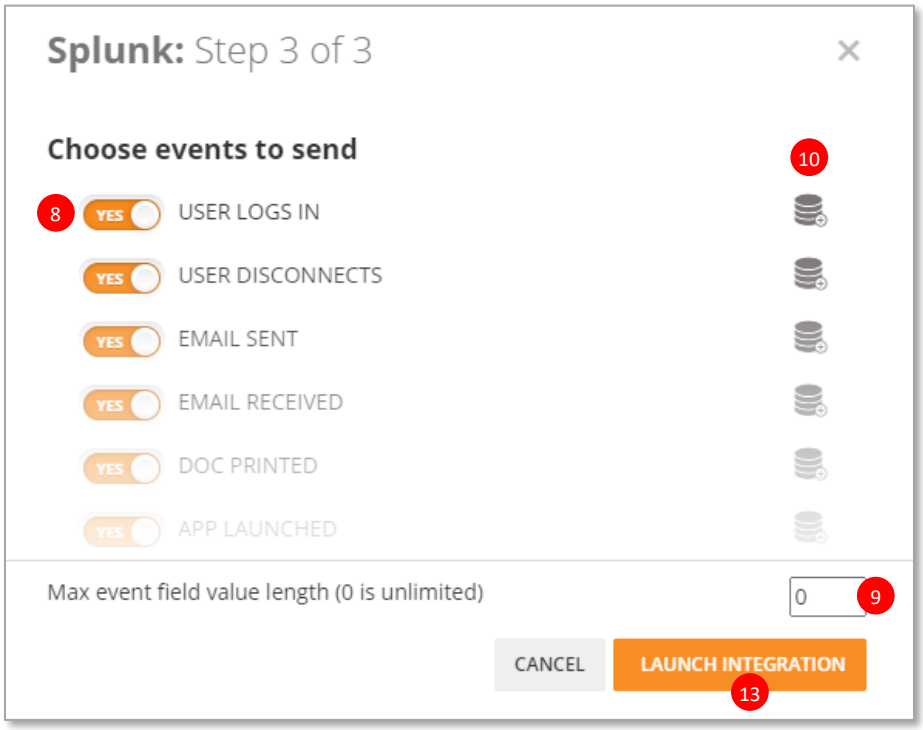
1. Click the **SETUP NEW INTEGRATION** button near the top-right corner of the Integrations screen. A setup wizard will pop-up:



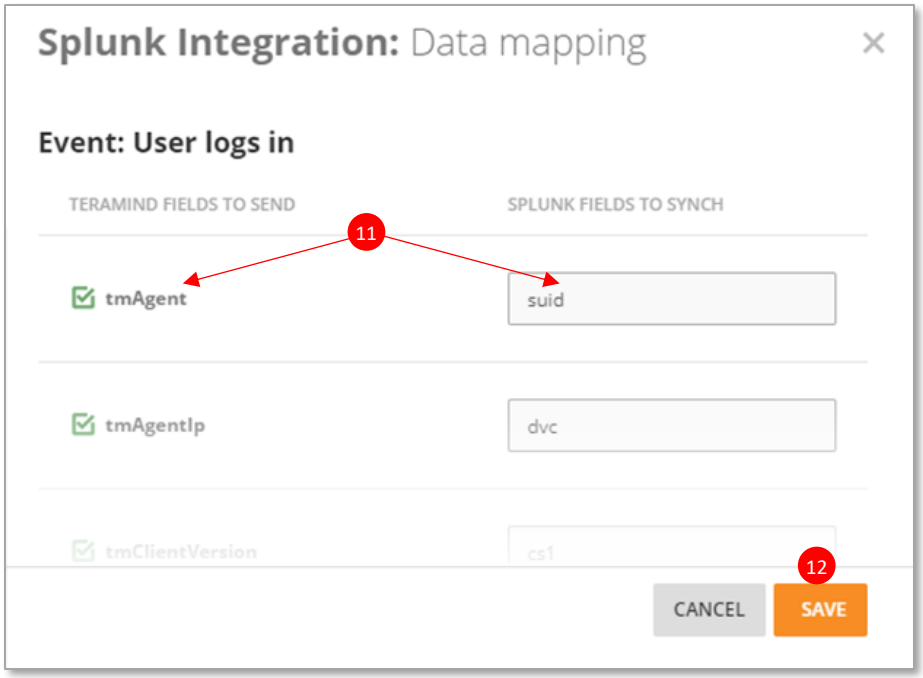
2. Select **SIEMs** from the list of product types.
3. Choose **Splunk** from the list of products.
4. Click the **NEXT STEP** button to continue to *Step 2*:



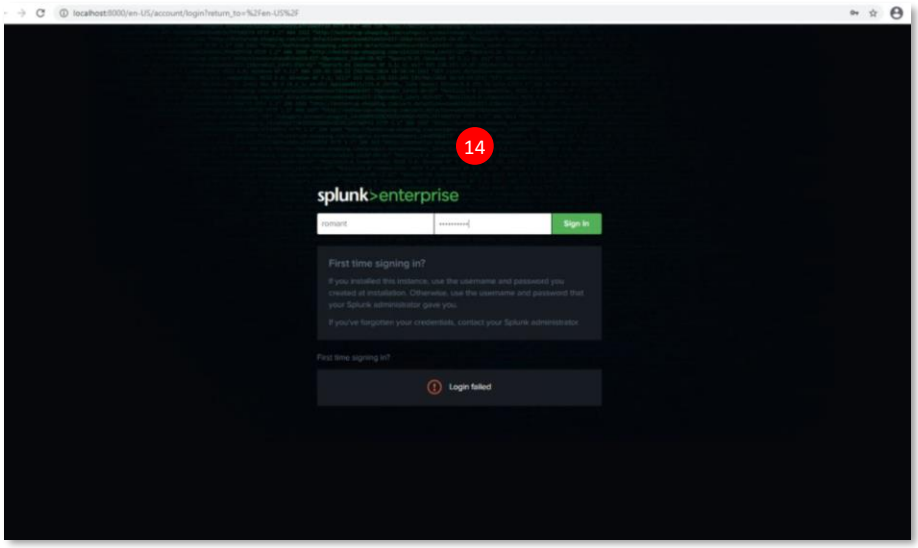
5. Select a Transport protocol, for example **TCP**.
6. Provide a **HOSTNAME** and **PORT** where the SIEM product is located at.
7. Click the **NEXT STEP** button to continue to *Step 3*:



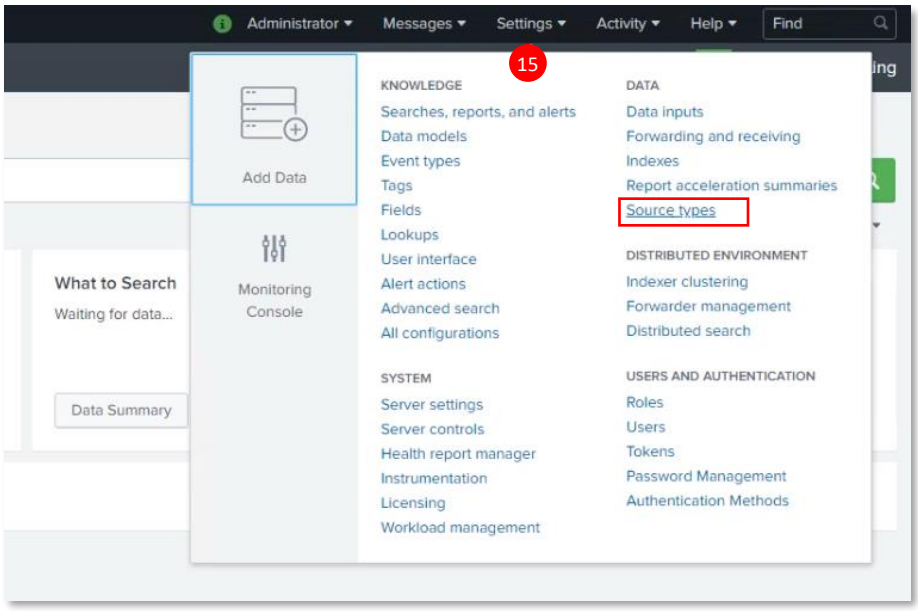
8. Click the **YES/NO** slider button to turn an event on/off. Events which are selected will be sent to the SIEM. By default, all events will be sent.
9. Optionally, you can specify the maximum field value length. Default is, 0 (unlimited).
10. Optionally, click on a **Database** icon for an event to configure its data mapping. A *Data mapping* window will pop-up:



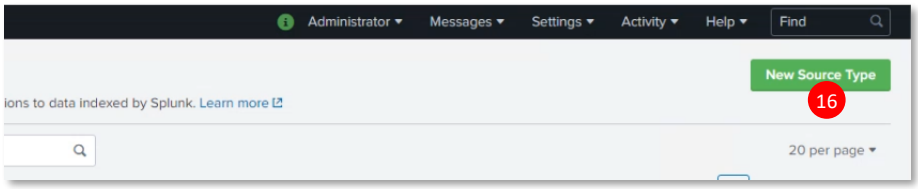
11. Map what SIEM field will be used for the corresponding Teramind field. You can use the checkbox in front of a field to turn it on/off.
12. When data mapping is done, click the **SAVE** button to close the *Data mapping* window and return to the *Step 3* window.
13. Click the **LAUNCH INTEGRATION** to save and launch the integration. Next, you will need to configure Splunk to accept the data sent to it from Teramind:



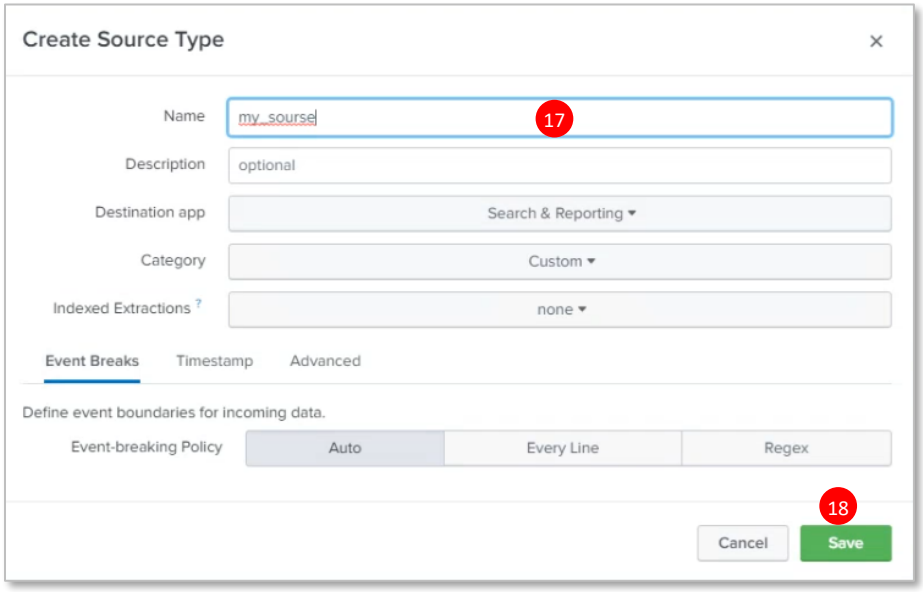
14. Login to your Splunk account dashboard as an administrator.



15. From the menu on top, select **Settings** > **Source types**.

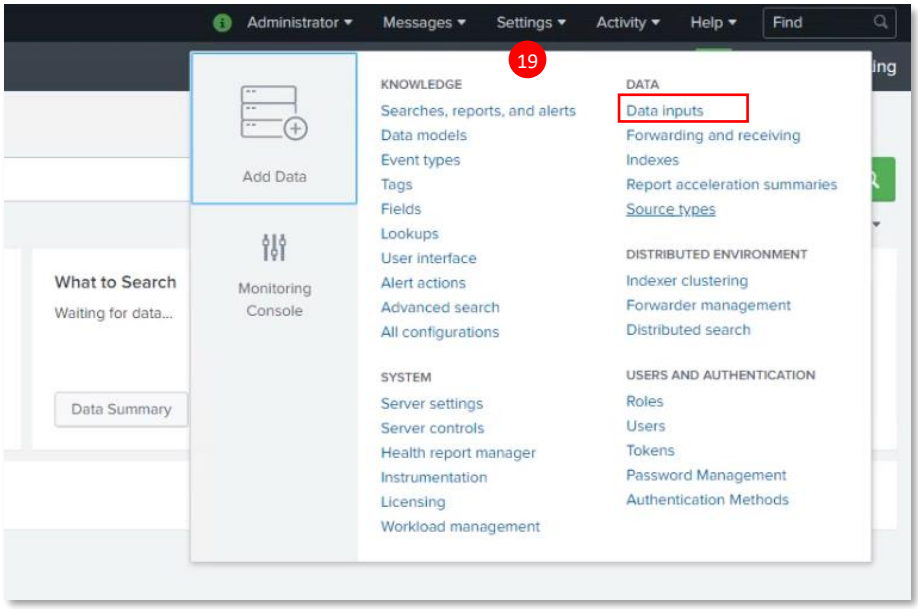


16. Click the **New Source Type** button near the top-right corner. A pop-up window will open:

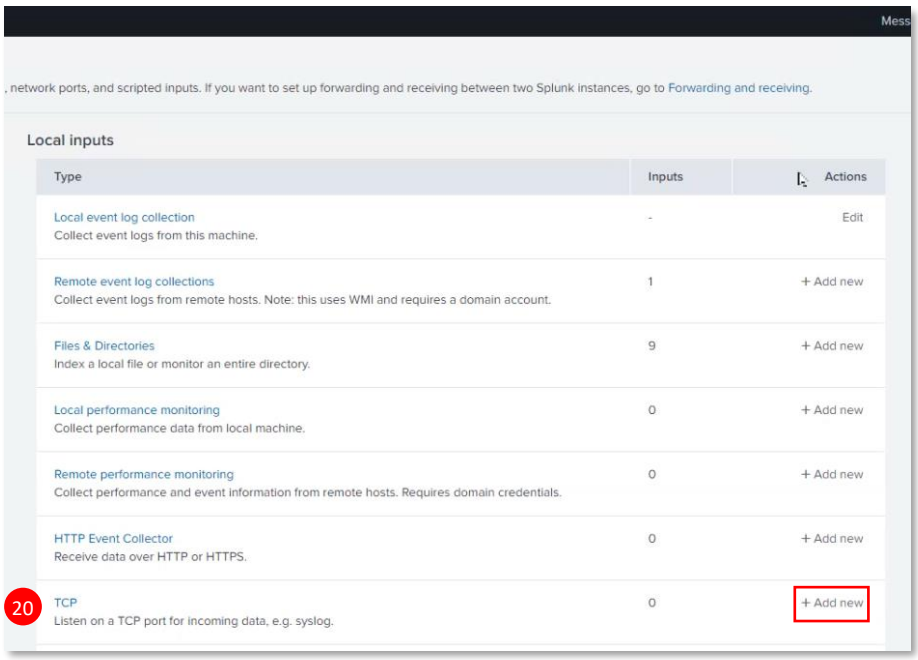


17. Give the source a **Name**. You can configure other options for the *Source* from this window. For this exercise, we just need the Name parameter.

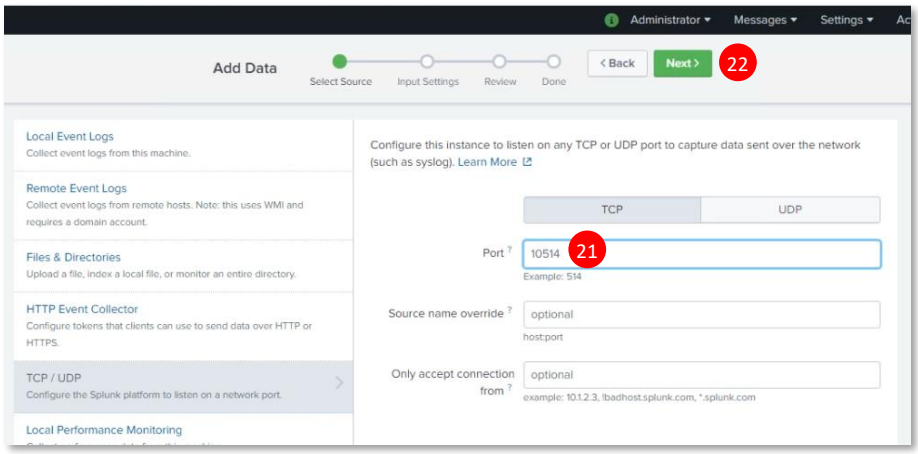
18. Click the **Save** button when you are done with setting up the *Source*.



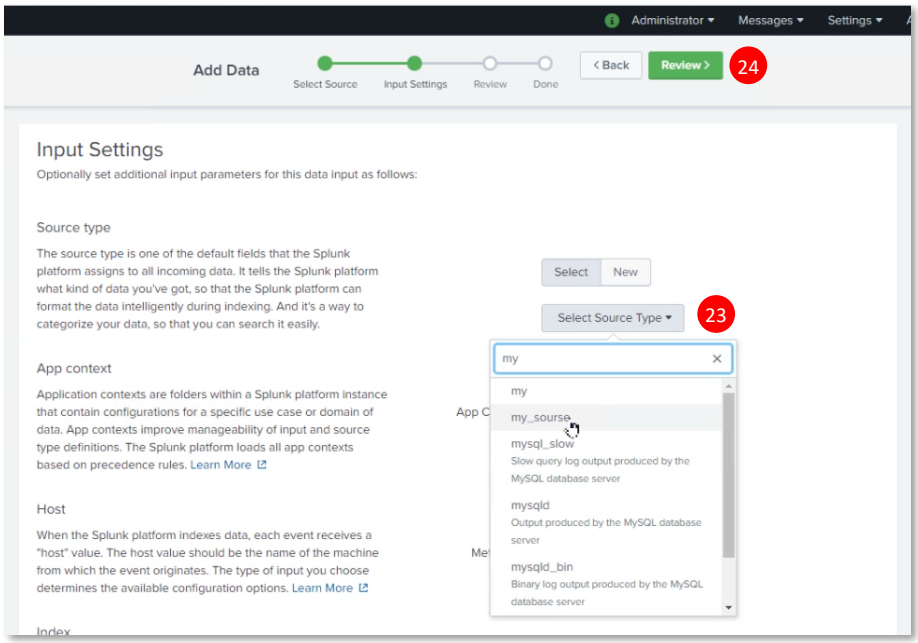
19. From the menu on top, select **Settings** > **Data inputs**.



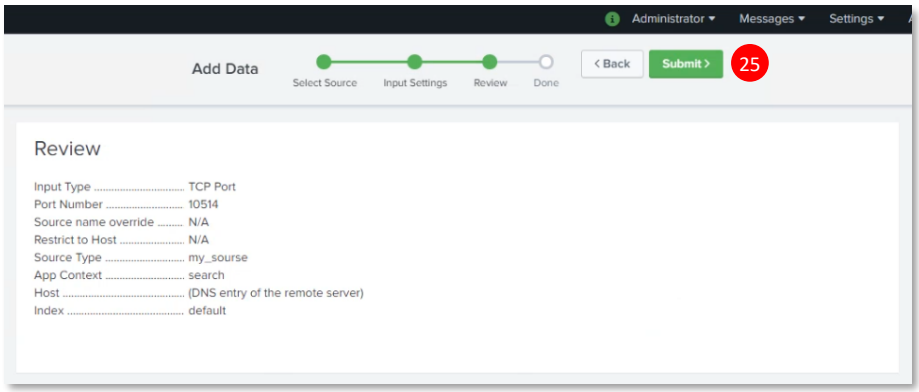
20. From the list of local inputs, click the **+ Add new** link next to the **TCP** row. You will be taken to the *Add Data* wizard screen:



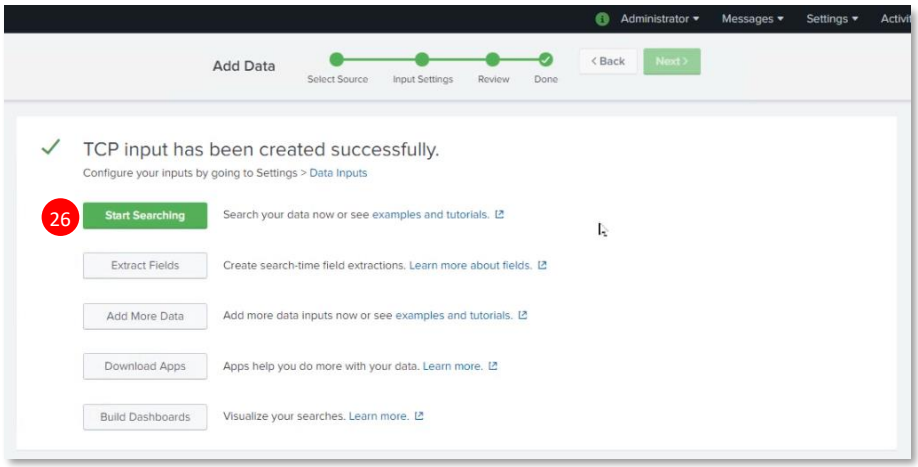
21. On the first step, *Select Source*, enter the **Port** number you chose in ***Step 6*** before. You can optionally set other parameters such as override source name, restrict connection to a specific host etc. For this exercise, we only need the Port parameter.
22. Click the **Next >** button to go to the next step.



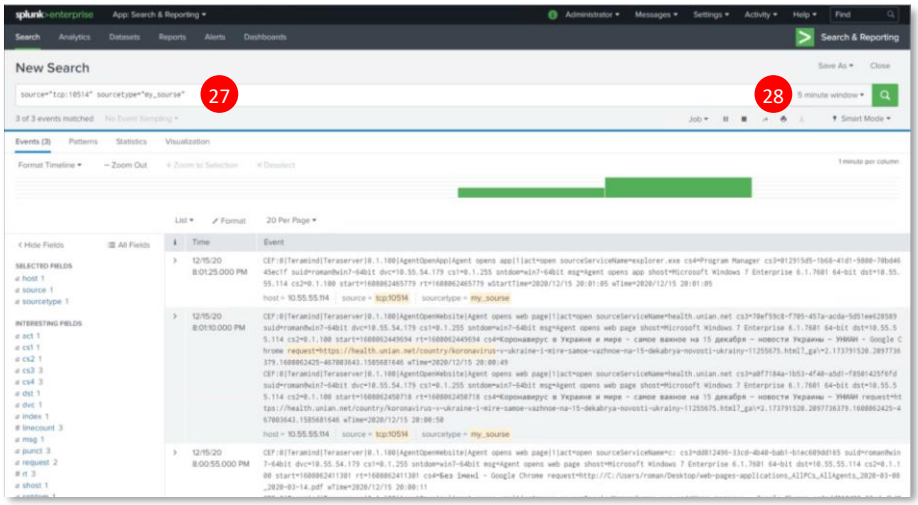
23. On the second step, *Input Settings*, click on the **Select Source Type** drop-down box and select the Source you created in ***Step 16*** before (e.g. `my_sourse`). You can optionally set other parameters such as app context, method, index etc. For this exercise, we only need the Source Type parameter.
24. Click the **Next >** button to go to the next step.



25. On the third step, *Review*, review the configuration. Click the **Submit >** button to finish setting up the data input and go to next step.

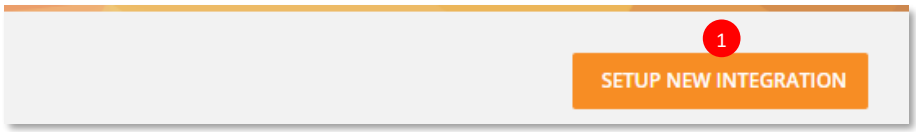


26. On the final step, *Done*, click the Start Searching button to view the data coming from your Teramind integration:

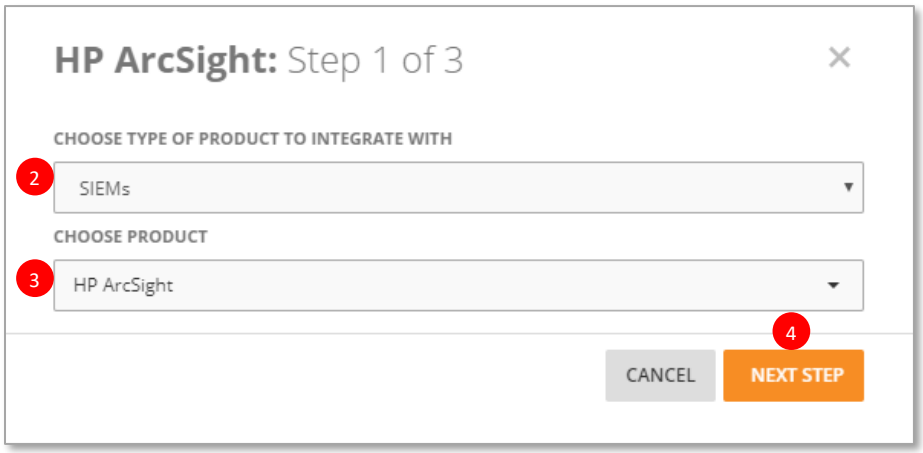


27. To find the data easily, you can optionally specify parameters such as `source` and `sourcetype` in the **Search** field.
28. Optionally, you can specify the interval (e.g. **5 minute window**) located right next to the search field.

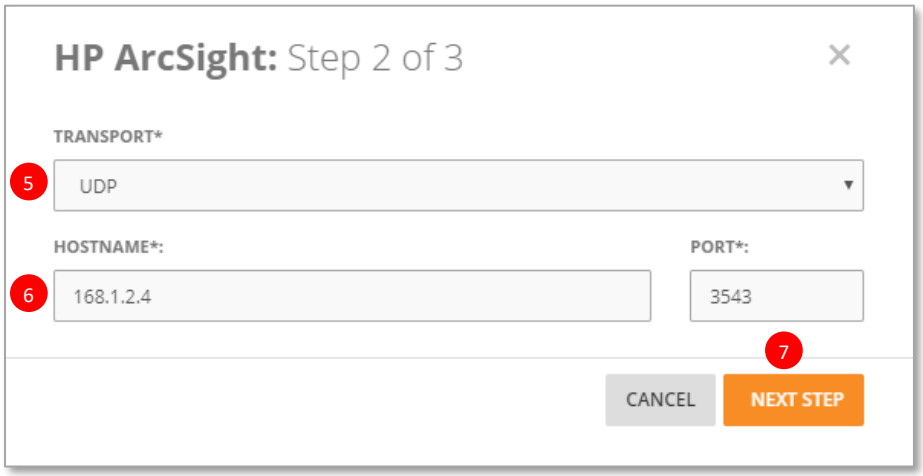
13.6.3 Setting Up a New SIEM Integration with HP ArcSight



29. Click the **SETUP NEW INTEGRATION** button near the top-right corner of the Integrations screen. A setup wizard will pop-up.

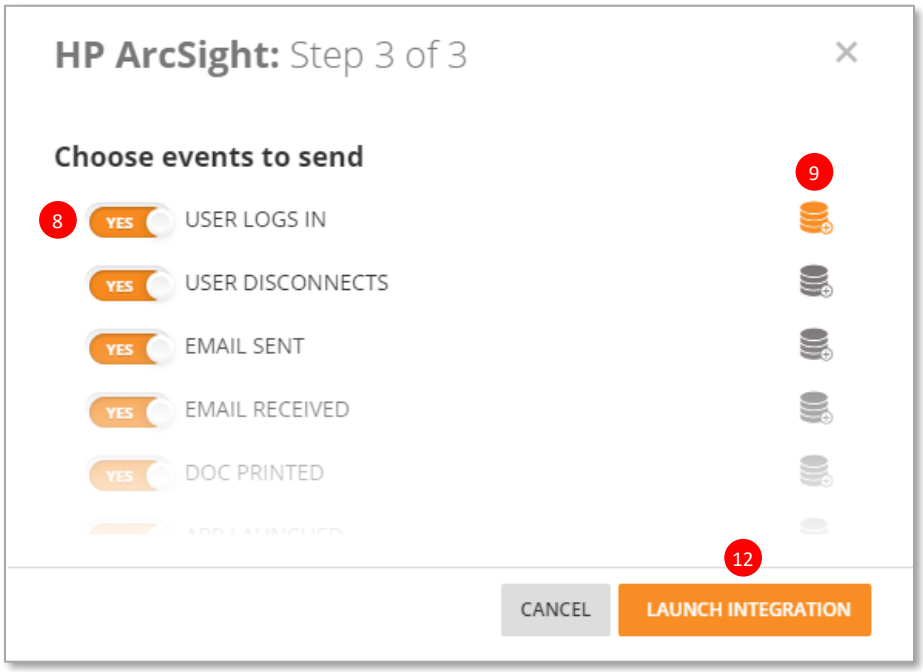


30. Select **SIEMs** from the list of product types.
31. Choose a SIEM product from the list of products. For example, **HP ArcSight**.
32. Click the **NEXT STEP** button to continue to *Step 2*.

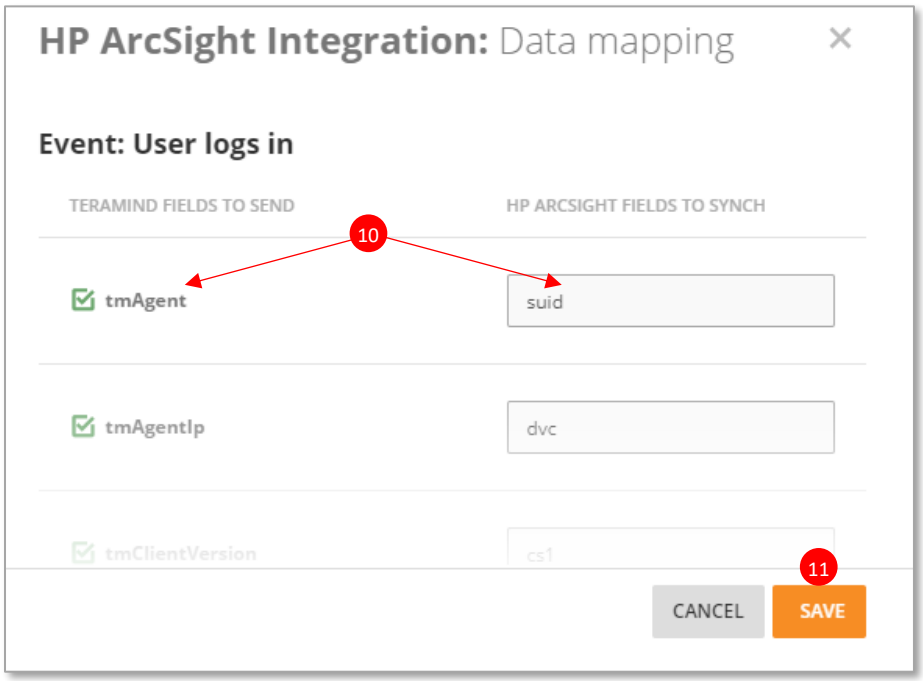


33. Select the **Transport** protocol (UDP or TCP).

34. Provide a **Hostname** and **Port** where the SIEM product is located at.
35. Click the **NEXT STEP** button to continue to *Step 3*.



36. Click the **YES/NO** slider button to turn an event on/off. Events which are selected will be sent to the SIEM.
37. Click on a Database icon to configure its data mapping. A *Data mapping* window will pop-up.



38. Map what SIEM field will be used for the corresponding Teramind field. You can use the checkbox in front of a field to turn it on/off.
39. When data mapping is done, click the **SAVE** button to close the *Data mapping* window and return to the *Step 3* window.
40. Click the **LAUNCH INTEGRATION** to save and launch the integration.

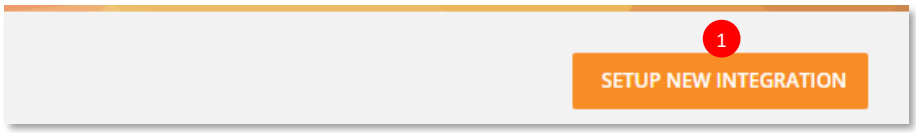
13.6.4 Setting Up a New SIEM Integration Using the Generic CEF Option

When creating a new SIEM integration, you will notice that there is a *Generic CEF* option on the SIEMs product list. CEF (Common Event Format) is a text-based, open messaging standard and log format developed by ArcSight™ and used by HP ArcSight™ products.

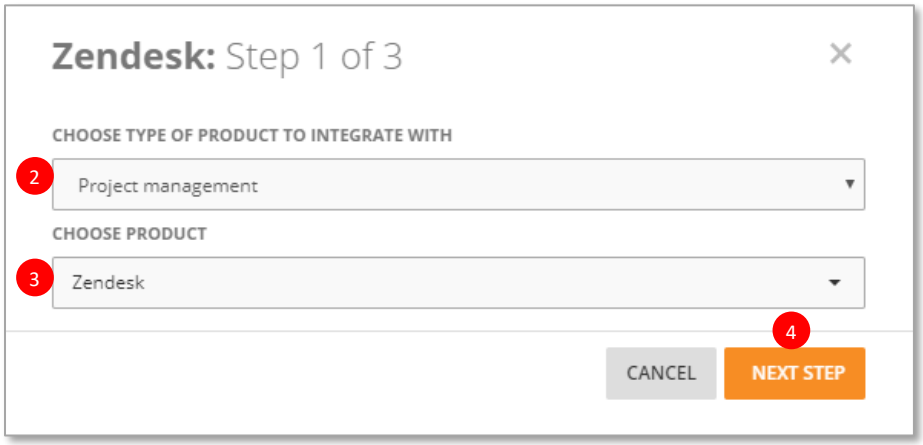
If you use this option, Teramind will output data over the Syslog protocol using CEF data format. This will help you integrate with various SIEM tools for which Teramind does not have a built-in option.

The integration process is very similar to HP ArcSight. See the [Setting Up a New SIEM Integration with HP ArcSight] for step-by-step instructions.

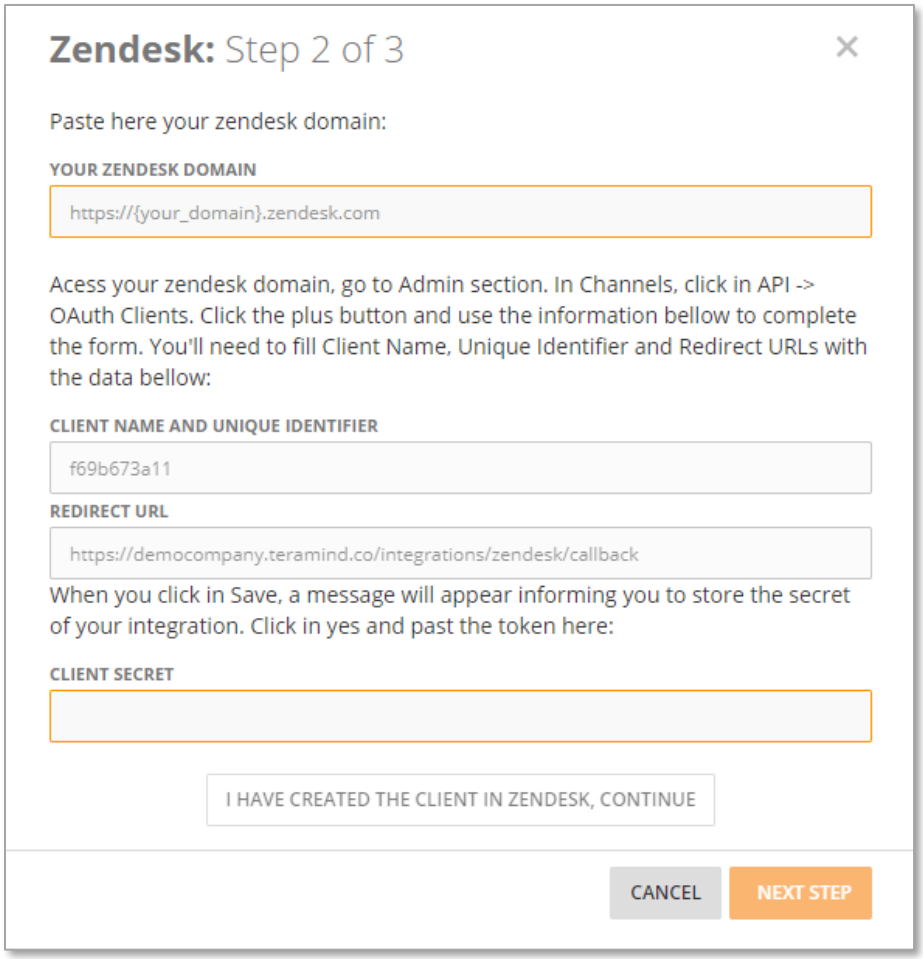
13.6.5 Setting Up a New PM Integration with Zendesk



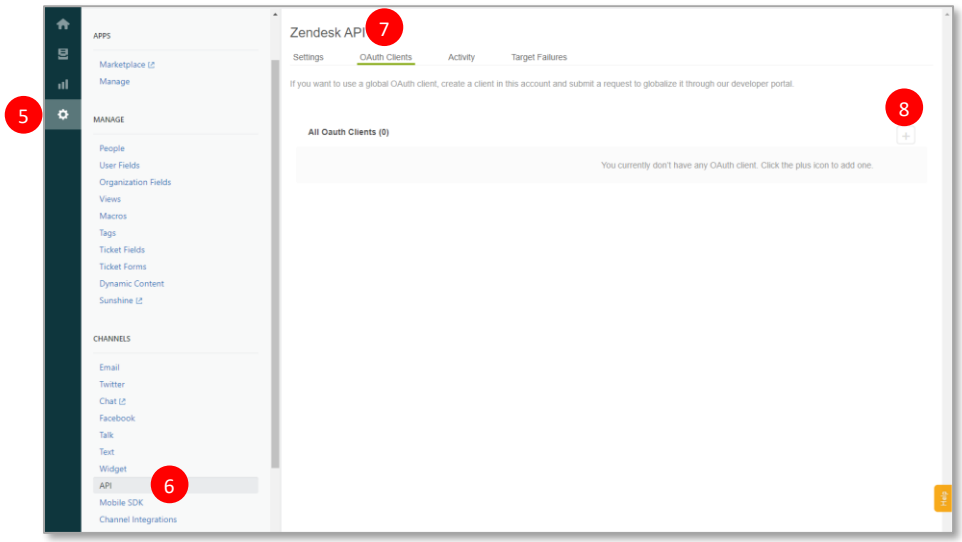
1. Click the **SETUP NEW INTEGRATION** button near the top-right corner of the Integrations screen. A setup wizard will pop-up.



2. Select **Project management** from the list of product types.
3. Choose **Zendesk** from the list of products.
4. Click the **NEXT STEP** button to continue. You will be taken to the *Step 2 of 3* screen.

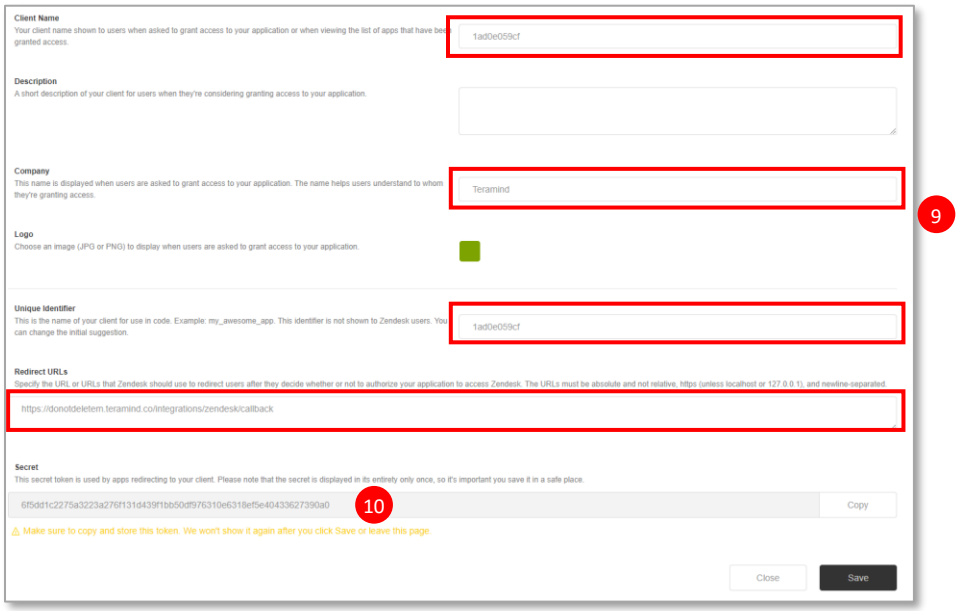


Before you continue with to Step 2, you need to create an OAuth Client in Zendesk. To do so:

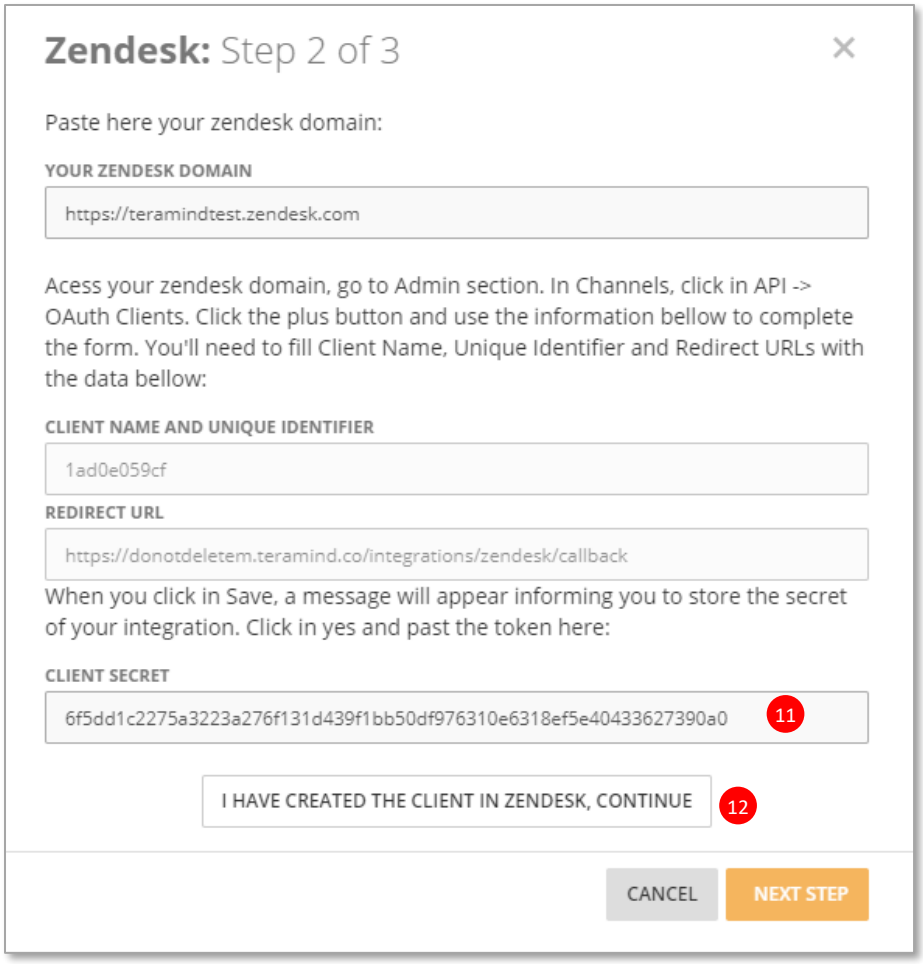


5. Access your Zendesk domain, go to **Admin** section.
6. Click **API** under the *Channels* section.

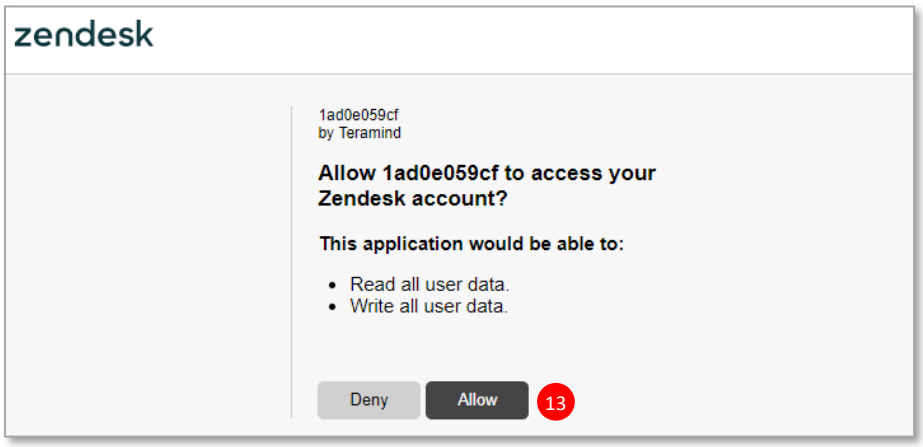
7. Click the **OAuth Clients** tab.
8. Click the **+** button to add a client.



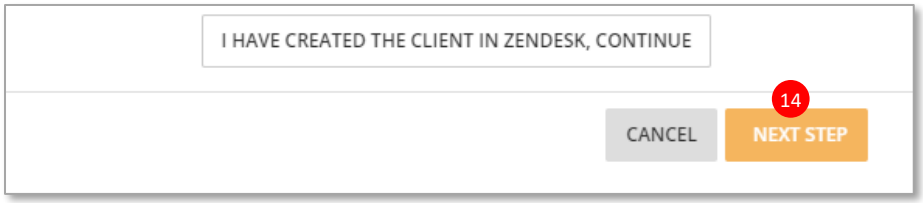
9. Use the information from the Teramind's integration wizard (*Step 2 of 3* screen) to complete the form. You'll need to fill up the **Client Name**, **Company**, **Unique Identifier** and **Redirect URLs** fields with the data provided by Teramind's *Step 2 of 3* screen.
10. Copy the data displayed on the **Secret** field. Go back to the *Zendesk Step 2 of 3* screen on Teramind.



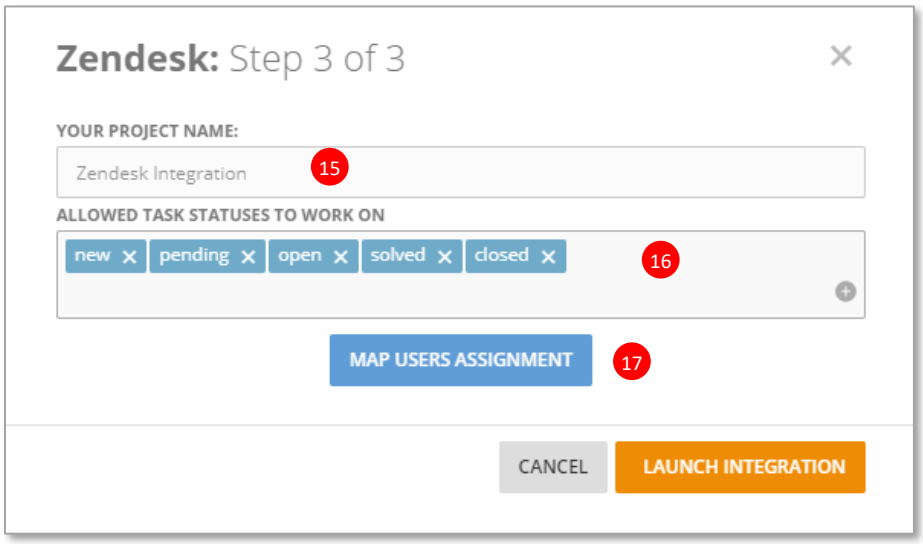
11. Paste the *Secret* key you copied from Zendesk on the **CLIENT SECRET** field.
12. Click **I HAVE CREATED THE CLIENT IN ZENDESK, CONTINUE**. A pop-up window will open:



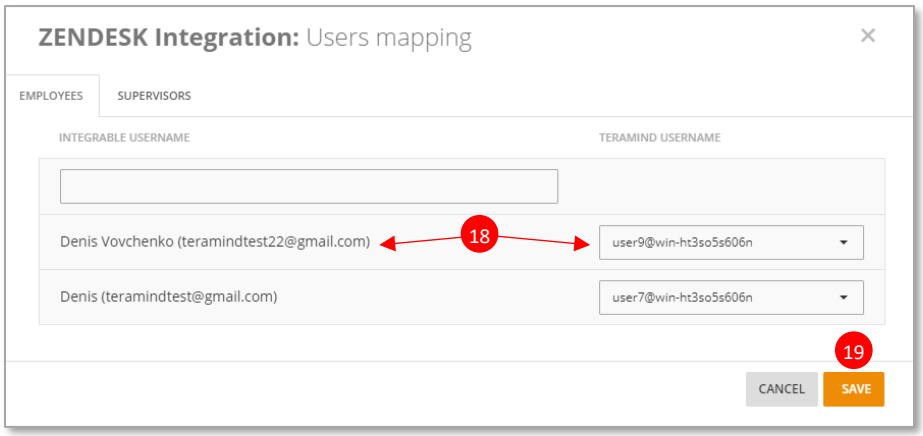
13. Click the **Allow** button. Go back to the Teramind integration wizard.



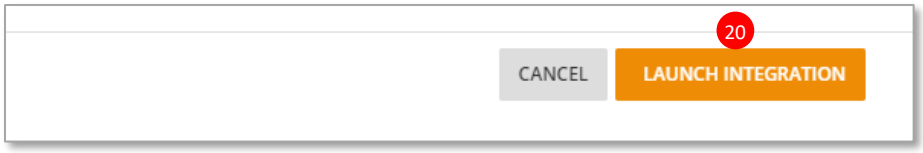
14. On the Teramind integration wizard (*Zendesk: Step 2 of 3* screen), click the **NEXT STEP**. You will be taken to the *Step 3 of 3* screen.



15. Give your project a name.
16. Add the task statuses to work on.
17. Click the **MAP USERS ASSIGNMENT** button. You will be taken the user mapping screen.

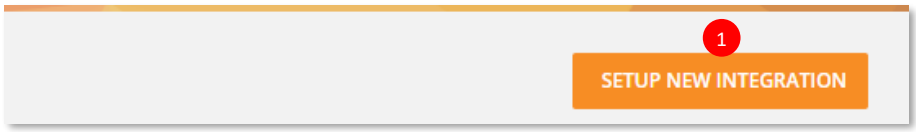


18. Map the employees and supervisors. Enter the Zendesk's usernames on the **INTEGRABLE USERNAME** field and then select the corresponding Teramind username from the **TERAMIND USERNAME** pull-down menu.
19. Click the **SAVE** button when done. You will be taken back to the *Step 3 of 3* screen.

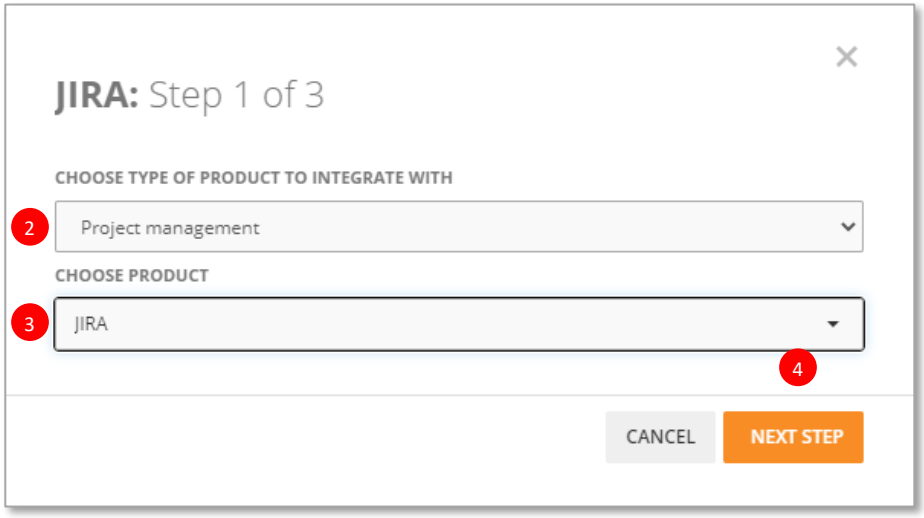


20. Click the **LAUNCH INTEGRATION** button on the *Step 3 of 3* screen to save and launch your integration.

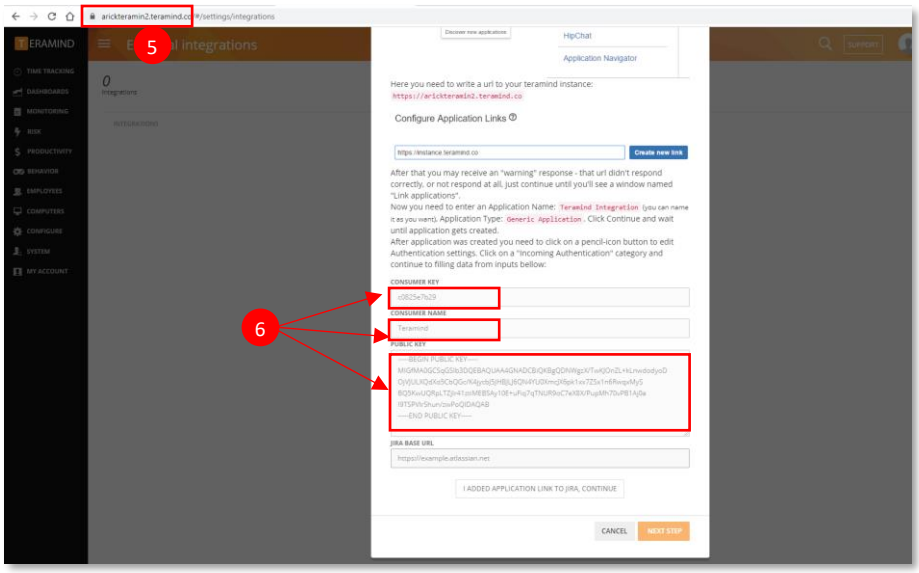
13.6.6 Setting Up a New PM Integration with Jira



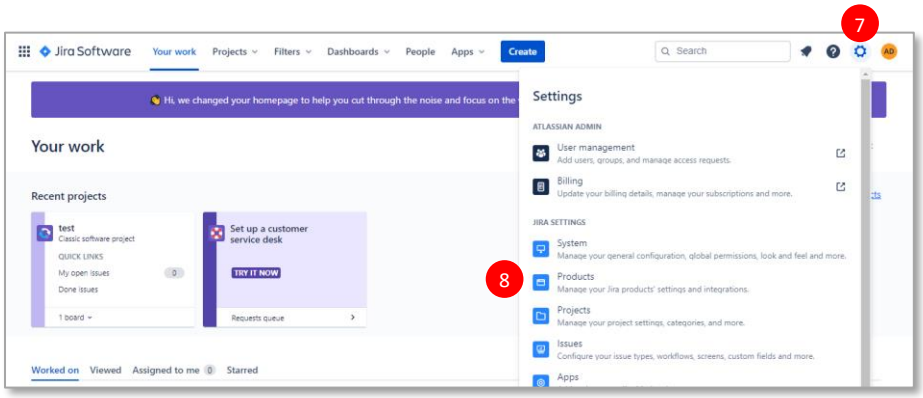
1. Click the **SETUP NEW INTEGRATION** button near the top-right corner of the Integrations screen. A setup wizard will pop-up.



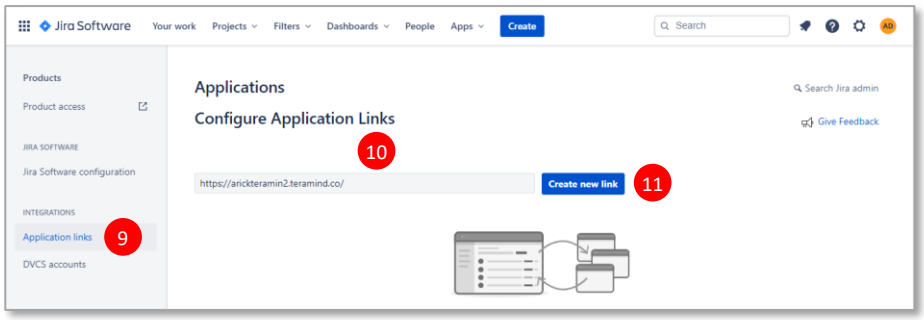
2. Select **Project management** from the list of product types.
3. Choose **Jira** from the list of products.
4. Click the **NEXT STEP** button to continue. You will be taken to the *Step 2 of 3* screen:



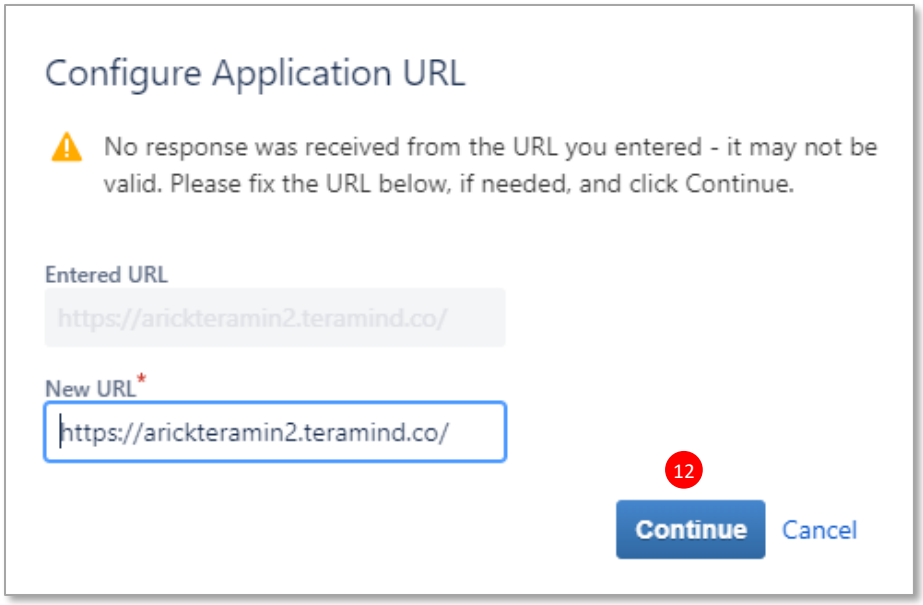
5. Note the **instance** / **URL** of your deployment. You will need it in *Step 10* below.
6. Scroll down a little, note the **CONSUMER KEY**, **CONSUMER NAME** and the **PUBLIC KEY** values. You will need these three values in the *Step 17* below. Keep this window open.



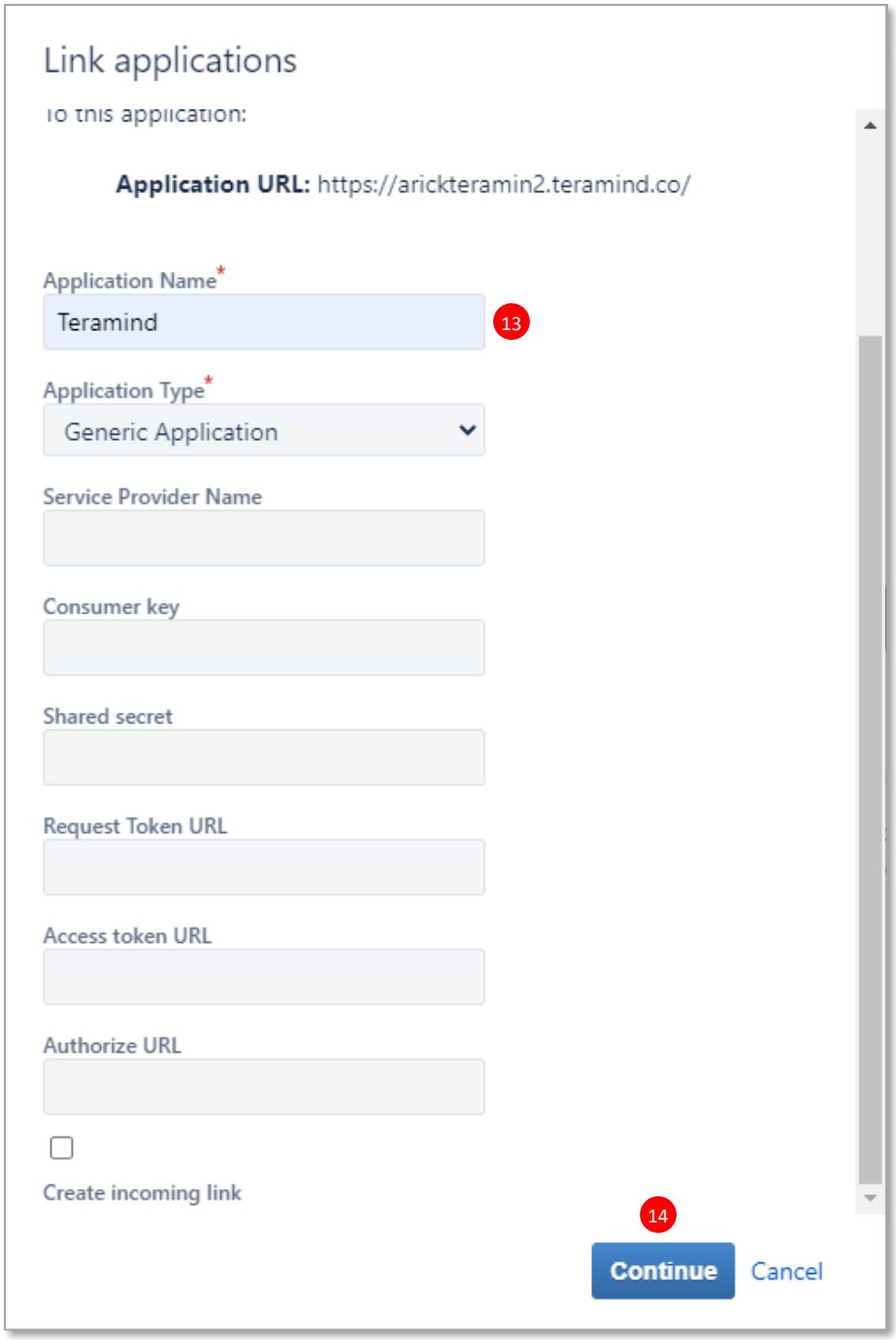
7. Log in to you Jira dashboard. Click the **Settings** icon near the top-right corner.
8. Select **Products** from the drop-down menu. You will be taken to a new window:



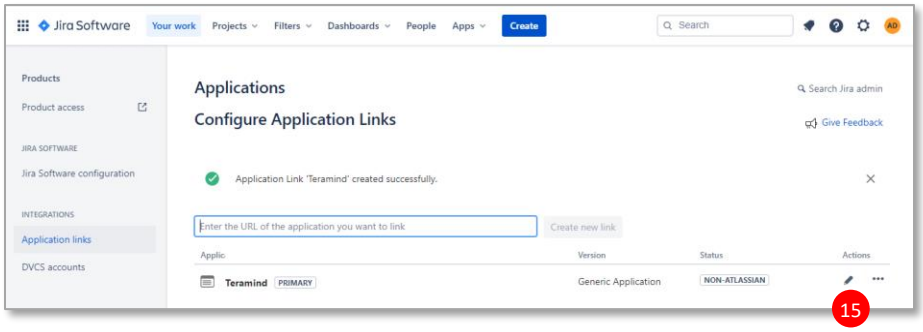
9. Click the **Application links** from the left panel.
10. Enter the **instance** / **URL** of your deployment you copied from *Step 5* above.
11. Click the **Create new link** button. You might see a pop-up window like the one below:



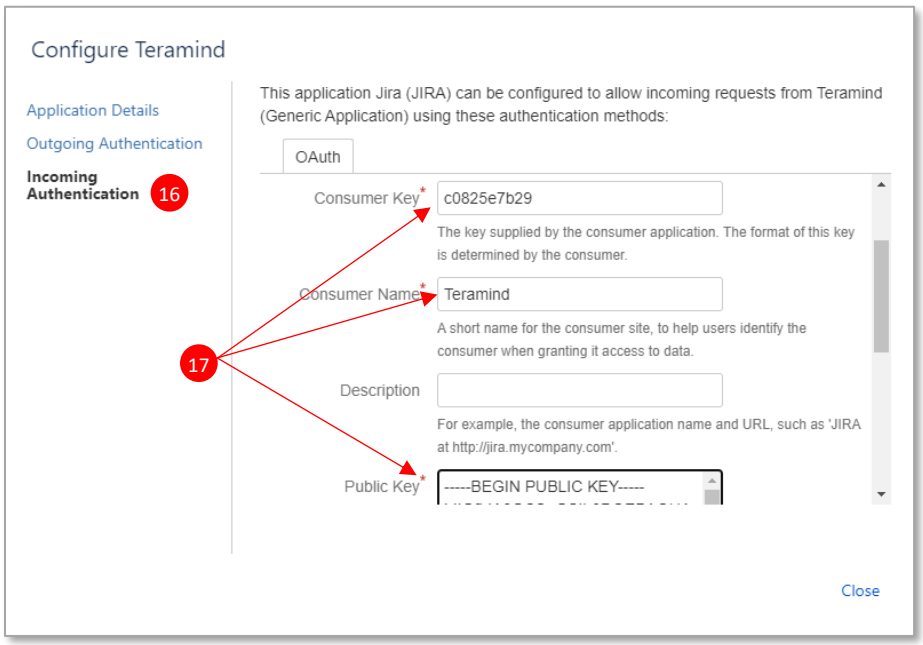
12. Just click the **Continue** button. You will see another pop-up window, *Link applications*:



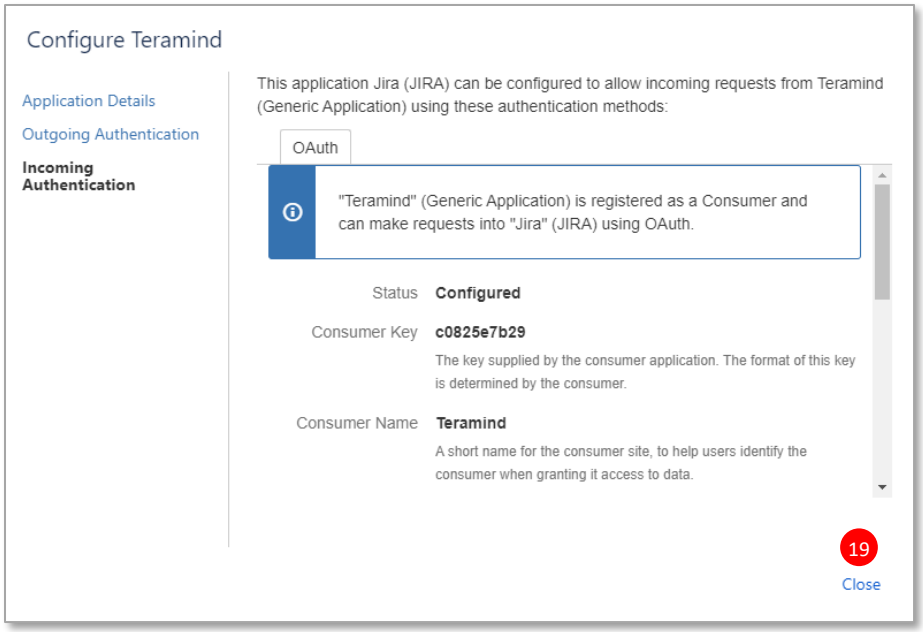
13. Enter an **Application Name**, for example, '`Teramind`'.
14. Click the **Continue** button. Jira will process the configurations and after a while, you will see the *Applications* window and your application on the list:



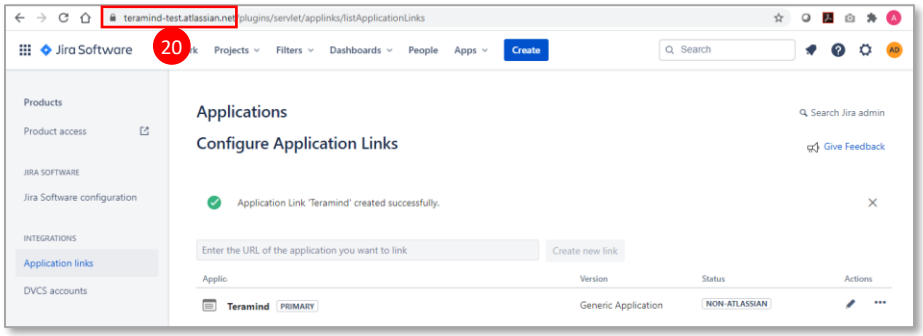
15. Click the small **Pencil** icon next to your application. A configure window will pop-up:



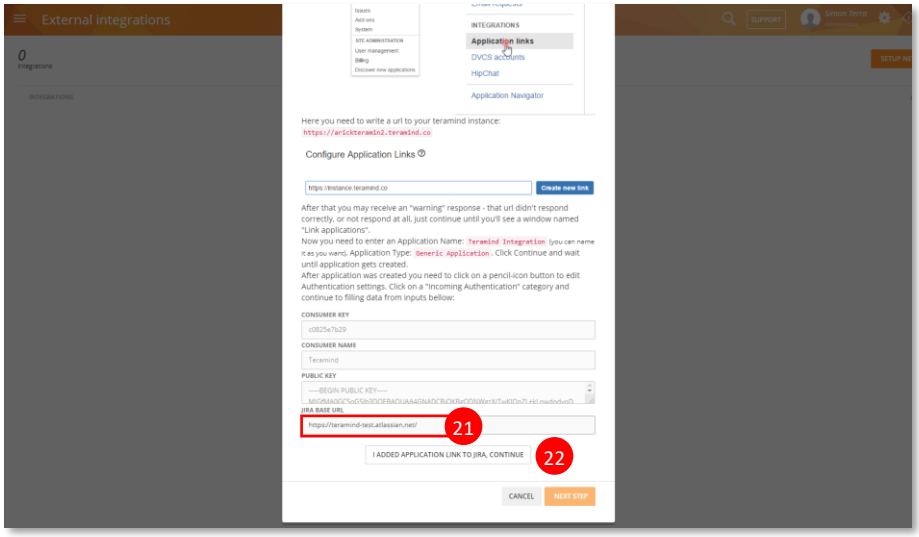
16. Click the **Incoming Authentication** tab on the left panel.
17. Enter the **Consumer Key**, **Consumer Name** and the **Public Key** values you copied in *Step 5*.
18. Scroll down and click the **Save** button to save you configurations. You will see a confirmation that your application is registered:



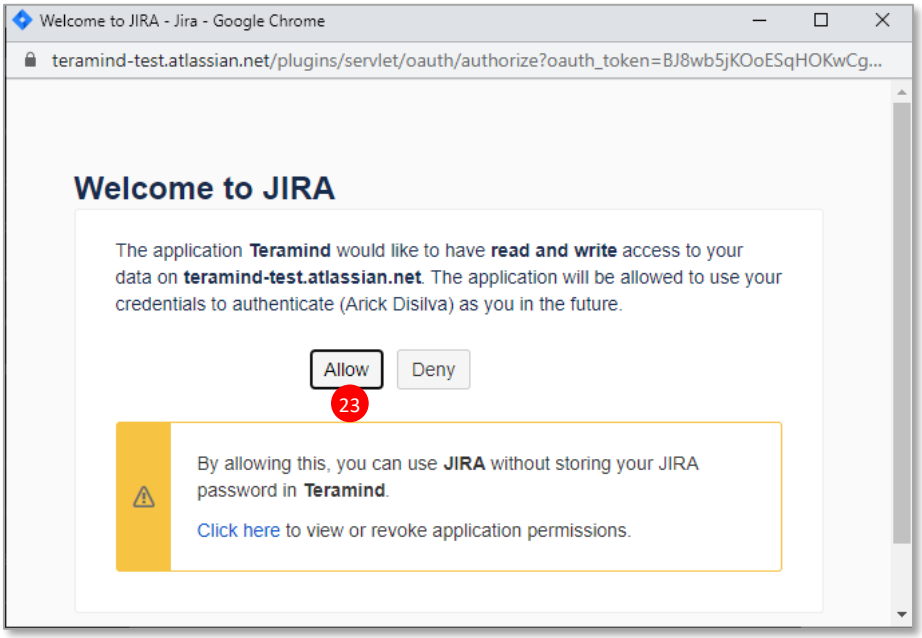
19. Click the **Close** button to close the window and return to the *Applications* page.



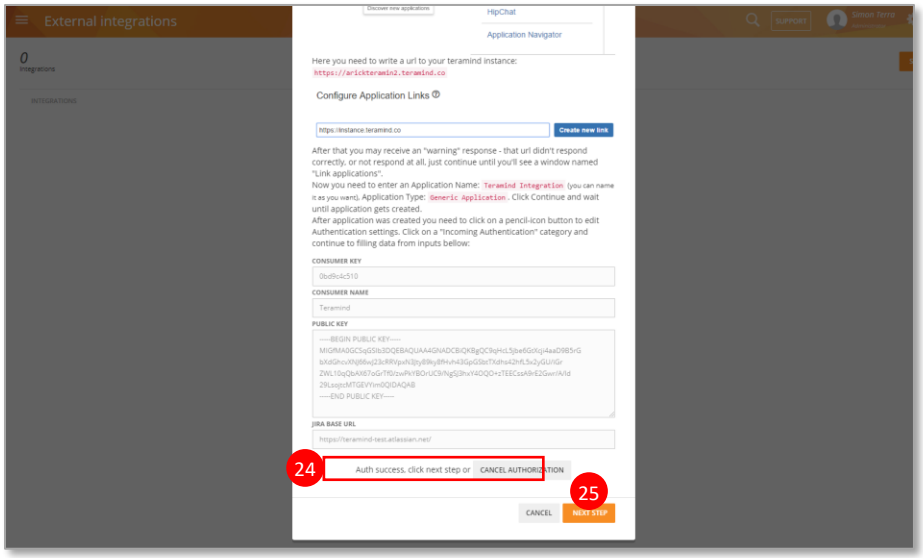
20. Copy the **domain address** / **URL** of your Jira deployment. You will need it in the next step, on the Teramind Dashboard:



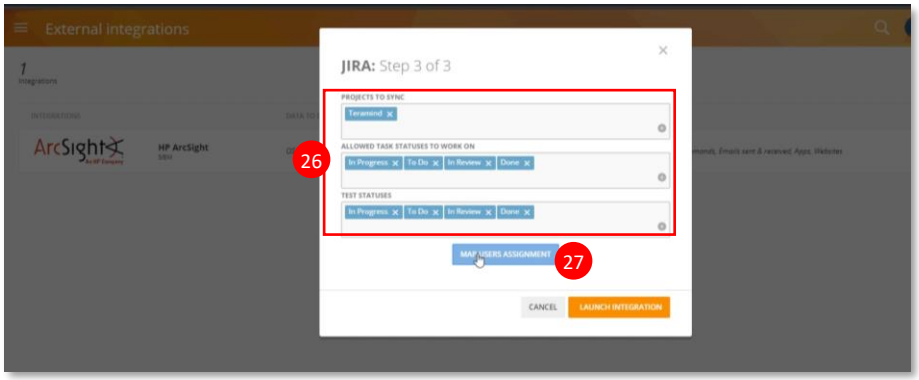
21. Go back to your Teramind Dashboard. Enter the **domain address** / **URL** of your Jira deployment you copied in the previous step into the **JIRA BASE URL** field.
22. Click the **I ADDED APPLICATION LINK TO JIRA, CONTINUE** button. A *Welcome to JIRA* window will pop-up:



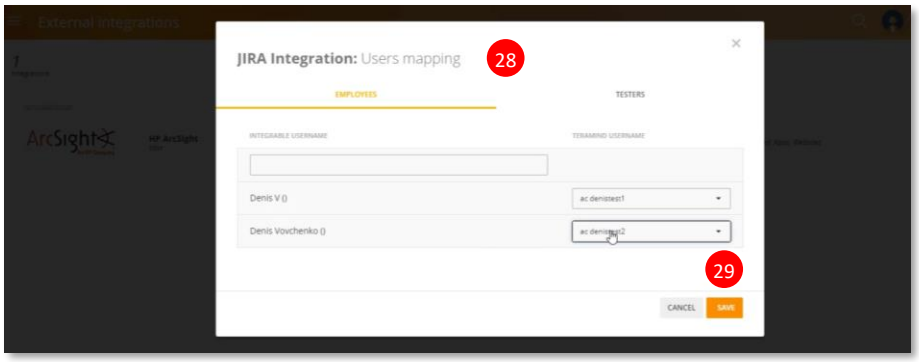
23. Click the **Allow** button to authenticate your application. The window will close and you will be back on the *JIRA: Step 2 of 3* screen:



24. Wait a few seconds and then you will see an ***Auth success*** message.
25. Click the **NEXT STEP** button to continue to *JIRA: Step 3 of 3* screen:

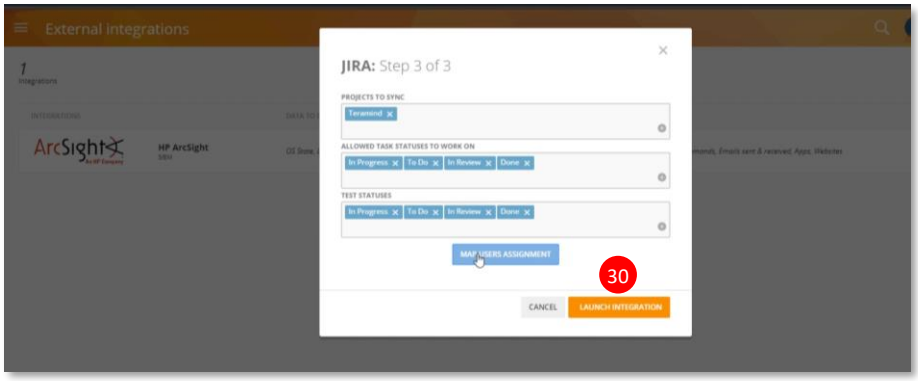


26. Select your **PROJECTS**, **ALLOWED TASK STATUSES** and **TEST STATUSES** from the corresponding fields.
27. Click the **USERS ASSIGNMENT** button to set up user mappings:

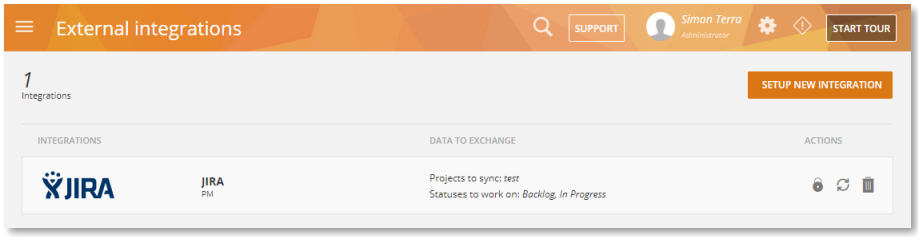


28. You can map **EMPLOYEES** and **TESTERS**. Assign **INTEGRABLE USERNAME** with **TERAMIND USERNAME**, assign roles etc.

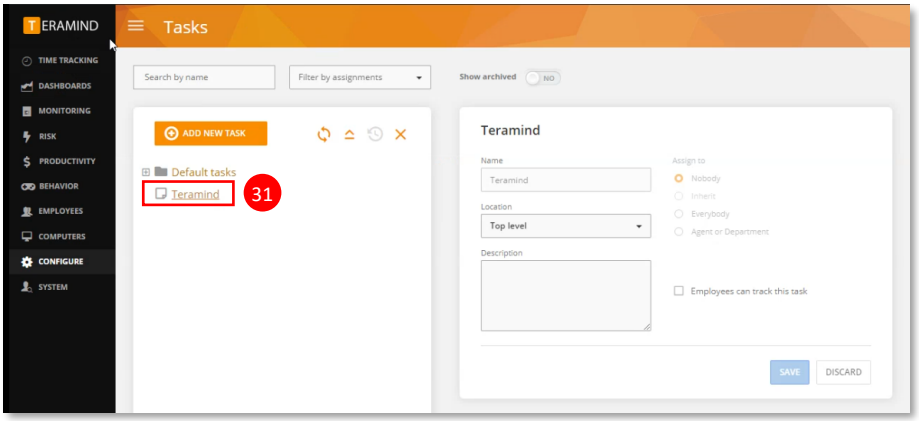
29. Click the **SAVE** button when you are done with the user mapping. You will be taken back to the to *JIRA: Step 3 of 3* screen:



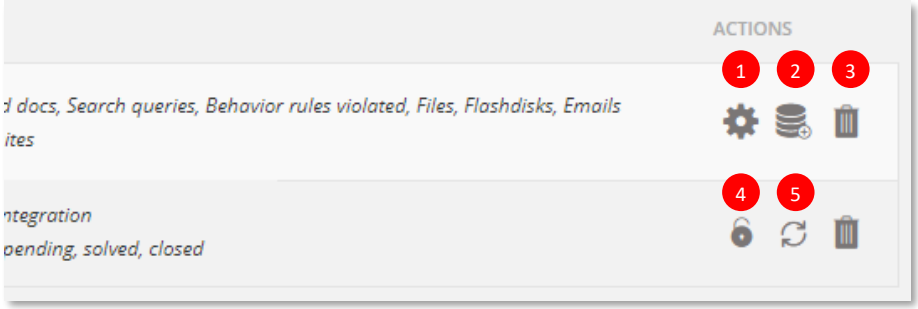
30. Click the **LAUNCH INTEGRATION** button to save your integration and return to the *External Integration* screen where you will see your Jira integration:



31. You should now be able see and import your Jira projects and tasks from the **TIME TRACKING** > **TASKS** menu:



13.6.7 Editing / Deleting an Integration

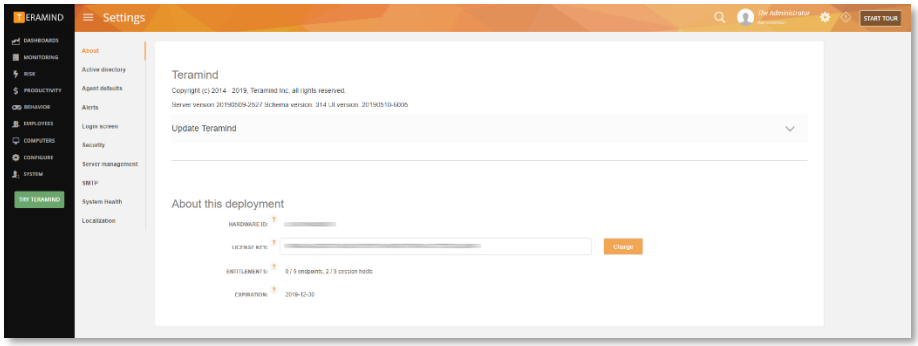


From the main Integration screen, under the ACTIONS column:

1. Click the **Settings** icon to change the connection settings for a SIEM integration.
2. Click the **Database** icon to change the events mapping for a SIEM integration.
3. Click the **Trash Can** icon to delete/remove an integration.
4. Click the **Pad Lock** icon to edit the app link/authorization settings for a PM integration.
5. Click the **Refresh** icon to change the project name, task statuses and user mapping for a PM integration.

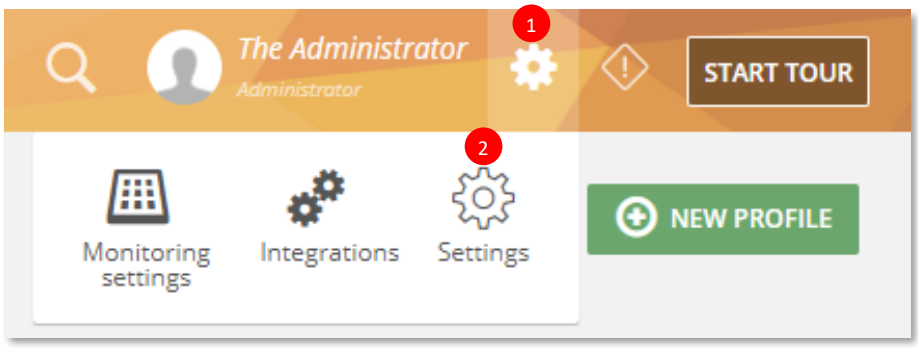
13.7 Settings

Settings menu allows you to configure different parts of the Teramind Dashboard, Agent, Security, Active Directory Integration etc. Note that, most of the settings on the Settings screen are applicable to the On-Premise / Private Cloud (AWS, Azure etc.) deployments. Except for: *Agent defaults*, *Alerts*, *Security* and *Localization;* these are available on all deployment options.



Please follow the *Teramind On-Premise Deployment Guide*, *Teramind on AWS Deployment Guide* or the *Teramind on Azure Deployment Guide* to learn how to deploy and setup Teramind on-premise/private cloud servers. You can find the deployment guides on https://www.teramind.co/company/resources under the *Product Guides* category.

13.7.1 Accessing the Settings Menu



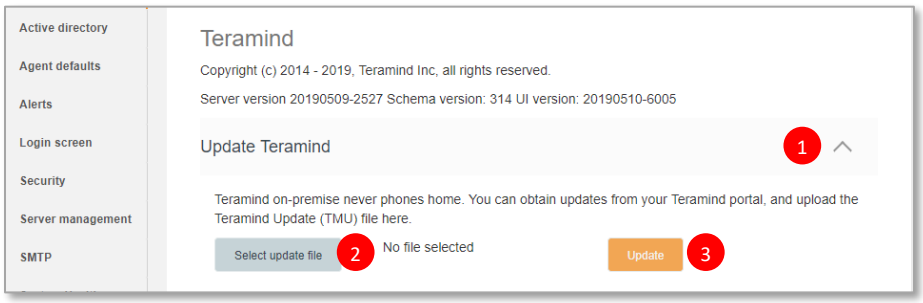
5. Click the **Gear** icon near the top-right corner of the Teramind Dashboard.
6. Click **Settings** underneath the pop-up menu.

13.7.2 Server Updates and License Key

Click the **About** tab on the Settings screen. You will see some details for your Teramind deployment. From here, you can also update your on-premise server image and change the license key.

13.7.2.1 Updating Teramind On-premise

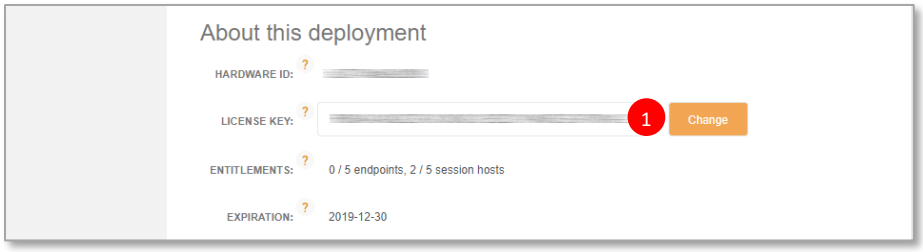
To update your server, download the latest server image from the Self-Hosted portal at https://www.teramind.co/portal/download. Scroll to *Step 2. Download Packages*. Download the *Teramind Update* file (with a TMU extension) by clicking the **download** button. Then do the following:



1. Click the **Update Teramind** link to expand it.
2. Click the **Select update file** button and select the TMU file you downloaded from the Self-Hosted portal.
3. Click the **Update** button. Depending on your deployment, Teramind will update the server in few minutes.

13.7.2.2 Changing the License Key

If for any reasons, you wanted to change the license key (i.e. you upgraded from a trial to a paid account), you can do that from the About tab.



1. Enter your license key in the LICENSE KEY field located under the *About the deployment* section and then click the **Change** button. Once done, the system will display the updated entitlements for your license key.

13.7.3 Active Directory

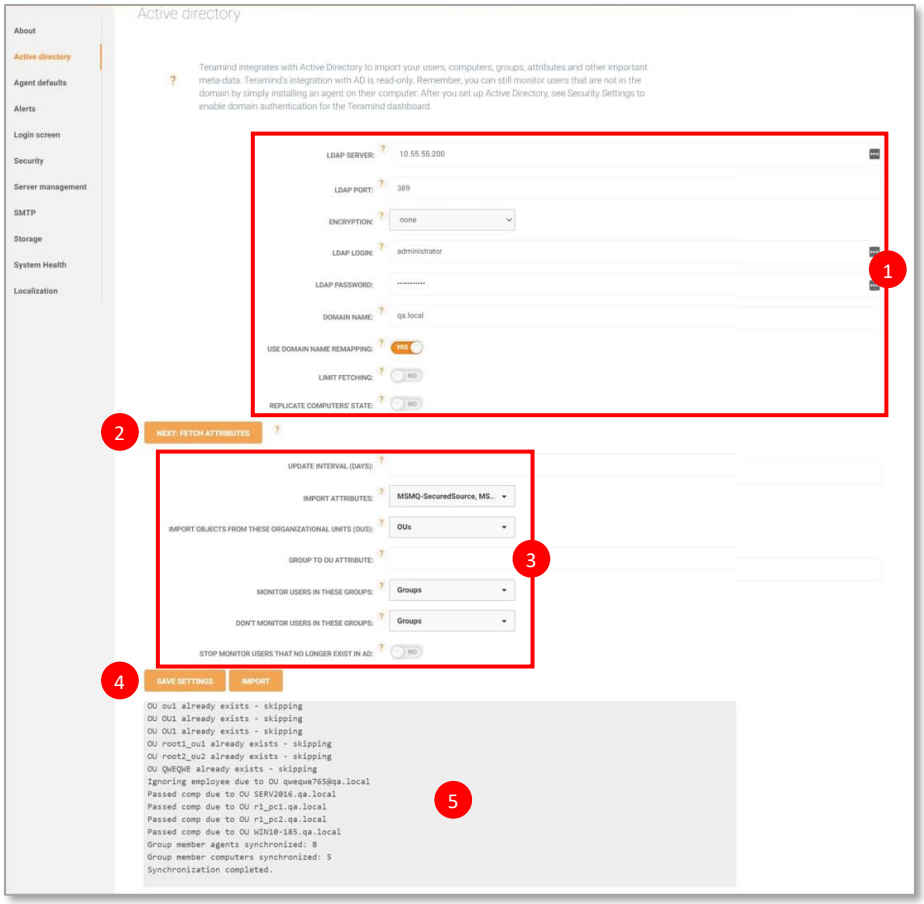
Though not mandatory, Teramind can be integrated with Active Directory to import your users, computers, groups, attributes and other important meta-data. Teramind's integration with Active Directory is read-only. Remember, you can still monitor users that are not in the domain by simply installing an agent on their computer. Active Directory/LDAP integration will provide the following benefits:

- The ability to report based on OU's
- The ability to filter reports with attributes
- The ability to apply rules to OU's and/or groups
- The ability to remote install to computers based on name, or AD group membership
- The ability to use Teramind only on a specific group
- The ability to exclude a group from being monitored
- The ability to log into dashboard via domain authentication

Note that Teramind treats Active Directory Organization Units (OUs) as Departments. You can set up special AD Groups and OUs to import and monitor users, PCs or disable monitoring. If you select all groups and OUs, Teramind will monitor all users and PCs present in AD.

Teramind can also import attributes. To import attributes, you will need to configure the *Fetch* objects (see below for more information). Teramind can also import custom attributes. You can use the attributes to filter the BI Reports.

Active Directory synchronization can be set up as follows:



1. Populate the upper set of fields as follows:

LDAP SERVER	Hostname or IP address of your domain controller, e.g. `10.55.55.200`.
LDAP PORT	In most cases the default port `389` should work.
ENCRYPTION	You can use `tls`, `ldaps` or `none`. Note that you might need to change the LDAP PORT if you change the encryption method.
LDAP LOGIN	Enter an account, e.g. `administrator`. A regular domain account is required to sync data from your active directory.
LDAP PASSWORD	Password for the above mentioned account
DOMAIN NAME	Your Active Directory domain name, e.g. `qa.local`.

USE DOMAIN NAME REMAPPING	If enabled, allows remapping of a domain name in accordance with the rules, e.g. `user@qa.com` -> `user@remapped.com` and it is configured in DB (`domain_remap_rule` table)
LIMIT FETCHING	If enabled, Teramind will show additional options where you can specify OUs and groups.
- HIERARCHY	If enabled, will fetch child OUs and groups only (respect hierarchy)
- FETCH ONLY THESE OUS	Limit fetching by entered OUs (comma separated names). If left empty, Teramind will fetch all OUs.
- FETCH ONLY THESE GROUPS	Limit fetching by entered groups (comma separated names). If left empty, Teramind will fetch all groups.
REPLICATE COMPUTERS' STATE	*ON:* replicate AD computer state with Teramind. AD-enabled computers will be imported as auto-monitored. AD-disabled computers will be imported as non-monitored. *OFF:* ignore AD computer state (old behavior, default)

2. Click the **NEXT: FETCH ATTRIBUTES** button to fetch the attributes.
3. As soon as fetching is done, you will be able to specify additional options for attributes according to the table below. *Note: If something went wrong during the fetch process, error messages will be displayed on the message area near the bottom of the screen (see item 5 below)*.

Please note that `msDS-ManagedPassword` attribute is not readable from AD and attempting to import it will throw an error message during the import process, "`Error: Trying to pass 'msDS-ManagedPassword' attribute over insecure connection. Please change connection settings or uncheck the attribute`". As a workaround, uncheck the `msDS-ManagedPassword` attribute in the **IMPORT ATTRIBUTES** field and repeat the import process.

UPDATE INTERVAL (DAYS)	Enter how often (in days) to perform active directory syncs. `0` means do not sync.

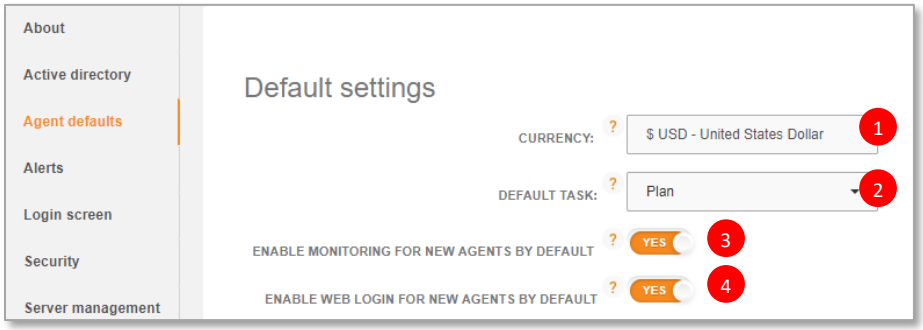
IMPORT ATTRIBUTES	Attributes can be sync'd to allow more detailed reporting and user grouping. Select the attributes you want to sync into Teramind. Default is `all`.
IMPORT OBJECTS FROM THESE ORGANIZATIONAL UNITS (OUS)	Import users and computes from the selected organizational units into Teramind. Default is `all`.
GROUP TO OU ATTRIBUTE	Groups with this attribute set to `true` are treated as OUs.
MONITOR USERS IN THESE GROUPS	Enable monitoring for users in these groups and disable monitoring for users not in these groups.
DON'T MONITOR USERS IN THESE GROUPS	Disable monitoring for users in these groups.
STOP MONITOR USERS THAT NO LONGER EXIST IN AD	If enabled, Teramind will automatically disable monitoring of all computers that is not in the AD or out of the synced OU.

4. Click the **SAVE SETTINGS** button to save the settings. Click the **IMPORT** button to initiate the import process. You might have to wait for a couple of minutes depending on AD object count and hierarchy. Once the import is done, refresh the page to view the changes. *Note: If something went wrong during the import process, error messages will be displayed on the message area near the bottom of the screen (see item 5 below)*.
5. The messages area below the screen shows the task progress and any error the system might encounter.

After you have set up Active Directory, visit Security tab to enable domain authentication for the Teramind Dashboard.

13.7.4 Agent Defaults

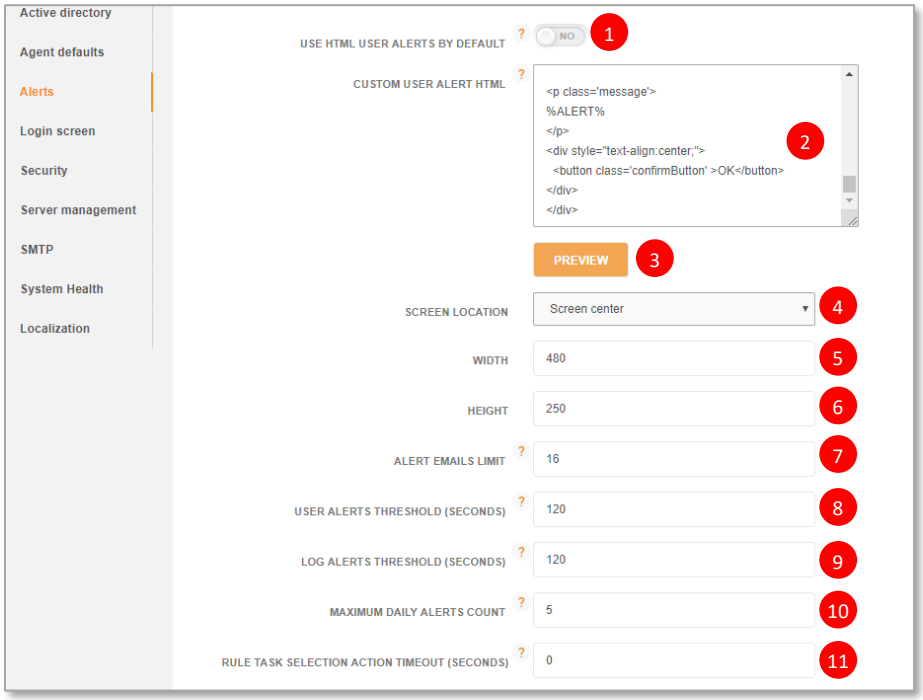
This tab allows you to change the default settings for the Teramind Agent.



1. You can change the currency used. Most of the recognized internationally circulating currencies are supported. The currency you choose will be used to display the wage/salary in the BI > Productivity report, TIME TRACKING > Employee Cost, TIME TRACKING > Task Cost, Payroll Widgets, Employee Profile, etc. - anywhere the currency is used.
2. You can assign a default task for employees when they start their shift (this is applicable if the employee is using the Hidden Agent). Restart the user machine(s) after changing the default task for it to take affect.
3. If ENABLE MONITORING FOR NEW AGENT… is turned on and your license allows it, new agent installations will have monitoring enabled by default. If disabled, new agent installations will not be monitored until you activate them from the dashboard.
4. Enable WEB LOGIN… if you want your users to be able to log into the dashboard to see their own work stats, enable this option.

13.7.5 Alerts

Alerts tab allows you to define how rule violation messages will be displayed to the users. It's a good idea to customize your alert messages so that they are visually distinctive and match with you company's branding.

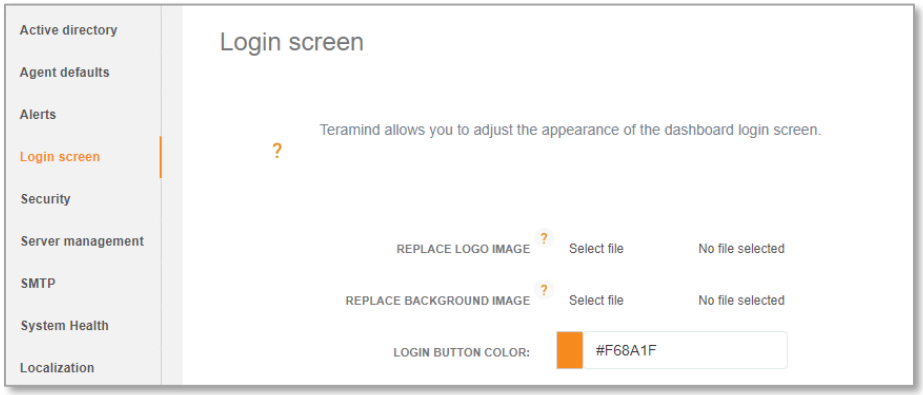


1. You can use the HTML template by default for all rules.
2. You can customize the look and feel of your message box by editing the HTML in the CUSTOM USER ALERT HTML field. There are a few dynamic variables such as ALERT, DETAILS you can use in your message. In addition, the alert can have buttons like: OK, CANCEL. You can also include base64-encoded images in your HTML. This is great for displaying icons or logos.
3. You can preview how the alert will look by clicking the **PREVIEW** button.
4. SCREEN LOCATION defines where the alert will be displayed (i.e. Center, Top-Left etc.).

5. WIDTH changes the width of the alert box.
6. HEIGHT changes the height of the alert box.
7. ALERT EMAIL LIMIT defines the threshold where the system will group the alerts into a single email. The system will send this many identical alert emails, and then it will group them together into an email digest. If set to 0, it will send each alert individually.
8. USER ALERT THRESH HOLD applies to rules with a Warn or Block action. The threshold sets the minimum time, in seconds, to wait between alerts that the user sees. If set to 0, users will see all alerts they violate, regardless of the frequency.
9. LOG ALERT THRESH HOLD sets the minimum time, in seconds, to wait between logging alerts to the Teramind system. If set to 0, it will not limit the number of alerts that are logged.
10. MAXIMUM DAILY ALERTS COUNT limits the total number of alerts which get logged by Teramind on a daily basis per alert type.
11. You can build rules in Teramind to set a user's task based on their activity. RULE TASK SELECTION ACTION TIMEOUT (SECONDS) defines the time out when switching tasks. If the user switches activity and remains in the new activity for the defined seconds, the rule will be re-evaluated.

13.7.6 Login Screen

You can customize the appearance of the dashboard login screen to match with your company's branding or user preference.

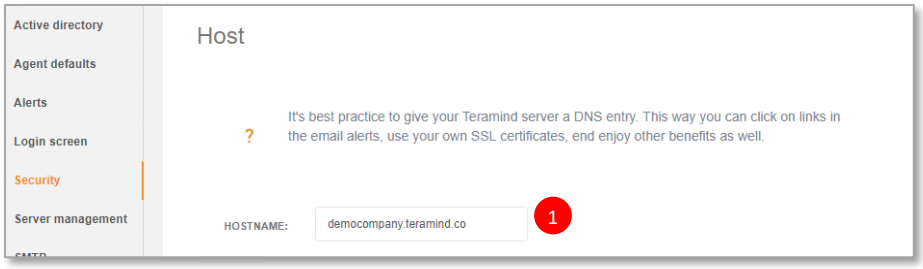


1. Use a LOGO IMAGE for uploading a logo image. Suggested resolution is 190x54 pixels.
2. Use a BACKGROUND IMAGE for uploading background image. Suggested resolution is 1400x933 pixels.
3. You can also change the LOGIN BUTTON COLOR by specifying a color in HTML/Hex format.

13.7.7 Security

13.7.7.1 Host

It's best practice to give your Teramind server a DNS entry. This way you can click on links in the email alerts, use your own SSL certificates, and enjoy other benefits as well.



1. Enter a hostname such as `dashboard.teramind.co`.

13.7.7.2 SSL

Teramind strongly recommends proper configuration of SSL in order to avoid browser warnings and restrictions. Some browsers will not allow web sockets communications if the certificates are invalid. This may prevent you from watching live screens or record them.

For convenience, Teramind comes pre-shipped with an SSL certificate that's valid for the hostname *onsite.teramind.io*.

> To learn how to generate your own self-signed certificates, check out this article on Teramind Knowledge Base.

If you wish to proceed without implementing your own certificates, you should add a line to your local hosts file and then access Teramind by browsing to https://onsite.teramind.io. You can do this by editing `C:\Windows\System32\Drivers\Etc\hosts` as Administrator and appending the following line to the file:

```
xxx.xxx.xxx.xxx onsite.teramind.io
```

Where **`xxx.xxx.xxx.xxx`** is the IP you assigned to your Teramind Virtual Machine.

In the long run, you should deploy your organization's SSL certificates within Teramind, and add a DNS entry in your corporate name server for your Teramind implementation.

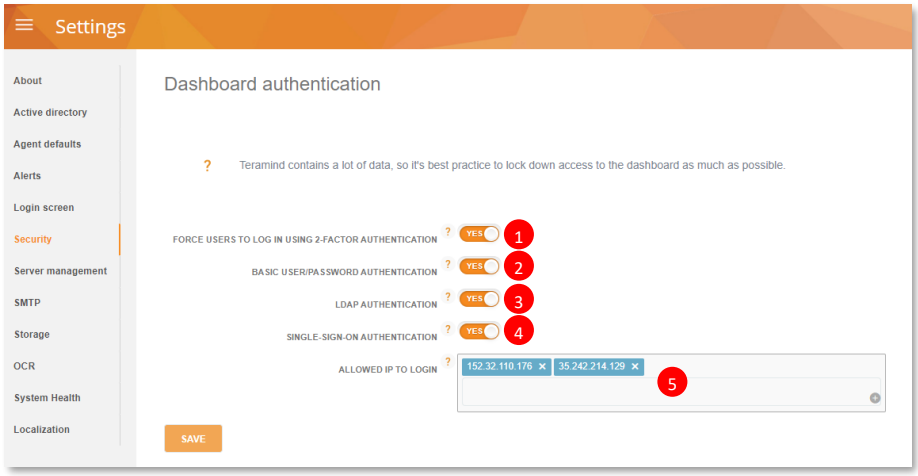
> Note that all certificates should be in the PEM format.

Here's how you should setup the SSL:

1. Upload your server's Private Key (usually a .key file), Public Key (usually a .crt file), Intermedia Key (a concatenated list of CA certificates that validates your server certificate) and the Root CA Key.
2. Click the **VALIDATE KEYS** button. After you're done, please access Teramind via the new hostname. You'll be asked to log-in again.

13.7.7.3 Dashboard Authentication

Teramind processes large volumes of confidential and private data, so it is a best practice to lock down access to the dashboard as much as possible.

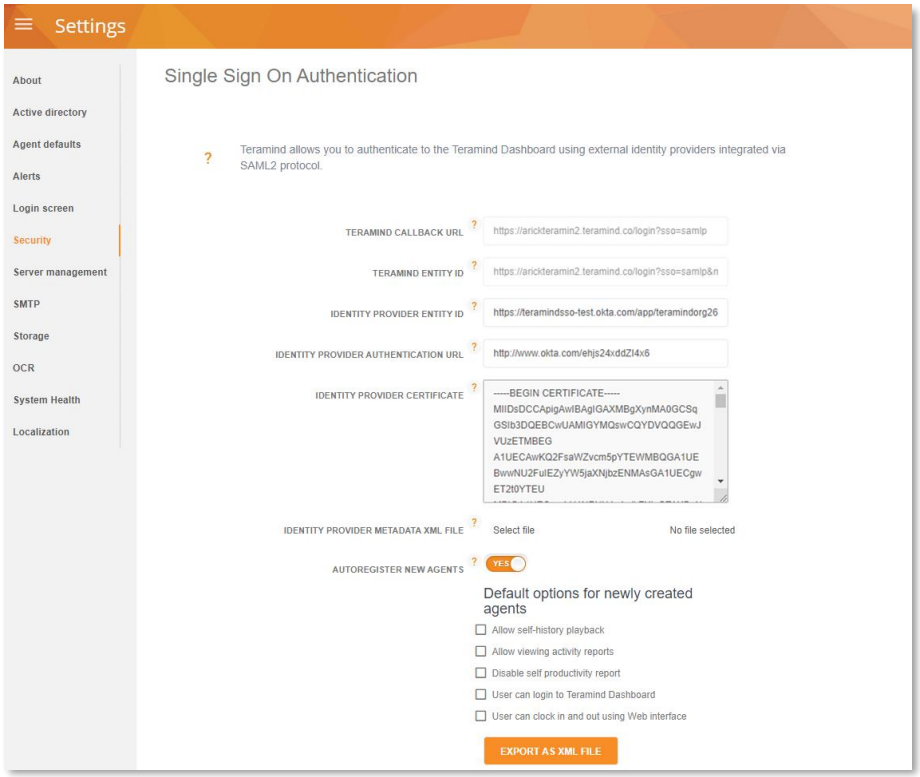


1. If you enable the FORCE USERS TO LOG IN USING 2-FACTOR AUTHENTICATION option, next time administrators log in they will be forced to enable 2FA before being given access to their dashboard. Teramind supports 2FA apps like Google Authenticator or Authy. Check out this Knowledge Base article to learn how to set up 2FA for a user.
2. Enabling the BASIC USER/PASSWORD AUTHENTICATION option will allow you to authenticate to the dashboard using the user-password credentials you created in Teramind. Check out this Knowledge Base article to learn how to create/change password for a user.

3. If you have successfully set up Active Directory integration, you may want to use your domain credentials to login. In such a case, you can turn on the LDAP AUTHENTICATION option. Check out the Active Directory section to learn more about AD setup.
4. If you enable the SINGLE-SIGN-ON AUTHENTICATION option, it will reveal the Single Sign On Authentication section. Please see below for details on this section.
5. The ALLOWED IP TO LOGIN option lets you specify which IP addresses are allowed to login to the dashboard.

13.7.7.4 Single Sign On Authentication

SINGLE-SIGN-ON AUTHENTICATION option allows you to authenticate to the dashboard using a Single Sign On (SSO) service such as Okta, One Login etc. via SAML2 protocol. Newly generated users will still need to set password in order to make further changes to account or login using Teramind revealed agent.

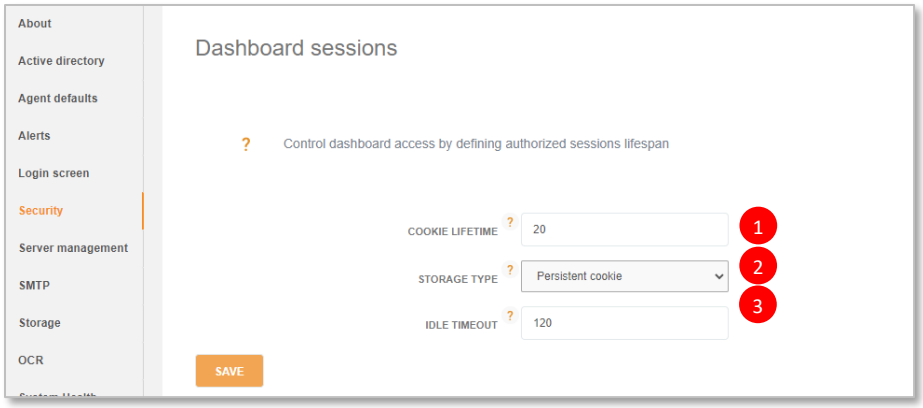


Enabling the SSO option will reveal several options which you can use to configure the SSO integration. You will also see an AUTO REGISTER NEW AGENT option. If enabled, this will let you specify default options for newly registered users/agents on SSO.

Check out this Knowledge Base article for details on these options and step by step instructions on setting up a SSO integration.

13.7.7.5 Dashboard Sessions

With these settings, you can control exactly how you want to mange your dashboard sessions such as cookie lifetime, session storage type and idle timeout.



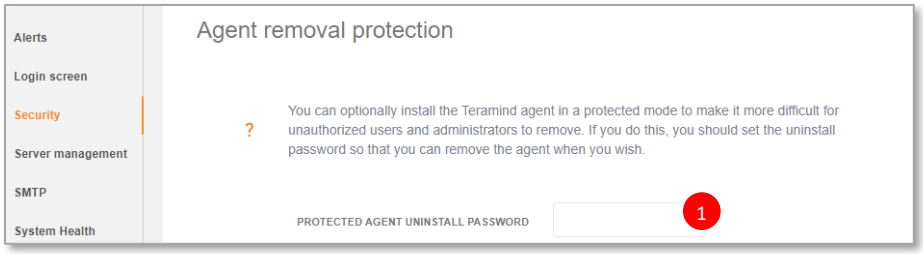
You can now control exactly how you want to mange your dashboard sessions including:

1. COOKIE LIFETIME defines how long an authorization cookie will be valid (in minutes). An authorization cookie is a temporary secret used to authenticate the browser. It will be automatically updated in the background while the user is active. The update process takes a few seconds before it is going to expire. If the user closes the browser before the secret was updated, the session will be closed, and the user will need to authorize again.
2. STORAGE TYPE defines whether it will be Persistent storage or Session storage. A Persistent cookie is kept for the duration/lifetime of the Cookie lifetime. A Session cookie gets flushed when you close your browser (different per browser settings) or until Cookie lifetime expire.
3. IDLE TIMEOUT defines how long a session will remain active when the user is idle (in minutes). If the user is not active for the number of minutes defined, a pop-up window will ask the user if they want to resume the session:

If there is no response, the session will be closed automatically, even if the COOKIE LIFETIME is still valid.

13.7.7.6 Agent Removal Protection

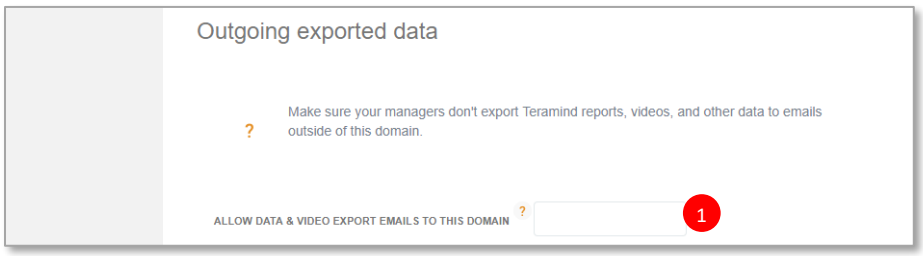
You can optionally install the Teramind Hidden Agent in protected mode to make it more difficult for unauthorized users and administrators to remove it. If you do this, you should set the uninstall password so that you can remove the agent when you wish.



1. Enter a password to protect the Agent uninstallation.

13.7.7.7 Outgoing Exported Data

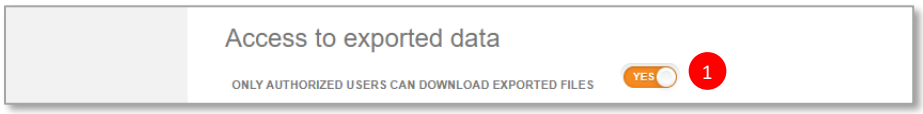
By default, Teramind allows you to export reports and video recordings to any email address. But you can change the settings to restrict export to certain domain only.



1. Enter a domain address to restrict export emails to that domain only.

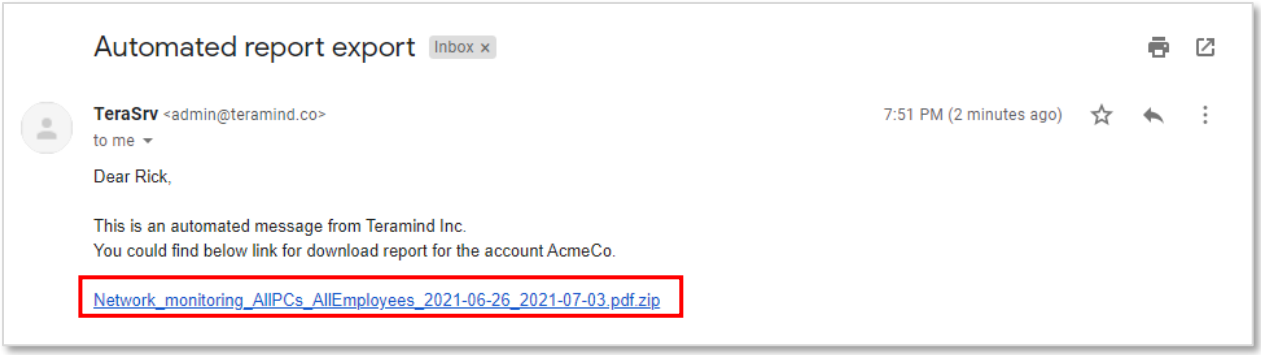
Note that this option does not affect scheduled reports (see *Schedule export* option under the Exporting a BI Report section to learn more about scheduled reports). You can still send scheduled reports to email recipients who are not on the Teramind Dashboard (i.e. they are not on the List of employees screen). To prevent access to such exported reports, enable the ONLY AUTHORIZED USERS CAN DOWNLOAD EXPORTED FILES option under the Access to exported data section.

13.7.7.8 Access to Exported Data



1. Click the **Yes**/**No** toggle button for the ONLY AUTHORIZED USERS CAN DOWNLOAD EXPORTED FILES option to enable/disable it.

If you enable this feature and then use the BI Reports > Export > Schedule Export option to add an email recipient who is not on the Teramind Dashboard, the email recipient will still get the automated email, but the report download link in the email will not work:



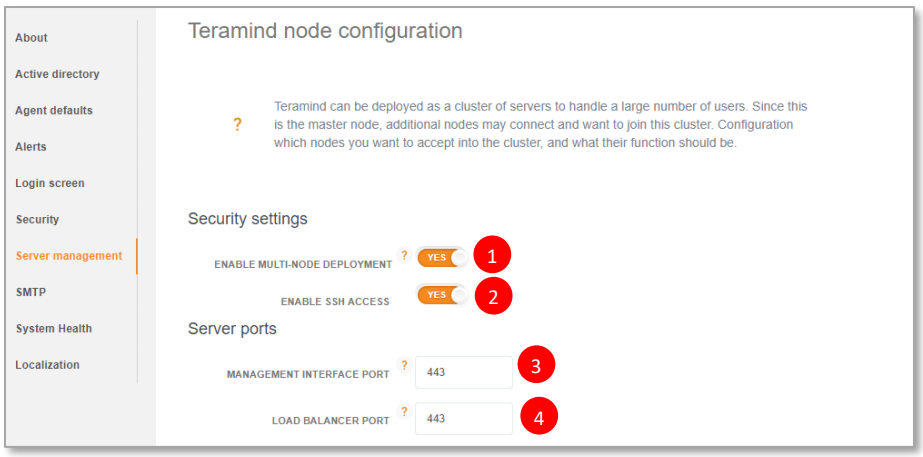
This option would enable you to better control the privacy and security of your data. For example, if a recipient of the automated report accidentally or intentionally forwards the email to someone else, the other person will not be able to access this report unless they are authorized.

> This option applies to scheduled export reports only. It does not apply to the reports available on the *SYSTEMS > Video export* and *SYSTEM > Report export* screens. It also does not affect the Session Player's Video Download/Export option.

13.7.8 Server Management

13.7.8.1 Multi-Node Configuration

Teramind can be deployed as a cluster of servers to handle a large number of users. If you can see this setting on your dashboard, then it means you are on a Master node. Additional nodes (such as the OCR database and screen mining nodes) may connect and want to join this cluster. Here you can configure which nodes you want to accept into the cluster, and what their function should be.



1. You can enable/disable multi-node deployments with the ENABLE MULTINODE DEPLOYMENT toggle button. It is necessary to keep it turned on if you have more than one Teramind servers.
2. Turn SSH access on or off with the ENABLE SSH ACCESS toggle button. SSH is needed for remote login and configuration of Teramind servers, especially, during the deployment phase.

3. Managers and administrators will be able to access the Teramind dashboard on the MANAGEMENT INTERFACE PORT. Make sure the port is available before using it*.
4. Teramind Agent will query this LOAD BALANCER PORT instead of the default 443 when looking for a Teramind server to connect to. If you change it something other than 443, you will need to use the TMROUTER parameter when installing the Teramind Agent. For example*:

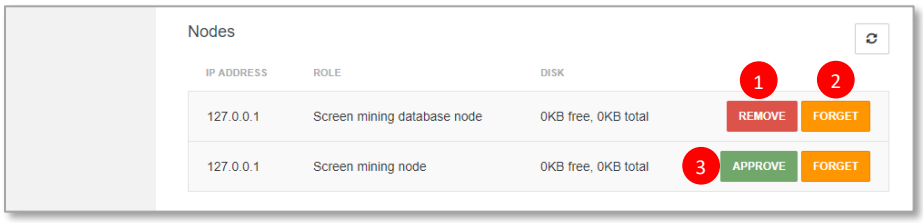
```
c:\msiexec /i teramind_agent_x64_s.msi TMROUTER=101.12.1.2:xxx /qn
```

Where **xxx** is the load balancer port.

> * **Reserved Ports:**
> The following ports are reserved and cannot be used for the Management Interface or Load Balancing: 22, 111, 5432, 4730, 8000, 8001, 8002, 9000, 6379, 10000, 10001.

13.7.8.2 OCR Nodes

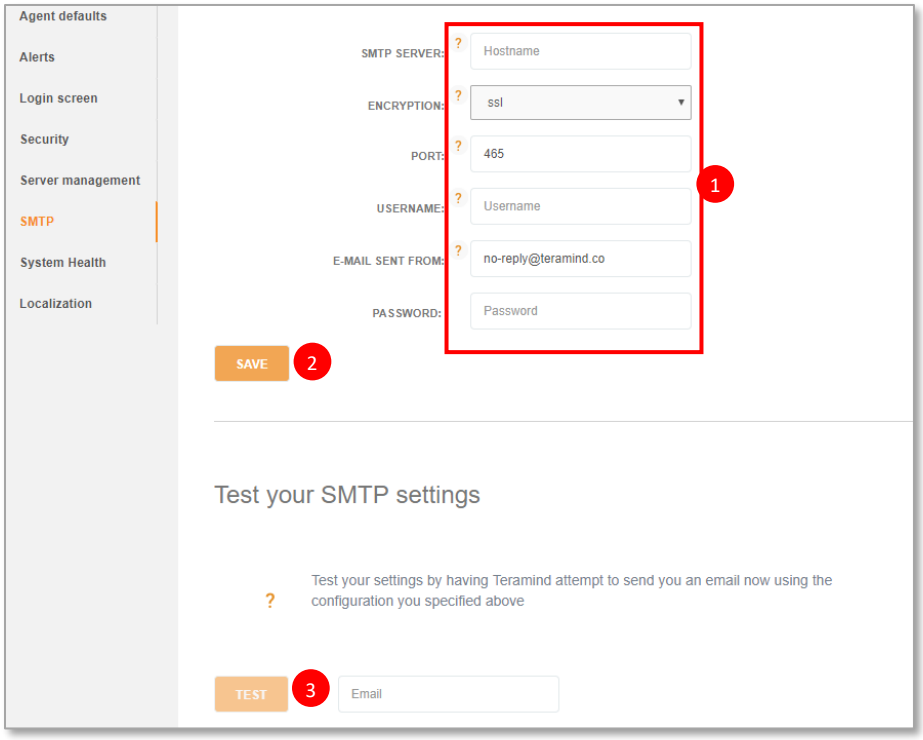
If you have setup an *OCR database node* or an *OCR mining node*, you will see the nodes displayed under the *Nodes* section on the Server Management tab. Please consult the relevant deployment guide to learn how to setup the OCR nodes. You can find the deployment guides on https://www.teramind.co/company/resources under the *Product Guides* category.



1. Click the **REMOVE** button to cancel approval (un-approve) for a previously approved node.
2. Click the **FORGET** button to completely delete a node. For example, if you deleted a Virtual Machine used by an OCR node, you can delete the node from here.
3. Click the **APPROVE** button to approve any pending node connection requests.

13.7.9 SMTP

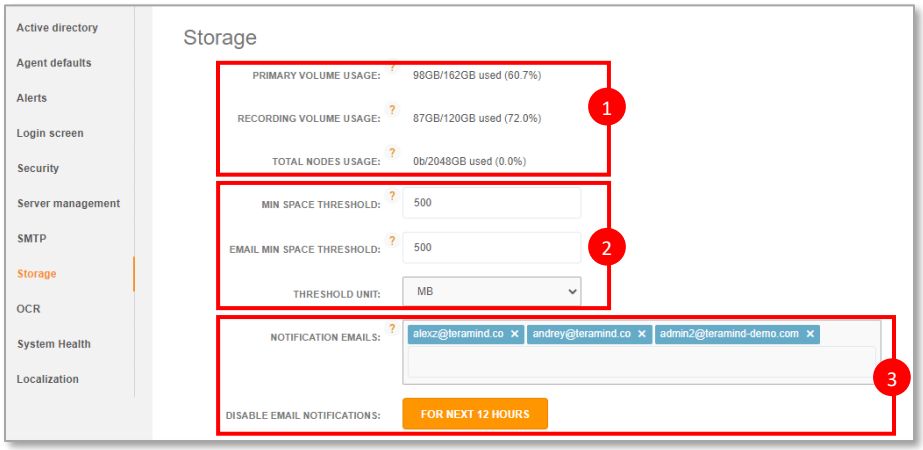
Teramind uses the SMTP email standard to send notifications, deliver scheduled reports and other communications purposes. You can specify your SMTP server configuration here so that Teramind can access it properly.



1. Provide details for the server, encryption, port, username, email and password. Consult your email server's settings for the SMTP configuration or contact your email provider.
2. Click the **SAVE** button.
3. Test your settings by having Teramind attempt to send you an email using the configuration you specified.

13.7.10 Storage

The Storage tab shows the usage statistics of various internal volumes and lets you configure thresholds and alerts when they reach certain levels.



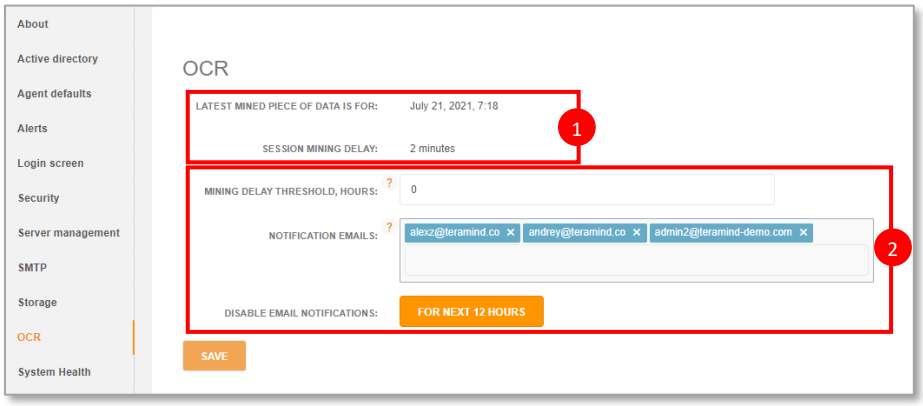
1. The first three sets of data show the size and usage statistics for the three types of storage volumes used by Teramind:

- The PRIMARY VOLUME USAGE indicates the size and usage of the main system volume. This volume typically contains the Teramind database.
- The RECORDING VOLUME USAGE shows the status of the screen recording volume. You can always adjust the volume usage by tweaking your screen recording settings and retention policies. Check out the Editing Screen Settings section to learn more.
- The TOTAL NODES USAGE shows information about the OCR/TeraServer nodes.

2. The second three sets of fields allow you to configure threshold for the recording volume:
   - The MIN SPACE THRESHOLD tells Teramind to stop recording when it reaches this minimum space threshold. You can specify a value in MB or % (see THRESHOLD UNIT below). Please note that Teramind will automatically disable recordings at *500MB*.
   - The EMAIL MIN SPACE THRESHOLD determines at what point an email alert will be sent. *This value must be equal to or greater than minimum space threshold*. You can specify a value in MB or % (see THRESHOLD UNIT below). A value of 0 will disable the email alert.
   - The THRESHOLD UNIT lets you specify what unit is used for the above two thresholds. You can select MB or %.
3. The NOTIFICATION EMAILS field lets you specify who will receive the notification email for the EMAIL MIN SPACE THRESHOLD alert. You can disable the notifications temporarily by clicking the **FOR NEXT 12 HOURS** button. You can turn off email notifications completely by leaving the NOTIFICATION EMAILS field empty or by specifying a value of '0' in the EMAIL MIN SPACE THRESHOLD field.

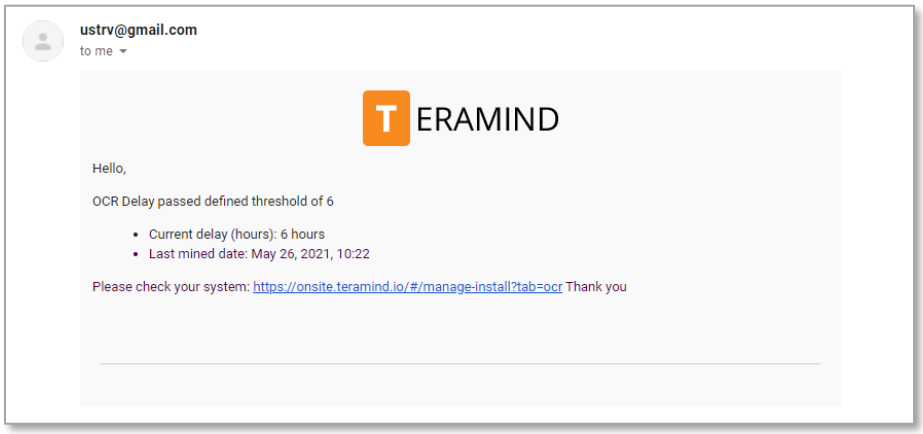
13.7.11 OCR

The OCR tab shows the usage statistics of the OCR session mining node and lets you configure thresholds and alerts when its usage reaches certain level.



1. The first two data sets show the OCR processing status. LATEST MINED PIECE OF DATA IS FOR shows the date and time when the OCR engine last processed a screen image, and the OCR DELAY shows the time it took for the OCR engine to analyze the last screenshot and detect text inside that image.
2. The second three sets of fields allow you to configure threshold and email alerts for the recording volume. With the MINING DELAY THRESHOLD, HOURS you can set up a threshold (in hours) and specify email address(es) in the NOTIFICATION EMAILS field. If the mining delay

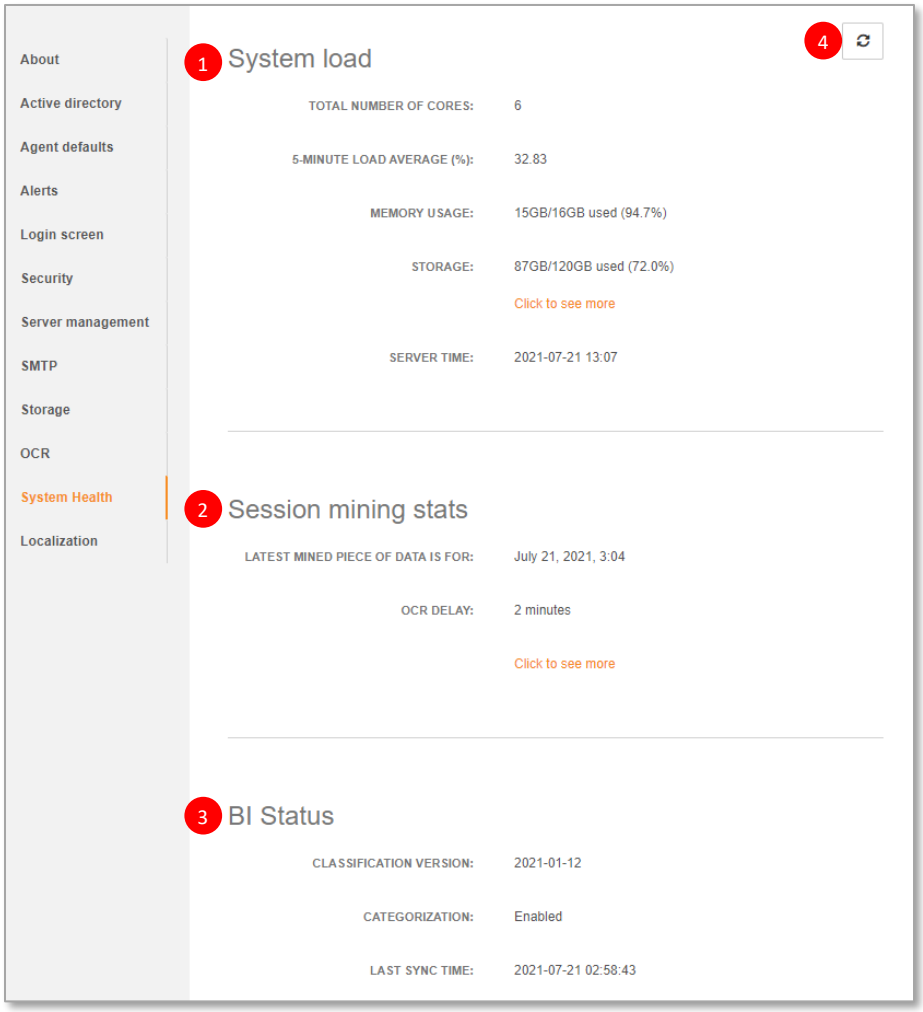
crosses the defined threshold, the recipients in the emails will get a notification like the below example:



You can disable the notifications temporarily by clicking the **FOR NEXT 12 HOURS** button. You can turn off email notifications completely by leaving the NOTIFICATION EMAILS field empty or by specifying a value of '0' in the MINING DELAY THRESHOLD, HOURS field.

13.7.12 System Health

System Health tab gives you a quick snapshot of the current status of the server load, session mining (OCR process) status and the BI status.



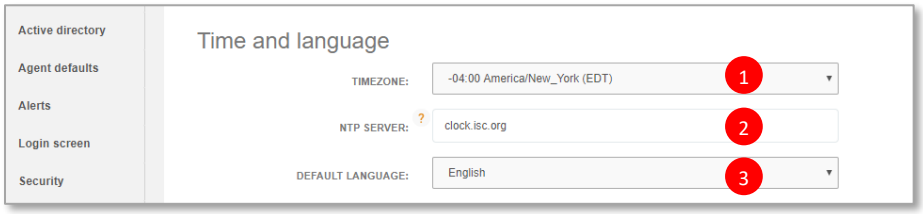
1. The *System load* section shows the TOTAL NUMBER OF CORES the CPU has, 5-MINUTE LOAD AVERAGE (%), MEMORY USAGE, STORAGE and SERVER TIME. Clicking the *Click to see more* link will take you to the Storage tab where you can view more information about the storage usage and set up threshold alerts.
2. The *Session mining stats* shows the OCR processing status. LATEST MINED PIECE OF DATA IS FOR shows the date and time when the OCR engine last processed a screen image, and the OCR DELAY shows the time it took for the OCR engine to analyze the last screenshot and detect text inside that image. Clicking the *Click to see more* link will take you to the OCR tab where you can view more information about the OCR usage and set up threshold alerts.
3. The *BI Status* shows three pieces of information:
   - The first field shows the current CLASSIFICATION VERSION used by the BI engine. Check out this Knowledge Base article to learn how to update your BI Classifications.
   - The second field shows if the CATEGORIZATION of apps/websites is enabled. When enabled, Teramind will use the inCompass® NetSTAR, a comprehensive web categorization and filtering technology to automatically classify websites and their reputations. The update package contains these classification definitions.

- The data displayed on the BI reports is not real-time. It can take up to 4 hours for it to refresh. The third field under *BI Status* shows the LAST SYNC TIME when BI the engine processed the reports.

4. Click the **Refresh** button to refresh the screen.

13.7.13 Localization

Localization tab allows you to change the time and language settings.

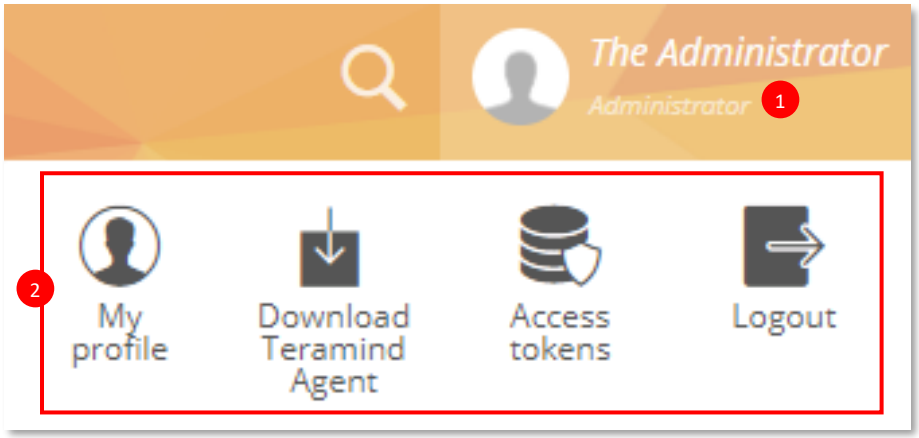


1. You can change the TIMEZONE you want to use.
2. Use the NTP SERVER to specify a time server. Teramind will automatically sync the clock with the server. You can select a generic server like *clock.isc.org* if your deployment has internet connectivity. Note that, for the best result make sure all your monitored endpoints and the Teramind server are on the same NTP. Otherwise, you may see discrepancy between the time an activity happened vs. the time it's recorded in Teramind. Note that, this option is not available on Cloud deployments.
3. You can change the DEFAULT LANUGE used by the system. Teramind supports English, Spanish, Chinese, Portuguese, Russian and Turkish. Note that, you can change the language for an employee/user from their Profile page.

14 Administrator Menu

The Administrator menu allows you to change the currently logged in administrator's profile, download the Teramind Agent and setup access tokens for the Teramind API.

14.1 Accessing the Administrator Menu



1. Click the **Username** near the top-right corner of the Teramind Dashboard. A pop-up menu will be displayed.
2. From the pop-up menu, select an item from: **My profile**, **Download Teramind Agent**, **Access tokens** or **Logout**.

14.2 My Profile

When you click the My Profile menu, it will open a pop-up window where you can edit your personal information, account information, 2-Factor authentication and monitoring options. You edit your profile the same way you would edit an employee's profile. Please check out the Entering / Editing Employee Profiles section to learn how to edit your profile.

14.3 Download Teramind Agent

> If you encounter any issue installing the Agent, please check out the Troubleshooting section of the Knowledge Base.

Teramind Agent is the application that runs natively on the Windows and Mac computers and tracks the users' activities. It must be installed on every machine that you want to track. It is the application that generates all the data needed for every use case of the Teramind platform.

Notes for the Teramind Mac Users

- At the moment, Teramind on Mac has limited functionalities and are only supported on macOS 18 (Monterey), macOS 11 (Big Sur), macOS 10.15 (Catalina) and macOS 10.14 (Mojave). Check out this article to learn which Teramind features are available on the Mac.
- You cannot run the installer from the browser directly on Mac. You need to run it from the Launcher / Finder.
- After installing the Agent, you may need to configure some MacOS permissions for the agent to function properly. Check out the macOS Permission Settings section below to learn more.
- On Apple M1 computers, Rosetta needs to be installed first for the Hidden Agent to work properly. You can use the following command to install it:
  `/usr/sbin/softwareupdate --install-rosetta --agree-to-license`

There are two versions of the Agent you can download: Hidden Agent and Revealed Agent.

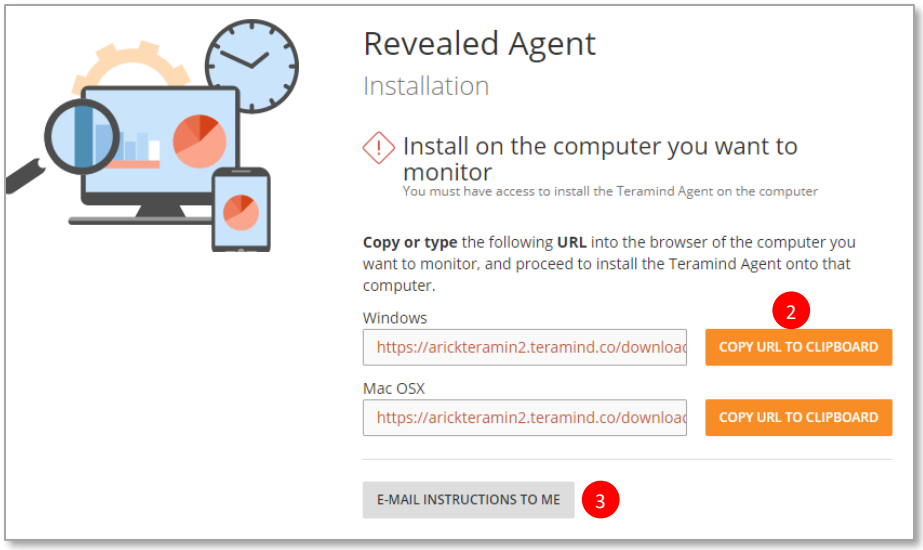
14.3.1 Revealed Agent

The Revealed Agent tracks users and computers but only when the user is logged-in on the Agent. When a user launches a Revealed Agent, they have to login using an account created in the Teramind Dashboard by an administrator. All the activities tracked will be linked to this account. Since the hours they work are clearly defined by the clock-in and clock-out times from the Revealed Teramind Agent, the payroll can be calculated, and tasks can be assigned to the users. This Agent is the perfect choice for monitoring contractors, vendors and freelancers or when you want to let your employees choose how and when they are to be monitored.

14.3.1.1 Downloading the Revealed Agent

To download the Revealed Agent, do the following:

1. On the Download Teramind Agent screen, choose **Yes** when asked, *'Do you want your users to know that they are being monitored*?'. You will be given the option to choose an Agent version.

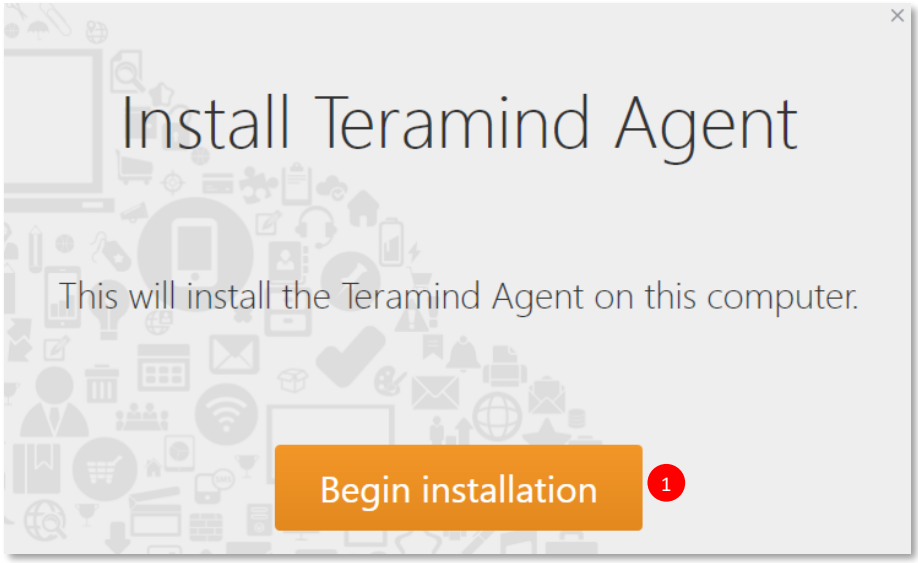


You can open the Teramind Dashboard on the target PC and download the Agent directly from this page. Or you can do the following:

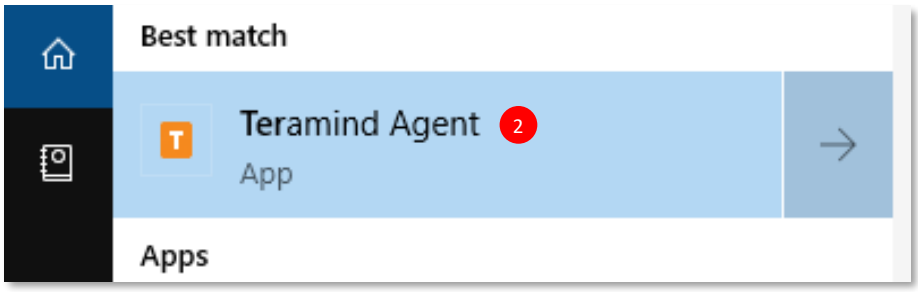
2. You can copy one of the URLs, open it in your browser and save the installer file on a USB stick and take it to the target computer.
3. You can email yourself the instruction, login to the target computer and download the Agent from the links in the email.

14.3.1.2 Installing the Revealed Agent

Run the Agent installer file on the computer. Notice that, you will need administrator privilege to install the Agent properly.



1. Click the Begin installation button to install the Agent.



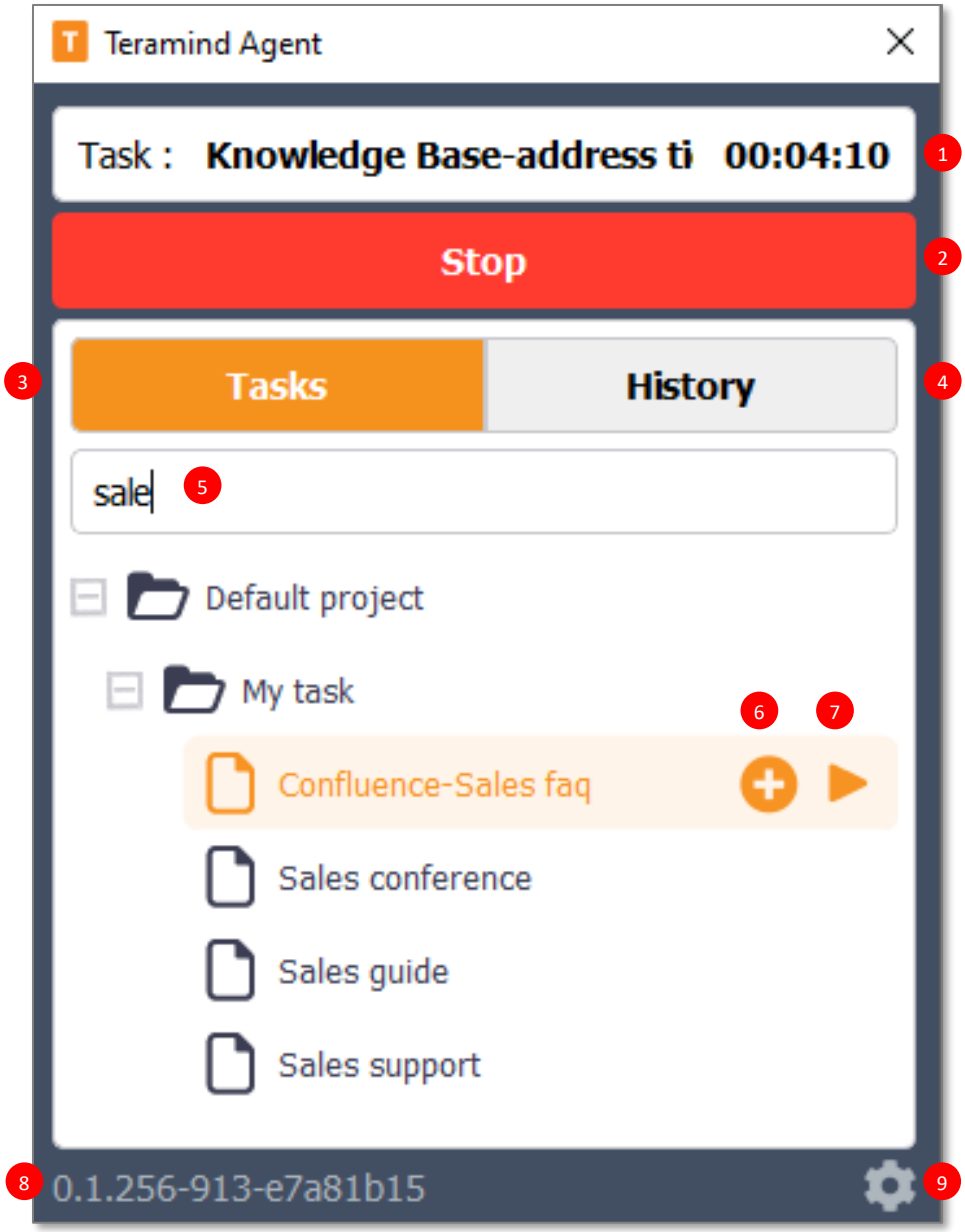
2. When the installation is complete, the user can launch the Agent from the Start Menu (Windows) or from the Launcher/Finder (macOS).

Mac OS Permission Settings:
You might need to change some permission settings while installing the Teramind Agent on Mac. Follow the instructions under the macOS Permission Settings for Installing the Teramind Agent section below to learn how.

14.3.1.3 Using the Revealed Agent

Launch the Revealed Agent from the Start Menu (Windows) or from the Launcher/Finder (macOS).

1. Enter your **username** and **password**. If you do not have your credentials, please ask your admin to add you as a user/employee.
2. Click the **Advanced** link to select your server. This will bring up a pull-down menu where you can select your server.
3. If you are cloud customer, just select Teramind Cloud from the pull-down list. If you are an on-premise customer, enter the server instance name (the URL of your Teramind dashboard without the *https* part.).
4. Click the **Sign in** button to start the Agent:



1. On the top of the interface, you will see the currently active task or a 'Not active' status.
2. To start/stop clock-in/clock-out: Select a task from the list and click the **Start** / **Stop** button.
3. To view a list of tasks: Click the **Tasks** tab.
4. To view past activities: Click the **History** tab.
5. To search for a task: Click on the **Search** field and start typing.
6. To add a task or sub-task: Hover over a task or sub-task. Click the **Plus** icon to add a task.
7. To start a task: Hover over a task or sub-task. Click the **Play** icon to start the task.
8. At the bottom left, you will see the agent version.
9. Click the **Gear** icon at the top-right corner to **Refresh tasks**, **Sign out** or **Exit** the agent.

14.3.2 Hidden Agent

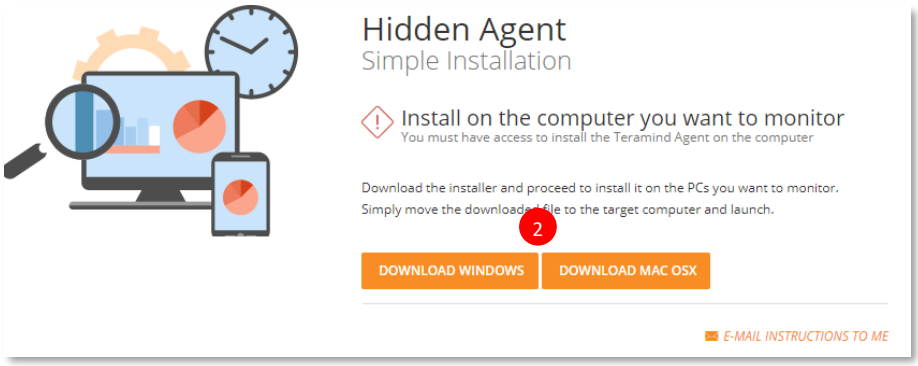
The Hidden/Stealth Agent tracks computers (and not users), so the data that comes from the Agent will be linked to a computer and not a user. The computers tracked appear automatically in the dashboard. Computer names must be unique. If you are trying to monitor multiple computers with the same computer name, only the first one will be monitored. The names are taken directly from the registered machines. If a computer is renamed, Teramind will auto-update. The Hidden Agent is useful when you do not want your users to know that they are being monitored.

14.3.2.1 Downloading the Simple Hidden Agent

To download and install the Hidden Agent, do the following:

1. On the Download Teramind Agent screen, choose **No** when asked, *'Do you want your users to know that they are being monitored*?'. You will be given the option to choose the installation process.

2. When asked, '*Which kind of installation process do you prefer*?', select **Simple Installation**.



3. Download one of the Agent installers, copy it to the target machine. Alternatively, you can open the Teramind Dashboard on the target PC and download it directly from this page.

4. You can also email yourself the instruction, login to the target computer and download the Agent from the links in the email.

14.3.2.2 Installing the Simple Hidden Agent

Run the Agent installer the same way you would install a Revealed Agent. The only exception is that, the Agent will not show up as an application after installation is finished.

14.3.2.3 Installing the Hidden Agent with Group Policy Object (GPO)

Group policy object (GPO) based installation requires Active Directory. Please download agent .msi package.

You have to pass `TMROUTER` parameter (Teramind server address/IP) to the MSI and therefore you need to create an MST file. That can be done with 3rd party tools like *Orca*.

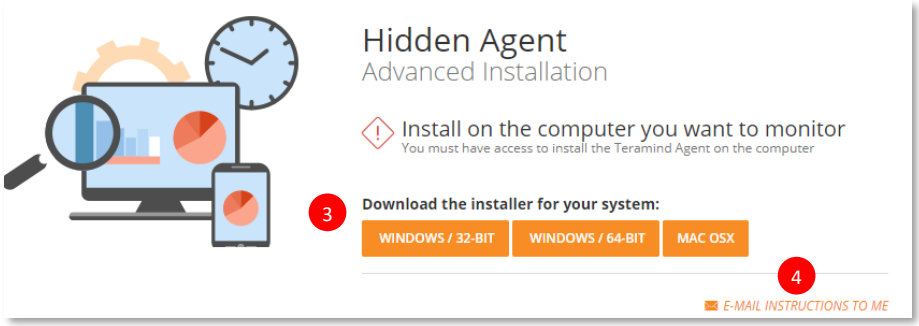
After that, please create a Group Policy Object and select 'Advanced' option and specify the `.msi` and `.mst` files.

14.3.2.4 Downloading the Advanced Hidden Agent

To download and install the Advanced versions of the Hidden Agent, do the following:

1. On the Download Teramind Agent screen, choose **No** when asked, *'Do you want your users to know that they are being monitored*?'. You will be given the option to choose the installation process.

2. When asked, '*Which kind of installation process do you prefer*?', select **Advanced Installation**.



3. Download one of the Agent installers, copy it to the target machine. Alternatively, you can open the Teramind Dashboard on the target PC and download it directly from this page.
4. You can also email yourself the instruction, login to the target computer and download the Agent from the links in the email.

14.3.2.5 Installing the Advanced Hidden Agent – GUI Method

Note that this option is available for Windows only.

Run the Agent installer MSI the same way you would install a Revealed Agent. The only exception is, apart from some popups from the OS asking for permissions for the installation, there is no other user input. After the installation, the computer is monitored immediately.

14.3.2.6 Installing the Advanced Hidden Agent – Command Line Method

Windows:

MSIEXEC can be used in either command line or from within a script, as follows:

```
C:\> msiexec /i <//path-to/teramind/agent.msi>
```

Where **<//path-to/teramind/agent.msi>** is either a URL, network, or local path to the Teramind Agent MSI file.

You can use these optional parameters:

/qn	Enables silent installation.
TMROUTER=**< ip-of-vm:port>**	Load balancer IP and port. Please see Server Management section for more information.
TMINSTANCE=**<account-name>**	Provide an **<account-name>** or use **onsite** for on-premise deployment.
TMDISABLEAUDIO=**1**	Turns audio off.
TMDOMAINOVERRIDE=**<domain-name>**	To override your domain/PC name with the specified-**<domain-name>**.

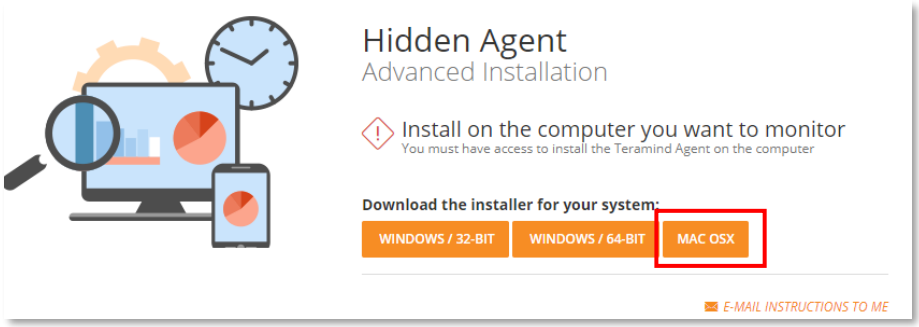
`DO_PROTECTION=yes`	Installs the hidden agent in protected mode. Installing the Agent in protected mode helps: • prevent users from seeing the Agent in system services list • prevent the stopping of the service using commands such as: '`sc stop`' • prevents corruption of the service registration • prevent uninstall by unauthorized admins You can specify the protection password in the Agent Removal Protection section of the dashboard.

Mac:

To install macOS Hidden Teramind Agent run this command in the Terminal (**Applications** > **Utilities** > **Terminal**)

```
curl //path-to/teramind-mac-installer/ | sudo bash -
```

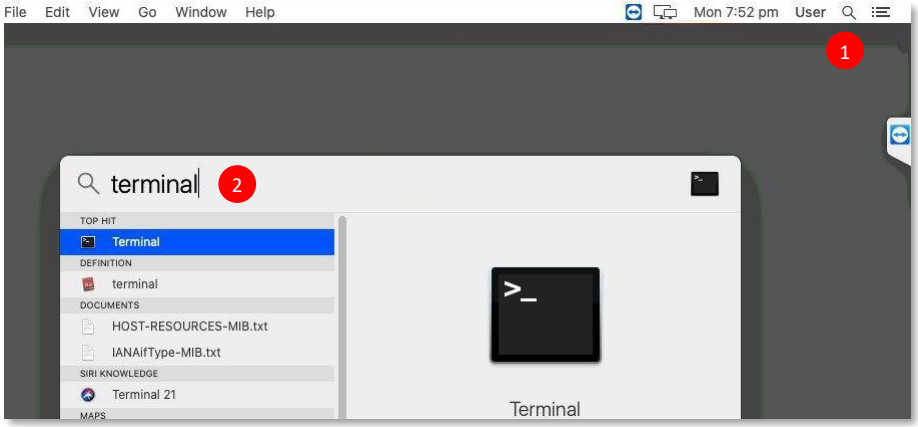
You can get the **//path-to/teramind-mac-installer/** from Advanced Hidden Agent's download screen by clicking the **MAC OSX** button:



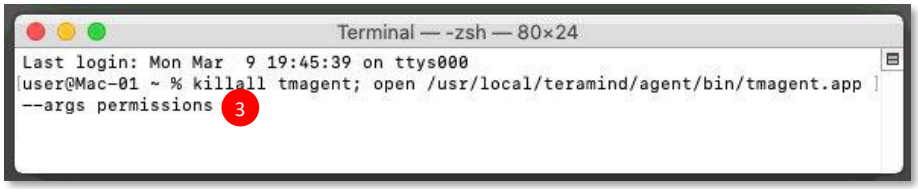
Follow the macOS Permission Settings for Installing the Teramind Agent section below to install the agent.

14.3.3 macOS Permission Settings for Installing the Teramind Agent

There are two permissions required for the Mac Agent to function properly. Follow the steps below the set them up.



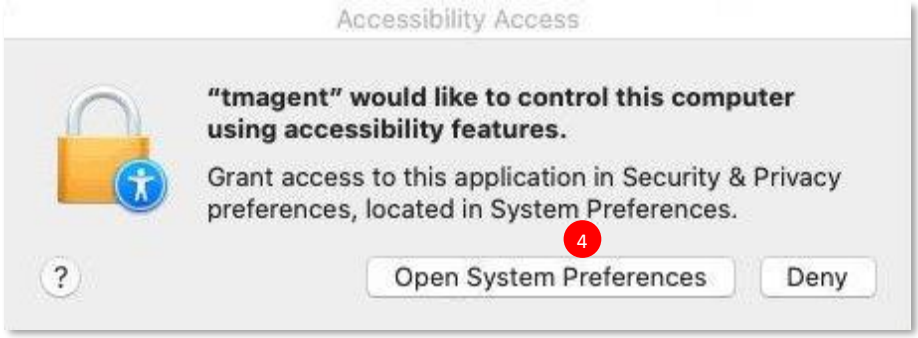
1. Click the **Search** icon from your Mac menu.
2. Type '`terminal`' in the search box to find the *Terminal* app. Select the Terminal app and press **Enter** to run it.



3. Type the following command on the Terminal window and press **Enter**:

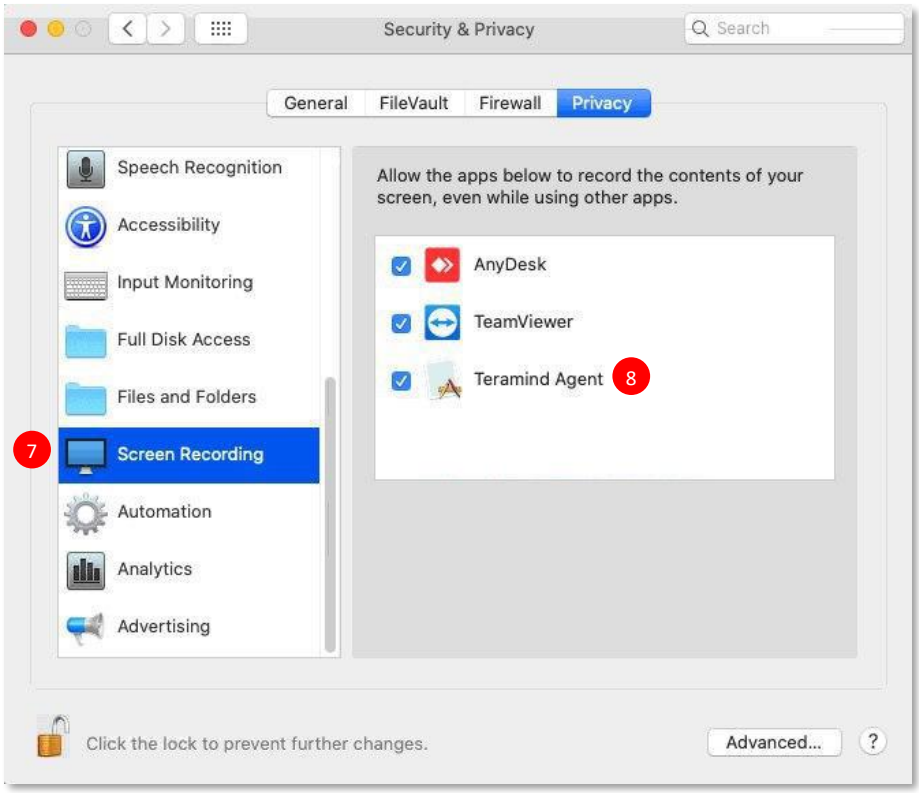
```
killall tmagent; open /usr/local/teramind/agent/bin/tmagent.app --
args permissions
```

A pop-up window will appear.



4. On the *Accessibility Access* pop-up window, click the **Open System Preferences** button. This will take you to the *Accessibility* settings option.

5. On the *Security & Privacy* settings window, first click the **Lock** icon at the bottom to unlock the settings.
6. Then, click the checkmark next to the *Teramind Agent* to grant it the accessibility permission. Do not close this window yet.



7. On the same *Security & Privacy* settings window, scroll up/down to find the Screen Recoding item on the left. Select it.
8. Click the checkmark next to the *Teramind Agent* to grant it screen recording permission. This will open a pop-up window.

9. Click the **Quit Now** button when the system shows, *"tmagent" will not be able to…* warning message. The Agent will restart and should work properly from now on.

14.3.4 Antivirus Considerations

Teramind Agent and its drivers come digitally signed with an extended-validation certificate. We made every effort to coordinate our signature with the major antivirus vendors, and as a result, Teramind will not introduce any issue with the vast majority of antivirus software. Nevertheless, if you encounter any problems while downloading, installing or updating the Agent, consult the *Antivirus Configuration Guide* found on our Resources page or check out the Knowledge Base.

14.3.5 Uninstalling the Agent

Please do not delete the Teramind folder, files or use Windows' or Mac's built-in app remover or any other third-party uninstallers to remove the Teramind Agent. Use the following methods to remove the Agent instead.

Windows (local):

To uninstall the Agent, run the Teramind Agent Removal Tool. On-Premise or Private Cloud (Azure/AWS) customers can download the tool from: https://www.teramind.co/portal. Cloud customers can download it from: https://teramind.co/d/teramind-remover.exe. Run the remover tool on the user machine you want the agent uninstalled from.

If you are removing a protected Agent locally:

An admin can protect an Agent from unauthorized uninstall (see the Agent Removal Protection section to learn more). To uninstall such a protected Agent, use the following command on the Windows Command Prompt (make sure you have admin access):

```
teramind_remover.exe /PASSWORD=<your-pass>
```

Where **<your-pass>** is the password you used to protect the Agent. You do not have to use the `/PASSWORD` option if you are the same admin who installed the Agent originally.

Windows (remote):

1. Click the **COMPUTERS** menu.
2. Click a computer's name from the list of computers.
3. Click the **UNINSTALL AGENT FROM PC** button.

If you are removing a protected Agent remotely:

An admin can protect an Agent from unauthorized uninstall (see the Agent Removal Protection section to learn more). To uninstall such a protected Agent, use the following command on the Windows Command Prompt (make sure you have admin access):

```
psexec \\remote_pc -u admin_username -p admin_password -s teramind-
remover.exe /PASSWORD=your_pass
```

Where, **`remote_pc`** is the IP/resolved name of the PC you want to remove the agent from. For example, `johns_pc`. The **`admin_username`** and **`admin_password`** are your admin username and password and **`your_pass`** is the password you used to protect the Agent. You do not have to use the `/PASSWORD` option if you are the same admin who installed the Agent originally.

Mac (Hidden Agent):

Run the following command in the Terminal (**Applications** > **Utilities** > **Terminal**) to uninstall a Hidden Agent:

```
curl //path-to/teramind/uninstall-mac | sudo bash -
```

Where **//path-to/teramind-server/** is the URL of your Teramind Server.

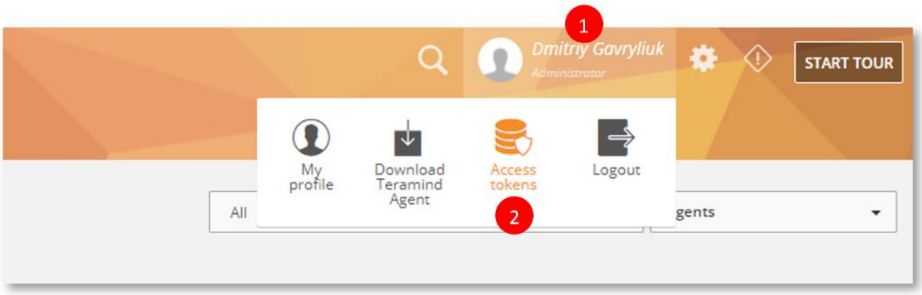
Mac (Revealed Agent):

Run the following command in the Terminal (**Applications** > **Utilities** > **Terminal**) to uninstall a Revealed Agent:

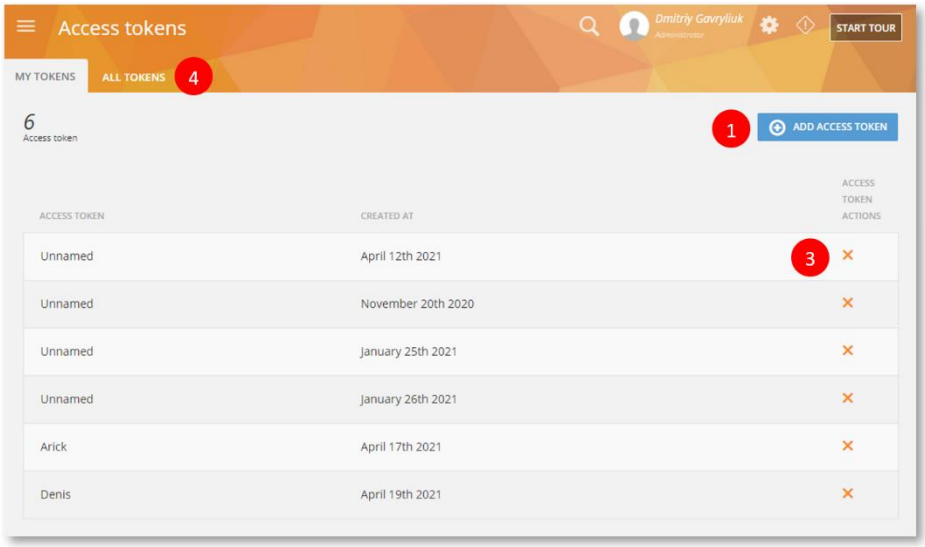
```
sudo /usr/local/teramind/agent/bin/uninstall.sh
```

14.4 Access Tokens

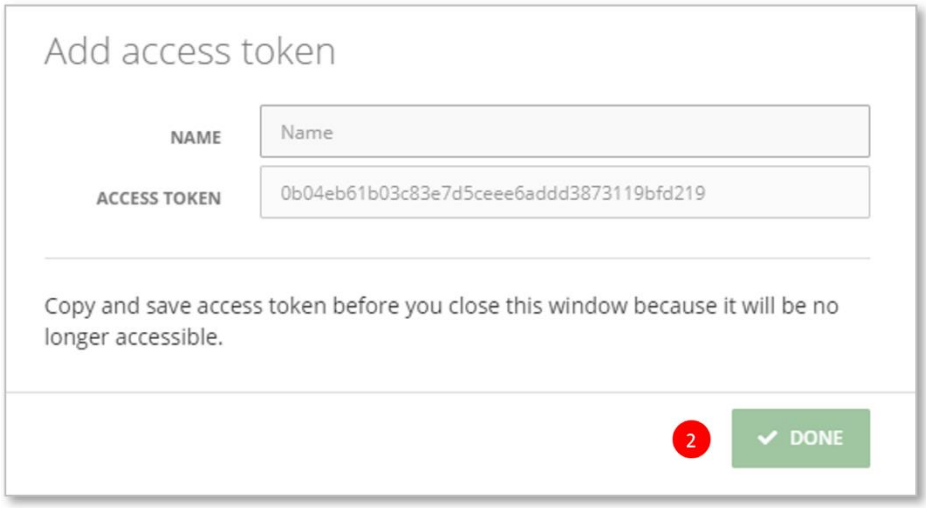
Access Tokens menu allows you to create access tokens for use with the Teramind API. You can see the current access tokens, create/delete tokens. If you are admin, you can also manage tokens created by other users. To access the Access tokens screen:



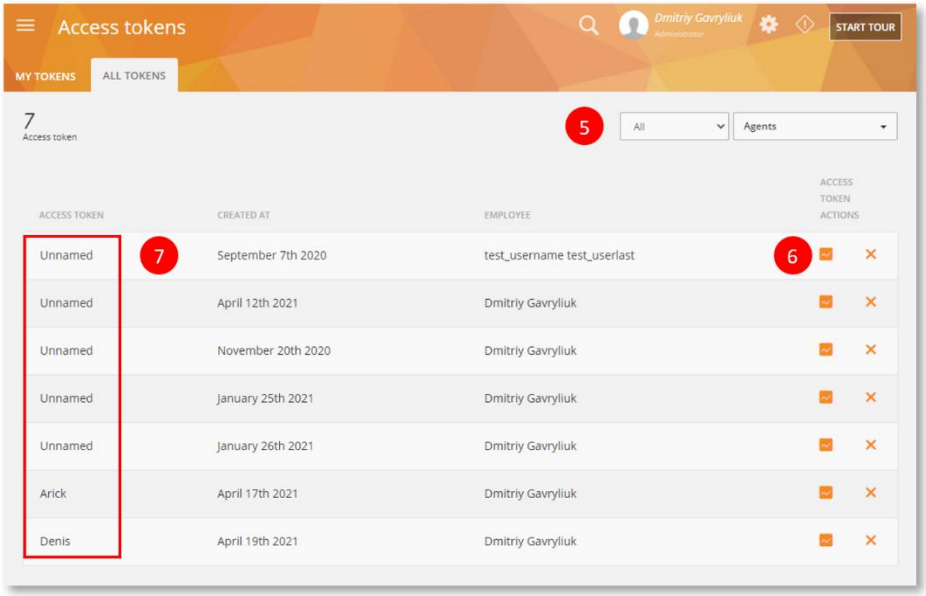
1. Click the **Username** near the top-right corner of the Teramind Dashboard. A pop-up menu will be displayed.
2. From the pop-up menu, select **Access token**.



1. To create an access token, click the **ADD ACCESS TOKEN** button. A pop-up window will show up:



2. Enter a name for your token and click the **DONE** button.
3. You can delete a token by clicking the X icon.
4. If you are an admin, click the **ALL TOKENS** tab to view tokens created by other users:

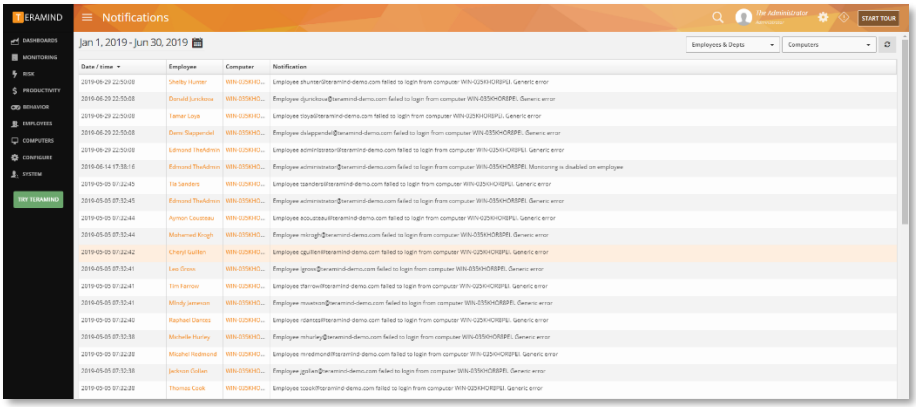


5. You can filter the list of access tokens by account type (e.g., administrator, employee etc.) using the first filter menu or select individual users from the second pull-down menu.
6. Clicking the **Stats** icon on the ALL TOKENS tab will take you to the SYSTEM > System Log screen and apply the selected token as a filter to display the log.
7. Note that, access token created in an earlier version of the dashboard will be displayed as 'Unnamed'.

Teramind has a powerful set of APIs you can use to programmatically control virtually all aspect of the platform including controlling the interface, managing rules, configuring users, installing or removing Agents etc. You can download the Teramind API documentation from the How to use the Teramind API article on our Knowledge Base.

15 Notifications

Notifications shows the status of recent notifications such as login failures, monitoring issues etc.

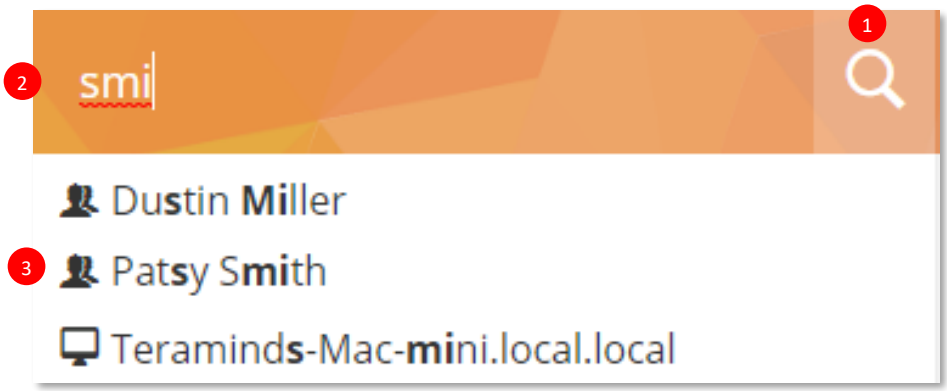


15.1 Accessing the Notifications Menu

1. Click the **Exclamation** icon near the top-right corner of the Dashboard to access the Notifications menu.

16 Global Search

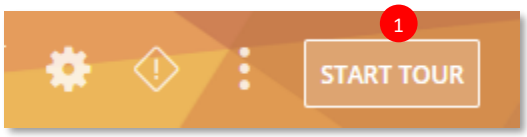
You can search for an employee or computer from anywhere on the Dashboard using the Global Search feature.



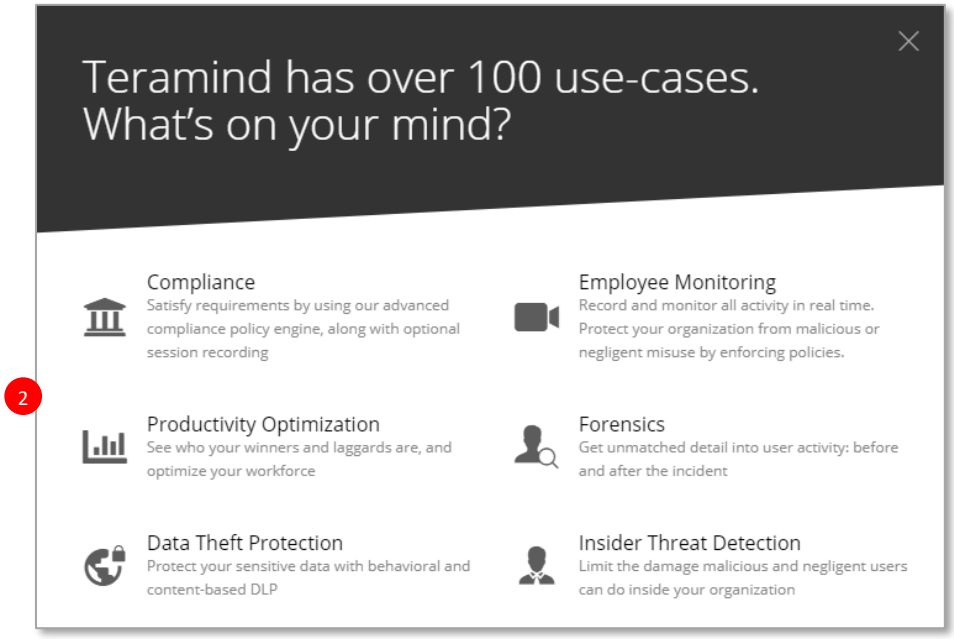
1. Click the **Global Search** button on the top of the Dashboard.
2. Start typing. Teramind will show any matching employees/computers as you type.
3. Pick an employee/computer from the suggested list to view the report for the selected employee/computer. Or, press the **ENTER / RETURN** key to view search results (in a separate window).

17 Guided Tour

Teramind has an interactive Guided Tour feature with over 100 use-cases. You can use this feature to learn how to utilize Teramind features and capabilities.



1. Click the **START TOUR** button at the top-right corner of the Dashboard. A pop-up window will appear.



2. Click any of displayed options (i.e. Compliance, Productivity Optimization etc.). Teramind will guide you through the tour step by step.

18 Help & Support

18.1 Tooltips and Hints

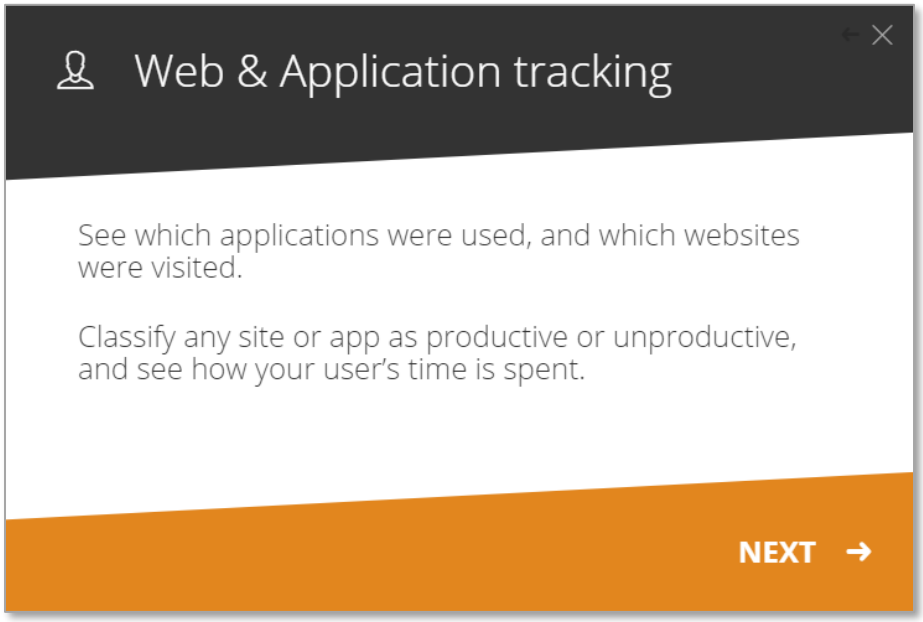
Tooltips usually describing the action of an icon or a button. Hover over an element a second or so, to view the tooltips for that element.

Additionally, you can see context sensitive hints for some elements. Whenever you see this icon, hover over it to see a hint about the relevant item or action.

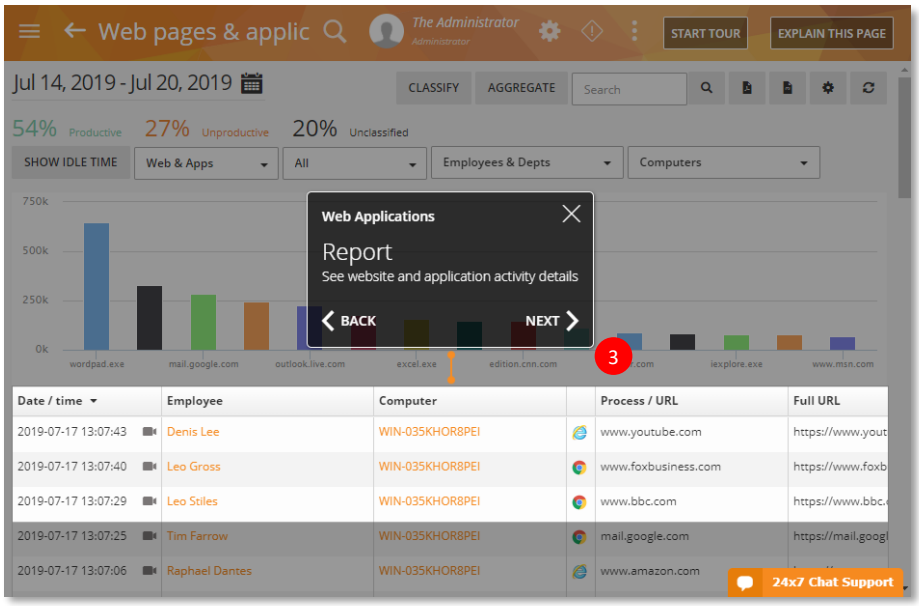
18.2 Page Explanation

When you visit certain pages (such as the Monitoring Reports or the Productivity page), you will notice that an extra button titled, 'EXPLAIN THIS PAGE' is displayed at the top-right corner of the dashboard:

1. Click the **EXPLAIN THIS PAGE** button. Teramind will display an overview for the page:



2. Click the **NEXT** button.



3. Teramind will explain you, step by step, important parts of the current page highlighting each section in turn. You can click the **BACK** and **NEXT** button to browse through the explanations.

18.3 Contacting Support

Technical Support:	Billing Enquiries:	Sales / Customer Care
• IN-APP: My Account > Support. • EMAIL: support@teramind.co • PHONE: +1 212 603 9617	• EMAIL: billing@teramind.co	• EMAIL: sales@teramind.co • PHONE: +1 212 603 9617