# Table of Contents

1  **Dashboards** ......................................................................................................................................... 7
   1.1 Introduction to Dashboards ........................................................................................................... 7
      1.1.1 Focused Dashboard .............................................................................................................. 7
      1.1.2 Enterprise Dashboard ........................................................................................................... 7
   1.2 Accessing the Dashboards Menu .................................................................................................... 8
   1.3 Creating a New Dashboard ............................................................................................................. 8
   1.4 Editing / Deleting a Dashboard ................................................................................................... 9
   1.5 Introduction to Widgets ................................................................................................................ 10
   1.6 Widget Types and Usage ............................................................................................................... 10
      1.6.1 Monitoring Widgets ............................................................................................................ 11
      1.6.2 Productivity Widgets .......................................................................................................... 13
      1.6.3 Security and Risk Widgets .................................................................................................. 15
   1.7 Adding Widgets to the Dashboard ................................................................................................ 15
   1.8 Moving and Resizing the Widgets ................................................................................................. 16
   1.9 Configuring / Editing a Widget ...................................................................................................... 17
   1.10 Removing Widgets from the Dashboard .................................................................................... 17

2  **Monitoring Reports** ......................................................................................................................... 18
   2.1 Introduction to Monitoring Reports ............................................................................................ 18
   2.2 Accessing the Monitoring Report Menus .................................................................................... 19
   2.3 Performing Common Reporting Tasks ......................................................................................... 19
      2.3.1 Setting a Data Range .......................................................................................................... 19
      2.3.2 Sorting the Report Columns ............................................................................................... 20
      2.3.3 Searching in a Report .......................................................................................................... 20
      2.3.4 Exporting Reports ............................................................................................................... 20
      2.3.5 Changing the Report Settings ............................................................................................ 20
      2.3.6 Using the Report Filters ..................................................................................................... 22
      2.3.7 Viewing Session Records .................................................................................................... 23
      2.3.8 Creating / Saving a Custom Report ..................................................................................... 23
      2.3.9 Deleting a Saved Report ..................................................................................................... 24
      2.3.10 Printing a Report ............................................................................................................... 25
   2.4 OCR (Optical Character Recognition) ............................................................................................ 25
4.2 Accessing the Risk Menu ............................................................................................................... 44
4.3 Plotting the Risk Trend .................................................................................................................. 45
4.4 Identifying High Risk Users, Rules and Objects ............................................................................. 45
5  Productivity ........................................................................................................................................ 46
   5.1 Introduction to the Productivity Report ....................................................................................... 46
   5.2 Accessing the Time Worked Menu ............................................................................................ 46
   5.3 Time Worked Report ..................................................................................................................... 46
   5.4 Summary vs. Detailed View ........................................................................................................... 47
6  Behavior ............................................................................................................................................ 48
   6.1 Introduction to the Behavior ......................................................................................................... 48
   6.2 Policies ......................................................................................................................................... 48
   6.3 Accessing the Policies Menu ........................................................................................................ 49
   6.4 Creating a New Policy .................................................................................................................... 49
   6.5 Moving / Exporting / Editing / Deleting Policies ......................................................................... 50
   6.6 Creating / Editing Rules ................................................................................................................ 51
   6.7 Moving / Exporting / Editing / Deleting Rules ............................................................................. 51
   6.8 Rules Editor ................................................................................................................................ 51
      6.8.1 General Tab – Setting the Rule Basics ................................................................................ 52
      6.8.2 User Tab – Specifying Users and Groups ............................................................................ 55
      6.8.3 Categories Tab – Setting Rules Conditions ......................................................................... 55
      6.8.4 Content Tab – Defining Sensitive Data Types ..................................................................... 57
      6.8.5 Actions Tab – Responding to Rule Violation Incidents ....................................................... 62
   6.9 Alerts ............................................................................................................................................ 66
      6.9.1 Accessing the Alerts Menu ................................................................................................. 67
      6.9.2 Applying Alert Filters .......................................................................................................... 67
      6.9.3 Showing / Hiding Rule Triggers ........................................................................................... 68
   6.10 Anomaly Rules ............................................................................................................................. 68
      6.10.1 Accessing the Anomaly Rules Menu ................................................................................. 68
      6.10.2 Filtering / Editing / Deleting / Copying Anomaly Rules .................................................... 69
      6.10.3 Creating Anomaly Rules .................................................................................................... 69
      6.10.4 Anomaly Rules Editor ....................................................................................................... 70
7  Employees .......................................................................................................................................... 73
   7.1 Introduction to the Employees ..................................................................................................... 73
7.2 Accessing the Employees Menu .................................................................................................... 73
7.3 Adding a New Employee ............................................................................................................... 74
  7.3.1 Entering / Editing Employee Profiles .................................................................................. 74
7.4 Importing Employees .................................................................................................................... 76
7.5 Employee Action Menu ................................................................................................................. 77
7.6 Viewing an Employee’s Monitoring Reports ................................................................................. 77
7.7 Editing / Deleting an Employee ..................................................................................................... 78

8 Computers ........................................................................................................................................ 79
  8.1 Introduction to the Computers ..................................................................................................... 79
  8.2 Accessing the Computers Menu .................................................................................................. 79
  8.3 Remote Installing the Teramind Agent ......................................................................................... 79
  8.4 Computer Action Menu ................................................................................................................. 81

9 Configure .......................................................................................................................................... 82
  9.1 Introduction to the Configurations ............................................................................................... 82
  9.2 Departments ................................................................................................................................. 82
    9.2.1 Accessing the Departments Menu ..................................................................................... 82
    9.2.2 Creating a New Department ............................................................................................... 83
    9.2.3 Viewing the Employees in a Department ........................................................................... 83
    9.2.4 Editing / Deleting a Department ........................................................................................ 84
  9.3 Schedules ....................................................................................................................................... 84
    9.3.1 Accessing the Schedules Menu .......................................................................................... 85
    9.3.2 Switching Between Combined vs Daily Views .................................................................... 85
    9.3.3 Managing Employee Schedule ........................................................................................... 86
    9.3.4 Managing Position Schedules ............................................................................................. 88
    9.3.5 Managing Templates .......................................................................................................... 89
  9.4 Access Control ............................................................................................................................... 91
    9.4.1 Accessing the Access Control Menu ................................................................................... 91
    9.4.2 Creating a New Access Control Policy ................................................................................ 92
    9.4.3 Viewing / Editing / Deleting an Access Control Policy ........................................................ 92
    9.4.4 Access Control Policy Editor ............................................................................................... 93
  9.5 Shared Lists .................................................................................................................................... 95
    9.5.1 Accessing the Shared Lists ................................................................................................. 95
    9.5.2 Creating a New Shared List .................................................................................................. 96
9.5.3 Editing a Shared List ........................................................................................................... 97
9.5.4 Deleting a Shared List ......................................................................................................... 97

10 System .................................................................................................................................. 97

10.1 Introduction to the System .................................................................................................. 97
10.2 Missing Users / Computers .................................................................................................. 98
  10.2.1 Accessing the Missing Users / Computers Menu ......................................................... 98
  10.2.2 Searching for Missing Users / Computers ...................................................................... 98
10.3 System Log .......................................................................................................................... 99
  10.3.1 Accessing the System Log Menu .................................................................................. 100
  10.3.2 Applying System Log Filters ......................................................................................... 100
  10.3.3 Viewing Additional Details for a Log ............................................................................ 100

11 Dashboard Settings .............................................................................................................. 101

11.1 Monitoring Settings............................................................................................................. 101
11.2 Accessing the Monitoring Settings Menu .......................................................................... 102
11.3 Creating a New Monitoring Profile .................................................................................... 102
11.4 Editing a Monitoring Profile .............................................................................................. 103
11.5 Editing the Settings for Monitored Systems ....................................................................... 104
11.6 Integrations .......................................................................................................................... 113
  11.6.1 Accessing the Integrations Menu .................................................................................. 113
  11.6.2 Setting Up a New SIEM Integration ............................................................................. 113
  11.6.3 Setting Up a New Project Management Integration .................................................... 116
  11.6.4 Editing / Deleting an Integration ................................................................................ 121
11.7 Settings .................................................................................................................................. 121
  11.7.1 Accessing the Settings Menu ......................................................................................... 122
  11.7.2 Server Updates and License Key ................................................................................. 122
  11.7.3 Active Directory .......................................................................................................... 123
  11.7.4 Agent Defaults .............................................................................................................. 124
  11.7.5 Alerts ........................................................................................................................... 125
  11.7.6 Login Screen ............................................................................................................... 126
  11.7.7 Security ....................................................................................................................... 126
  11.7.8 Server Management ..................................................................................................... 129
  11.7.9 SMTP .......................................................................................................................... 130
  11.7.10 System Health ........................................................................................................... 131
1 Dashboards

1.1 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:

1.1.1 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.

1.1.2 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.
1.2 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.

1.3 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.

### 1.4 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 Trash Can icon. Note that, if you have only one dashboard, it cannot be deleted.

1.5 Introduction to Widgets

Widgets are tiles that display 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.

1.6 Widget Types and Usage

There are three different types of widgets you can choose from:
1.6.1 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.

1.6.2 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.

1.6.3 Security and Risk Widgets

Alerts Log
Shows a log of all alerts and notifications.

Risk Widget
Shows risky users, rules or activities.

1.7 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.

### 1.8 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.

1.9 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.

1.10 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.
2 Monitoring Reports

2.1 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.

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

<table>
<thead>
<tr>
<th>Monitoring Report</th>
<th>Teramind Starter</th>
<th>Teramind UAM</th>
<th>Teramind DLP</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCR</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web Pages &amp; Applications</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Emailing</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Console Commands</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>File Transfers</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Instant Messaging</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Social Media</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Keystrokes</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Searches</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Printing</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Screen Snapshots</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sessions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
2.2 Accessing the Monitoring Report Menus

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

2.3 Performing Common Reporting Tasks

2.3.1 Setting a Data Range

1. Each monitoring report screen has a dates-selector at the top-left corner. Click the **dates-selector**.
2. Select a start date and an end date 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.
2.3.2 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.

<table>
<thead>
<tr>
<th>Employee</th>
<th>Computer</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albika Desheryev</td>
<td>WIN-035KHO...</td>
<td><a href="mailto:sergey.teramind@yahoo.com">sergey.teramind@yahoo.com</a></td>
<td><a href="mailto:sergey.teramind@gmail.com">sergey.teramind@gmail.com</a></td>
</tr>
<tr>
<td>Albika Desheryev</td>
<td>WIN-035KHO...</td>
<td><a href="mailto:sergey.teramind@yandex.com">sergey.teramind@yandex.com</a></td>
<td><a href="mailto:sergey.teramind@gmail.com">sergey.teramind@gmail.com</a></td>
</tr>
<tr>
<td>Albika Desheryev</td>
<td>WIN-035KHO...</td>
<td><a href="mailto:sergey.teramind@yandex.com">sergey.teramind@yandex.com</a></td>
<td><a href="mailto:sergey.teramind@gmail.com">sergey.teramind@gmail.com</a></td>
</tr>
</tbody>
</table>

2.3.3 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.

2.3.4 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.

2.3.5 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. You can specify the export date/time, number of days and the export format.
6. You can specify who will receive the export email. You can specify multiple recipients.

### 2.3.6 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.

2.3.7 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.

2.3.8 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**.

### 2.3.9 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.
2.3.10 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.

2.4 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.

2.4.1 Using the OCR Search Feature

To conduct an OCR search, do the following:

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

### 2.4.2 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:

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.

2.5 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. You can also categorize each application or URL into Productive / Unproductive or Custom class. This classification is then used to measure productivity for the employees.
2.5.1 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.

2.5.2 Classifying Web Pages and Applications

1. Click the **CLASSIFY** button near the top-right corner of the screen. You will notice that, an extra check mark column is added in front of the report table.

2. Click the **Check Mark** in front of an item to select/deselect it. You can select multiple items.

3. Click the **Select classification** drop-down list located at the top left corner of the screen. Select an option from **Productive**, **Unproductive** or **Unclassified**.

2.6 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.

2.7 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.
2.7.1 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.

2.7.2 Viewing / Saving / Printing Email Contents

1. To view the email content, click the Envelope 📦 icon. A pop-up window will open.
2. From the pop-up window, you can view the email, save it as a PDF file or print it.

### 2.7.3 Viewing / Saving Email Attachments

1. Click the name of the attachment on the Attachments column to save a copy of the file.

   Note that, you can save attachments from outgoing emails only.
2.8 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.

![File Transfers Report](image)

2.9 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.

![Instant Messaging Report](image)

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.
2.9.1 Viewing / Saving IM Messaging Contents

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

2. From the pop-up window, you can view the message content, load old messages and save the whole conversation as a PDF/CSV file.

2.10 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.

### 2.11 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.

2.11.1 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.

2.12 Searches

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

2.13 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.

2.13.1 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.
2.14 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.

2.15 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.
2.16 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.
2.16.1 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.

2.16.2 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.
3 Session Player

3.1 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.
3.2 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 turns Orange), you can click a Notification Indicator to jump to a time where a rule violation incident occurred.

3.3 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.

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

### 3.5 Downloading / Exporting Videos

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

   ![Video params pop-up window]

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.

   ![Start export button]

3. Your video export is complete. You can download it at [https://demo.company.teramind.co/video-export/546ebb1250e4c33249045b4f00e48256.mp4](https://demo.company.teramind.co/video-export/546ebb1250e4c33249045b4f00e48256.mp4) We recommend viewing using VLC player.
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.

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.

3.6 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.

4 Risk

4.1 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.

### 4.2 Accessing the Risk Menu

1. You can access the Risk report by clicking the **RISK** menu.
4.3 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*.

4.4 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).

5 Productivity

5.1 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, web and app classification and other configuration settings such as departments, schedules, user input from the Revealed Agent etc.

5.2 Accessing the Time Worked Menu

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

5.3 Time Worked Report

The report comes with the following special columns:
**Work:**

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've clocked in for a selected date range.

**Productive:**

Represents time spent on productive websites and applications; based on the classification you made in the Web Pages and Application report. Check out the [Classifying Web Pages and Applications](#) section for more information on activity classification.

**Unproductive:**

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

**Active:**

Represents time spent engaging the keyboard or mouse.

**Idle:**

Idle represents the absence of activity on keyboard and mouse.

**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%.

**Total:**

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 the [Entering / Editing Employee Profile](#) section to learn how to assign salary/wage to an employee.

**Daily work:**

Compares Activity, Active & idle time, and Productivity. You can click the **Check Box** in front of each categories to show ✅ or hide ⬜️ it.

### 5.4 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.

### 6 Behavior

#### 6.1 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.

#### 6.2 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.

### 6.3 Accessing the Policies Menu

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

### 6.4 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.

### 6.5 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.
6.6 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.

6.7 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.
5. To delete/remove a policy, click the **Delete Policy** button.

6.8 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.

### 6.8.1 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.

#### 6.8.1.1 Rule Name and Description

1. On the top fields, you can specify a name and optionally, a description for the rule.
6.8.1.2 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.
6.8.1.3 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.](image-url)
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.

### 6.8.1.4 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.

### 6.8.2 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 EXCLUDE FROM RULE field.

### 6.8.3 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** field 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 many 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 meet 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.

### 6.8.4 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. OCR, Clipboard, Files, Emails, IM).

6.8.4.1 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 OCR, you can create a rule that warns a user when it detects some
text on their screen. Or, using it with the Clipboard, you can detect anything copied on the clipboard.

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

6.8.4.2 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, Regula Expression match, List match etc. from the SELECT MATCH TYPE pull-down menu.
6.8.4.3 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, Regula Expression match, List match etc. for the FILE PATH field.
6.8.4.4 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, Regula Expression match, List match etc. from the SELECT MATCH TYPE pull-down menu.
6.8.4.5 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.

6.8.5 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, the Agent Schedule-based rules only support the NOTIFY action. 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.

**6.8.5.1 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).

If the ALLOW BYPASS WITH CONFIRMATION? option is selected, the user will be blocked, but they will also see a message asking them if they still want to continue. The user will be able to bypass the block after clicking a Yes button.

If the MANAGER CAN MAKE EXCEPTIONS option is selected, Teramind will send an email to the manager(s) specified in the email field. The manager(s) can then allow the user to bypass the block by clicking a link in the email.

**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).

ℹ️ This action works on Windows only.

**Redirect**

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

ℹ️ 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.

6.8.5.2 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.

### 6.9 Alerts

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.

### 6.9.1 Accessing the Alerts Menu

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

### 6.9.2 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.
6.9.3 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.

6.10 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.

6.10.1 Accessing the Anomaly Rules Menu

3. Hover your mouse over the BEHAVIOR menu, then
4. Select Anomaly rules from the sub-menu.
6.10.2 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.

6.10.3 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.

### 6.10.4 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.

#### 6.10.4.1 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.

### 6.10.4.2 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 **X** button next to a condition to delete it.

### 6.10.4.3 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**).

![Rule Risk Level](image)

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.

### 6.10.4.4 Rule Actions

Anomaly rules only support the **NOTIFY** action.

![Rule Actions](image)

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

### 6.10.4.5 Saving the Rule / Creating a Rule Template

![Save and Launch Rule](image)

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).

# Employees

## 7.1 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.

## 7.2 Accessing the Employees Menu

1. Click the **EMPLOYEES** menu to access its screen.
7.3 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.

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

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

**If you are adding a new employee:**

1. **CANCEL**
2. **ADD USER & SEND INVITATION**
3. **ADD USER**
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.

### 7.4 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 **DOWNLOAD 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.
7.5 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 excluded from the reports.
   - **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.

7.6 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.

**7.7 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. Note that when you delete an employee, they are not permanently deleted, just excluded from the reports. You can also delete/restore an employee from the Employee Action Menu.
8 Computers

8.1 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 and the what versions of the Teramind Agent they are using.

8.2 Accessing the Computers Menu

1. Click the COMPUTERS menu to access its screen.

8.3 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).

3. 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.

4. Under **Deployment Mode**, you can choose between PSEXEC or WMI mechanism to deploy the Agent.

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

   - **Domain administrator privileges are mandatory for the silent install.**

Check out the Settings > Active Directory section to learn how to integrate Active Directory with Teramind.
6. Under the *Teramind server*, enter host name or IP address of your Teramind server.
7. Click the **DEPLOY** button to begin the installation.

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

### 8.4 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. From 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.
   - **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.
   - **Update agents**: updates the installed Teramind Agent on the selected computers with the latest version.
   - **Cancel agents update**: cancels any pending Agent update tasks.
9 Configure

9.1 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.

9.2 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.

9.2.1 Accessing the Departments Menu

1. Hover your mouse over the CONFIGURE menu, then
2. Select Departments from the sub-menu.
9.2.2 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 departmental managers from the list of employees. Click the **APPLY CHANGES** button to create the department.

9.2.3 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*. 

   ![Department page](image)

   **New department**
   
<table>
<thead>
<tr>
<th>DEPARTMENT NAME:</th>
<th>Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPARTMENT DESCRIPTION (OPTIONAL):</td>
<td>Finance and accounts department</td>
</tr>
<tr>
<td>DEPARTMENT MANAGERS:</td>
<td></td>
</tr>
<tr>
<td>Shelby Hunter</td>
<td>Kevin Wainright</td>
</tr>
<tr>
<td><em><a href="mailto:shunter@teramind-demo.com">shunter@teramind-demo.com</a></em></td>
<td><em><a href="mailto:kwainright@teramind-demo.com">kwainright@teramind-demo.com</a></em></td>
</tr>
<tr>
<td><img src="image" alt="Apply Changes button" /></td>
<td></td>
</tr>
</tbody>
</table>
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.

9.2.4 Editing / Deleting a Department

1. While on the Department page, click the EDIT button at the top-right corner. An Edit department window will appear (similar to the New department window) where you can change the department’s name, description and managers.

2. While on the Department page, click the DELETE button at the top-right corner to delete the department.

9.3 Schedules

The Schedules screen allows you to manage schedules for your employees and contractors. You can control employee worktime, launch 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.
The screen has three separate tabs, SCHEDULING, POSITIONS and TEMPLATES where you can control daily and weekly schedules for your employees or positions. You can also create schedule templates to make managing schedules for large groups easier.

### 9.3.1 Accessing the Schedules Menu

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

### 9.3.2 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.
9.3.3 Managing Employee Schedule
You can manage schedules for individual employees from the SCHEDULING tab.

9.3.3.1 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.

   ![Notification Interface]

   1. COMBINED
   2. DAILY
   3. NOTIFY EMPLOYEES

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.
9.3.3.2 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.
9.3.3.3 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 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.

### 9.3.4 Managing Position Schedules

You can manage schedules for positions from the POSITIONS tab. You can manage weekly/daily schedules, add day offs, add a new position etc.

#### 9.3.4.1 Managing Weekly Position Schedules

The process is similar to [Managing Weekly Employee Schedules](#). Please follow the instruction there to manage weekly position schedules.

#### 9.3.4.2 Managing Daily Position Schedules and Day Offs

The process is similar to [Managing Daily Employee Schedules and Day Offs](#). Please follow the instruction there to manage daily position schedules.
9.3.4.3 Adding a New Position

Click the **NEW POSITION** button to add a new position. Note that, you can also create a new position when adding/editing an employee, under PERSONAL INFO, in the Position field.

9.3.5 Managing Templates

9.3.5.1 Adding a New Template

1. Click the **ADD TEMPLATE** button at the top-right corner of the TEMPLATES screen. 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.
9.3.5.2 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.
9.4 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.

### 9.4.1 Accessing the Access Control Menu

5. Hover your mouse over the **CONFIGURE** menu, then
6. Select **Access control** from the sub-menu.
9.4.2 Creating a New Access Control Policy

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

![New policy window]

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.

9.4.3 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.

### 9.4.4 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.

### 9.5 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.

#### 9.5.1 Accessing the Shared Lists

7. Hover your mouse over the **CONFIGURE** menu, then
8. Select **Shared lists** from the sub-menu.
9.5.2 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.
9.5.3 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 **X** button.

9.5.4 Deleting a Shared List

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

10 System

10.1 Introduction to the System

The System menu allows you to view any missing users/computers and view the system activities log.
10.2 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.

10.2.1 Accessing the Missing Users / Computers Menu

9. Hover your mouse over the SYSTEM menu, then
10. Select Missing users / computers from the sub-menu.

10.2.2 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.
10.3 System Log

The System Log screen allows you to see all administrator/manger 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.
10.3.1 Accessing the System Log Menu

![System Log Menu](image)

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

10.3.2 Applying System Log Filters

![Filter Options](image)

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.

10.3.3 Viewing Additional Details for a Log

![Additional Details](image)

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.

11 Dashboard Settings

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

11.1 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.

![Monitoring Settings Screen](image)

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.
11.2 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.

11.3 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 **YE/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).

### 11.4 Editing 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 small **Gear** icon at the right side 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.
5. Click the small **×** icon to delete the profile.
11.5 Editing the Settings for Monitored Systems

11.5.1.1 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.
11.5.1.2 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, Spanish and Turkish for the OCR.

You can turn ALLOW REMOTE CONTROL on/off. This will determine if Remote Control will be available on the Session Player’s Live Mode Controls.

SYNC SCREEN UPLOAD forces 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.

You can enable/disable RECORD LOCKED SESSIONS. By default, Teramind will not record any locked sessions.

By enabling RECORD ONLY WHEN BEHAVIOR RULE WAS VIOLATED, you can reduce the storage needed for the screen recordings. 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); specify the GRAYSCALE/COLOR option etc.

You can specify when the recordings will be automatically deleted under the DELETE HISTORY AFTER. You can also use the COMPRESS AFTER settings to reduce storage need. You can further reduce the storage requirements by enabling REDUCE TO 4-BIT GRAYSCALE option and reducing the SCALE SCREEN RECORDINGS percentage.
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.

11.5.1.3 Editing Audio Settings

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

ASYNC AUDIO UPLOAD forces 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 LISTEN ALL INPUT / OUTPUT options to enable/disable recording for all microphones, speakers and line-in/out.
11.5.1.4 Editing Applications Settings

You can turn monitoring on/off for the CONSOLE COMMANDS.

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).
11.5.1.5 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 screen 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.

SUSPEND MONITORING WHEN THESE WEBSITES ARE VISITED setting allows you to record the screen and keystrokes but suspend content parsing. For example, record the activity when the user is in Gmail, but don't capture the actual email content or any attachments.

SUSPEND MONITORING WHEN WEBSITE CONTENT CONTAINS setting allows you to determine intranet or proxy-generated websites.

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

You can also SUSPEND KEYSTROKE ... setting to suspend just the keystroke recording for the specified websites.

You can use the WSS PORT to specify web traffic redirection.
11.5.1.6 Editing Email Settings

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

You can use regular expressions (REGEX) to further filter to ignore any attachments you don’t want captured. For example, ignore all music and video files.

Finally, you can specify which email systems will be captured. Teramind supports the most popular email clients such as Outlook, Gmail, Yahoo etc. - both desktop and web versions.
11.5.1.7 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, NETWORK 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/RENAME/UPLOAD/DOWNLOAD/DELETE etc.
11.5.1.8 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 capture printer activities for that particular printer.

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

11.5.1.9 Editing Keystrokes / Key Logging Settings

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

11.5.1.10 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.
11.5.1.11 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.

11.5.1.12 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.

11.5.1.13 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.
11.6 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.

11.6.1 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.

11.6.2 Setting Up a New SIEM Integration

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 a SIEM product from the list of products. For example, **HP ArcSight**.
4. Click the **NEXT STEP** button to continue to **Step 2**.

5. Select the **Transport** protocol (UDP or 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.

9. Click on a Database icon to configure its data mapping. A Data mapping window will pop-up.

10. 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.

11. When data mapping is done, click the SAVE button to close the Data mapping window and return to the Step 3 window.
12. Click the **LAUNCH INTEGRATION** to save and launch the integration.

### 11.6.3 Setting Up a New Project Management Integration

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 a PM product from the list of products. For example, **Zendesk**.
4. Click the **NEXT STEP** button to continue. You will be taken to the *Step 2 of 3* screen.

The following steps are different for each product. For this exercise, we will use Zendesk as an example. However, we have provided detailed instructions for other products on the Step 2 of the integration wizard. If you still need help completing this step, please contact support@teramind.co.
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.

![OAuth Clients form](image)

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.

### 11.6.4 Editing / Deleting an Integration

![Actions icons](image)

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.

### 11.7 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.
11.7.1 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.

11.7.2 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.

11.7.2.1 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.
11.7.2.2 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.

11.7.3 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 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

Active Directory synchronization can be set up as follows:
1. Populate the LDAP server, port, encryption etc.
2. Click **NEXT: FETCH ATTRIBUTES**.
3. As soon as fetching is done, choose the attributes, OUs, monitored and non-monitored groups.
4. Click the **SAVE SETTINGS & IMPORT** button to initiate the import process. You might have to wait for a little while (couple of minutes depending on AD object count and hierarchy). Once the import is done, refresh the page to view the changes.

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

### 11.7.4 Agent Defaults

This tab allows you to change the default settings for the Teramind Agent.
1. You can change the currency 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).
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.

### 11.7.5 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 your 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 THRESHOLD 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 THRESHOLD 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.

11.7.6 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.

11.7.7 Security
11.7.7.1 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.

11.7.7.2 SSL

Teramind strongly recommends proper configuration of SSL in order to avoid browser warnings and restrictions. Some browsers will not allow websockets 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. 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.

11.7.7.3 Dashboard Authentication

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

1. You can force the user to use 2-Factor authentication by enabling this setting. Teramind supports 2FA apps like Google Authenticator or Authy. If you force 2FA in your deployment, next time an administrator logs in, they will be forced to enable 2FA before being given access to the dashboard.
2. If you have successfully set up Active Directory integration, you may want to use your domain credentials to log in. You can choose from: BASIC: use only Teramind authentication. AD: use only Active Directory credentials. Both: use either Active Directory, or Teramind for authentication.

11.7.7.4 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.
11.7.7.5 Outgoing Exported Data

By default, Teramind allows you to export reports, video recordings and other data 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.

11.7.8 Server Management

11.7.8.1 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’s 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.

11.7.8.2 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.

11.7.9 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.

11.7.10 System Health

System Health tab gives you a quick snapshot of the current status of the server load, storage condition and session mining (OCR process) status.
1. The System load section shows the TOTAL NUMBER OF CORES the CPU has, 5-MINUTE LOAD AVERAGE (%) and MEMORY USAGE status.

2. The Storage section shows the PRIMARY VOLUME USAGE and the RECORDING VOLUME USAGE information. Primary volume typically contains the Teramind database and the recording volume contains the OCR screen recordings. You can always adjust your usage by tweaking your screen recording settings and retention policies. Check out the Editing Screen Settings section to learn more. You can also use MINIMUM SPACE THRESHOLD setting to tell Teramind to stop recording when reaching this minimum space threshold (in MB).

3. The Session mining stats shows the OCR processing status. ISM DELTA = number of records not processed yet, ISM DAY DELTA = number of days not processed yet; and the ISM SCORE = overall performance of the session mining process.

11.7.11 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 LANGUAGE 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.

12 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.

12.1 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.

12.2 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.
12.3 Download Teramind Agent

The following instructions are for downloading and installing the Teramind Agent for a Cloud deployment. The process is similar for an On-Premise or Private Cloud deployments, but the exact instructions and some options are different. Please check out the Teramind On-Premise Deployment Guide, Teramind on AWS Deployment Guide or the Teramind on Azure Deployment Guide for more information on downloading the Agent for those deployment options. You can find the guides on https://www.teramind.co/company/resources under the Product Guides category.

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's the application that generates all the data needed for every use case of the Teramind platform.

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

12.3.1 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.

12.3.1.1 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.

12.3.1.2 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 (Mac OS).

12.3.1.3 Using the Revealed Agent

**Starting / Stopping Monitoring:**

Each time the user logs into the Agent, they will be able to select from a Task (project) and a Subtask they want to work on.

1. Select a **Task** and then a **Subtask** from the drop-down lists.
2. Click the **Start** button to start monitoring activities and track times.
3. Click the **Stop** button to stop monitoring activities and time tracking.
4. Below the Start/Stop buttons, there is a list of all the tasks that the user worked on during the previous days.

**Creating a New Subtask:**
1. Click the **task menu** and choose a task.
2. Click the **sub-task menu** and choose the **-- Create New Subtask --** option. A text field will appear with the text **New Subtask Name**. Type a sub-task name.
3. Click the **Check Mark** to save the task. Next time the subtask will be listed on the Subtask menu.

12.3.2 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.

12.3.2.1 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.

12.3.2.2 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.

12.3.2.3 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.

12.3.2.4 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.

12.3.2.5 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/qn</td>
<td>Enables silent installation.</td>
</tr>
<tr>
<td>TMROUTER=<a href="">ip-of-vm:port</a></td>
<td>Load balancer IP and port. Please see Server Management section for more information.</td>
</tr>
<tr>
<td>TMINSTANCE=&lt;account-name&gt;</td>
<td>Provide an <code>&lt;account-name&gt;</code> or use onsite for on-premise deployment.</td>
</tr>
<tr>
<td>TMDISABLEAUDIO=1</td>
<td>Turns audio off.</td>
</tr>
<tr>
<td>TMDOMAINOVERRIDE=&lt;domain-name&gt;</td>
<td>To override your domain/PC name with the specified <code>&lt;domain-name&gt;</code>.</td>
</tr>
</tbody>
</table>
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 OS / OSX 10.7+:

To install Mac OS X 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:

12.3.3 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 for the Teramind Agent found on our Resources page, under the Products Guides section.

12.3.4 Uninstalling the Agent

Windows:

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, use the following command:

```
teramind_remover.exe /PASSWORD=<your-pass>
```

Where `<your-pass>` is the password you used to protect the Agent. You specify the protection password
in the Agent Removal Protection section of the dashboard. You do not have to use the `/PASSWORD`
option if you are the same admin who installed the Agent originally.

**Mac:**

Run the following command in the Terminal (Applications > Utilities > Terminal)

```
curl //path-to/teramind/uninstall-mac | sudo bash -
```

Where `//path-to/teramind-server/` is the URL of your Teramind Server.

### 12.4 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 a new token or delete an existing token for the Access Tokens screen.

1. Click the **ADD ACCESS TOKEN** button at the top-right corner to create a new access token.
2. Click the **X** button at the right side of an access token to delete it.

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. Contact support@teramind.co to access the Teramind API Documentation.
13 Notifications

Notifications shows the status of recent notifications such as login failures, monitoring issues etc.

13.1 Accessing the Notifications Menu

1. Click the Exclamation icon near the top-right corner of the Dashboard to access the Notifications menu.

14 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).

15 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.

16 Help & Support

16.1 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.
16.2 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:

   ![Web & Application tracking]
   
   See which applications were used, and which websites were visited.
   
   Classify any site or app as productive or unproductive, and see how your user's time is spent.

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.

### 16.3 Contacting Support

<table>
<thead>
<tr>
<th>Technical Support:</th>
<th>Billing Enquiries:</th>
<th>Sales / Customer Care</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IN-APP: <a href="#">My Account &gt; Support</a></td>
<td>• EMAIL: <a href="mailto:billing@teramind.co">billing@teramind.co</a></td>
<td>• EMAIL: <a href="mailto:sales@teramind.co">sales@teramind.co</a></td>
</tr>
<tr>
<td>• EMAIL: <a href="mailto:support@teramind.co">support@teramind.co</a></td>
<td></td>
<td>• PHONE: +1 212 603 9617</td>
</tr>
<tr>
<td>• PHONE: +1 212 603 9617</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>