Teramind Rules Guide

Last Updated: 25 APRIL 2025



Table of Contents

1 About This Guide 7

2 Related Resources 8

3 Rules Overview 9

3.1 Common Use Cases 10

3.1.1 Preventing Data Loss 10

3.1.2 Detecting Insider Threats 10

3.1.3 Identifying Abusive Behavior and Accidental Threats 10

3.1.4 Detecting Malicious Intent 11

3.1.5 Improving Productivity and HR Management 11

3.1.6 Conforming with Regulatory Compliance 11

3.1.7 Implementing the MITRE ATT&CK™ Framework 12

4 Steps for Creating a Rule 13

4.1 Why are You Creating the Rule? 13

4.2 What Activity, Content or Behavioral Anomaly You Want to Detect? 13

4.3 Where is the Activity Performed or Content Located? 13

4.4 When Should the Rule be Active? 13

4.5 Whom Should it Apply to? 13

4.6 What Makes the Data Sensitive? 14

4.7 What Scenarios Violate the Rule? 14

4.8 What Action(s) Do You Want to Take? 14

5 Understanding Common Rule Elements 15

5.1 Rule Name and Description 15

5.2 Rule Template 15

5.3 Displaying the Rule in OMNI 16

5.4 Tags 16

5.5 Schedule 17

5.6 Rule Violation Severity 17

5.7 Rule Conditions 17

5.7.1 Contains 18

5.7.2 Equals 18

5.7.3 Match RegExp 18

5.7.4 Match Glob 19
5.7.5 Match List 19
5.7.6 Equals List 20
5.8 Rule Logic 20
5.8.1 Condition Logic 20
5.8.2 Content Logic 20
5.9 Risk Level 22
5.9.1 Setting the Risk Levels in a Regular Rule 22
5.9.2 Setting the Risk Level in an Anomaly Rule 23
5.10 Rule Summary 23
6 Creating Regular Rules 25
6.1 Setting Up the Rule Basics 25
6.2 Selecting Rule Categories and Types 25
6.3 Defining Users 26
6.4 Defining Detection Criteria 27
7 Agent Schedule Rules: What Schedule Violations Can You Detect (Windows)? 28
7.1 Agent Schedule Rule Examples 28
7.2 Agent Schedule Rule Criteria 28
8 Activity Rules: What Activities Can You Detect (Windows & Mac)? 33
8.1 Webpages (Windows & Mac) 33
8.1.1 Webpages Rule Examples 33
8.1.2 Webpages Rule Criteria 33
8.2 Applications (Windows & Mac) 40
8.2.1 Applications Rule Examples 40
8.2.2 Applications Rule Criteria 40
8.3 OCR (Windows & Mac) 46
8.3.1 OCR Rule Examples 46
8.3.2 OCR Rule Criteria 47
8.4 Keystrokes (Windows & Mac) 48
8.4.1 Keystrokes Rule Examples 48
8.4.2 Keystrokes Rule Criteria 48
8.5 Files (Windows & Mac) 51
8.5.1 Files Rule Examples 52

8.5.2 Files Rule Criteria 52
8.6 Emails (Windows) 57
8.6.1 Emails Rule Examples 57
8.6.2 Emails Rule Criteria 58
8.7 IM – Instant Messaging (Windows) 61
8.7.1 IM Rule Examples 61
8.7.2 IM Rule Criteria 61
8.8 Browser Plugins (Windows) 63
8.8.1 Browser Plugins Rule Examples 63
8.8.2 Browser Plugins Rule Criteria 63
8.9 Printing (Windows & Mac) 64
8.9.1 Printing Rule Examples 64
8.9.2 Printing Rule Criteria 64
8.10 Networking (Windows & Mac) 66
8.10.1 Networking Rule Examples 66
8.10.2 Networking Rule Criteria 66
8.11 Registry (Windows) 69
8.11.1 Registry Rule Examples 69
8.11.2 Registry Rule Criteria 69
8.12 Camera Usage (Windows) 71
8.12.1 Camera Usage Rule Examples 71
8.12.2 Camera Usage Rule Criteria 72
8.13 Windows Log Event (Windows) 73
8.13.1 Windows Log Event Rule Examples 74
8.13.2 Windows Log Event Rule Criteria 74
9 Content Sharing Rules: What Contents Trigger the Rules (Windows)? 76
9.1 The Content Tab 76
9.2 Clipboard 82
9.2.1 Clipboard Rule Examples 82
9.2.2 Clipboard Rule Criteria 83
9.3 Files 84
9.3.1 Files Rule Examples 85
9.3.2 Files Rule Criteria 85

9.4 Emails 87
9.4.1 Emails Rule Examples 88
9.4.2 Emails Rule Criteria 88
9.5 IM 91
9.5.1 IM Rule Examples 91
9.5.2 IM Rule Criteria 91
9.6 Keystrokes 92
9.6.1 Keystrokes Rule Examples 93
9.6.2 Keystrokes Rule Criteria 93
10 Creating Anomaly Rules (On-Premise/Windows) 96
10.1 Rule Examples 96
10.2 Setting Up the Rule Basics 96
10.3 Detection Criteria - What Behavioral Anomalies Trigger the Rules? 97
11 Defining Rule Actions 102
11.1 Simple Mode Actions 102
11.1.1 Notify (Windows & Mac) 103
11.1.2 Block (Windows & Mac) 104
11.1.3 Lock Out User (Windows & Mac) 105
11.1.4 Redirect (Windows) 106
11.1.5 Warn (Windows & Mac) 106
11.1.6 Set User's Active Task (Windows) 107
11.1.7 Record Video (Windows) 107
11.1.8 Command (Windows) 107
11.2 Advanced Mode Actions 108
12 Customizing the Rule Messages and Alerts 110
12.1 The USE HTML TEMPLATE Option 110
12.2 Customizing the HTML Alert Template 110
12.2.1 Using Images / Icons in the HTML Alert Template 113
12.2.2 Configuring Other Alert Options 115
13 Using the Prebuilt Rule-Templates 117
13.1.1 Using the Regular Rule Templates 117
13.1.2 Using Anomaly Rule Templates 117
14 Enforcing the Rules 119

14.1 Automatic Enforcement 119
14.2 Manual Enforcement 119
15 Investigating the Rule Violation Incidents 121
15.1 Using the Behavioral Alerts Report 121
15.1.1 Using the BI Report's Investigate / View Record Feature 121
15.2 Using the Alerts Log Widget 122
15.3 Using the Session Player 122
15.4 Using the Risk Report 123
15.5 Using the Risk Widget 124
15.6 Using OMNI 124
16 Sample Rules Walkthrough 125
16.1 Rule Sample 1: User logs in during off hours 125
16.1.1 Rule Summary 125
16.1.2 Setting up the Rule 125
16.1.3 Viewing the Rule Alerts 126
16.1.4 Viewing the Session Recording 127
16.2 Rule Sample 2: User sending emails with attachments to non-business address 128
16.2.1 Rule Summary 128
16.2.2 Setting up the Rule 128
16.2.3 Viewing the Rule Alerts 130
16.2.4 Viewing the Session Recording 130
16.3 Rule Sample 3: User attempting to upload a sensitive file to a cloud drive 131
16.3.1 Rule Summary 131
16.3.2 Setting up the Rule 131
16.3.3 Viewing the Rule Alerts 132
16.3.4 Viewing the Session Recording 133
16.4 Sample Rule 4: User attempting to share files containing sensitive content 134
16.4.1 Rule Summary 134
16.4.2 Setting up the Rule 134
16.4.3 Viewing the Rule Alerts 135
16.4.4 Viewing the Session Recording 136
16.5 Sample Rule 5: Employee productivity anomaly 136
16.5.1 Rule Summary 136

16.5.2 Setting up the Rule 137
16.5.3 Viewing the Rule Alerts 138
16.5.4 Viewing the Session Recording 138
17 Appendix 139
17.1 List of Prebuilt Rule Templates 139
17.2 List of Prebuilt Anomaly Rule Templates 140
17.3 List of Pre-Defined Classified Data 140

1 About This Guide

This guide explains how to utilize Teramind's behavioral rules to detect insider threats, protect your organization from malicious or accidental security incidents, prevent data loss, conform with regulatory compliances or improve the productivity of your team. The guide explains rule structures, conditions, logic, data types etc. It shows you the steps for creating a rule, their uses cases, best practices and advanced capabilities.

The guide is designed for the managers, administrators and security personnel who are responsible for configuring and maintaining the Teramind solution in your organization.

You can access the most up-to-date version of the guide on our Knowledge Base here.

2 Related Resources

- **Teramind User Guide** –contains detailed explanation of Teramind's user interface. It's also an excellent reference manual that can help you quickly locate information or show you how to use Teramind on a day to day basis. The Rules Guide contains context sensitive links to relevant sections on the Teramind User Guide where needed.
- **Teramind Knowledge Base** – contains web versions of the Rules Guide, User Guide, How-To Articles, Deployment Guides, FAQ and other resources.
- **Guided Tour** – Teramind has an interactive tour feature with over a hundred use-cases. You can use this feature to learn how to utilize Teramind features and capabilities and see how some of the common rules work. Click the 

button at the top-right corner of the Teramind Dashboard to access the Guided Tour feature.

3 Rules Overview

Behavioral rules are a core part of Teramind's automated insider threats detection and data loss prevention capabilities. They allow you to identify unproductive, harmful or dangerous activity in real-time and optionally, act on your behalf to thwart such threats. The Intelligent Rules Engine is tightly integrated throughout Teramind platform:

- The Rules Engine utilizes Teramind's granular Activity Monitoring (using the BI Reports) capabilities, such as: apps, websites, emails etc. to determine what activity or content the rule should detect.
- It uses the User Profiles to determine whom the rule will apply to.
- You can use the Configurations settings to supply additional inputs such as employee Schedule, Shared List etc. for use with the Rules Editor to speedup the rule creation process and to share parameters across different rules.
- You can use the Monitoring Settings to control when and how the rule should work, minimizing privacy concerns.
- You can get detailed report of the rule violation incidents and associated risks on the BI Reports > Behavior Alerts, view recordings and gather evidence from the Session Player and get notified with the Rule Notification Emails.
- Teramind Agent enforces the rules you create from the Teramind Dashboard on the user's computer.

With hundreds of pre-built rule templates, pre-defined data categories and sample rules, you can get started with Teramind right away. You can create your own rules very easily with an intuitive, visual Rules Editor. The editor allows you to use natural language, regular expressions, shared list and pre-built data classifications to define what makes an activity or data sensitive and use simple conditions that will trigger a rule violation incident. When a rule is violated, you can be notified about the incident and optionally, the system can take actions automatically in different ways, such as: warning the user, blocking the activity etc.

Teramind keeps detailed records of each rule violation incident complete with detailed information and relevant metadata. You can see the rule violations report from the Alerts screen and quickly search for an incident.

Teramind also captures video and optionally, audio for a rule violation incident. You can view the recordings with the Session Player. The player allows you to see what rule notifications the user received and the trail of activities leading up to the incident. You can also export recordings for evidence or forensic investigation purposes. These recordings are automatically analyzed and index by Teramind's advanced OCR-engine. You can conduct high-speed OCR search for on-screen content or create OCR-based rules that will activate whenever certain text is detected on the screen, in real-time.

You can conduct risk analysis and identify high risk rules, users or objects from the Risk report. This also gives you ideas on how to adjust your rules' detection settings to focus on key areas of vulnerabilities or reduce false positives.

Finally, you can get scheduled delivery of rule violation reports or 'just-in-time' notifications in your inbox with the Email Notifications feature.

3.1 Common Use Cases

3.1.1 Preventing Data Loss

- Uploading documents that contain sensitive data to personal Cloud drives.
- Sharing documents outside the organization that has a confidential watermark.
- Sending out emails with sensitive files to non-corporate emails.
- Sending out emails with large attachments, too many attachments or zipped files.
- Printing during irregular hours.
- Printing a large number of sensitive documents.
- Taking screenshots, using screen capture or snipping tools.
- Copying CRM data and pasting it in emails, an external site or in an unauthorized application.
- Non-authorized use of Cloud sharing drives as an attempt to exfiltrate data.
- Saving files on a removable media.
- Sharing files with protected properties such as Tags, Attribute, Document Category etc.
- Employees communicating with competitors.

3.1.2 Detecting Insider Threats

- Sign of discontent, harassment, legal threats or other sentiment in emails or IM chats indicating underlying issues.
- Development team using production data for testing and development.
- IT department storing authentication information such as credit card magnetic data which is prohibited under compliance laws.
- Accessing internet from restricted servers.
- Installing RDP clients or opening ports.
- User entering sensitive data such as passwords or personal details on potentially harmful or phishing sites.
- Employee using the browser's incognito/private mode frequently.
- Clearing browser history or deleting cache files.
- Sudden change in schedules or work pattern.
- Using code snippets in database queries.
- A vendor attempting to bypass security clearances and gain additional access by exploiting a bug, design flaw or configuration oversight in an operating system or software application.
- Contractor attempting to log in to database servers during off-hours or after the completion of a project.
- External user or freelancer accessing confidential customer and employee records.

3.1.3 Identifying Abusive Behavior and Accidental Threats

- Employees looking at materials online that are questionable, suspicious or otherwise dangerous. For example, hacking sites, pornography or piracy content.
- Abusing company resources, such as, printing unnecessary copies of documents, throttling the network etc.

- Customer agent asking for credit card numbers in unsecure email or support chat without using the proper communications channel.
- Sharing ‘not for the public’ files on social media or IMs.
- Employee opening emails that contain phishing links, viruses or malwares.
- Installing browser plugins that aren’t secure or known to be problematic.
- Entering passwords or personal details in unsecure websites.

3.1.4 Detecting Malicious Intent

- Unauthorized user reading a document they should not have access to.
- User trying to hide information in an image.
- Employee participating in insider trading by sharing embargoed information such as M&A documents.
- Searching the internet for suspicious keywords and phrases, such as: ‘how to disable firewall’, ’recover password’, ’steganography’ etc.
- Running the Tor browser or accessing the darknet sites.
- Attempting to bypass the proxy server.
- Installing VPN client.
- Running network snooper, registry editor or other dangerous applications.
- Running password crackers, keyloggers or other malicious tools.
- Running software from external media or Cloud services.
- Changing the configuration of the network or system settings.
- Opening up blocked ports in the router settings.
- RDP connection attempts to forbidden hosts or unauthorized use of RDP applications.
- Performing IT sabotage by deleting user accounts, files or directories.
- Sharing source codes outside the development team.
- Creating back-door accounts or fake user credentials.

3.1.5 Improving Productivity and HR Management

- Get notified when workers spending too much time on Facebook, watching YouTube videos or surfing online shopping sites.
- Flag when employees idling too much, coming to work late, frequently absent etc.
- Warn employees when they are spending excess time on personal tasks such as applying for jobs.
- Using applications or sites that are unproductive.
- Not following prescribed policy when dealing with customers.
- Not following corporate etiquette policy, for example, visiting gambling sites.
- Contractor submitting invoices that do not match work hours or task completion status.

3.1.6 Conforming with Regulatory Compliance

- Prevent exfiltration of PHI (Protected Health Information) such as EHR, FDA recognized drug names, ICD codes, NHS numbers etc. to comply with HIPAA and HITECH policies (HIPAA 164.500 - 164.532).

- Automatically log-out user when inactive for certain time (HIPAA 174.312).
- Block unauthorized traffic from EHR/EMR and clinical applications (HIPAA 164.306).
- Restrict access based on a user's 'need to know' clearance. For example, block IT admins from accessing cardholder data while performing support tasks (PCI-DSS 10.1).
- Use OCR-based rules to detect when user has access to full view of a PAN (Personal Account Number) violating *PAN-masking* or *PAN-unreadable* rules (PCI-DSS 3.4/3.5).
- Block file-write operation when credit card numbers or magnetic track data is detected that would violate the *storing of authentication data* rule (PCI-DSS 3.2).
- Prevent sharing of contact list containing EU PII (personally identifiable information) such as English names, EU addresses or EU phone numbers (GDPR 5).
- Warn user when sharing files containing data such as DNA profile, NHS/NI number and sexual orientation data, hence preventing the violation of *processing of special categories of personal data rule* (GDPR 9).
- Ensure that non-EU admins cannot access the records of EU employees preventing the violation of *transfers of personal data to third countries* rule (GDPR 44).
- Enforce security-compliant behavior and take immediate action on detection of anomalies or rule violations and train employees with detailed rule-alerts (ISO 27001, Standard Enforcement).

3.1.7 Implementing the MITRE ATT&CK™ Framework

Teramind MITRE ATT&CK Detection & Prevention Library has over 350 sample behavior policies and rules under 13 MITRE Tactics covering the Enterprise Attack Matrix. The rules are designed to detect threat-specific activity, content classification, pre-defined alerts and automated actions and a documented response playbook tailored to each defined scenario.

For more information about the Teramind MITRE ATT&CK Detection & Prevention Library please contact sales@teramind.co.

4 Steps for Creating a Rule

4.1 Why are You Creating the Rule?

Consider what you are trying to achieve. Do you want to monitor users' activities to prevent insider threats? Suspicious that an employee is committing a crime or colluding with an outsider? Or, are you trying to prevent IP leaks through external vendors? Do you need to comply with regulations, such as: HIPAA, GDPR, etc.?

Create a new policy or assign it under an existing policy that fits the rule's purpose.

4.2 What Activity, Content or Behavioral Anomaly You Want to Detect?

Are you trying to detect discrepancies in employees' schedule? Does it involve an 'activity' such as, uploading a document? Or do you need to protect some 'content' such as, sensitive information inside a document?

Select a **Rule Type** from the Rules Editor's *General* tab.

If you are trying to detect behavioral anomalies such as an employee sending abnormal amount of emails than normal, then you should consider creating an anomaly rule.

Create an anomaly rule from the **Behavior** > **Anomaly** rule menu.

4.3 Where is the Activity Performed or Content Located?

Next you need to figure out where the activity or content sharing takes place. Does it involve emails? Transfer of files? Or, are there multiple ingress/egress points that you need to monitor, for example, emails + IM + website uploads?

Select **Types of Activities** or **Types of Contents** from the Rules Editor's *General* tab.

4.4 When Should the Rule be Active?

Do you want the rule to run 24/7 or follow a schedule? For example, do you want the rule active during work hours but disable it during the employee lunch breaks?

You can turn rules on/off from the **Behavior** menu.

Or, you can select a schedule under **When is this rule active?** from the Rules Editor's *General* tab.

4.5 Whom Should it Apply to?

Do you need the rule for everyone? Certain users, groups or departments? How about setting up a terminal server to monitor all your vendors or external partners? Do you need to exclude anyone from the rule's enforcement?

You can choose all these from the *User* tab on the Rules Editor. You can also select users on a policy basis by turning on the **INHERIT POLICY SETTINGS**.

4.6 What Makes the Data Sensitive?

If you are trying to detect Content, can you describe how the data looks? Does it have a clear structure such as a credit card number? Or, do you need to detect information that are unstructured or dynamic in nature?

Use the **Content** tab on the *Rules Editor* to define your content. You can choose from a *Predefined Classified Data* or create your own custom data types by selection other options from the list.

4.7 What Scenarios Violate the Rule?

Now, you have to think about scenarios that will trigger the rule. You might need multiple conditions and logics to detect the rule violation. Remember, there are also multiple ways of achieving the same result.

For example, if you wanted to prevent uploading of files to a personal Cloud drive, you could use a condition to detect file operation 'upload'. And use a second condition, 'upload URL' and specify website addresses such as 'google.drive.com, dropbox.com' etc. Or, you could just select file operations for 'write' and select the 'Cloud providers' from the built-in list.

Use the individual **Categories** (i.e. Website, Application etc.) tab on the *Rules Editor* to define the conditions for the activity or content.

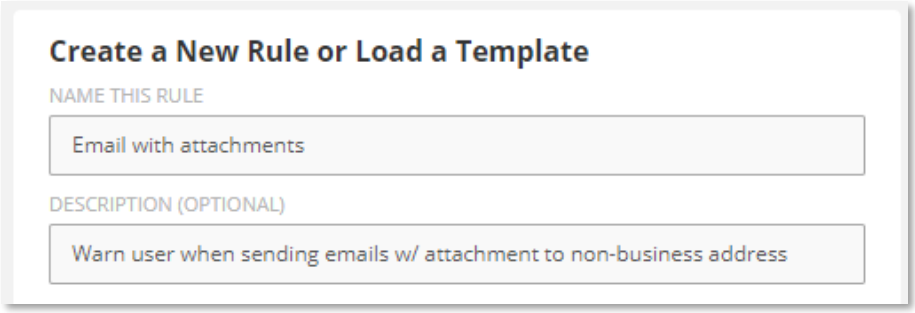
4.8 What Action(s) Do You Want to Take?

What should the system do when a rule is broken? Do you want it to notify you immediately? Or, do you want it to take some preventive actions too? For example, block the action? Or do you need to take a sequence of actions? For example, block the action but also record the incident? Or, take different action depending on how often they broke the rule? Assign a risk level to the action?

Use the **Actions** tab on the *Rules Editor* to define the action(s). Use the **Advanced Mode** to assign multilevel thresholds and risks.

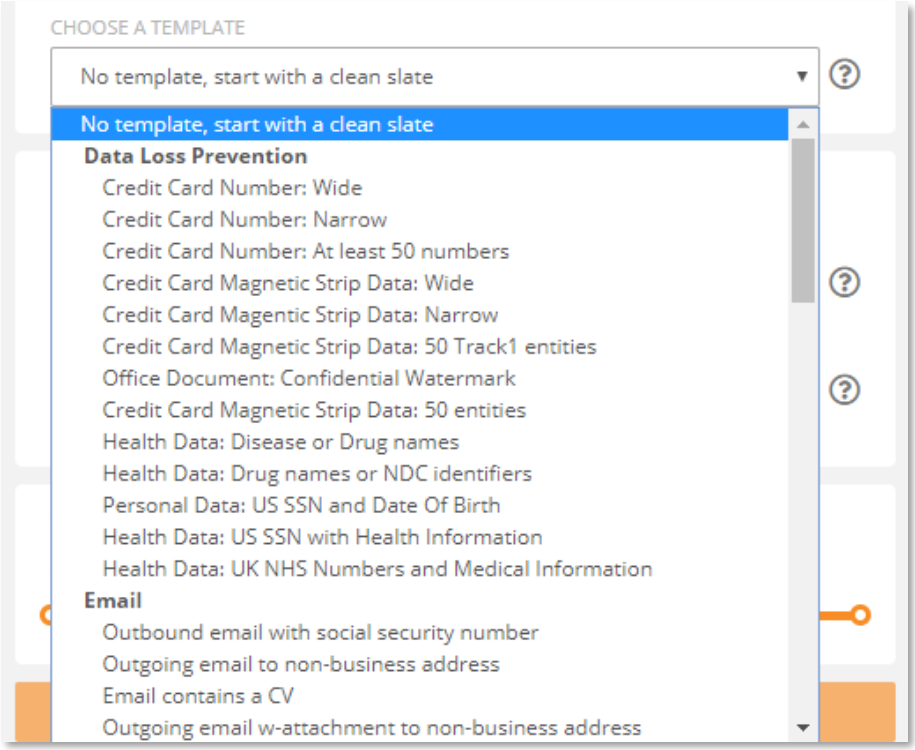
5 Understanding Common Rule Elements

5.1 Rule Name and Description



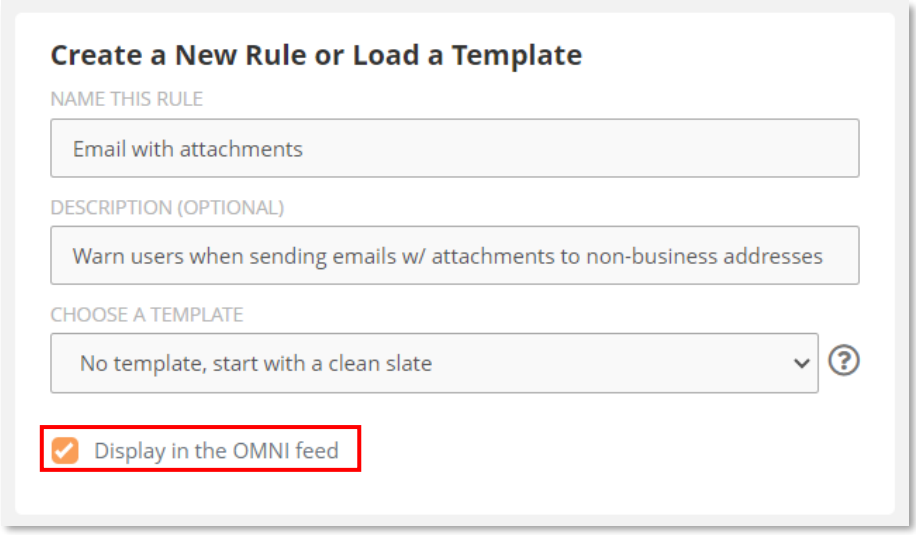
Each rule lets you specify a name and optionally, a description for the rule.

5.2 Rule Template



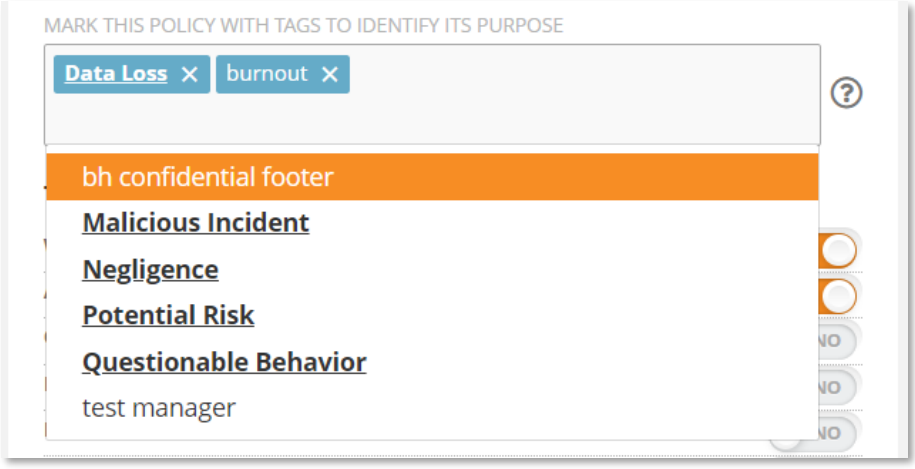
When creating a new rule, you can choose from a list of pre-built templates. Click the **CHOOSE A TEMPLATE** field to choose a template on the General tab. Teramind has many templates for Data Loss Prevention, Email, Applications, Websites, File Operations etc. Once you select a template, the rest of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

5.3 Displaying the Rule in OMNI



Just under the rule templates selection, you will notice an option, “Display in OMNI feed”. If enabled, the rule will show up on the OMNI dashboard (See the User Guide for information about OMNI).

5.4 Tags



Tags are keywords you can assign to a rule to easily identify it. They are useful in searching for the rule and can also be used as filters (i.e. on the Risk or Alerts report).

You might also see some built-in tags such as *Data Loss*, *Malicious Incident*, *Negligence*, etc. that you can assign to the rule. These special tags are used with *OMNI* to categorize different types of risks (see the User Guide to learn more about OMNI and dashboards).

Note that the built-in special tags are currently a request only feature. Please contact your customer service representative to activate the feature on your instance.

5.5 Schedule

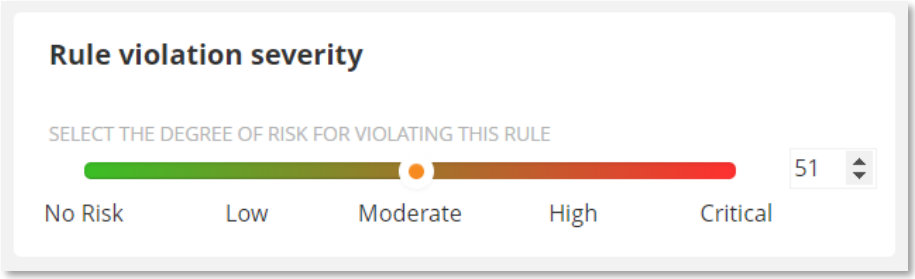


By default, the rule stays active for 24 hours. However, you can adjust it to match your employee work schedule. For example, you can have the rule active during work hours but disable it during the employee lunch breaks. To change when the rule is active, drag the two **Circles** ○ to adjust the time.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

The rule schedule is based on the Dashboard's localization settings (the *TIMEZONE* option under the *Settings* > *Localization* screen).

Agent Schedule rules and *Anomaly* rules do not have this scheduling module. Their scheduling is done in a different way.

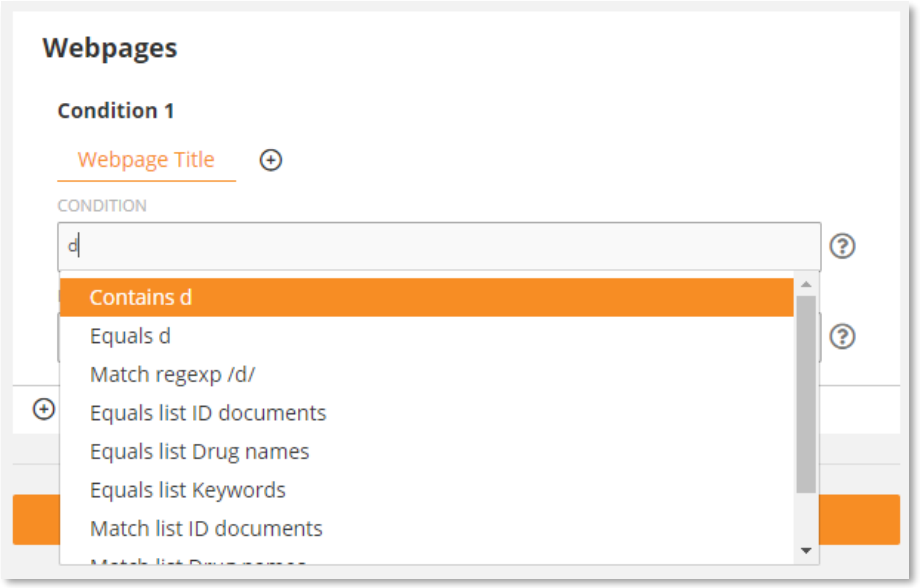
5.6 Rule Violation Severity



The Rule Violation Severity allows you to specify a risk level for the rule. You can either drag the slider or use the number field to enter a number between 0-100. This value is then used in places like *OMNI* to measure the overall risk score. Check out the user guide to learn about OMNI and dashboards.

5.7 Rule Conditions

You use the **CONDITION** fields in a rule to specify what values to compare the rule parameters with. To specify a rule condition, start typing in the relevant CONDITION field, then select an option from the pop-up to tell Teramind what type of value it is.



You can use multiple values in a CONDITION field by clicking on a blank space in the field.

There are several conditions you can use. For example:

5.7.1 Contains

Use the *Contains* conditions for a partial text match. So, say you were searching for "you" then the *Contains* condition will detect any of these texts: "YouTube", "youtube.com", "youth", "layout" since they all contain the text "you".

An example use of this condition can be to block certain applications from running, you can type them in the CONDITION field and choose one of these conditions.

Note that, this condition isn't case-sensitive. So, words like "You", "YOU", "you" – will have the same result.

5.7.2 Equals

Similar to the *Contains* condition but in this case, the text has to be an exact match. So, say you were searching for "you" then the *Equals* condition will NOT detect any of these texts: "YouTube", "youtube.com", "youth", "layout". However, it will detect "You", "YOU", "you" since they are exact matches even though the cases don't match, and that doesn't matter because the *Equals* condition isn't case sensitive.

5.7.3 Match RegExp

For complex matches, such as Credit Card Numbers, Social Security Numbers, etc., you can use the *Match RegExp* option. For example, the regular expression "[a-zA-Z]{2}[0-9]{12}" will detect

any text that starts with 2 alphabet characters and ends with 12 digits such as, “`PO123456789123`” or, “`ab123456789012`”.

Teramind supports the standard Regular Expression library available in C++.

Check out this article on our Knowledge Base to learn more about Regular Expressions.

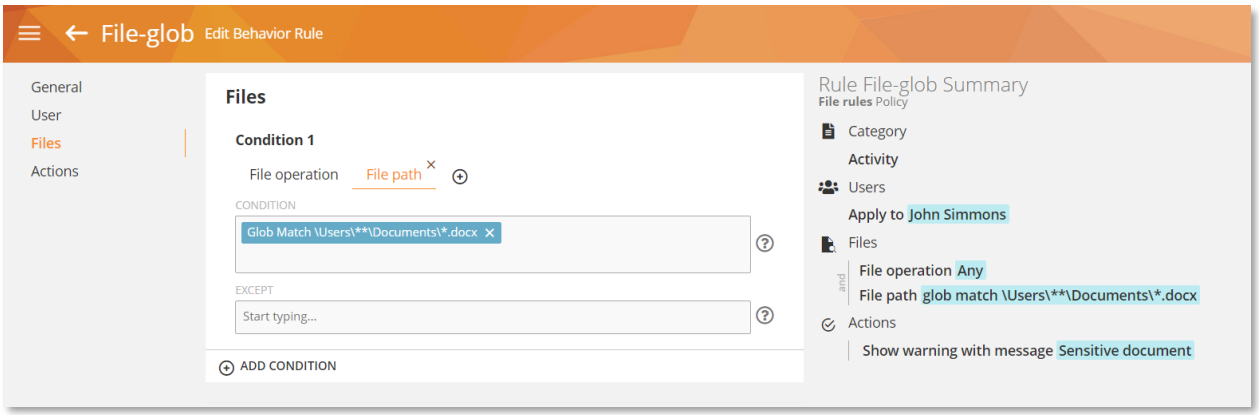
5.7.4 Match Glob

This condition can be used in some specific cases, e.g., in File-based rules. It finds texts which follow a specific pattern or 'glob'.

The `*` glob will match zero or more characters. For example, the pattern, glob match `*.exe` in the *File path* criteria of a File-based rule will match all the executable files.

The `?` glob will match exactly one character but you can also use more than one together. For example, glob match `Sales????.doc` will match “Sales2022.doc”, “SalesACME.doc”, “Sales23NA”, etc.

The special `**` glob (called "globstar") can be used to detect any directories and subdirectories. This allows for recursive directory searching easily. Here’s an example:



The above rule with the glob match `\Users\**\Documents\*.docx` condition will detect any word document in paths like:

- \Users\Danny\Documents
- \Users\Brian\Documents
- \Users\Public\Documents\Jason\Sales\Documents
- \Users\Joe\Sensitive\Proposals\Documents
- etc…

5.7.5 Match List

This is similar to the *Contains* condition but matches with any item on a Shared List. So, for example, if you had a shared list containing “`YouTube`”, “`youtube.com`”, “`youth`”, “`layout`” etc., then any text like, “`you`”, “`tube`”, “`You`”, “`Out`”, etc. will be detected.

Check out the Shared List section on the Teramind User Guide to learn more about Shared Lists.

5.7.6 Equals List

This is similar to the *Equals* condition but will check for an exact match with any item on a Shared List. So, for example, if you had a shared list containing "`YouTube`", "`youtube.com`", "`youth`", "`layout`" etc., then any text like, "`youtube`", "`Youtube`", "`YouTube`" will be detected. However, "`you`", or "`tube`", etc. will NOT be detected.

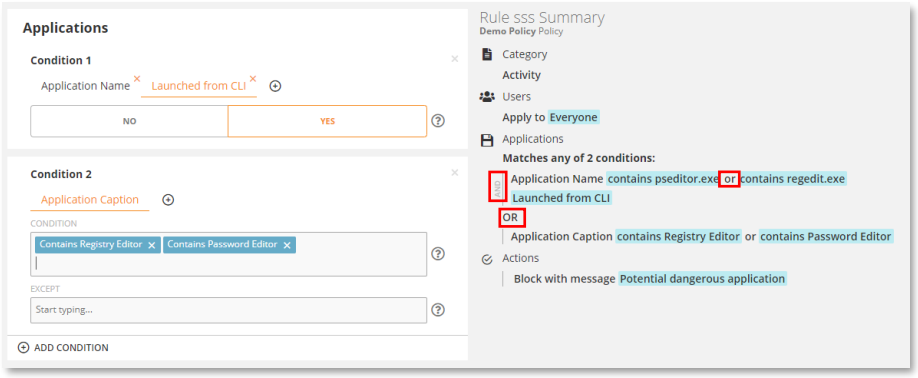
Check out the Shared List section on the Teramind User Guide to learn more about Shared Lists.

5.8 Rule Logic

Rule logic binds two or more Conditions or Content Definitions together. So, they can be applied to both the rule Conditions and the Content Definitions.

5.8.1 Condition Logic

Rule conditions can either have a 'OR' logic or an 'AND' logic.

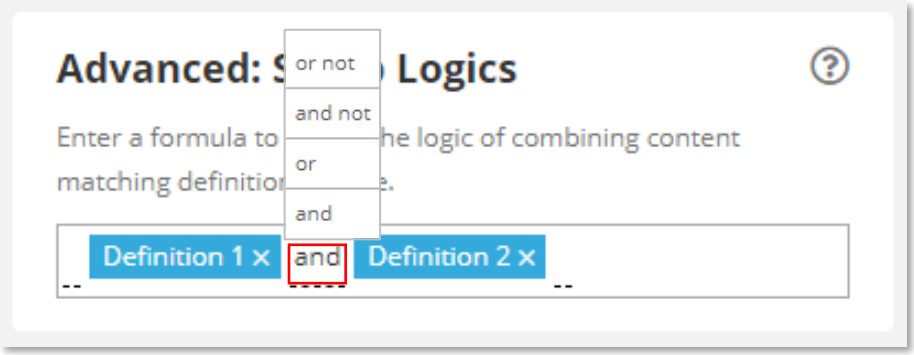


- Each value in a rule condition is considered as an 'OR' logic. In the above example, the rule will trigger if the 'Application Name' matches with 'regedit.exe' or 'pseditor.exe'.
- Each condition parameter is considered as an 'AND' logic. In the above example, the rule will trigger if the 'Application Name' and the 'Launch from CLI' parameters meets the condition.
- If you have multiple condition blocks, each new condition is considered as an 'OR' logic. In the above example, if either the Condition 1 or Condition 2 meets the criterion, the rule will be triggered.

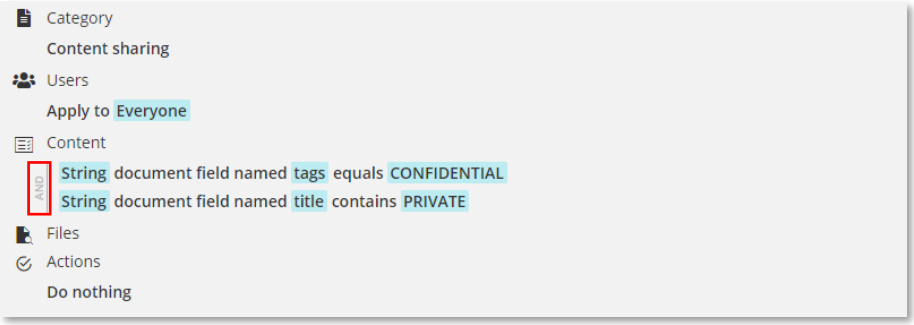
You can see how the rule condition logics relate to each other on the Rule's **Summary** panel.

5.8.2 Content Logic

When creating a Content S haring rule and you have multiple content definitions, you can use logics to bind the definitions together. You can do so under the *Advanced: Setup Logics* section of the **Content** tab. Click on the **logic** between two conditions, a pop-up menu will appear where you can select a logic out of four options.



You can see how the content definition logics relate to each other on the Rule's **Summary** panel.



The table below explains each type of logic and how they are evaluated:

Logic	Evaluates true if:	Example
AND	BOTH of the definitions are met.	In the above example, we are using the *tags* field from the *File Properties* in Definition 1 and the *title* field in Definition 2. The logic will return true if file tags equals the text 'CONFIDENTIAL' *and* the title contains 'PRIVATE'. So, basically, it will process the files that are both confidential and private.
OR	EITHER of the definitions is met.	Using the above example, the logic will return true if file tags equals the text 'CONFIDENTIAL' *or* the title contains the text 'PRIVATE'. So, basically, it will process the files that are either confidential or private.
AND NOT	the first definition is met AND the second definition is NOT met.	Using the above example, the logic will return true if file tags equals the text 'CONFIDENTIAL' *and* the title does *not* contain the text 'PRIVATE'. So, basically, it will process the files that are confidential and not private.
OR NOT	the first definition is met OR the second definition is NOT met.	Using the above example, the logic will return true if file tags equals the text 'CONFIDENTIAL' *or* the title does *not* contain

the text ‘PRIVATE’. So, basically, it will process all files except the private ones.

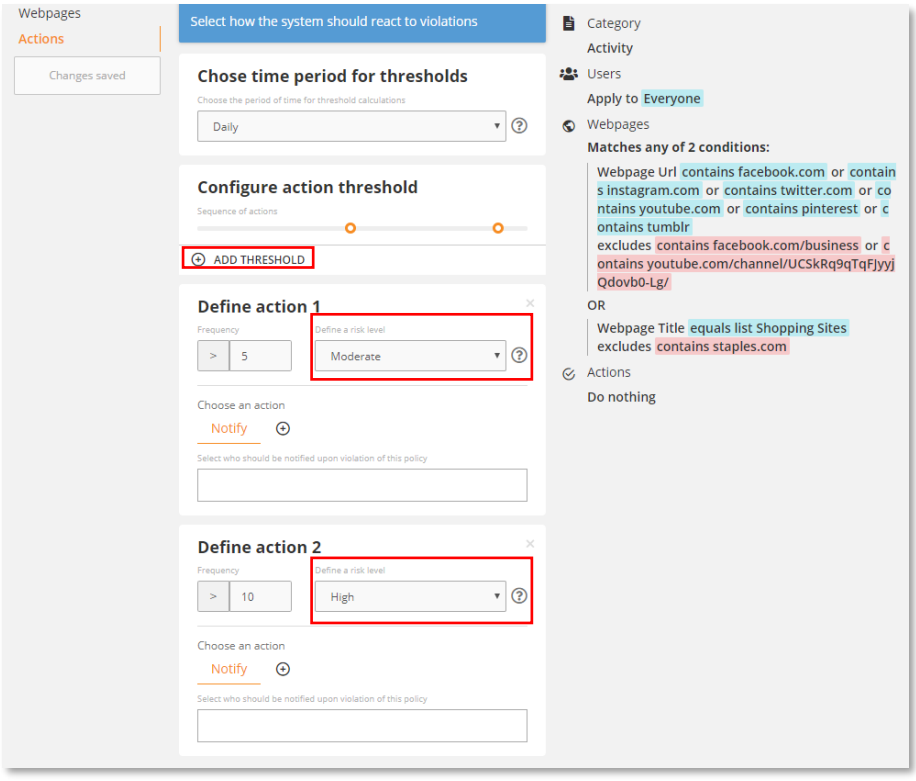
5.9 Risk Level

Note that each rule also contains a Rule Violation Severity which is also treated like a risk and used in *OMNI*. Check out the User Guide to learn more.

On Teramind, you can assign risk levels to the rules. While optional, assigning risk levels has some advantages. It will let you analyse risk on the Risk Report, view risk trend and identify high risk users and rules.

There are two places you can assign risks.

5.9.1 Setting the Risk Levels in a Regular Rule

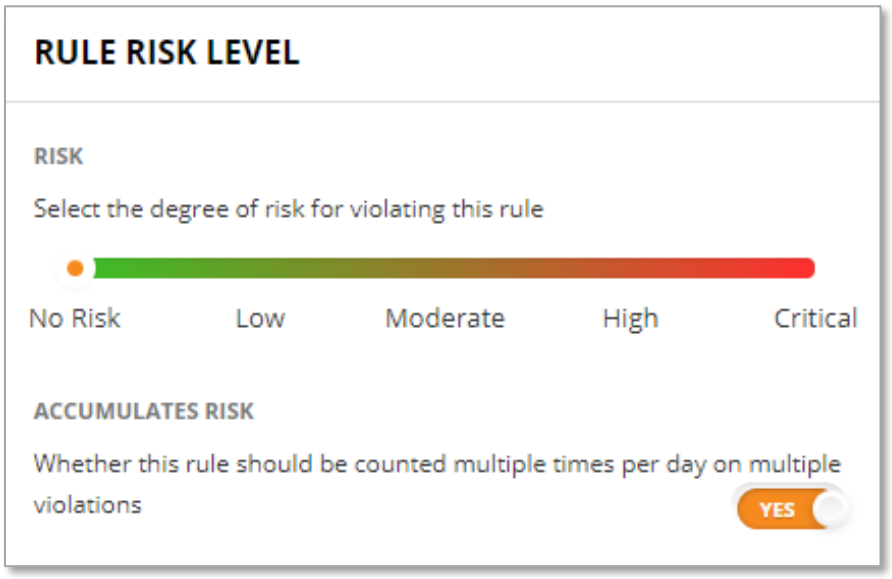


You assign risk level to a regular rule from the **Advanced Mode** of the *Rule Editor*’s **Actions** tab. You can choose from: No Risk, Low, Moderate, High and Critical.

You can assign risk levels to each action block separately (you create action blocks by clicking the **ADD THRESHOLD** button).

Check out the Advanced Mode Actions section to learn more.

5.9.2 Setting the Risk Level in an Anomaly Rule

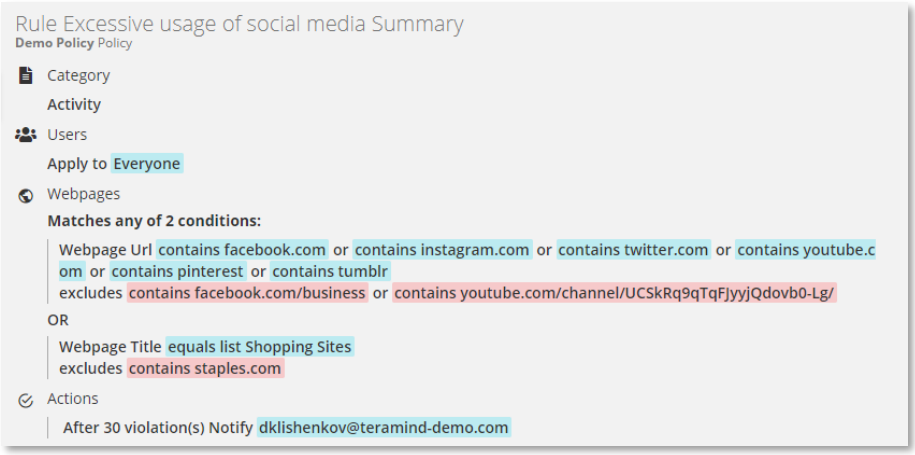


You assign risk level to an Anomaly rule Under its RULE RISK LEVEL section. You can choose from: No Risk, Low, Moderate, High and Critical. You can also turn on its ACCUMULATES RISK option on. If turned on, the risk associated with the rule will be counted multiple times for multiple violations. Otherwise it will be counted once for all violations. Unlike the regular rules which support multilevel risk assignments, you can assign only one risk level per anomaly rule.

5.10 Employees

5.11 Rule Summary

The right-most panel of the Rules Editor shows a summary of the rule in easy to follow language. You can see the values used in different tabs; what conditions are used and the logical connection among them; rule actions etc.



Note: Anomaly Rules Editor does not have a Summary panel.

6 Creating Regular Rules

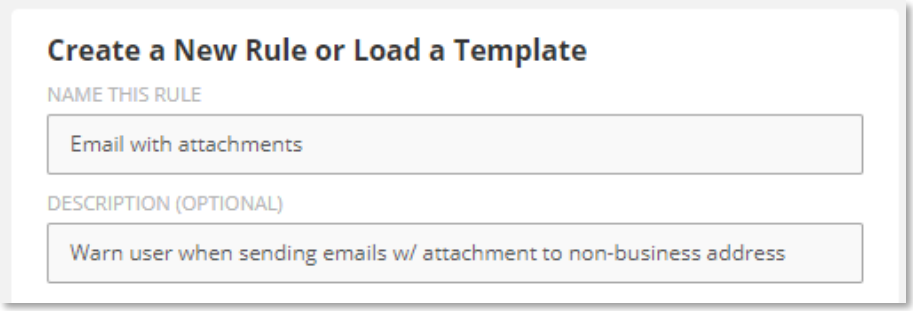
The Rules Editor is an intuitive, visual editor where you can create sophisticated threat detection, productivity optimization or data loss prevention rules easily without going through multiple screens or coding.

To access the Rules Editor, create a new rule or edit an existing rule from the **Behavior** > **Policies** menu.

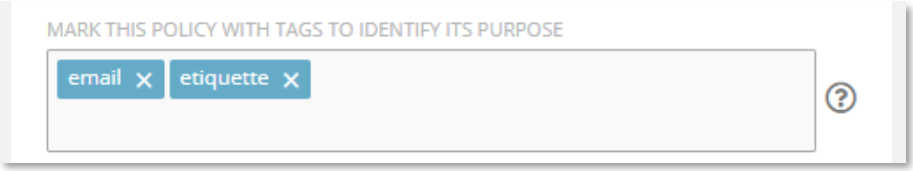
Check out the *Behavior* section on the Teramind User Guide to learn more about creating / editing rules, managing policies etc.

6.1 Setting Up the Rule Basics

You specify the basic settings for the rule on the Rules Editor's **General** tab.



On the top fields, specify a Name and optionally, a Description for the rule.



You can also specify the rule's Tags on this tab. Tags are keywords you can assign to a rule to easily identify it. They are useful in searching for the rule and can also be used as filters (i.e. on the Risk or Alerts report).

6.2 Selecting Rule Categories and Types

You can select the *Rule Category* and *Types of Activities* (for Activity-based rules) or the *Types of Content* (for Content Sharing rules) from the Rules Editor's **General** tab.

There are three types of rule categories you can choose from: Agent Schedule, Activity and Content Sharing. Each category further supports different activities or content types. The table below shows which categories supports which activity/content types and their use cases:

	Agent Schedule	Activity	Content Sharing
Use Cases	Useful for detecting discrepancies in employee schedules or workflow. For example, receive notification when an employee is late. Or, block remote login during odd-hours or from unrecognized IPs.	Useful for detecting and controlling user activities for a range of monitored objects. For example, restricting app/website usage. Or, preventing file transfer operations (copy, upload, download etc.) on a folder/app/URL.	Useful for protecting sensitive data. For example, block and email that contains personally identifiable information. Or, preventing file transfer operations when certain content is detected in the file.
Type of Activity/Content	• Schedule	• Webpages • Applications • OCR • Keystrokes • Files • Emails • IM (Instant Messaging) • Browser Plugins • Printing • Networking • Registry • Camera Usage • Windows Log Event	• Content • Clipboard • Files • Emails • IM (Instant Messaging) • Keystrokes

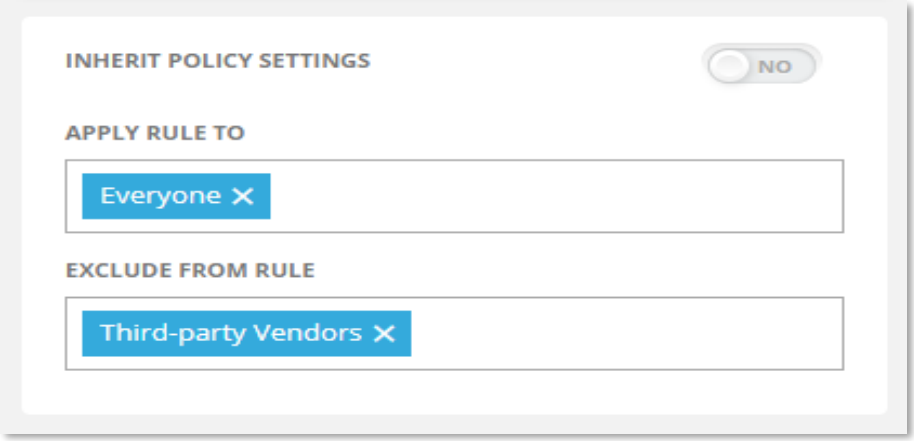
Notes:

- *Content Sharing* rules are only available on Teramind DLP
- *OCR* rule is only available on Teramind Enterprise
- Teramind Starter only has these rules available: *Agent Schedule*, *Webpages, Applications, IM, Browser Plugins, Registry, Windows Log Event*

6.3 Defining Users

You specify the users for the rules on the Rules Editor's **User** tab.

Here you specify which users, groups, departments or computers the rule will apply to. If you select a computer, the rule will apply to all the users on that computer.



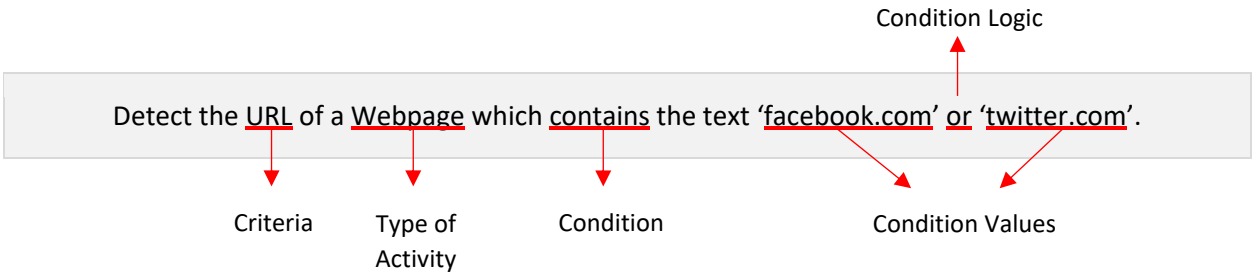
By default, the rule will inherit the user settings from the policy the rule is a part of. However, you can turn off the INHERIT POLICY SETTINGS to select users manually.

You can specify who the rule will apply to and optionally, exclude anyone you don't want to be included using the EXCULUDE FROM RULE field.

Check out the Teramind User Guide to learn how to add users, computers, groups and departments.

6.4 Defining Detection Criteria

After you have decided what type of rule you need and which users the rule will apply to, the next part is defining the detection criteria and scope. You will specify what, how or when the rule will be activated. You do this by selecting different parts of the selected Activity Type or Content Type. For example, the *URL* of the Webpage activity or the *Application Name* of the Clipboard content etc. You can then specify Condition Logics against the part(s) and the values you want to detect. Here's how a detection criterion may look like:



In the next few sections, we will walk you through all the available options for setting detection criteria for each rule type.

7 Agent Schedule Rules: What Schedule Violations Can You Detect (Windows)?

You can specify the detection criteria for the Agent Schedule-based rules from the **Schedule** tab. Agent Schedule-based rules are the easiest to define as most of it deals with only one detection criterion, schedule/time.

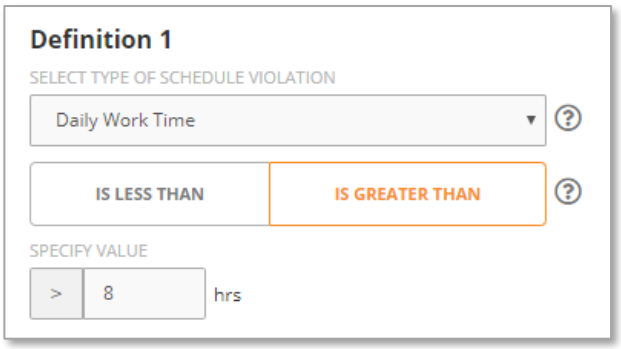
> Agent Schedule-based rules use the employee schedules and the time zone set in the Dashboard's localization settings to determine their detection criteria. Check out the Configure > Schedules section of the Teramind User Guide to learn how to configure schedules for employees.

7.1 Agent Schedule Rule Examples

- Get notified when a user attempts to login during abnormal hours or on off days.
- Warns user or automatically locks out their computer if they are idling for too long.
- Notify supervisor automatically when an employee is absent or late.
- Notify HR and/or payroll if employee's work time or scheduled work hours change.
- Create a list or range of restricted IPs and disallow login from those IPs.

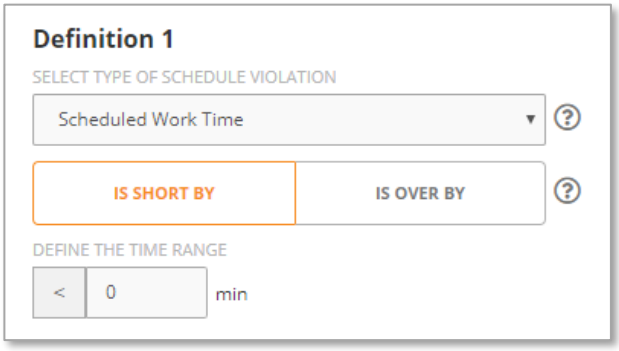
7.2 Agent Schedule Rule Criteria

The table below explains what criteria or schedule violation incidents the Agent Schedules supports and what conditions you can use with them.



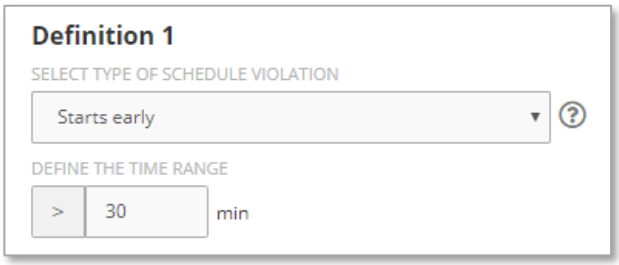
Daily Work Time
Used to detect if there are any discrepancies in the employee's daily work time. You can detect if their work hour is less than or more than specified hour(s).

Select either IS LESS THAN or IS GREATER THAN and enter an hour value in the SPECIFY VALUE field.



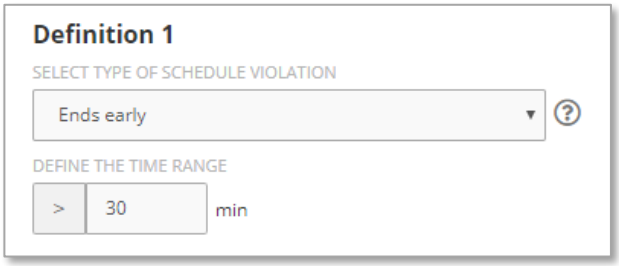
Scheduled Work Time
Used to detect if the employee is working longer or shorted than scheduled.

Select either IS SHORT BY or IS OVER BY and enter a minute value in the SPECIFY VALUE field.



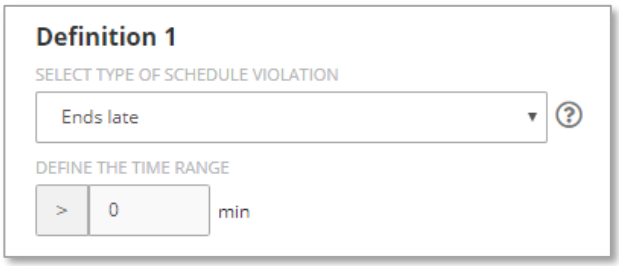
Starts Early
Detects if the employee started their work earlier than scheduled, by specified minutes.

Enter a minute value in the DEFINE THE TIME RANGE field.



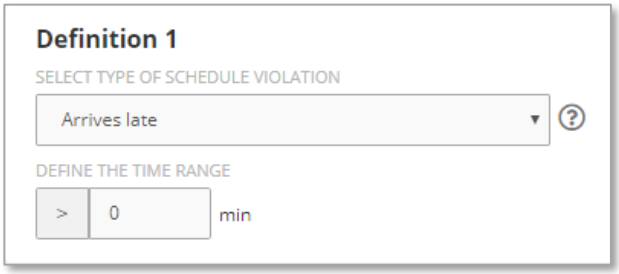
Ends Early
Detects if the employee ends their work earlier than scheduled, by specified minutes.

Enter a minute value in the DEFINE THE TIME RANGE field.



Ends Late
Detects if the employee ends their work later than scheduled, by specified minutes.

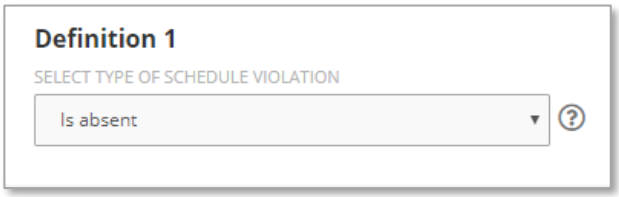
Enter a minute value in the DEFINE THE TIME RANGE field.



Arrives Late

Detects if the employee starts their work later than scheduled, by specified minutes. Note that, unlike the 'Is Late' condition, this will trigger the rule after the employee has logged in.

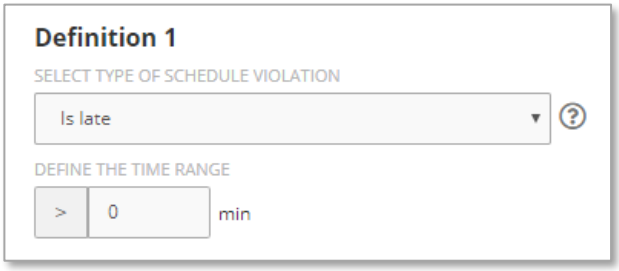
Enter a minute value in the DEFINE THE TIME RANGE field.



Is Absent

Detects if the employee is absent.

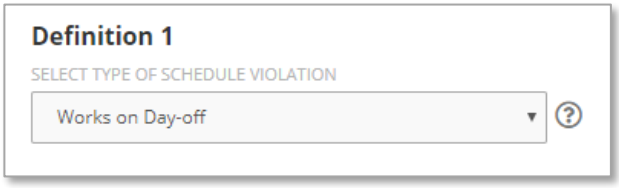
No other value is required.



Is Late

Detects if the employee is late in logging in to their computer according to their scheduled start time. Note that, unlike the 'Arrives Late' condition, this will trigger the rule before the employee has logged in.

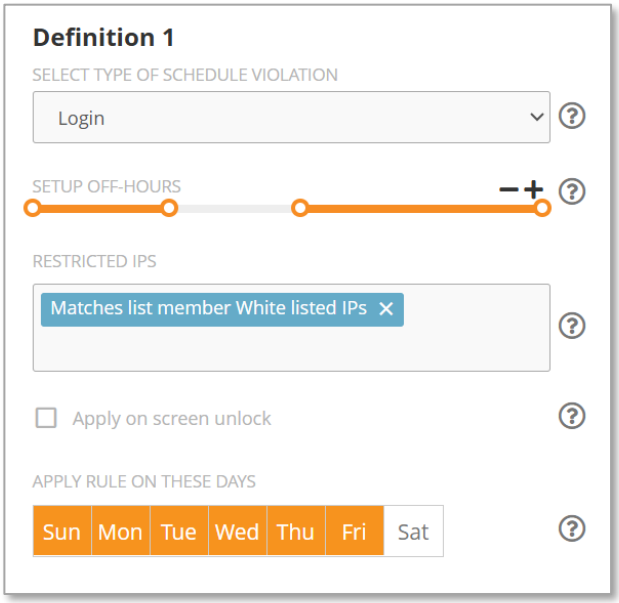
Enter a minute value in the DEFINE THE TIME RANGE field.



Works on Day-Off

Detects if the employee is working on their day off.

No other value is required.



Login (Stealth Agent)

Detects if the employee logs in during off hours and optionally also detects if they are trying to login from a restricted IP.

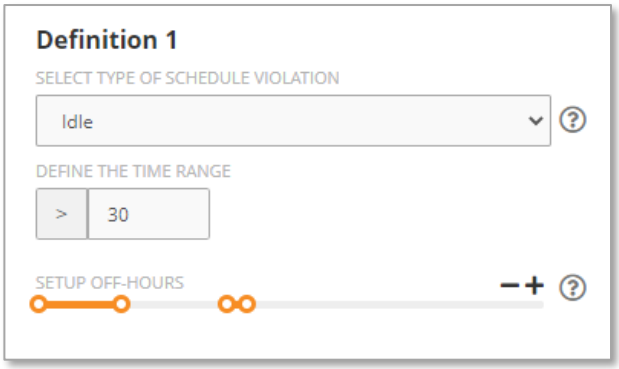
Set the off-hour range on the SETUP OFF-HOURS slider. You can click the **+** / **–** buttons to add/remove hours. Drag the slider **Circles** to adjust the hours. The rule will not apply during these time slots.

The rule will NOT be enforced for IP addresses enter in the RESTRICTED IPS field. You can enter any text in the IPv4 format, i.e.: 101.10.2.1/32 and choose a 'Equals' or 'Not Equals' conditions. Or, you can select a Shared List (Network-based) and specify a 'Match List' or 'Does Not Match' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

If you check the 'Apply on screen unlock' box, then the login event will be triggered as soon as the user unlocks their screen.

Click on weekdays under the APPLY RULE ON THESE DAYS section to select days when the rule will be enforced.

This criterion works for Stealth/Hidden Agent only.



Idle

Detects if the employee is idling (no keyboard or mouse activity) for more than specified minutes.

Enter a minute value in the DEFINE THE TIME RANGE field.

You can also set off-hours (breaks) by dragging the sliders under SETUP OFF-HOURS. The rule will be suspended during the off

hours. Click the small **–** or **+** buttons to add as many breaks as you want.

The *Idle* criterion will generate a single alert - when the rule is violated. This means, the rule will trigger when the user becomes idle for the duration specified in the rule's threshold (DEFINE THE TIME RANGE field). In the above case, the user will get a warning at the 30 minute mark. If the user continues to stay idle, they will not receive any more warnings. However, if the user becomes active and then goes to idling again, the rule will reset and issue a warning after another 30 minutes.

This criterion works independently of the IDLE TIME THRESHOLD value on the *Monitoring Settings* > *Applications* window.

8 Activity Rules: What Activities Can You Detect (Windows & Mac)?

You can specify the detection criteria for the Activity-based rules from their respective activity tab(s). For example, if you selected Webpages and Emails from the *Type of Activity* section (in the **General** tab), you will have two tabs called 'Webpages' and 'Emails' where you can add the rule conditions and values.

8.1 Webpages (Windows & Mac)

Webpages activity allows you to detect web browsing activities through URL, title and query arguments and browsing-related timing (i.e. idle/active).

8.1.1 Webpages Rule Examples

- Warn users when spending excessive time on social media or entertainment sites such as YouTube.
- Restrict access to non-whitelisted/unauthorized websites but allow managers to override if needed.
- Find out potential turnover by checking if employees are searching on jobsites. Get notified if the time spent on such sites exceeds a threshold.

8.1.2 Webpages Rule Criteria

The table below shows what criteria the Webpages activity supports and what conditions you can use with them.

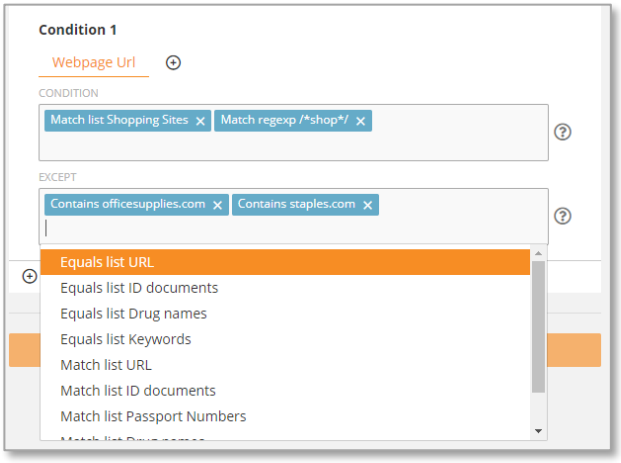
> On Mac, only the following criteria are supported: *Webpage Url*, *Webpage Title*, *Request type* and *Query argument name*, *Private Mode (Safari only)*.



Any

Lets you detect if a webpage is visited.

If you use this option without any other criteria, Teramind will trigger the rule anytime a webpage is visited.



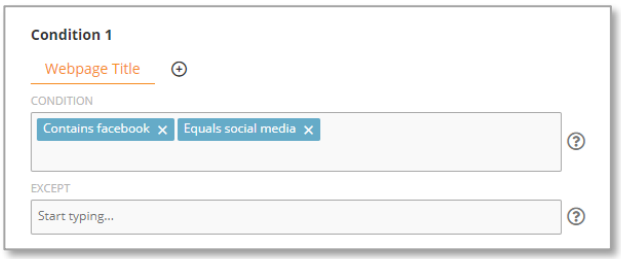
Webpage URL

Used to detect an URL (webpage address) or part of an URL.

You can enter some text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List and specify a 'Match List' or 'Equals' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any URLs in the EXCEPT field.

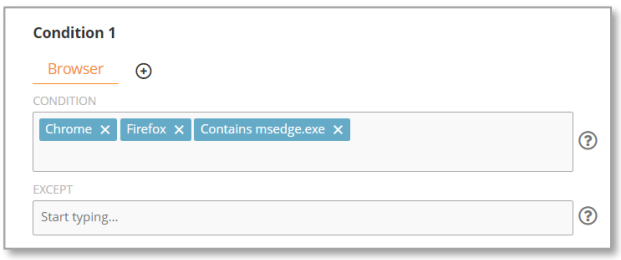
To avoid false positives, we recommend using most of the URL or the full URL if possible, when using any of the conditions. For example, use "https://www.facebook.com" instead of "facebook".



Webpage Title

Similar to the *Webpage URL* criterion, just use the webpage title instead.

If the rule fails to detect webpage titles, ensure that the TRACK WINDOW TITLE option is enabled in the *Monitoring Settings > Websites* window.



Browser

Allows you to specify one or more browsers to detect. You can choose from the list of predefined browsers. You can also enter the browser's process name (for example, enter `msedge.exe` for Microsoft Edge browser). *See the notes below for more information.

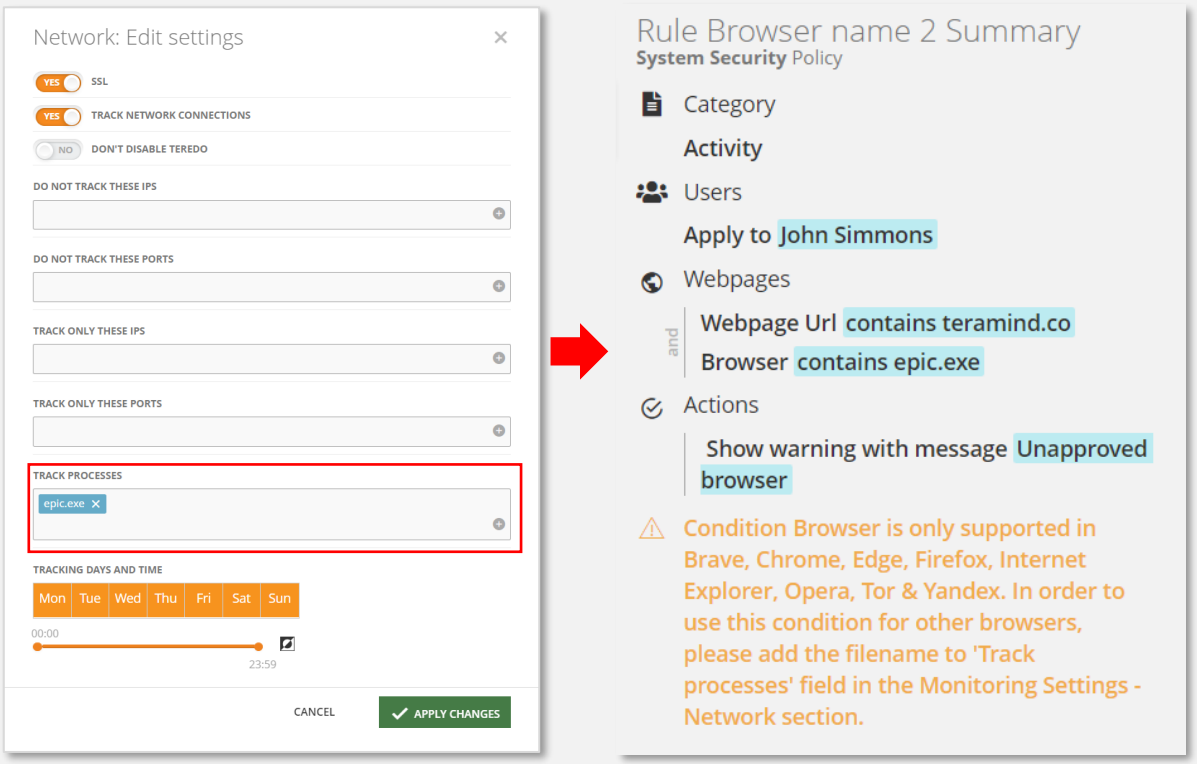
If you typed a browser name, you can enter some text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'.

Or, you can select a Shared List and specify a 'Match List' or 'Equals' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

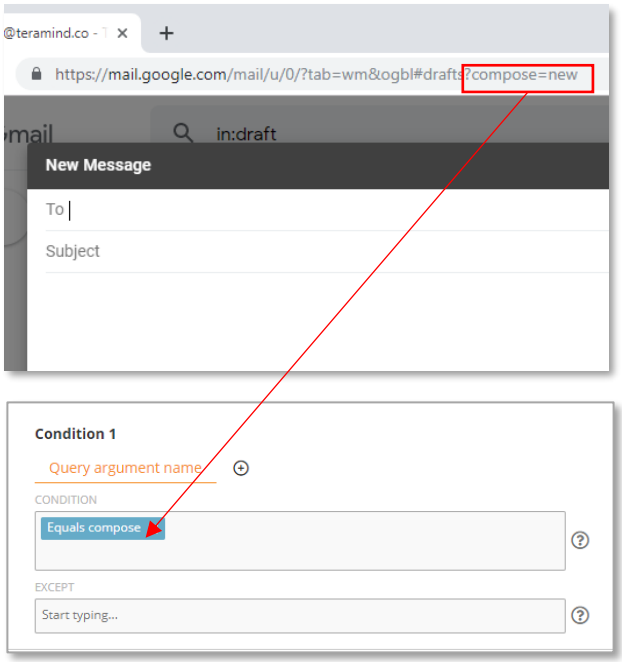
You can exclude any browser(s) from the condition in the EXCEPT field.

* Tracking Browsers not in the Predefined List

If you want to use the Browser criterion with a browser not in the predefined list, you will need to include it in the TRACK PROCESSES field (*Monitoring Settings* > *select a monitoring profile* > *Network*). For example, if you want to detect if the user is browsing a particular site (e.g., `teramind.co`) on the Epic Privacy Browser, you will need to specify it in the TRACK PROCESSES field and then use a rule like this:



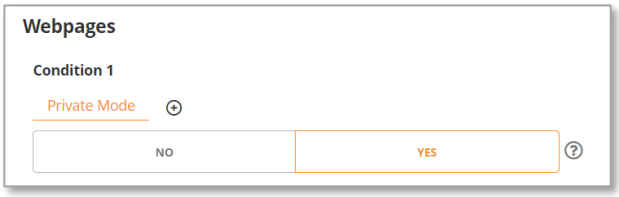
If you don't include the process name in the TRACK PROCESSES field, the rule might not work.



Query Argument Name

A query argument name is the portion of a URL where data is passed to a website. It usually starts with a '?' or '&'. For example: `www.contacts.com/saved?company=teramind`. Here, *company* is the query argument name.

Using this criterion, you can create interesting detection rules. For example, by checking for the 'compose' argument in the Gmail website, you can detect if the user is composing an email. Combining this with the *Webpage URL* or *Webpage Title* criterion, you can detect more granular activities. For example, using the text 'new' in the *Webpage URL* and specifying 'compose' in the *Query Argument Name*, you can tell if a user is composing a new mail or editing an existing draft.

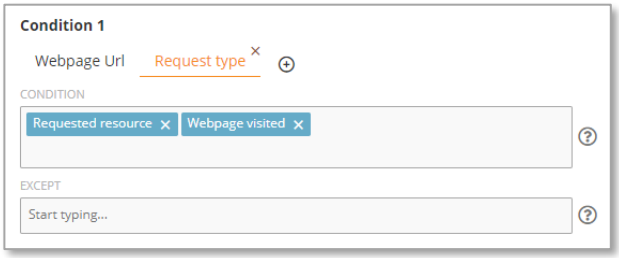


Private Mode

This criterion can be used to detect private/incognito/anonymous browsing.

On Windows, this criterion isn't supported on Firefox at the moment.

On Mac, this criterion is supported on Safari only at the moment.



Request Type*

This criterion allows you to further finetune when the rule action will trigger when the user visits an URL specified in the *Webpage URL* condition. It has two options:
Webpage Visited: detects visited pages, downloaded files, etc. When you select this option, the rule will trigger only when the user visits the webpage specified in the *Webpage URL* condition and not any automated/background browser request. Previously, there was no way to distinguish

user-initiated queries from secondary resource queries, therefore triggering false positives.

Consider this scenario:

1. You have a rule that blocks a *Webpage URL*, `twitter.com`.
2. User visits some unrelated website, such as `news.com`.
3. The user is blocked from visiting `news.com` because that website made a query to get some ads from `twitter.com`.

If you enable the *Request Type* > *Webpage Visited* option, the user can now visit `news.com` without the rule getting triggered.

Requested Resource: detects browser requests for static content, e.g., JS, CSS, images, etc., pages opened through an iframe, as well as API requests.

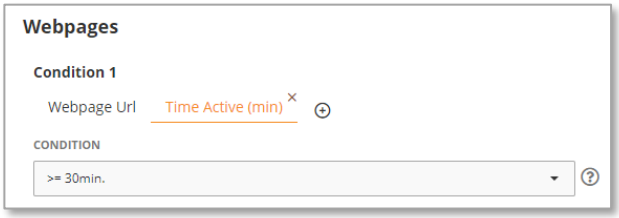
Consider this scenario:

4. You have a rule that blocks a *Webpage URL*, `facebook.com`.
5. User visits some unrelated website, such as `news.com` which has some Facebook ads.

If you enable the *Request Type* > *Requested Resource* option, the user will be allowed to visit `news.com` freely but the ads from Facebook will not load (404 error).

The *Request Type* criterion is only shown when you have already selected a *Website URL* criterion.

* *This feature may not work properly on older browsers. You need at least Chrome version 79, Edge version 79, Firefox version 89, Opera version 66, etc.*

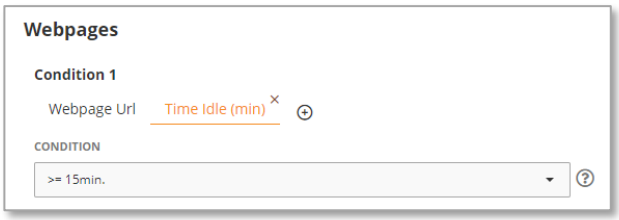


Time Active

Used to detect how long the user has been active on the website.

You can enter a minute value in the CONDITION field and use the '>=' logic.

The *Time Active* criterion is only shown when you have already selected a *Website Title* or a *Website URL* criterion.



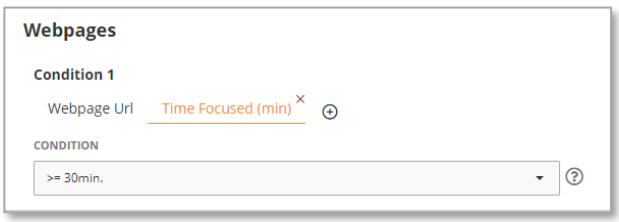
Time Idle

Similar to the *Time Active* criterion but detects how long the user has been idle/inactive on the site.

You can enter a minute value in the CONDITION field and use the '>=' logic.

The *Time Idle* criterion is only shown when you have already selected a *Website Title* or a *Website URL* criterion.

This criterion works independently of the IDLE TIME THRESHOLD value on the *Monitoring Settings* > *Applications* window.



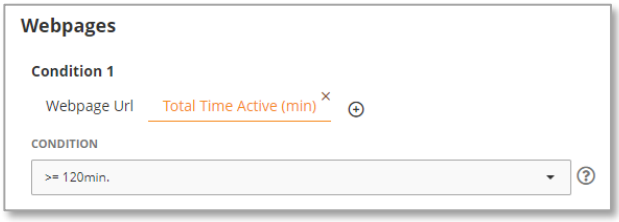
Time Focused

Time Focused = Time Active + Time Idle.

It detects if the user stayed on a webpage for the specified duration. It doesn't matter whether the user was active (e.g., keyboard/mouse is used) or idle (no keyboard/mouse activity); as long as they stayed on the webpage without switching to other webpages/tabs/windows, the condition will be triggered.

You can enter a minute value in the CONDITION field and use the '>=' logic.

The *Time Focused* criterion is only shown when you have already selected a *Website Title* or a *Website URL* criterion.



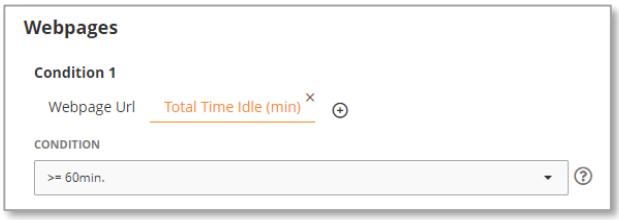
Total Time Active

Similar to the *Time Active* criterion but detects the *total* time active accumulated throughout the day.

The time will reset at the end of the day. This reset happens when the date of the last total time update differs from the current date. For the reset, the user's local time zone is followed.

You can enter a minute value in the CONDITION field and use the '>=' logic.

The *Total Time Active* criterion is only shown when you have already selected a *Website Title* or a *Website URL* criterion.



Total Time Idle

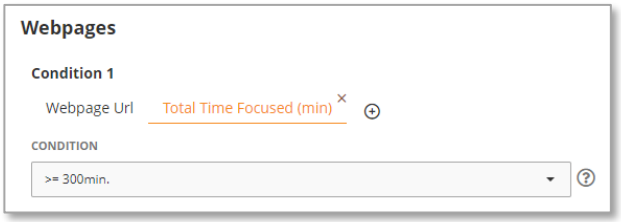
Similar to the *Time Idle* criterion but detects the *total* time idle accumulated throughout the day.

The time will reset at the end of the day. This reset happens when the date of the last total time update differs from the current date. For the reset, the user's local time zone is followed.

You can enter a minute value in the CONDITION field and use the '>=' logic.

The *Total Time Active* criterion is only shown when you have already selected a *Website Title* or a *Website URL* criterion.

This criterion works independently of the IDLE TIME THRESHOLD value on the *Monitoring Settings* > *Applications* window.



Total Time Focused

Similar to the *Time Focused* criterion but detects the *total* time focused accumulated throughout the day.

The time will reset at the end of the day. This reset happens when the date of the last total time update differs from the current date. For the reset, the user's local time zone is followed.

You can enter a minute value in the CONDITION field and use the '>=' logic.

The *Total Time Focused* criterion is only shown when you have already selected a *Website Title* or a *Website URL* criterion.

8.2 Applications (Windows & Mac)

Applications activity allows you to detect the launch of any application including the ones run from the command line interface or through the Windows Run command.

8.2.1 Applications Rule Examples

- Detect and block when a dangerous application (i.e. Windows Registry Editor) or an unauthorized application is launched.
- Warn users when spending time on unproductive applications such as games, music/video player etc.
- Detect when anonymous browsers, such as, 'Tor' is used.
- Detect when screen sharing applications, snipping tools or peer-to-peer file sharing/torrent software are used.

8.2.2 Applications Rule Criteria

The table below explains what criteria the Applications activity supports and what conditions you can use with them.

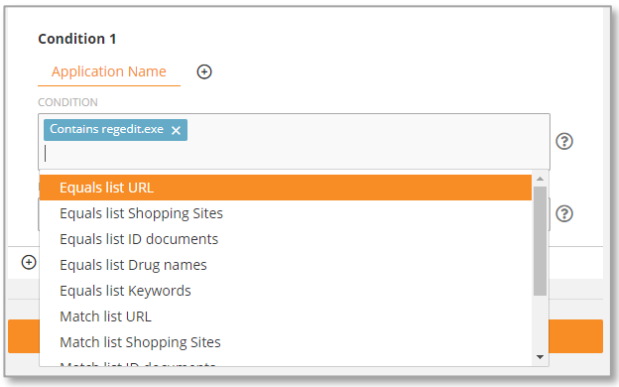
On Mac, only the *Application Name*, *Application Caption* and the *Time Active (min), Time Idle (min), Time Focused (min), Total Time Active (min), Total Time Idle (min), Total Time Focused (min)* criteria are supported at the moment.



Any

Lets you detect if an application is launched.

If you use this option without any other criteria, Teramind will trigger the rule anytime, any application is launched.

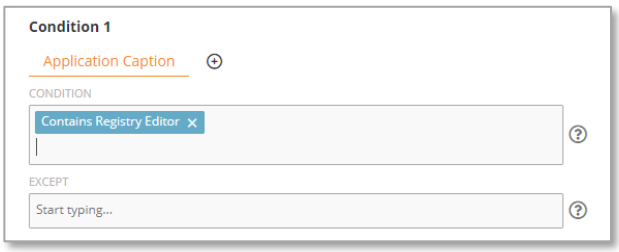


Application Name

Used to detect the name or part of the name of an application. For example: 'regedit.exe'.

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.



Application Caption

Similar to the *Application Name* criterion, just use the application caption instead. For example: 'Registry Editor'.

If the rule fails to detect application captions, ensure that the TRACK WINDOW TITLE option is enabled in the *Monitoring Settings > Applications* window.



Launched from CLI

Detects if an application is launched from the CLI (Command Line Interface).

Select YES or NO.



Running elevated

Detects if an application is launched with elevated permission using Windows User Account Control (UAC).

An app is usually run as elevated when you launch it from the Windows Start menu while holding down the `SHIFT+CTRL` keys. Or, when you run it from the Windows Explorer with the right-click and then select the *Run as administrator* option. An application is also run elevated when it might make changes to the system (e.g., a software being installed for all users instead of just the current user). In such cases, Windows will invoke the UAC and the application will be considered as running elevated.

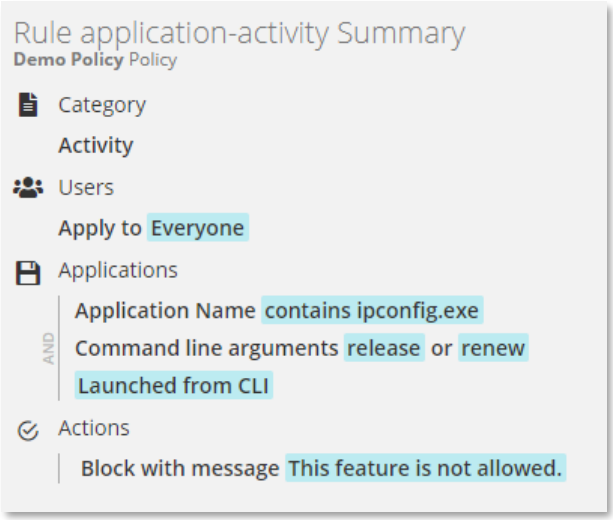
This criterion will help enhance the security of your system as software that usually requires admin permission might make changes to your system. It can also help you mitigate the impact of malware and prevent unauthorized privilege escalation, etc.

Select YES or NO.



Command Line Arguments

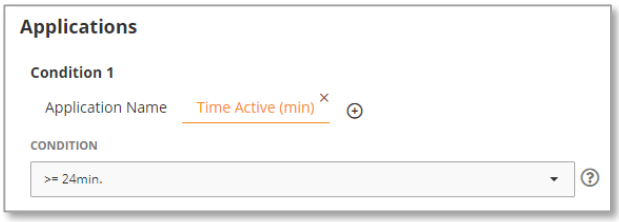
Command line arguments are additional parameters, options or values passed to an application when launching it from the CLI. They usually start with a '/', '-' or a space after the application name. For example: `C:\ipconfig /renew`. Here, *renew* is an argument.



Using this criterion, you can, for example, disable certain functions of an application. For example, in the second screenshot on the left, we blocked the launch of the *ipconfig* application when the *release* or *renew* arguments are used. Otherwise, it will run as usual.

You can only use text value with the 'Contains', 'RegExp' or exact text match conditions for the CONDITION field.

The *Command Line Arguments* criterion is only shown when you have already selected YES for the *Launched from CLI* criterion.

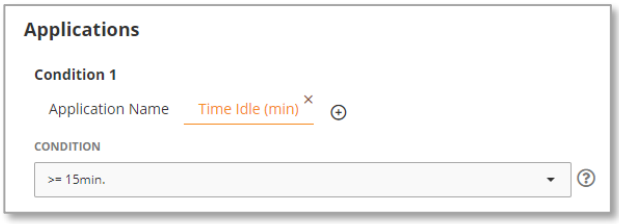


Time Active

Used to detect how long the user has been active on an application.

You can enter a minute value in the CONDITION field and use the '>=' logics.

The *Time Active* criterion is only shown when you have already selected an *Application Name* or an *Application Caption* criterion.



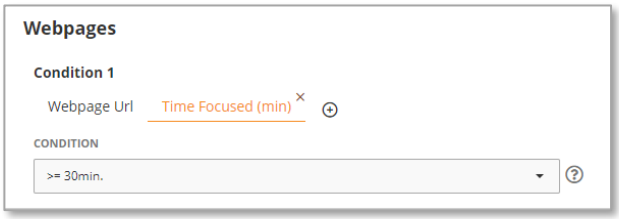
Time Idle

Similar to the *Time Active* criterion but detects how long the user has been idle/inactive on an application.

You can enter a minute value in the CONDITION field and use the '>=' logic.

The *Time Idle* criterion is only shown when you have already selected an *Application Name* or an *Application Caption* criterion.

This criterion works independently of the IDLE TIME THRESHOLD value on the *Monitoring Settings* > *Applications* window.



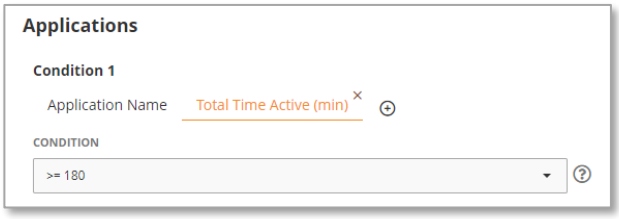
Time Focused

Time Focused = Time Active + Time Idle.

It detects if the user stayed on an application for the specified duration. It doesn't matter whether the user was active (e.g., keyboard/mouse is used) or idle (no keyboard/mouse activity); as long as they stayed on the app without switching to other apps, the condition will be triggered.

You can enter a minute value in the CONDITION field and use the '>=' logic.

The *Time Focused* criterion is only shown when you have already selected an *Application Name* or an *Application Caption* criterion.



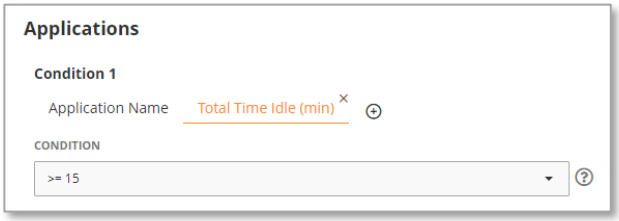
Total Time Active

Similar to the *Time Active* criterion but detects the total time active accumulated throughout the day.

The time will reset at the end of the day. This reset happens when the date of the last total time update differs from the current date. For the reset, the user's local time zone is followed.

You can enter a minute value in the CONDITION field and use the '>=' logics.

The *Total Time Active* criterion is only shown when you have already selected an *Application Name* or an *Application Caption* criterion.



Total Time Idle

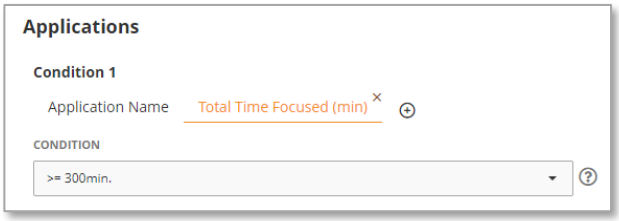
Similar to the *Time Idle* criterion but detects the total time idle accumulated throughout the day.

The time will reset at the end of the day. This reset happens when the date of the last total time update differs from the current date. For the reset, the user's local time zone is followed.

You can enter a minute value in the CONDITION field and use the '>=' logics.

The *Total Time Idle* criterion is only shown when you have already selected an *Application Name* or an *Application Caption* criterion.

This criterion works independently of the IDLE TIME THRESHOLD value on the *Monitoring Settings* > *Applications* window.



Total Time Focused

Similar to the *Time Focused* criterion but detects the total time focused accumulated throughout the day.

The time will reset at the end of the day. This reset happens when the date of the last total time update differs from the current date. For the reset, the user's local time zone is followed.

You can enter a minute value in the CONDITION field and use the '>=' logics.

The *Total Time Focused* criterion is only shown when you have already selected a *Application Name* or an *Application Caption* criterion.



OS Version

Can be used to detect the name or part of the name of the operating system installed on the user's computer. For example: 'Windows 10', 'Windows 11', etc. As an example, you can use this criterion to block certain apps on Windows 10 but not on Windows 11.

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any operating systems you do not want to track in the EXCEPT field.

Notes:

1. This feature is available on request. Please contact your customer service representative to activate this feature on your instance.
2. Minimum Windows Agent 24.35.1996 and Server 24.35.5836 are required to use this feature.

8.3 OCR (Windows & Mac)

The OCR detects on-screen text in real-time, even inside images or videos. It works with multi-screen setups, virtual desktops and terminal servers. By default, OCR detects English text. But you can also use few other languages (check out the Teramind Agent specifications and supported platforms article on our Knowledge Base to learn which languages are supported).

You can change the OCR language from *Monitoring Settings* > *OCR*.

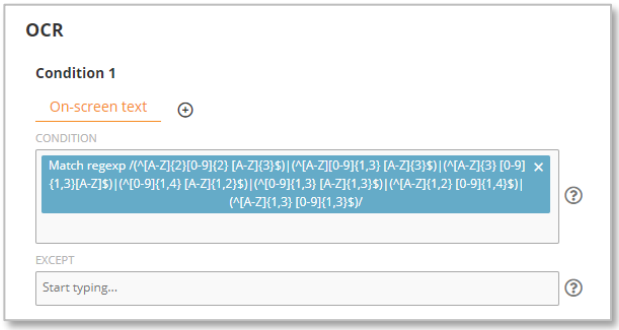
8.3.1 OCR Rule Examples

- Generate an alert when a user sees a full credit card number on the screen violating the PCI DSS compliance requirements.
- Get notified when your employees visit sites that contain illegal or questionable content, such as: hacking, pornographic or piracy related content.

- Detect if an unauthorized user is viewing a document that contains sensitive words.
- Prevent steganographic data exfiltration by detecting information hidden inside images or videos.

8.3.2 OCR Rule Criteria

The table below shows what criteria the OCR supports and what conditions you can use with them.



On-Screen Text

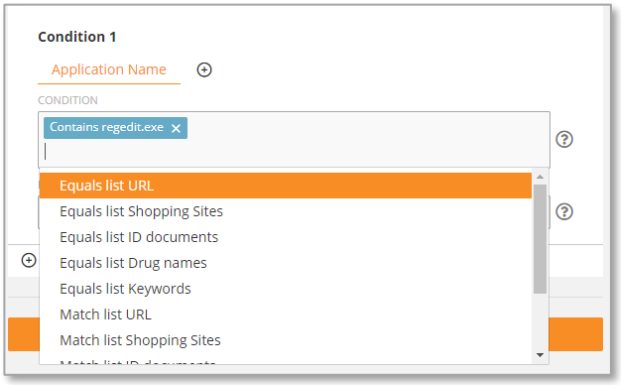
Used to specify the text to detect on-screen.

If you type anything in the field, you can choose from 'Contains', 'Match regexp', 'Match list' as conditions. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' condition without typing any text. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can use the EXCEPT field to do detect any text except for the ones defined in this field.

Be careful while using the EXCEPT field as it will detect all text on the screen except the ones you exclude, triggering the rule every time!

If you are using any regular expressions (e.g., *Match regexp*, *Match list* with a regular expression based shared list) in the *On-Screen Text* field, please remember that Teramind supports the Elasticsearch regular expression syntax for OCR rules. More information can be found about it in Elastic documentation.



Application Name

Used to specify the applications in which the OCR content will be detect.

You can choose from 'Contains', 'Equals' or 'Equals List' with any text as conditions. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Equals List' or 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.

The *Application Name* criterion is only shown when you have already specified an *On-Screen Text* condition.

8.4 Keystrokes (Windows & Mac)

Keystrokes activity is used to detect keystrokes entered by the users in applications or websites. In addition to regular keys, you can also detect the clipboard operations (copy/paste commands), use of special keys such as the Print Screen or multiple simultaneous keypress or combo keys such as CTRL+C.

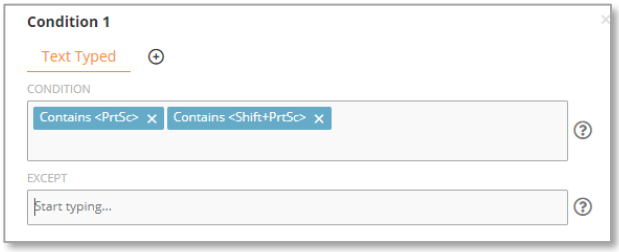
8.4.1 Keystrokes Rule Examples

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

8.4.2 Keystrokes Rule Criteria

The table below shows what criteria the Keystrokes activity supports and what conditions you can use with them.

On Mac, only the *Text Typed*, *Word Typed*, and the *Application Name* criteria are supported.



Text Typed

Used to detect continuous text without any word break. For example, if text typed = "password", the rule will be triggered when the last letter 'd' is typed.

You can enter any text in the CONDITION field and choose the 'Contains' or 'Match RegExp' option. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Equals List' or 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any text you do not want to detect in the EXCEPT field.



Word Typed

Used to detect word typed with breaks. For example, if word typed = "password" the rule will be triggered when you finish typing the word and then type separation key, such as: `<Space>` or '!' or '.' (dot).

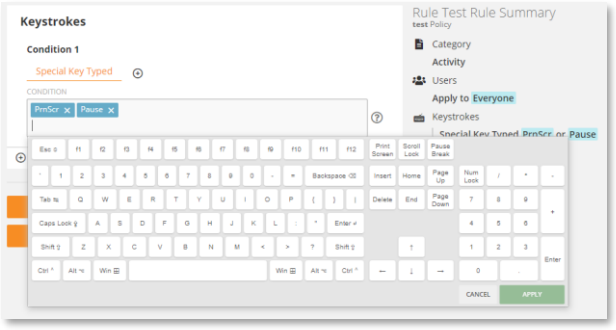
You can enter any text in the CONDITION field and choose the 'Contains', 'Equals' or 'Match RegExp' option. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Equals List' or 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any word you do not want to detect in the EXCEPT field.

Difference Between *Text Typed* and *Word Typed*

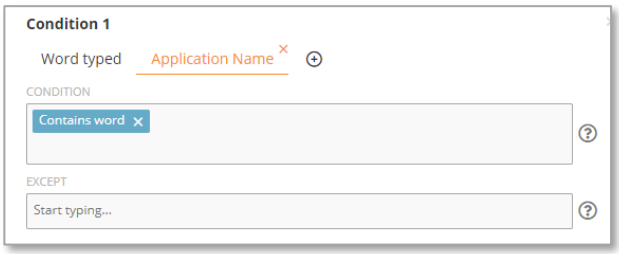
Text Typed will detect any partial text while *Word Typed* will detect only full words. For example, if you are looking to detect `'club'`, and the user typed `'golfclub'`, *Text Type*

will detect it but *Word Typed* will not. If the user typed `'golf club'`, then both the *Text Typed* and *Word Typed* criteria will detect the keystrokes.



Special Key Typed

You can detect special keys such as the function keys (i.e. `F1`), `PrtScr` or key combinations such as `<Shift+P>`. When you select the *Special Key Typed* criteria and click on the CONDITION field, Teramind will pop-up a virtual keyboard where you can select the special keys.



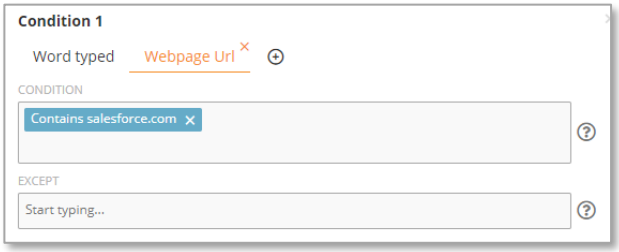
Application Name

Specifies which applications will be tracked.

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.

The *Application Name* criterion is only shown when you have already selected a *Text Typed* or *Word Typed* criterion. Also, if you use this criterion, you cannot use the *Webpage URL* criterion in the same condition block. However, you can use both criteria in separate condition blocks (i.e. *Condition 1* and *Condition 2*).



Webpage URL

Specifies which websites will be tracked. This is same as the *Webpage URL* criterion under the Webpages activity.

The *Webpage URL* criterion is only shown when you have already selected a *Text Typed* or *Word Typed* criterion. Also, if you use this criterion, you cannot use the *Application Name* criterion in the same condition block. However, you can use both criteria in separate condition blocks (i.e., *Condition 1* and *Condition 2*).

8.5 Files (Windows & Mac)

Files activity lets you detect file operations such as access, read, write, upload, download, create folder, rename folder, etc. Each operation allows you to further specify additional detection criteria. For example, the *Download* operation lets you detect the program, file name, URL and file size.

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

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

Note that not all criteria are available for all file operations. Teramind will automatically show or hide the criteria based on which file operation you select. For example, if you select the *Insert* or the *Eject* operation, you will only see the *Program* and *Drive* criterion. Or, when you select the *Copy* or *Move* operation, you will see options to specify the source (e.g., *Source file path*, *Source network host*, *Source drive*, etc.).



Select a file operation by clicking the CONDITION filed.

Click the ⊕ button to add a criterion to the operation.

If you choose the 'Any' file operation without any other criteria, Teramind will trigger the rule for any file operations.

8.5.1 Files Rule Examples

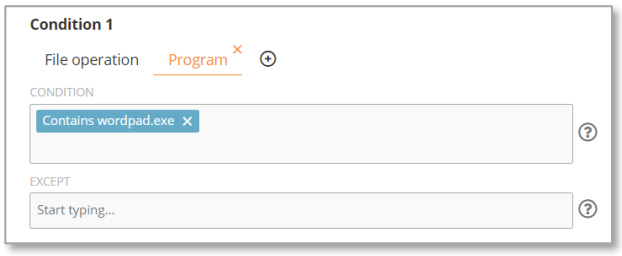
- Detect/block access to sensitive folders.
- Turn a folder or drive write proof, preventing any changes to the files in that folder.
- Get notified when files are uploaded to Cloud sharing sites, such as, Drobox, Google Drive etc.
- Block files from being copied to/from removable media, such as, USB drives.
- Prevent changes of program settings or tampering of configuration files.
- Block certain file transfer protocols, such as, FTP.
- Restrict the transfer of large files.

8.5.2 Files Rule Criteria

On Mac, only the following criteria and conditions are supported:

- **File Operation** conditions: *Access*, *Copy*, *Write*, *Rename*, and *Delete*). *Upload* condition is only supported for Google Drive web uploads. You can use relevant criteria such as *Upload URL*, *Upload File Name*, with that condition.
- **Program** conditions: *Contains* and *Equals*.
- **File Path** conditions: *Contains* and *Equals*.
- **Drive** conditions: *All drives* and *All external drives*.

The table below describes the criteria you can use for the Files activity, and which file operations are supported for each criterion.

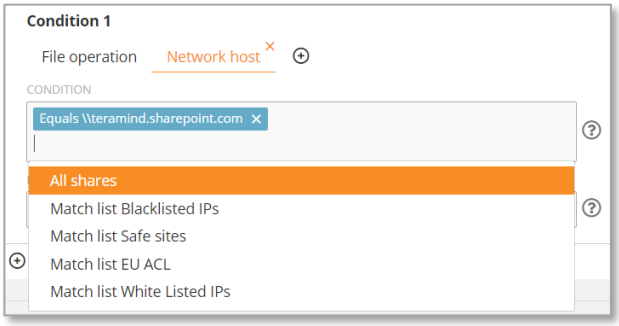


Program

Lets you specify in which program/app the file operation took place.

You can choose from 'Contains', 'Equals' or 'Match RegExp'.

Similarly, you can exclude any programs you do not want to track in the EXCEPT field.



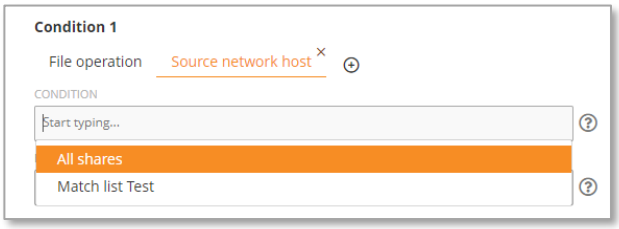
Network Host

Used for network-based file operations. It detects the host name of the file operation. For example: `http://sharepoint.com`, `ftp://filevault.net` etc.

You can choose from 'Contains', 'Equals', 'All Shares'. Or, you can select a Shared List (Network-based) and specify a 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any hosts you do not want to track in the EXCEPT field.

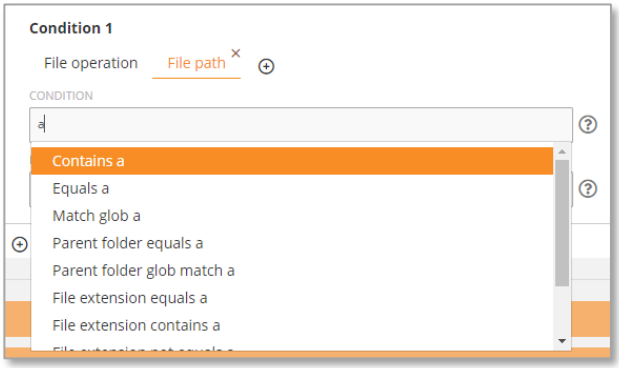
This criterion is not supported in: Insert, Eject, Download and Upload operations.



Source Network Host

Similar to the *Network Host* criteria but detects the source network host of a *Copy* or *Move* operation.

This criterion is only available with the Any, Copy, Move and Rename operations.



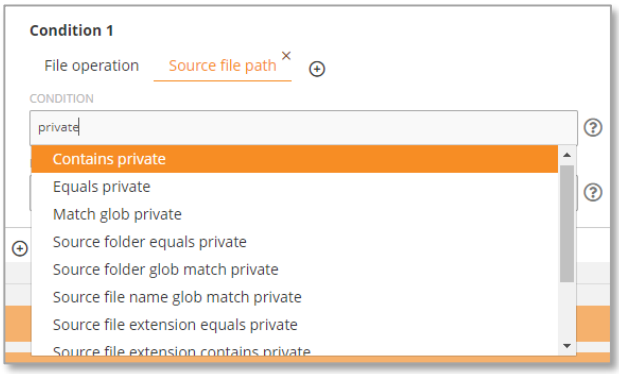
File Path

Used to detect a parent folder or file extensions. For example: `document`, `c:\windows` etc. File extension are used to identify a file type and usually starts with a '. (dot)'. For example: *.doc*, *.pdf* etc. Note: you do not need to specify the '.' when entering the extension.

You can choose from various 'Contains', 'Equals', 'Match' conditions. When using one of the 'match' options, you can use a wildcard such as `*`, `?`, `[abc]`, `[a-z]`, etc. For example, `?at` will match `Cat`, `cat`, `Bat` or `bat`.

You can exclude any path(s) you do not want to track in the EXCEPT field.

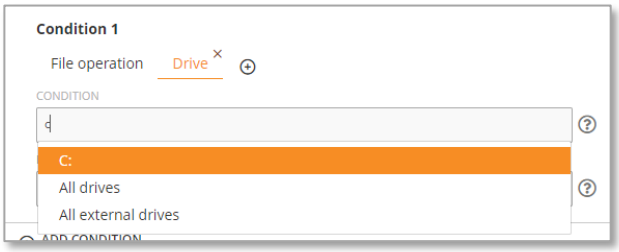
This criterion is not supported in: Insert, Eject, Download and Upload operations.



Source File Path

Similar to the *File Path* criteria but detects the source folder, file name or extension of a *Copy* or *Move* operation.

This criterion is only available with the Any, Copy, Move and Rename operations.

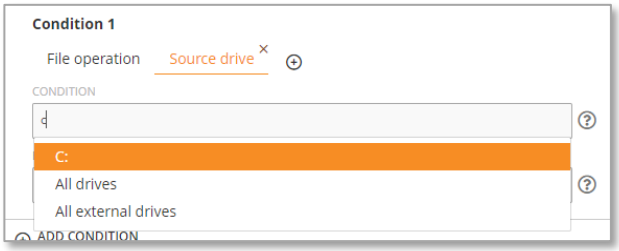


Drive

Detects the local, network or external drives.

You can enter a drive name (e.g., ‘c’) and select that particular drive or choose from ‘All Drives’ or ‘All External Drives’ conditions.

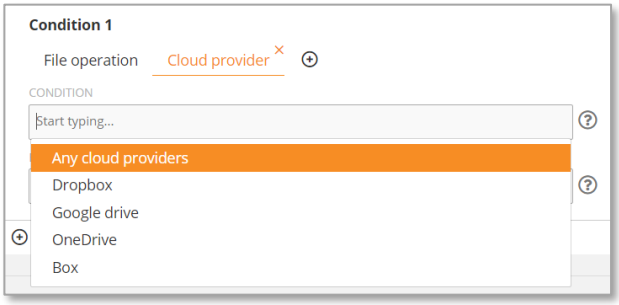
This criterion is not supported in: Download and Upload operations.



Source Drive

Similar to the *Drive* criteria but detects the source drive of a *Copy* or *Move* operation.

This criterion is only available with the Any, Copy, Move and Rename operations.



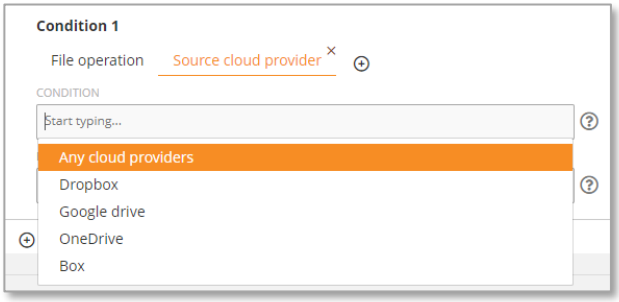
Cloud Provider

Used to detect the cloud provider.

You can choose from 'All Cloud Providers', 'Dropbox', 'Google Drive', 'OneDrive' or 'Box', etc.

Similarly, you can exclude any providers you do not want to track in the EXCEPT field.

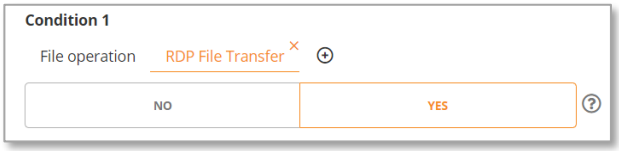
This criterion is not supported in: Insert, Eject, Download and Upload operations.



Source Cloud Provider

Similar to the *Cloud Provider* criteria but detects the source cloud provider of a *Copy* or *Move* operation.

This criterion is only available with the Any, Copy, Move and Rename operations.

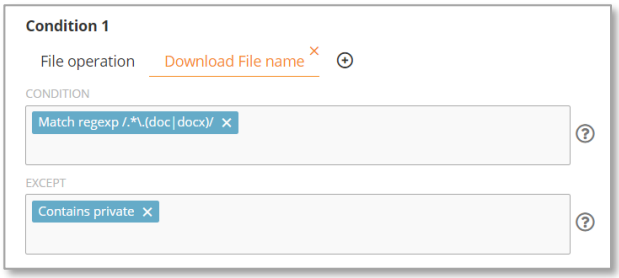


RDP File Transfer

Detects if the file copy operation is done over an RDP (Remote Desktop Protocol) session. This happens when you connect to a remote computer and copy files to/from it.

You can select either YES or NO.

This criterion is only supported in the Copy operation.



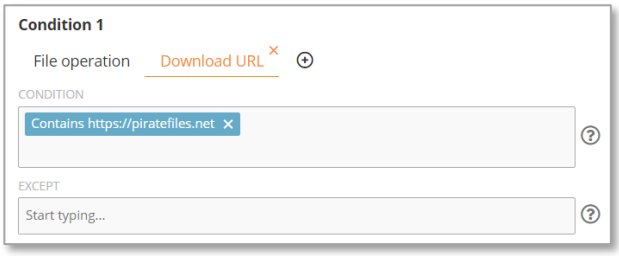
Download File Name

Lets you detect the download file name.

You can choose from 'Contains', 'Equals' or 'Match RegExp'.

Similarly, you can exclude any files you do not want to track in the EXCEPT field.

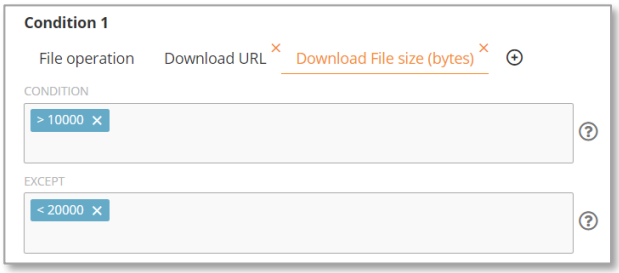
This criterion is only supported in the Download operation.



Download URL

Similar to the *Download File Name* criterion but used to detect the download URL instead.

This criterion is only supported in the Download operation.



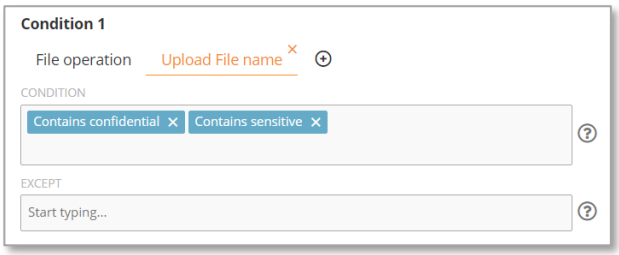
Download File Size

Used to detect the size (in bytes) of the file being downloaded.

You can enter a byte value in the CONDITION field and use '=', '>', '<', '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception.

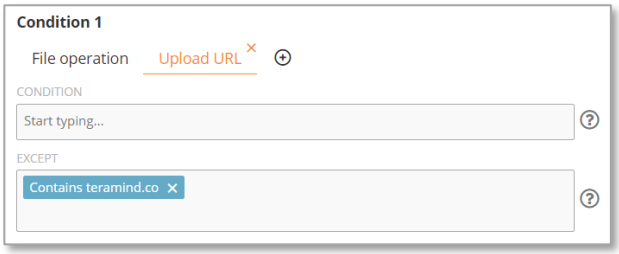
This criterion is only supported in the Download operation.



Upload File Name

Similar to the *Download File Name* criterion but used for Upload operation instead.

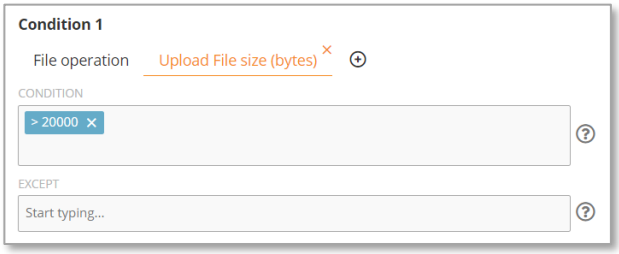
This criterion is only supported in the Upload operation.



Upload URL

Similar to the *Download URL* criterion but used for the Upload operation instead.

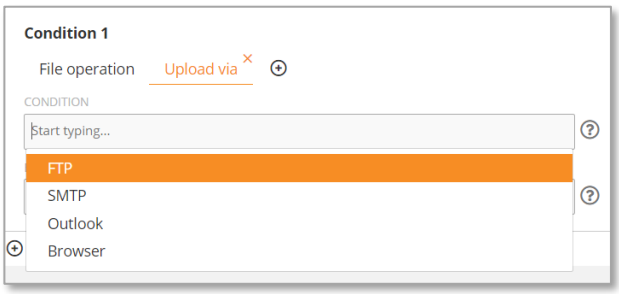
This criterion is only supported in the Upload operation.



Upload File Size

Similar to the *Download File Size* criterion but used for the Upload operation instead.

This criterion is only supported in the Upload operation.



Upload Via

Lets you detect what kind of application or protocol is used for the upload operation.

You can choose from 'FTP', 'SMTP', 'Outlook' or 'Browser'.

Similarly, you can use the EXCEPT field to ignore any protocol/application you do not want to track.

This criterion is only supported in the Upload operation.

8.6 Emails (Windows & Mac)

Emails activity lets you detect outgoing and incoming emails including any email attachments.

On Mac:

- **Criteria Supported:** *Mail Body, Mail Subject, Mail CC, Mail To, Mail From, Mail Direction, Mail Client, Has Attachments, Mail size.*
- **Mail Clients Supported:** *Gmail (web) and Outlook (web).*

8.6.1 Emails Rule Examples

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

8.6.2 Emails Rule Criteria

The table below shows what criteria the Email activity supports and what conditions you can use with them.



Any

Lets you detect if an email is sent or received.

If you use this option without any other criteria, Teramind will trigger the rule anytime an email is sent or received.

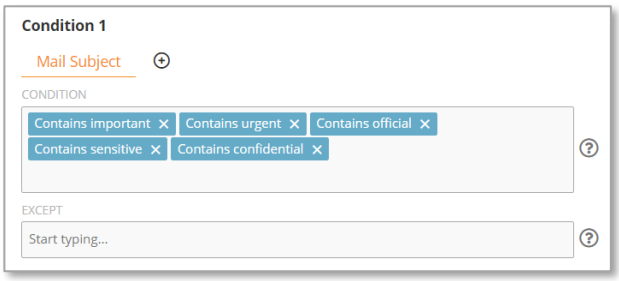


Mail Body

Used for detecting text inside the mail body.

You can choose from 'Contains' or 'RegExp' with any text. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.

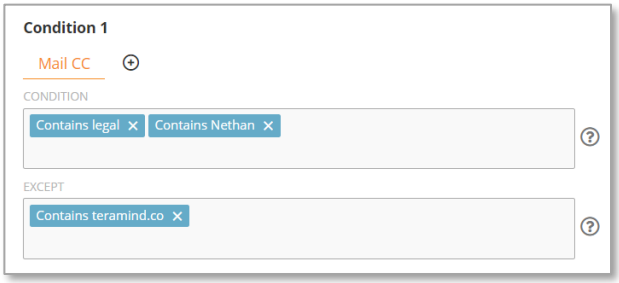


Mail Subject

Used for detecting text inside the mail subject.

You can choose from 'Contains', 'Equals' or 'RegExp' with any text. Or, you can select a Shared List and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.



Mail CC

Detects the CC addresses in an email.

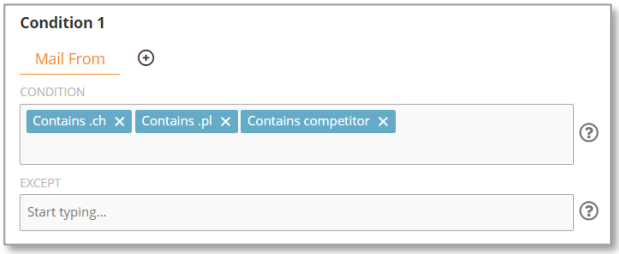
You can choose from 'Contains', 'Equals' or 'RegExp' with any text. Or, you can select a Shared List and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.



Mail To

Similar to *Mail CC* criterion but used to detect the *Mail To* addresses instead.



Mail From

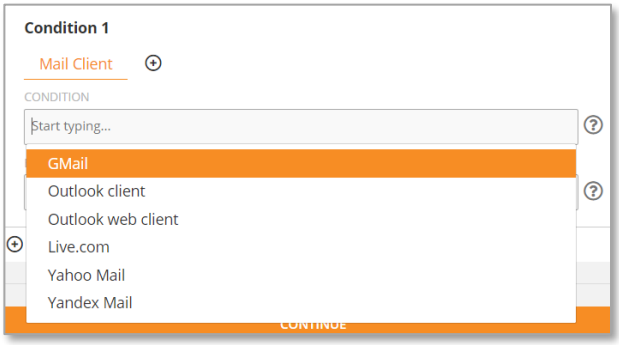
Similar to *Mail CC* and *Mail To* criterion but used to detect the *Mail From* addresses instead.



Mail Direction

Lets you detect if the mail is being sent or received.

Select either the INCOMING or OUTGOING option.



Mail Client

Used to specify the mail client you want to detect.

You can choose from 'Gmail', 'Outlook Client', 'Outlook Web Client', 'Live.com', 'Yahoo Mail', and 'Yandex Mail'. Teramind keeps adding support for new clients so you might see more clients than mentioned here.

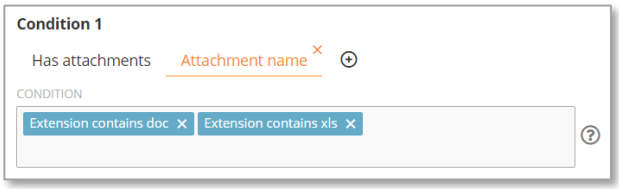
Similarly, you can exclude any client(s) you do not want to track in the EXCEPT field.



Has Attachments

Used to detect if the mail has any attachment.

Select either the YES or NO option.



Attachment Name

Used to detect the names or extensions for the attached files. A file extension is used to identify a file type and usually starts with a '. (dot)'. For example: *.doc, .pdf* etc. Note: you do not need to specify the '.' when entering the extension.

You can choose from 'Contains', 'Equals' or 'RegExp' with any text. Or, you can check for file extensions using one of the 'Extension Contains', 'Extension Equals', 'Extension Does Not Contain' options.

The *Attachment Name* criterion is only shown when you have already selected YES for the *Has Attachment* criterion.



Mail Size

Used to detect the size (in bytes) of the mail.

You can enter a byte value in the CONDITION field and use the '=', '>', '<', '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception.

8.7 IM – Instant Messaging (Windows)

IM activity lets you detect instant messaging conversations and group chats for popular IMs such as: Skype, Slack etc. You can detect both incoming and outgoing messages, detect the participants and search the message body for keywords or text.

8.7.1 IM Rule Examples

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

8.7.2 IM Rule Criteria

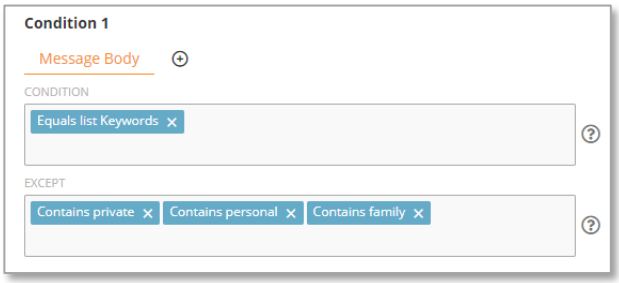
The table below shows what criteria the IM activity supports and what conditions you can use with them.



Any

Lets you detect if an IM is sent or received.

If you use this option without any other criteria, Teramind will trigger the rule anytime an IM is sent or received.



Message Body

Used for detecting text inside the message body.

You can choose from 'Contains' or 'RegExp' with any text. Or, you can select a Shared List (Text-based or Regular Expressions-based) and

specify a ‘Match List’ or ‘Equals List’ condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

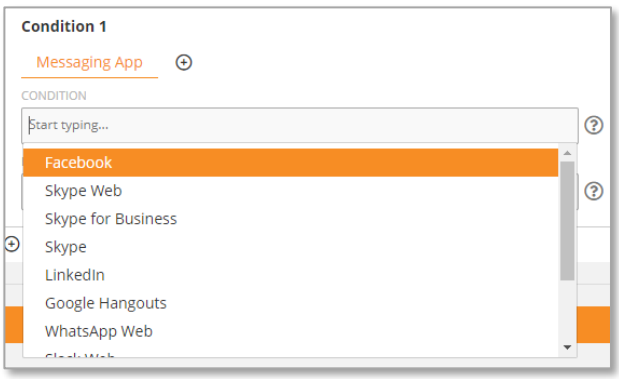
Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.



Message Direction

Lets you detect if the message is being sent or received.

Select either the INCOMING or OUTGOING option.



Messaging App

Used to specify the messaging app you want to detect.

You can choose from ‘Facebook, ‘Skype Web’, ‘Skype for Business’, ‘LinkedIn’, ‘Google Hangouts’, ‘WhatsApp Web’, ‘Slack Web’, ‘Slack’, ‘Microsoft Team Web’ and ‘Microsoft Team’. Teramind keeps adding support for new apps so you might see more clients than mentioned here.

Similarly, you can exclude any app(s) you do not want to track in the EXCEPT field.



Contact Name

Used to detect the contacts/participants of the IM conversation.

You can choose from ‘Contains’, ‘Equals’ or ‘RegExp’ with any text as conditions.

Similarly, you can exclude any contacts you do not want to track in the EXCEPT field.

8.8 Browser Plugins (Windows)

Browser Plugins activity lets you detect any installed browser, plugins or extensions, what they are doing or what data they are accessing.

8.8.1 Browser Plugins Rule Examples

- Restrict the use of a browser such as an older version of a browser that has security flaws.
- Block user installation browser plugins and extensions by regular users to prevent malware infection and prevent security or privacy breaches.
- Prevent a plugin from utilizing certain permissions such as the ability to access critical proxy settings or user data.

8.8.2 Browser Plugins Rule Criteria

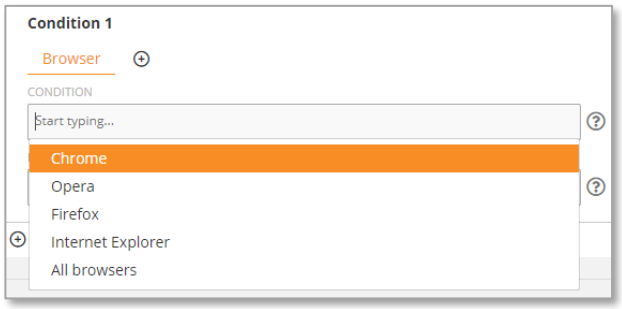
The table below shows what criteria the Browser Plugins activity supports and what conditions you can use with them.



Any

Lets you detect if a browser is launched/activated.

If you use this option without any other criteria, Teramind will trigger the rule anytime a plugin is launched or activated.

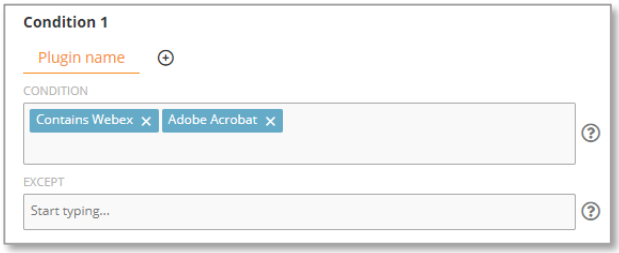


Browser

Used to specify the browser you want to detect.

You can choose from ‘Chrome’, ‘Opera’, ‘Firefox’, ‘Internet Explorer’ or ‘All Browsers’. Teramind keeps adding support for new browsers so you might see more clients than mentioned here.

Similarly, you can exclude any client(s) you do not want to track in the EXCEPT field.

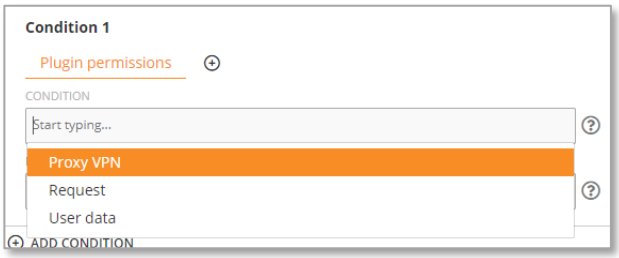


Plugin Name

Used to specify the plugin you want to detect.

You can choose from 'Contains', 'RegExp' or exact match with any text as conditions.

Similarly, you can exclude any plugins you do not want to track in the EXCEPT field.



Plugin Permissions

You can detect what permissions the plugin is using.

You can choose any of these conditions:

- **Proxy VPN** - detects if the plugin is accessing the browser's proxy settings.
- **Request** - detects if the plugin is making a web request. This permission allows a plugin to observe and analyze traffic and intercept, block, or modify web requests.
- **User Data** - detects if the plugin is accessing any user data such as cookies.

Similarly, you can exclude any permission you do not want to track in the EXCEPT field.

8.9 Printing (Windows & Mac)

The Printing activity lets you detect print jobs across local or network printers. You can use criteria, such as: the document and printer and number of pages being printed.

8.9.1 Printing Rule Examples

- Prevent data leaks over hardcopies by restricting what documents can be printed.
- Warn the user about large print jobs to reduce waste.
- Restrict how many pages can be printed in a certain printer to reduce expense when taking an expensive/color print.
- Implement printer use policies by users/departments. For example, which departments/users can use which printer, how much or what they can print.

8.9.2 Printing Rule Criteria

The table below shows what criteria the Printing activity supports and what conditions you can use with them.

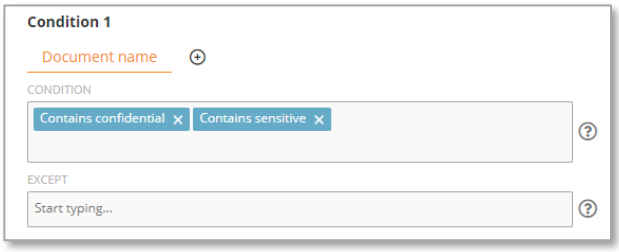
On Mac, only the following criteria are supported: *Number of Pages*, *Document Name*, and *Printer Name*.



Any

Lets you detect if any print job is sent to the printer.

If you use this option without any other criteria, Teramind will trigger the rule anytime a print job is sent to the printer.

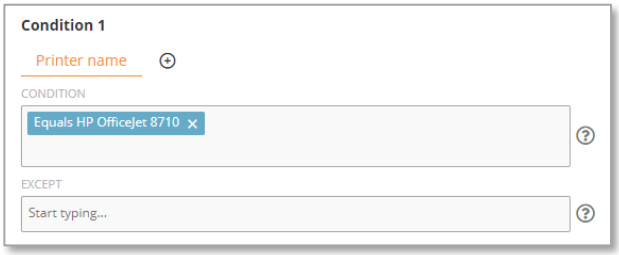


Document Name

Used to specify the document names you want to detect.

You can choose from ‘Contains’, ‘Equals’ or ‘RegExp’ with any text as conditions.

Similarly, you can exclude any plugins you do not want to track in the EXCEPT field.



Printer Name

Used to specify the printers you want to track.

You can choose from ‘Contains’, ‘Equals’ or ‘RegExp’ with any text as conditions.

Similarly, you can exclude any plugins you do not want to track in the EXCEPT field.



Number of Pages

Used to detect the number of pages of the document being printed.

You can enter a page value in the CONDITION field and use the ‘=’, ‘>’, ‘<’, ‘>=’ logics.

Similarly, you can use the EXCEPT field to specify an exception.

8.10 Networking (Windows & Mac)

The Networking activity lets you detect print jobs across local or network printers. You can use criteria, such as: the document and printer and number of pages being printed.

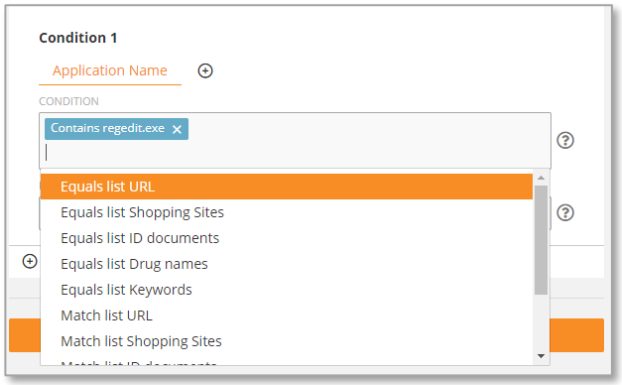
8.10.1 Networking Rule Examples

- Implement network security related rules, for example, restrict outgoing internet traffic from the payment server (to comply with PCI DSS regulation).
- Limit network access such as, disable login via RDP (Remote Desktop Protocol).
- Implement geo-fencing, for example, restrict access to your EU server from the US users.
- Get notified when abnormal network activity (i.e. sudden spike in network traffic) is detected which might indicate an intrusion.
- Using the Local IP criterion, you can detect if a user has established a connection to a peripheral local or VPN network or has changed the network route to bypass your corporate VPN. This might indicate a serious security threat.

8.10.2 Networking Rule Criteria

The table below explains what criteria the Networking activity supports and what conditions you can use with them.

> On Mac, only the following criteria are supported: *Application Name*, *Remote Host*, *Remote Port*, *Bytes Sent* and *Bytes Received*.

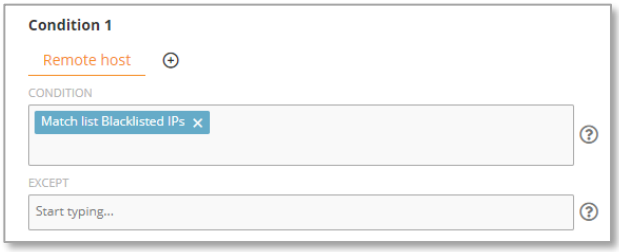


Application Name

Used to specify the app you want to detect sending/receiving the network connection.

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.



Remote Host

Used to specify the network the remote host is connected to.

You can enter a host address (such as: `google.com`) or an IP address (such as: `10.52.22.1/32`) in the CONDITION field or you can select a Shared List (Network-based) and specify a 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any host you do not want to track in the EXCEPT field.



Remote Port

Used to detect the port of the network connection.

You can enter a port value in the CONDITION field and use the '=' logic.

Similarly, you can use the EXCEPT field to specify an exception.



Bytes Sent

Used to specify the number of bytes sent over the network connection.

You can enter a byte value in the CONDITION field and use the '=', '>' or the '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception.



Bytes Received

Used to specify the number of bytes received over the network connection.

You can enter a byte value in the CONDITION field and use the '=', '>' or the '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception.



Local IP

Used to detect local IP addresses.

You can enter an IP address (such as: `11.1.1.2/32`) in the CONDITION field or you can select a Shared List (Network-based) and specify a 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

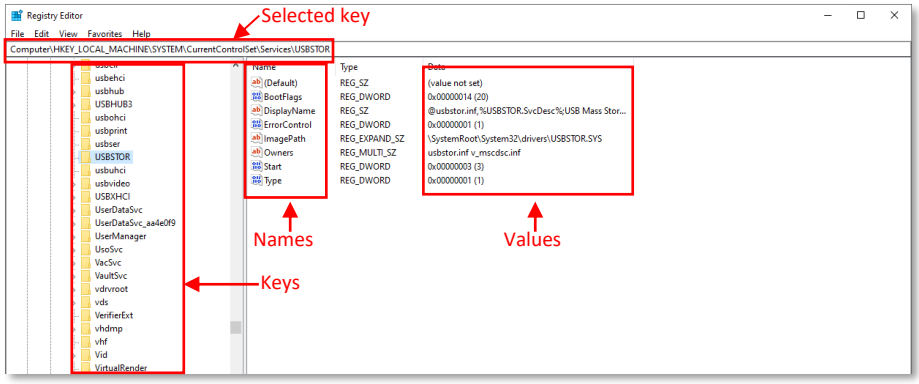
Similarly, you can exclude any IP you do not want to track in the EXCEPT field.

This criterion detects local IP addresses in a network connection and adds another layer of security to subnets and enables you to detect and enforce policies pertaining to local and external VPN connections. For example:

- If your company uses a work VPN connection - it will mean that the user has connected to an extraneous local or VPN network or has changed the network route to work not through a working VPN.
- If your company doesn't use a work VPN connection - it will mean that the user has connected to an extraneous local or VPN network from a working computer.

8.11 Registry (Windows)

The Registry-based activity rules let you detect changes to the registry. You can detect registry key, name, value/data and program.



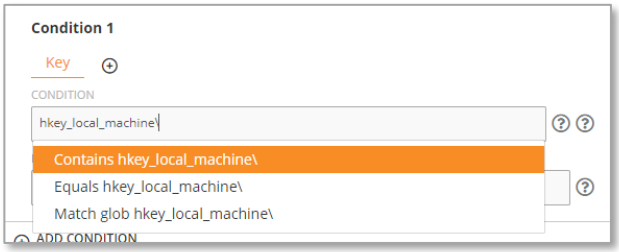
Windows Registry Editor

8.11.1 Registry Rule Examples

- Prevent changes to sensitive keys/programs or other items in the registry. For example, network or internet settings, security policies, etc.
- Detect/prevent unauthorized changes of permissions or privileges of files, folders, drives or applications. For example, a malicious user or intruder can change the USBSTOR values to enable the use of external drives compromising security. By monitoring the registry key, you can prevent such changes.
- Detect if a user is trying to install a dangerous or problematic software by monitoring what changes the software is making to the system.

8.11.2 Registry Rule Criteria

The table below explains what criteria the Registry activity supports and what conditions you can use with them.



Key

You can enter any text in the CONDITION field and choose from 'Contains' or 'Equals' conditions. Or, you can select the 'Match glob' condition and use wildcards such as `*`, `?`, `[abc]`, `[a-z]`, etc. For example, `?at` will match `Cat`, `cat`, `Bat` or `bat`.

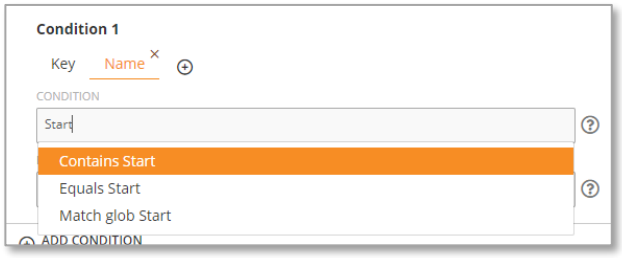
Similarly, you can exclude any key you do not want to track in the EXCEPT field.

Note that actual registry keys differ from what it looks like in the Windows Registry Editor.

For example, "`\registry\machine`" key is represented as "`Computer\HKEY_LOCAL_MACHINE`" on the Registry Editor. Or, the "`\registry\users`" represented as "`Computer\HKEY_USERS`".

Teramind will use the actual keys to match the conditions instead of what's shown on the Windows Registry. For convenience if string condition for the key starts with one of the following, it will be recoded for the actual search accordingly:

- `hkey_current_user\`
- `hkcu\`
- `hkey_local_machine\`
- `hklm\`
- `hkey_users\`

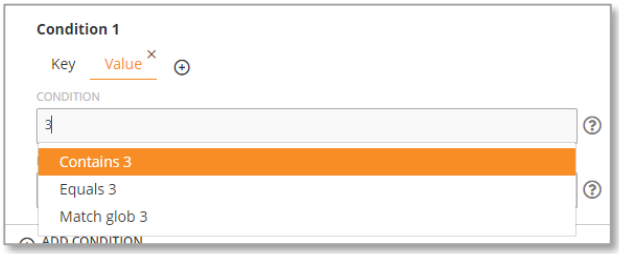


Name

Used to specify the name of a registry value. For example, the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR` key may contain a value called "Start".

You can enter any text in the CONDITION field and choose from 'Contains' or 'Equals' conditions. Or, you can select the 'Match glob' condition and use wildcards such as `*`, `?`, `[abc]`, `[a-z]`, etc. For example, `?at` will match `Cat`, `cat`, `Bat` or `bat`.

Similarly, you can exclude any name you do not want to track in the EXCEPT field.

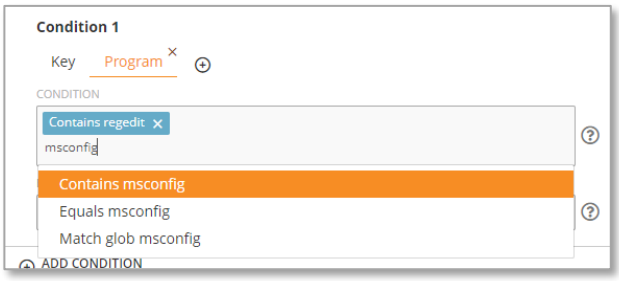


Value

Used to detect the value of a registry name. Windows registry value can contain a String, Multi-String, Binary, etc. So, enter a value accordingly.

You can enter any text in the CONDITION field and choose from 'Contains' or 'Equals' conditions. Or, you can select the 'Match glob' condition and use wildcards such as `*`, `?`, `[abc]`, `[a-z]`, etc. For example, `?at` will match `Cat`, `cat`, `Bat` or `bat`.

Similarly, you can exclude any name you do not want to track in the EXCEPT field.



Program

Can help identify which application or service is responsible for making the registry changes.

You can enter any text in the CONDITION field and choose from 'Contains' or 'Equals' conditions. Or, you can select the 'Match glob' condition and use wildcards such as `*`, `?`, `[abc]`, `[a-z]`, etc. For example, `?at` will match `Cat`, `cat`, `Bat` or `bat`.

Similarly, you can exclude any name you do not want to track in the EXCEPT field.

8.12 Camera Usage (Windows)

The Camera Usage-based activity rule lets you detect when a camera/webcam is used. You can detect the camera name and the application in which the camera is being used.

8.12.1 Camera Usage Rule Examples

- Implement privacy-friendly Webcam recording feature without actually interfering with an employee's camera. For example, create a Camera Usage rule with the RECORD VIDEO action to automatically start recording the screen when camera use is detected so that you can, for example, record meeting sessions.
- Allow webcam usage only in your company's approved apps such as Webex and lock out the user when other apps try to use the camera to reduce security and privacy risks.

- Respect user privacy by only recording a specific camera. For example, record screen sessions of remote users by tracking the camera supplied by the company and not record when the user is using their personal/built-in webcam.

8.12.2 Camera Usage Rule Criteria

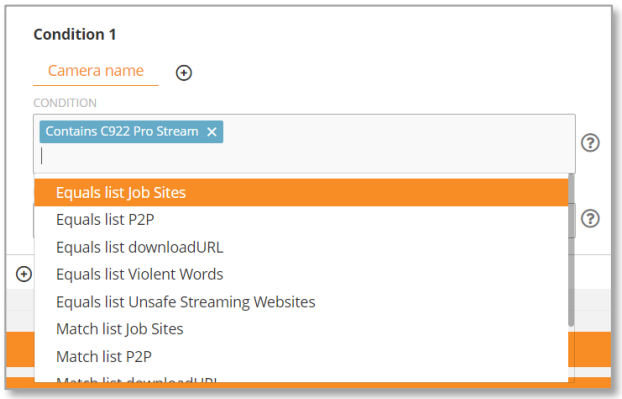
The table below explains what criteria the Camera Usage activity supports and what conditions you can use with them.

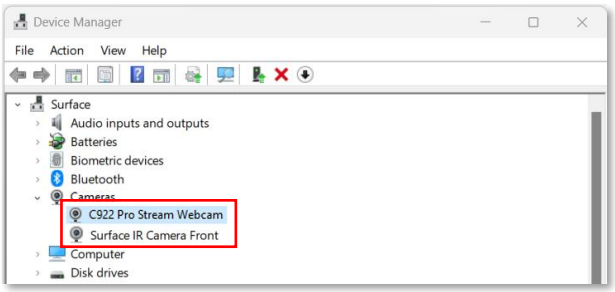


Any

Lets you detect if any camera is turned on in any application.

If you use this option without any other criteria, Teramind will trigger the rule for any camera in any application.



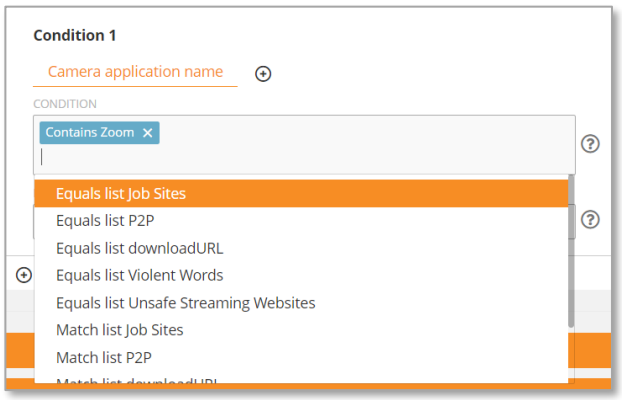


Camera Name

Used to specify the camera you want to detect. Note: you can find the name of all the available cameras (built-in or external) on the Windows Device Manager, under *Cameras*.

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any camera you do not want to track in the EXCEPT field.



Camera Application Name

Used to specify the application using the camera.
You can enter any text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.

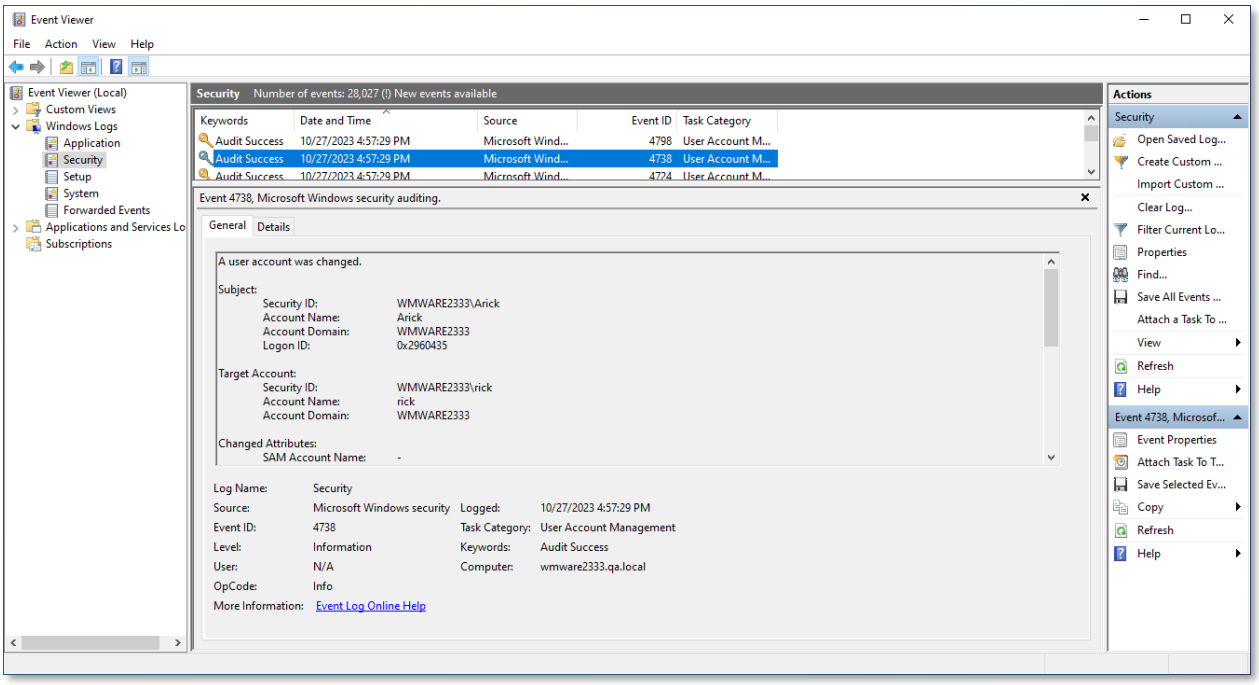
8.13 Windows Log Event (Windows)

This is a preview feature and might not always produce the expected results. We do not recommend using it for any critical operations.

We also do not recommend using this rule on a shared machine such as a Citrix/RDP server. There are often multiple users - all contributing to a much bigger event log. This might cause performance issues.

If you have any feedback or bug reports about this feature, please send them to support@teramind.co.

Windows events are all the activities tracked by the OS. These include Applications, System, Security, Hardware, etc. You can see these events on the Windows *Event Viewer*:



The ability to detect these events is a very powerful tool, because it allows an administrator to identify issues with the computer, discover security gaps and stop potential threats.

The Windows Log Event rule allows you to detect these Windows events.

8.13.1 Windows Log Event Rule Examples

- Detect if a user or an app has cleared the audit log (e.g., event ID 1102) that's often used by attackers to cover their footprint.
- Identify failed attempts to login (event ID 4625) by potential hackers.
- Detect unplanned hash access (event ID 4798) that might indicate malicious activity.
- Monitor if scheduled tasks were created (4698) because malwares often create automated tasks to provide persistent access to a compromised system.
- Diagnose errors, system failures, performance issues and other problems.

8.13.2 Windows Log Event Rule Criteria

The Windows Log Event activity comes with only one criterion:



Event ID

Lets you specify one or more Windows event IDs.

You can enter numeric values in the CONDITION field and use the '=', '>', the '>=', '<' logics.

Similarly, you can use the EXCEPT field to specify an exception.

9 Content Sharing Rules: What Contents Trigger the Rules (Windows)?

Content Sharing rules are used to detect content or text inside an object. The object can be a file, an email or IM chat, data in the clipboard or even any text displayed on the screen. You can use these powerful rules 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.

You can specify the detection criteria for the Content Sharing rules in two places:

- On the special *Content* Tab: This tab allows you to define what makes the content sensitive and specify the data values to look for. This tab is automatically added when you select the *Content Sharing* rule type (in the **General** tab).
- On the selected *Content Type* Tabs: For example, if you selected Clipboard and Emails from the *Type of Content* section (in the **General** tab), you will have two tabs called 'Clipboard' and 'Emails' where you can add the rule conditions and values.

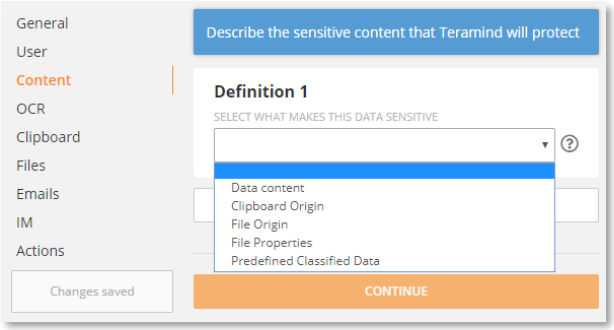
The basic premise of the Content Sharing rule is: you describe the data in the *Content* tab and then you tell Teramind where to look for that data in the *Content Type* Tabs. You need to use both of them for creating a Content Sharing rule.

Teramind Agent will allow a maximum of 1 second to scan a file for content. If it cannot scan the file within that time (e.g., file too large, slow disk, etc.), it will discard that file. This may prevent content from being detected for larger files.

Note that Content-Sharing rules doesn't support the xls and doc files. However, xlsx and docx files are supported.

9.1 The Content Tab

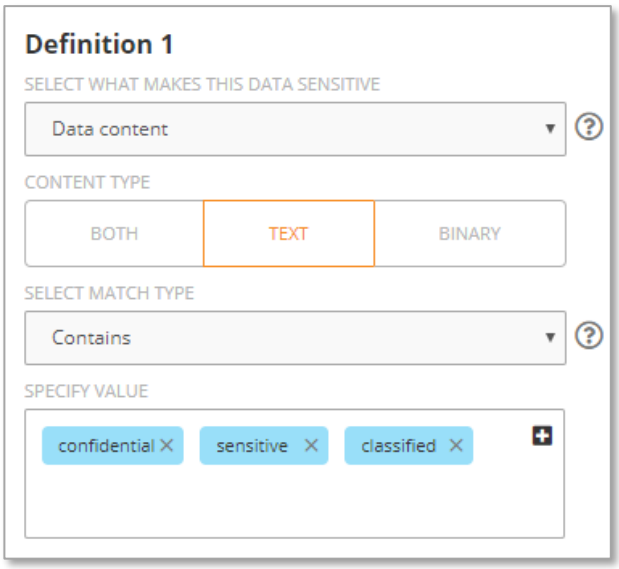
This tab allows you to define what makes the content sensitive and specify the values to look for. You need to select at least one *Types of Content,* such as: Clipboard, File etc. to be able to use the Content tab.

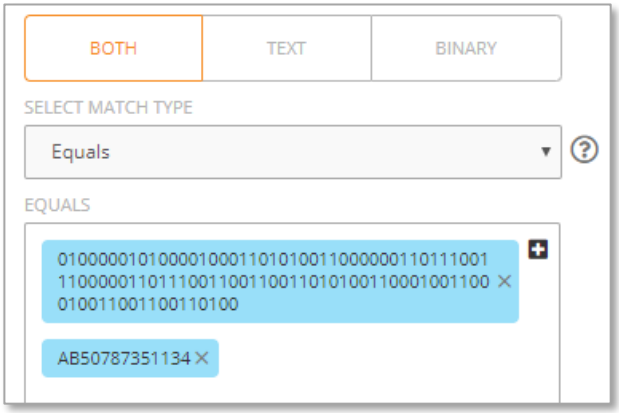


You can select from different data definitions depending on what *Types of Content* you have selected in the **General** tab (i.e. Clipboard, Files, Emails, IM).

For example, if you have selected the Clipboard content type, then you will see the 'Clipboard Origin' in the data definition list.

The table below shows what criteria the Content definition supports and what conditions you can use with them.





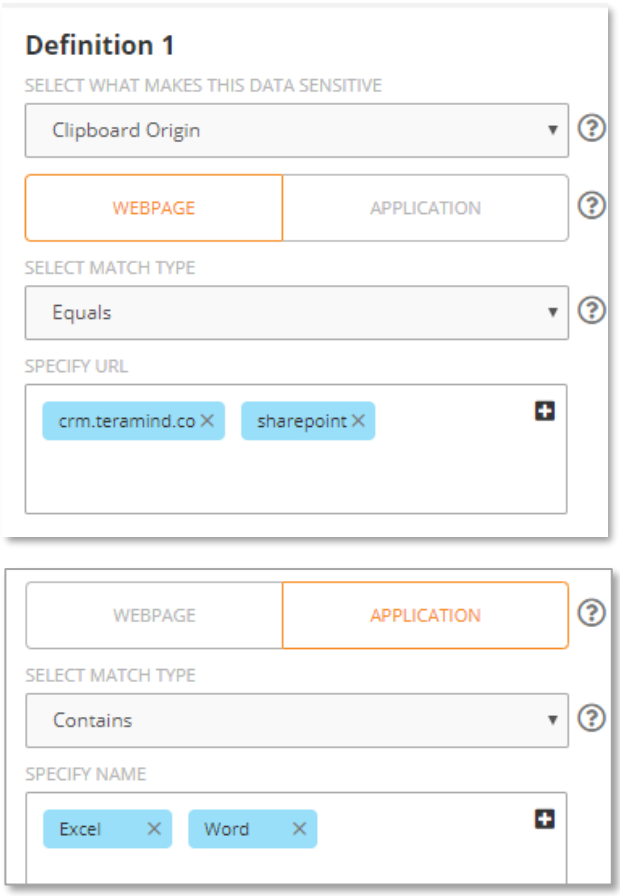
Data Content

Data Content is a generic criterion that can be used to look for any text or binary data. For example, by using it with the Clipboard, you can detect anything copied on the clipboard.

You can select TEXT, BINARY or BOTH as the CONTENT TYPE.

For SELECT MATCH TYPE, you can choose 'Contains', 'Equals' or 'RegExp' and specify the text or binary values in the bottom field. Use the ⊞ button to add multiple values. Or, you can choose 'Match List Member' or 'Equals List Member' as a match type and then select a Shared List (Text-based or Regular Expressions-based) from the SELECT SHARED LIST drop-down menu. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

The *Data Content* criterion can be used with any content types (i.e. Files, Email etc.).



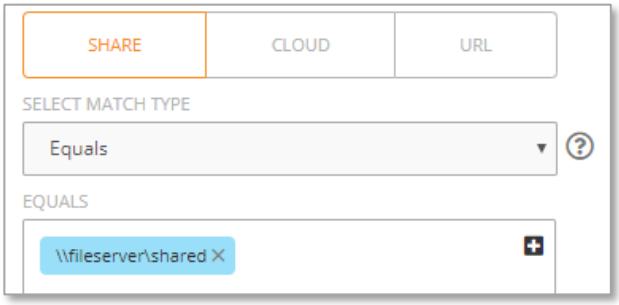
Clipboard Origin

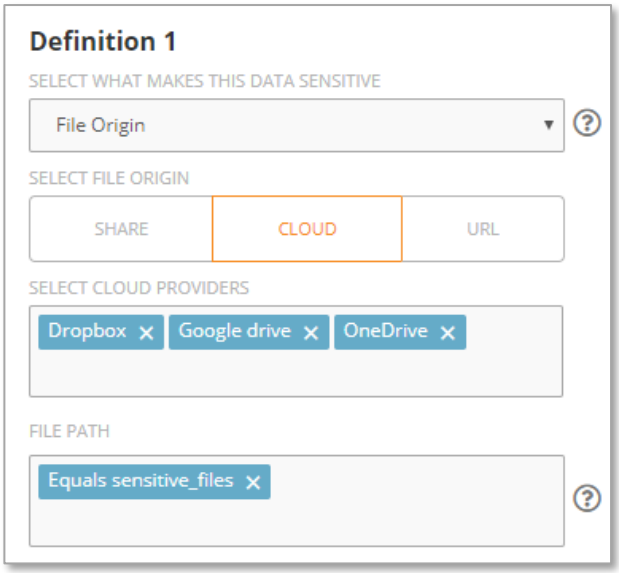
Clipboard Origin detects data pasted into the clipboard from a specific webpage or application. By using it you can, for example, build a rule that prevents copy pasting of customer data from your CRM site.

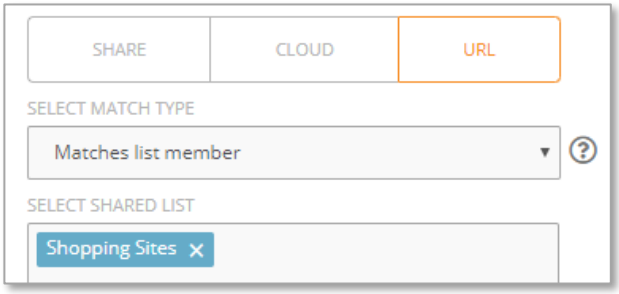
You can select WEBPAGE or APPLICATION as the source of the clipboard copy operation.

For SELECT MATCH TYPE, you can choose 'Contains', 'Equals' or 'RegExp' and specify the text values in the bottom field. Use the ⊞ button to add multiple values. Or, you can choose 'Match List Member' or 'Equals List Member' as a match type and then select a Shared List (Text-based or Regular Expressions-based) from the SELECT URL or SELECT NAME drop-down menu. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

ℹ The *Clipboard Origin* criterion can only be used with the Clipboard content type.







File Origin

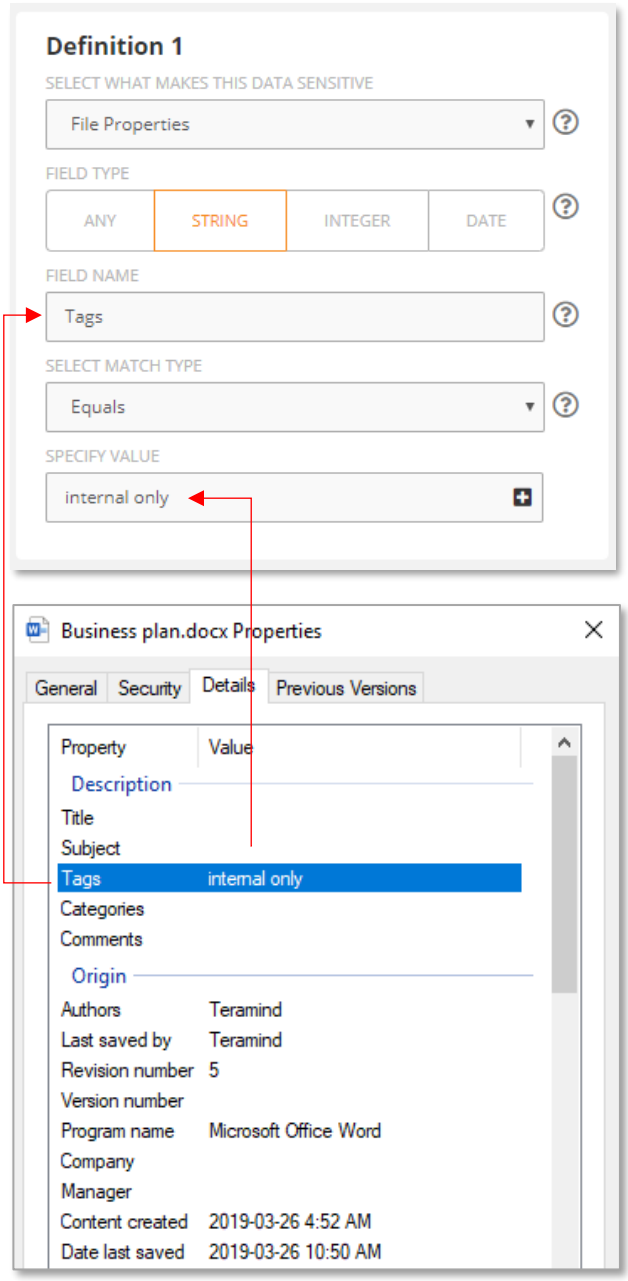
File Origin detects file sharing based on its origin or source. It supports local, Cloud and web sharing. By using it you can, for example, build a rule that prevents sharing of files to Cloud drives.

You can select from several sharing options under the SELECT FILE ORIGIN section. SHARE = any type of network shares, CLOUD = sharing over Cloud services, such as, Dropbox and URL = sharing over any websites.

Depending on which origin (SHARE / CLOUD / URL) you selected, you can choose from 'All Share', 'Contains', 'Equals' or 'RegExp' in the SELECT MATCH TYPE field and specify the text values in the bottom field. Use the ⊞ button to add multiple values. Or, if available, you can choose the 'Match List Member' or 'Equals List Member' as a match type and then select a Shared List (Network-based) from the SELECT URL or SELECT NAME drop-down menu. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

ℹ The *File Origin* criterion can only be used with the Files content type.

ℹ When you select a Cloud provider, it will detect content from the Cloud app (not the web version).



A File Properties window in Windows Explorer

File Properties

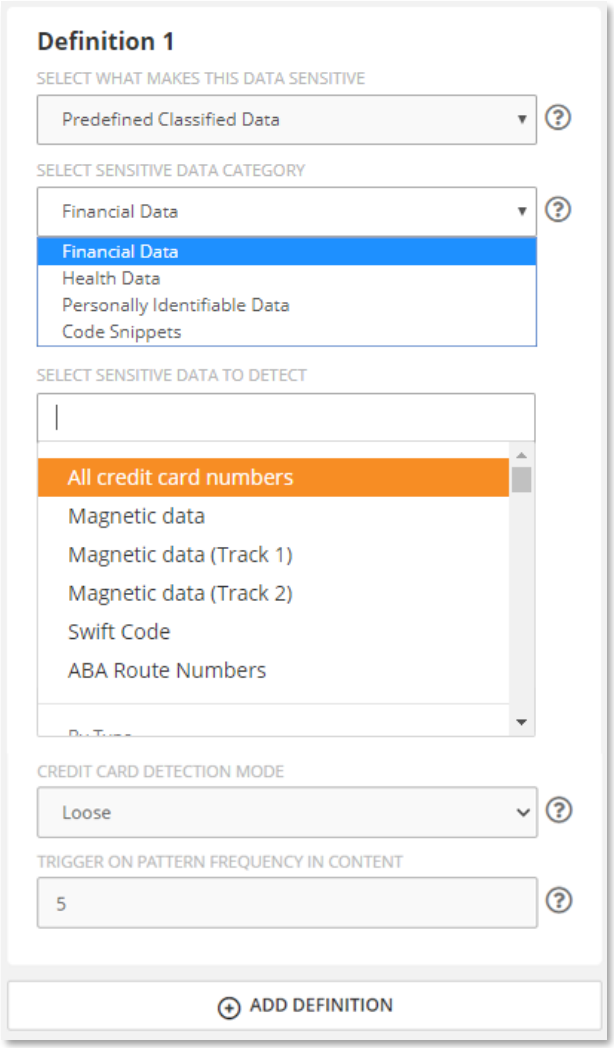
File Properties detect files based on their meta-tags(also know as 'file property' or 'field'). By using it you can, for example, build a rule that prevents sharing of any documents outside your company that has a *Tags* property containing the string value of 'internal only'. You can create such tags/fields/properties from an application (such as Microsoft Word) or from the Windows Explorer.
You can select ANY, STRING, INTEGER or DATE for the FIELD TYPE.

If needed, enter the name of the field/property in the FIELD NAME.

If you select the STRING field type, you can choose from 'Contains', 'Equals' or 'RegExp' in the SELECT MATCH TYPE field and specify the text values to detect in the SPECIFY VALUE field. Use the ⊞ button to add multiple values. Or, you can choose the 'Match List Member' or 'Equals List Member' as a match type and then select a Shared List from the SELECT URL or SELECT NAME drop-down menu. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

If you choose an INTEGER or DATE value, you can choose one of the '=', '>', '<' logics in the MATCH TYPE field and provide a numeric or date value in the SPECIFY VALUE field.

ℹ The *File Properties* criterion can only be used with the Files content type.



Predefined Classified Data

Predefined Classified Data detects content based on pre-defined data categories.

There are several types of data categories you can choose from: Financial Data, Health Data, Personally Identifiable Data etc.

The SENSITIVE DATA TO DETECT field 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', 'SWIFT code' etc. Or, if you choose the Health Data, you can choose from 'Common drug names', 'DNA profile' etc.

If you choose the *Financial Data* from the SELECT SENSITIVE DATA CATEGORY field, then you will see an option: CREDIT CARD DETECTION MODE. This option will let you select the sensitivity of the algorithm to detect credit card numbers. For more information, see the notes under **Adjust the Sensitivity of Credit Card Detection** below.

Finally, you can specify how often a data pattern can appear in the content before the rule is triggered in the TRIGGER ON PATTERN… field.

Check out the Appendix section for a list of all the pre-defined classified data supported in Teramind.

Adjusting the Sensitivity of Credit Card Detection

You can detect credit card numbers using the built-in *Predefined Classified Data*. However, the way the algorithm works, it might incorrectly detect specially formatted strings as credit card numbers. For example, it might detect this URL sting, `4.574%201.252.695%202` as a credit card number (e.g., `4574201252695202`).

To avoid such false positives, you can adjust the sensitivity of the algorithm using the CREDIT CARD DETECTION MODE option. The option supports three detection modes:

- **Loose:** This is how the algorithm works currently and is the default mode. In this mode, Teramind will detect credit card numbers in text sequences, even if the number is broken up by other characters. For example:
  ```
  4* 4*4*4-44&4% %4-44%44- 4&444
  ABcdef44*444*444 444_444&44Xyz
  abcdef4%4*4%4#4*4!!4##4_ 4#44_4%4%4&44Xyz
  ```

- **Medium:** In this mode, Teramind will check sequences with the same delimiter/separator character. Any spaces will be ignored, and several consecutive delimiters will be included in the detection. For example:
  ```
  4%444%%44%44%4444%44%44
  ABcdef4 %%4444%444%4444%%444%4Xyz
  abcdef4_4444_44_44_4_4_4_4444Xyz
  ```

- **Strict:** Only standalone credit card expressions will be included. Delimiters must be the same per expression and one of NONE/SPACES/HYPENS delimiters will be allowed. Several consecutive delimiters will not be allowed. For example:
  ```
  4444444444444444
  44-44-4444-444-4-44-44
  44 44 4444 444 4 44 44
  ABcde 4444444444444444 Xyz
  ```

9.2 Clipboard



The Clipboard-based behavior rules may not work as expected if you have some other software installed that also tracks clipboard operations.

The Clipboard content type detects text copied to the clipboard from any applications or websites.

9.2.1 Clipboard Rule Examples

- Prevent sharing of customer data outside of your CRM site.
- Warn users when they copy social security numbers from an Excel spreadsheet and paste it on an email client like Outlook.
- Prevent data marked as sensitive in the *Predefined Classified Data* list to be pasted on an image application. So that the user cannot later upload the image to bypass your document upload rules.

9.2.2 Clipboard Rule Criteria

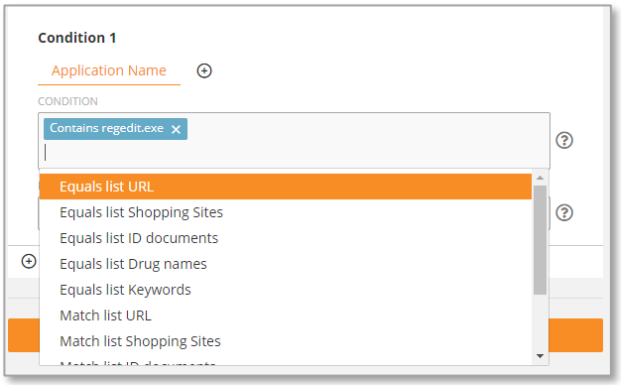
The table below shows what criteria the Clipboard supports and what conditions you can use with them.



Any

Lets you detect the clipboard text in any applications or websites.

If you use this option without any other criteria, Teramind will trigger the rule anytime a clipboard paste operation is performed in any applications or websites where the content is detected.



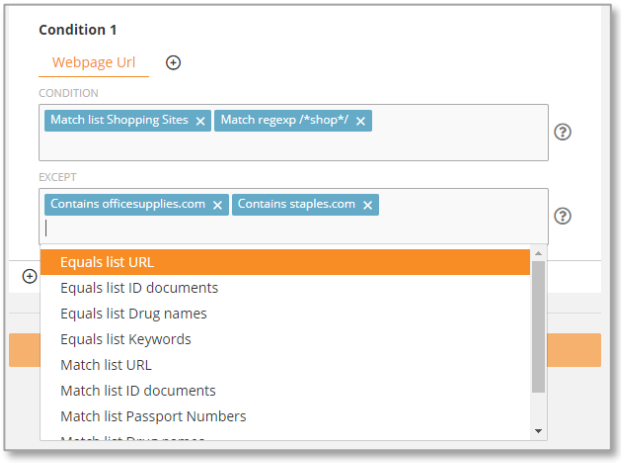
Application Name

Used to specify the applications in which the clipboard action will be detected.

You can choose from 'Contains', 'Equals' or 'Equals List' with any text as conditions. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Equals List' or 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.

The *Application Name* and the *Webpage URL* criterion cannot be used together in the same condition block.



Webpage URL

Used to specify the webpage URL (website address) in which the clipboard action will be detect.

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any URLs in the EXCEPT field.

The *Application Name* and the *Webpage URL* criterion cannot be used together in the same condition block.

9.3 Files

Note that Content-Sharing rules doesn't support the xls and doc files. However, xlsx and docx files are supported.

Files content type works in the same way as it does in the Files Activity rules. However, there are certain file operations that you cannot use in the Content Sharing rules. For example, the *Download* operation or none of the *folder* operations are supported.

Note that not all criteria are available for all file operations. Teramind will automatically show or hide the criteria based on which file operation you select. So, if you select the *Access* or the *Delete* operation, you will only see the *Program* criterion. Some file operation may have additional detection criteria. For example, the *Upload* operation lets you specify the *Upload URL*.



Select a file operation by clicking the CONDITION filed.

Click the ⊕ button to add a criterion to the operation.

If you choose the 'Any' file operation without any other criteria, Teramind will trigger the rule for any file operation where the content is detected.

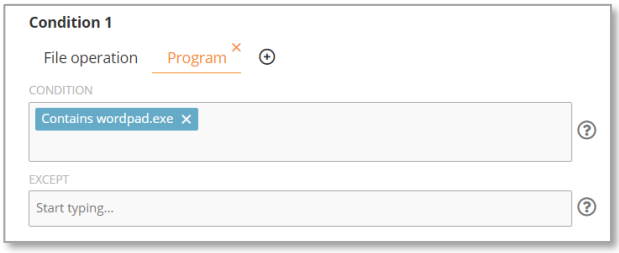
9.3.1 Files Rule Examples

- Prevent sharing of files that contain sensitive information, such as: Credit Card Numbers, Social Security Numbers, Health Records or your own custom data type.
- Prevent sharing of a file based on certain properties, such as, when a document contains a 'confidential' watermark.
- Create rules based on file origin, such as, stop all network sharing from certain applications.

These are some examples of Content Sharing rules for Files. For other examples of the Files rules, check out the Files Activity rule examples.

9.3.2 Files Rule Criteria

The table below describes the criteria you can use for the Files sharing rules, and which file operations are supported for each criterion.

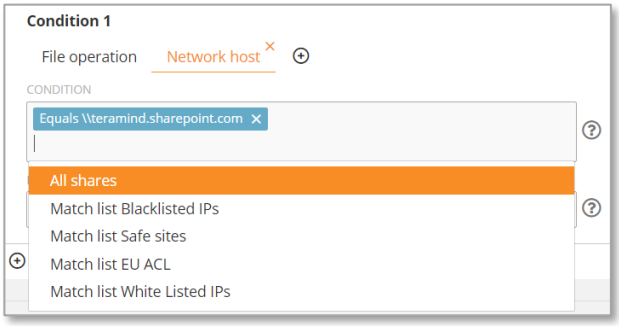


Program

Lets you specify in which program/app the file operation took place.

You can choose from 'Contains', 'Equals', 'Match RegExp' or 'Match Glob'.

Similarly, you can exclude any programs you do not want to track in the EXCEPT field.



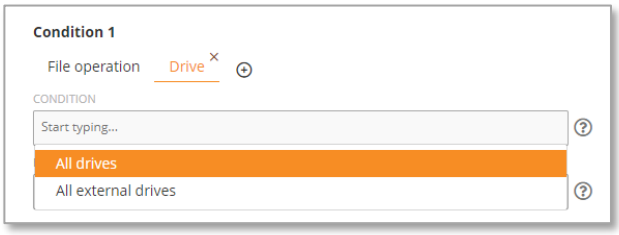
Network Host

Used for network-based file operations. Detects the host name of the file operation. For example: `http://sharepoint.com`, `ftp://filevault.net` etc.

You can choose from 'Contains', 'Equals', 'All Shares'. Or, you can select a Shared List (Network-based) and specify a 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any hosts you do not want to track in the EXCEPT field.

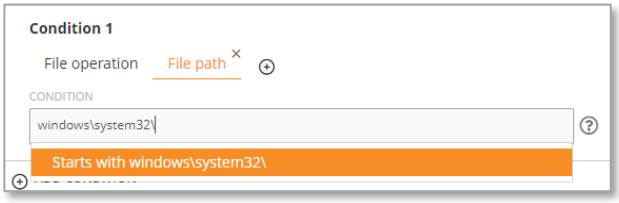
This criterion is only supported in the *Write* and *Copy* operations.



Drive

Detects the local, network or external drives.

You can enter a drive name (e.g., 'c') and select that particular drive or choose from 'All Drives' or 'All External Drives' conditions.

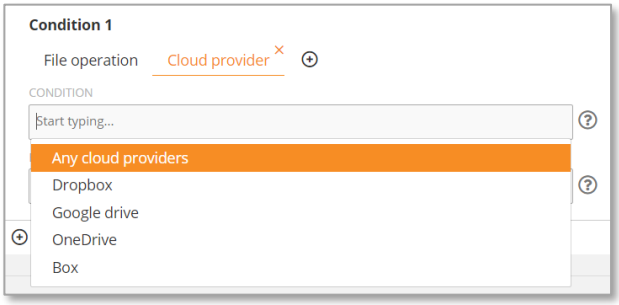


File Path

Used to detect a file path. For example: `\windows\system32\`.

You can only choose the 'Starts with', condition with any path you enter.

The path is treated as relative if root is defined, otherwise it's treated as absolute.



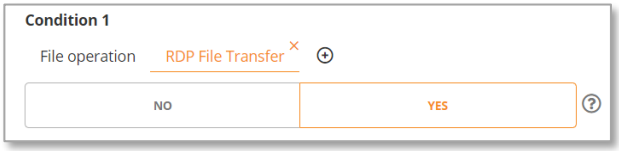
Cloud Provider

Used to detect cloud providers.

You can choose from 'All Cloud Providers', 'Dropbox', 'Google Drive', 'OneDrive' or 'Box', etc.

Similarly, you can exclude any provider you do not want to track in the EXCEPT field.

This criterion is only supported in the *Write* and *Copy* operations.

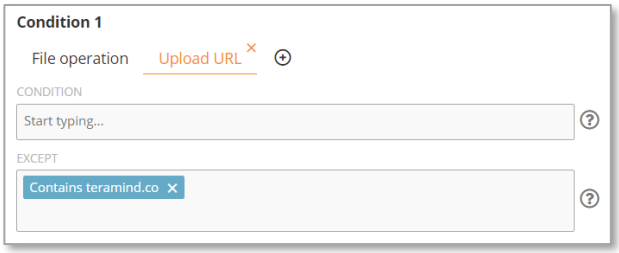


RDP File Transfer

Detects if the file copy operation is done over an RDP (Remote Desktop Protocol) session. This happens when you connect to a remote computer and copy files to/from it.

You can select either YES or NO.

This criterion is only supported in the *Copy* operation



Upload URL

You can choose from 'Contains', 'Equals' or 'RegExp'. Or, you can select a Shared List and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any URLs you do not want to track in the EXCEPT field.

This criterion is only supported in the *Upload* operation.

9.4 Emails

Emails content type works in the same way as it does in the Email Activity rules. Except, the *Mail Body* criterion is not supported, and the *Mail Direction* criteria only supports the outgoing emails.

Emails lets you detect content sharing over outgoing and incoming emails, draft emails* and email attachments.

*Rules on a draft email is trigged when the draft is saved.

9.4.1 Emails Rule Examples

- Detect sensitive information like Credit Card Numbers, Social Security Numbers, Health Records or your own custom data types inside attachments and act based on what's detected.
- Detect if an internal memo is shared outside the company.
- For example, warn the user when sending out an email that contains a document containing contacts to prevent data exfiltration or comply with privacy laws.

These are some examples of Content Sharing rules for Emails. For other examples of the Emails rules, check out the Emails Activity rule examples.

9.4.2 Emails Rule Criteria

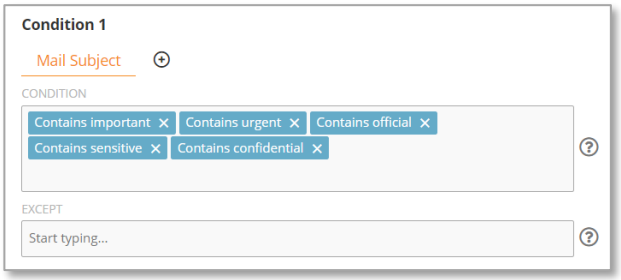
The table below shows what criteria the Emails sharing supports and what conditions you can use with them.



Any

Lets you detect if an email is sent or received.

If you use this option without any other criteria, Teramind will trigger the rule anytime an email is sent or received.

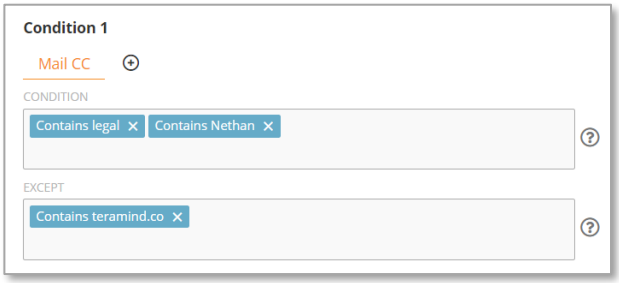


Mail Subject

Used for detecting text inside the mail subject.

You can choose from 'Contains', 'Equals' or 'RegExp' with any text. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.



Mail CC

Detects the CC addresses in an email.

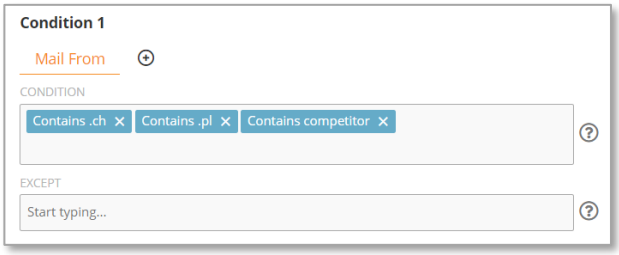
You can choose from 'Contains', 'Equals' or 'RegExp' with any text. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Match List' or 'Equals List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any text/list you do not want to track in the EXCEPT field.



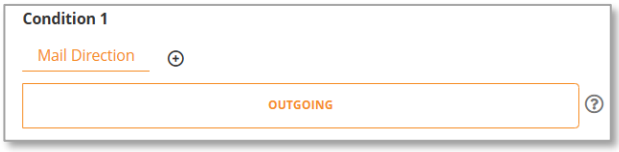
Mail To

Similar to *Mail CC* criterion but used to detect the *Mail To* addresses instead.



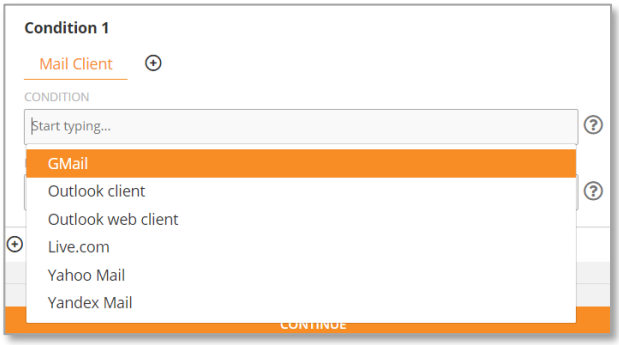
Mail From

Similar to *Mail CC* and *Mail To* criterion but used to detect the *Mail From* addresses instead.



Mail Direction

Email Content Sharing rules only support the OUTGOING option for the *Mail Direction* criteria.



Mail Client

Used to specify the mail client you want to detect.

You can choose from 'Gmail', 'Outlook Client', 'Outlook Web Client', 'Live.com', 'Yahoo Mail', and 'Yandex Mail'. Teramind keeps adding support for new clients so you might see more clients than mentioned here.

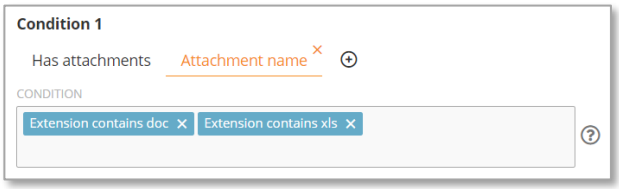
Similarly, you can exclude any client(s) you do not want to track in the EXCEPT field.



Has Attachments

Used to detect if the mail has any attachment.

Select either the YES or NO option.



Attachment Name

Used to detect the names or extensions for the attached files. File extension are used to identify a file type and usually starts with a '. (dot)'. For example: *.doc, .pdf* etc. Note: you do not need to specify the '.' when entering the extension.

You can choose from 'Contains', 'Equals' or 'RegExp' with any text. Or, you can check for file extensions using one of the 'Extension Contains', 'Extension Equals', 'Extension Does Not Contain' options.

The *Attachment Name* criterion is only shown when you have already selected YES for the *Has Attachment* criterion.



Mail Size

Used to detect the size (in bytes) of the mail.

You can enter a byte value in the CONDITION field and use the '=', '>', '<', '>=' logics.

Similarly, you can use the EXCEPT field to specify an exception.

9.5 IM

IM content type works in the same way as it does in the IM Activity rules. Except, the *Message Body* criterion is not supported, and the *Message Direction* criteria only supports the outgoing messages.

IM lets you detect content sharing over instant messaging conversations and group chats for popular IMs such as: Skype, Slack etc. You can detect both incoming and outgoing messages, detect the participants and search in the message body for keywords or text.

9.5.1 IM Rule Examples

- Improve productivity and data security. For example, detect if customer service agents are not responding to complaints or queries coming through your Instant Messaging channels.
- Create rules that warn the HR about angry exchanges, harassments or other potential negative sentiments in chat conversations.
- Detect if a user is targeted for phishing or social engineering online.

These are some examples of Content Sharing rules for IM. For other examples of the IM rules, check out the IM Activity rule examples.

9.5.2 IM Rule Criteria

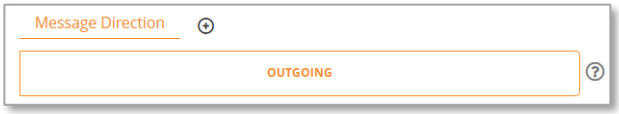
The table below shows what criteria the IM sharing supports and what conditions you can use with them.



Any

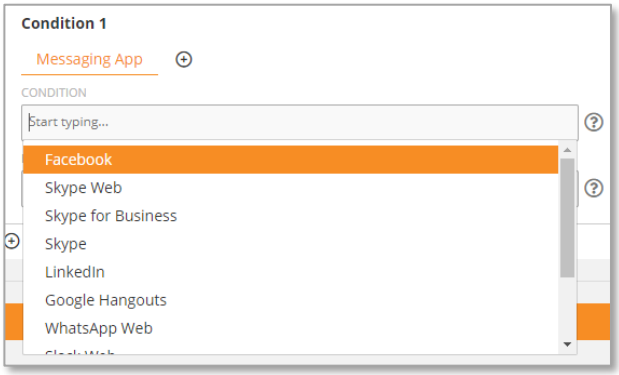
Lets you detect if an IM is sent or received.

If you use this option without any other criteria, Teramind will trigger the rule anytime an IM is sent or received where the content is detected.



Message Direction

IM Content Sharing rules only support the OUTGOING option for the *Message Direction* criteria.



Messaging App

Used to specify the messaging app you want to detect.

You can choose from 'Facebook, 'Skype Web', 'Skype for Business', 'LinkedIn', 'Google Hangouts', 'WhatsApp Web', 'Slack Web', 'Slack', 'Microsoft Team Web' and 'Microsoft Team'. Teramind keeps adding support for new apps so you might see more clients than mentioned here.

Similarly, you can exclude any app(s) you do not want to track in the EXCEPT field.



Contact Name

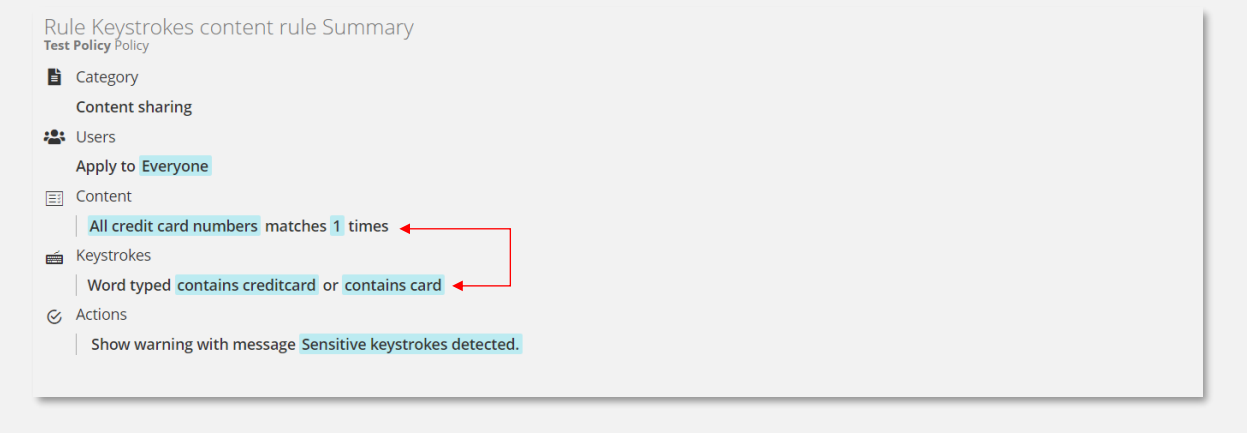
Used to detect the contacts/participants of the IM conversation.

You can choose from 'Contains', 'Equals' or 'RegExp' with any text as conditions. Similarly, you can exclude any contacts you do not want to track in the EXCEPT field.

9.6 Keystrokes

A Keystrokes Content Sharing rule works similarly to the Keystrokes Activity rule. Except, it also comes with the Content tab with support for the *Data Content* and *Predefined Classified Data* definitions. This allows you to detect two sets of specialized contents easily.

A Keystrokes Content Sharing rule will only trigger if both the condition(s) under the *Keystrokes* tab and the definition(s) under the *Content* tabs are met. For example, the rule below will trigger if the user types something like, "creditcard 4233198522419042". But if the user typed just a credit card number, such as "4233198522419042", the rule will not trigger.

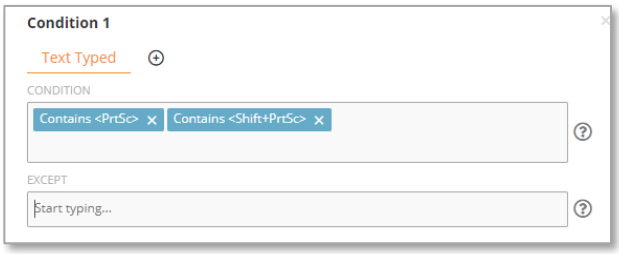


9.6.1 Keystrokes Rule Examples

- Detect sensitive content as they are being typed by a user to proactively prevent potential data leaks.
- Detect two sets of data and specialized contents easily. For example, a user typing something like “Credit Card XXXXXXXXXXXXXXX”. Where, “Credit Card” is a static text while “XXXXXXXXXXXXXXX” can be any credit card number.

9.6.2 Keystrokes Rule Criteria

The table below shows what criteria the Keystrokes content sharing rules support and what conditions you can use with them.



Text Typed

Used to detect continuous text without any word break. For example, if text typed = "password", the rule will be triggered when the last letter ‘d’ is typed.

You can enter any text in the CONDITION field and choose the ‘Contains’ or ‘Match RegExp’ option. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a ‘Equals List’ or ‘Match List’ condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any text you do not want to detect in the EXCEPT field.



Word Typed

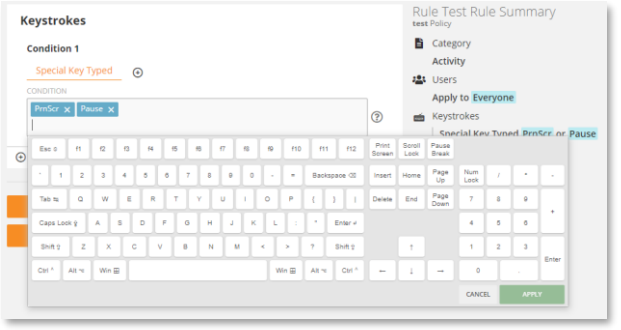
Used to detect word typed with breaks. For example, if word typed = "password" the rule will be triggered when you finish typing the word and then type separation key, such as: `<Space>` or '!' or '.' (dot).

You can enter any text in the CONDITION field and choose the 'Contains' option. Or, you can select a Shared List (Text-based or Regular Expressions-based) and specify a 'Equals List' or 'Match List' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any word you do not want to detect in the EXCEPT field.

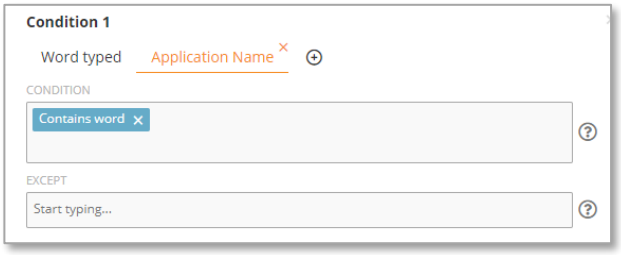
Difference Between *Text Typed* and *Word Typed*

Text Typed will detect any partial text while *Word Typed* will detect only full words. For example, if you are looking to detect `'club'`, and the user typed `'golfclub'`, *Text Type* will detect it but *Word Typed* will not. If the user typed `'golf club'`, then both the *Text Typed* and *Word Typed* criteria will detect the keystrokes.



Special Key Typed

You can detect special keys such as the function keys (i.e. `F1`), `PrtScr` or key combinations such as `<Shift+P>`. When you select the *Special Key Typed* criteria and click on the CONDITION field, Teramind will pop-up a virtual keyboard where you can select the special keys.



Application Name

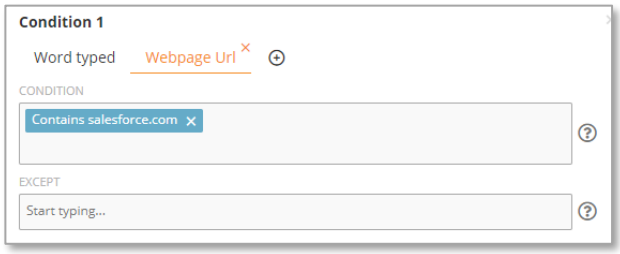
Specifies which applications will be tracked.

You can enter any text in the CONDITION field and choose from 'Contains', 'Equals' or 'Match RegExp'. Or, you can select a Shared List (Text-based or Regular Expressions-based) and

specify a 'Match List' or 'Equals' condition. Check out the Shared List section on the Teramind User Guide to learn how to create shared lists.

Similarly, you can exclude any applications you do not want to track in the EXCEPT field.

The *Application Name* criterion is only shown when you have already selected a *Text Typed* or *Word Typed* criterion. Also, if you use this criterion, you cannot use the *Webpage URL* criterion in the same condition block. However, you can use both criteria in separate condition blocks (i.e. *Condition 1* and *Condition 2*).



Webpage URL

Specifies which websites will be tracked. This is same as the *Webpage URL* criterion under the Webpages activity.

The *Webpage URL* criterion is only shown when you have already selected a *Text Typed* or *Word Typed* criterion. Also, if you use this criterion, you cannot use the *Application Name* criterion in the same condition block. However, you can use both criteria in separate condition blocks (i.e., *Condition 1* and *Condition 2*).

10 Creating Anomaly Rules [deprecated]

> The Anomaly Rules feature is being discontinued. Existing customers with this feature can continue to use it, but there will be no future updates or support available.

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.

The Anomaly Rules Editor is an intuitive, visual editor where you can create sophisticated behavioral-anomaly rules on a single screen.

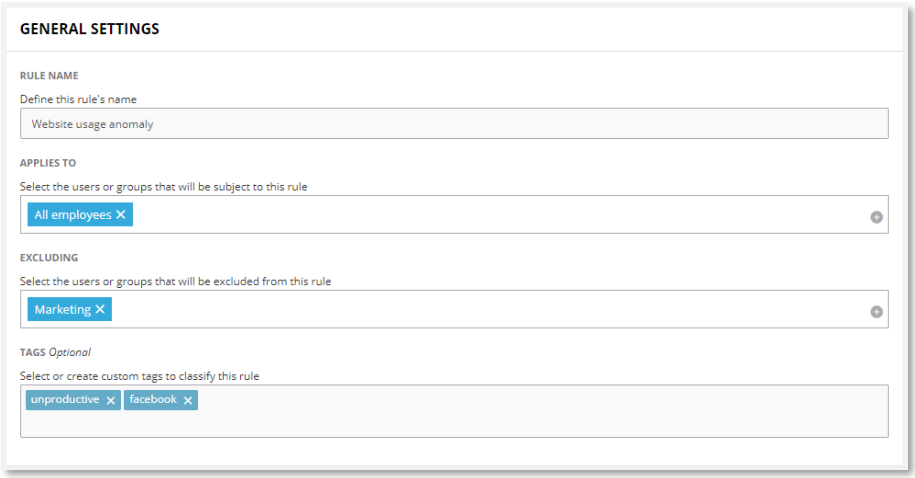
To access the Anomaly Rules Editor, create a new anomaly rule or edit an existing rule from the **Behavior** > **Anomaly rules** menu.

10.1 Rule Examples

- Detect when employees spend more than certain percentage of their workhours on unproductive or entertainment sites such as Facebook, YouTube etc.
- Detect if an employee is idling for too long.
- Get notified if an employee's productivity drops by certain rate.
- Get notified when a user sends an unusual number of emails than they normally do in a day-to-day basis.
- Detect if the file upload activity of a user exceeds some threshold.
- Detect if your network activity suddenly spikes or drops indication potential attacks.

10.2 Setting Up the Rule Basics

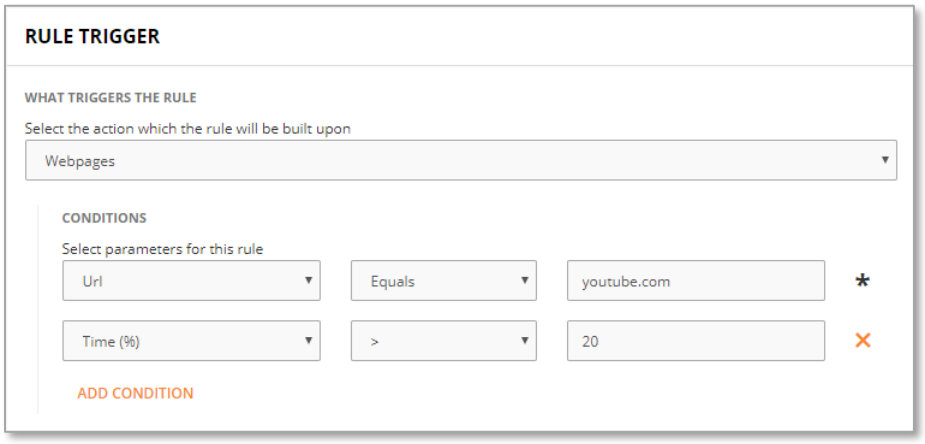
You specify the basic settings for an anomaly rule on the Anomaly Rules Editor's **General Settings** section.



You can specify a name for the rule in the RULE NAME field. You can select which users, groups, departments or computers the rule will apply to in the APPLIES TO field. If you select a computer, the rule will apply to all the users on that computer. Optionally, you can exclude anyone you don't want to be included using the EXCLUDING field. You can also specify the rule's tags in the TAGS field. Tags are keywords you can assign to a rule to easily identify it. They are useful in searching for the rule and can also be used as filters on various reports (i.e. Risk or Alerts report).

10.3 Detection Criteria - What Behavioral Anomalies Trigger the Rules?

You define the detection criteria under the RULE TRIGGER section of the Anomaly Rules Editor.

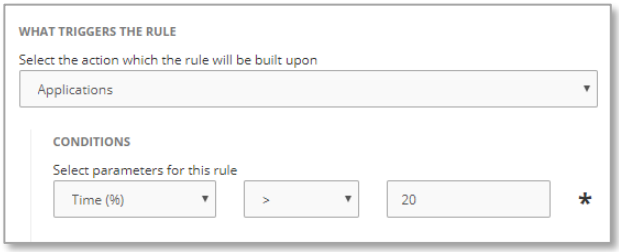


You can select an action that will trigger the rule and then specify the conditions to evaluate. There are several types of actions you can choose from: Applications, Websites, Emails, Activity, Files, Network etc.

Each action has different conditions you can select from, such as: Time, Name, Anomaly Baseline etc. After you have selected a condition, you can choose a logic, such as: '>', '<', 'Equals' etc. from the middle field. Finally, you specify value(s) to detect in the right-most field.

You can add multiple conditions to an action by clicking the ADD CONDTION button. For example, you can create an anomaly rule using the *URL* condition and a *Time* condition with a *Websites* action to detect if a user spent >20% in 'youtube.com'.

In the next few sections, we will walk you through all the available options for setting detection criteria for each action type.

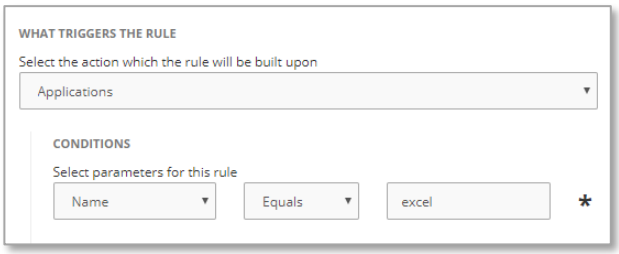


Time

Detects time spent (%) in an application or website.

Enter a percent value and use the '>' or '>=' logic for the condition.

This condition is only supported in the *Applications* and *Webpages* actions.

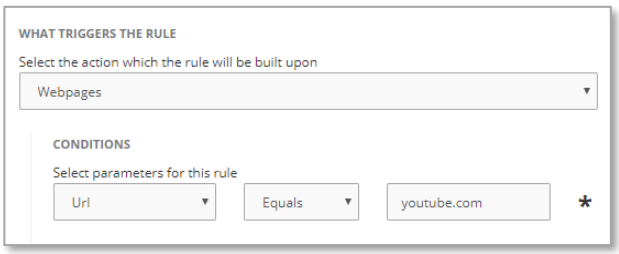


Name

Used to specify a name for an application.

Enter a text value and use the 'Equals', 'Contains', 'Does Not Contain' 'Regular Expression Match', or 'Regular Expression Not Match' logic for the condition.

This condition is only supported in the *Applications* action.

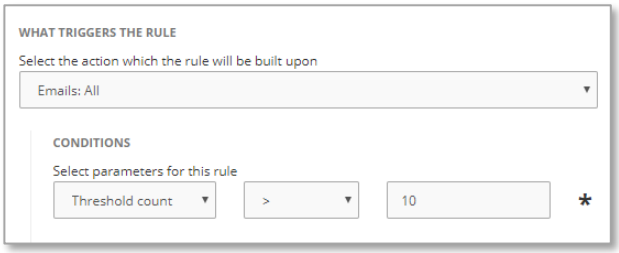


URL

Used to detect the URL of a webpage.

Enter a text value and use the 'Equals', 'Contains', 'Does Not Contain' 'Regular Expression Match', or 'Regular Expression Not Match' logic for the condition.

This condition is only supported in the *Webpages* action.

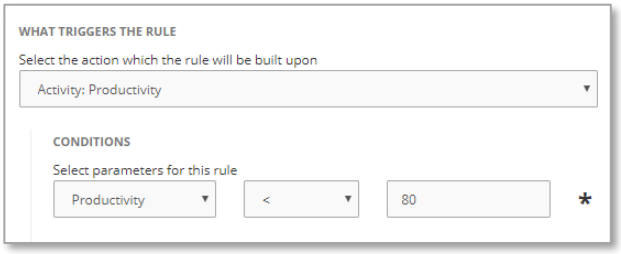


Threshold Count

Sets the threshold count for how many times an activity occurs before triggering the rule. For example, no. of emails sent, no. of download operation, no. documents printed etc.

Enter a number value and use the '>' or '>=' logic for the condition.

This condition is supported in all actions except for *Applications* and *Webpages*.

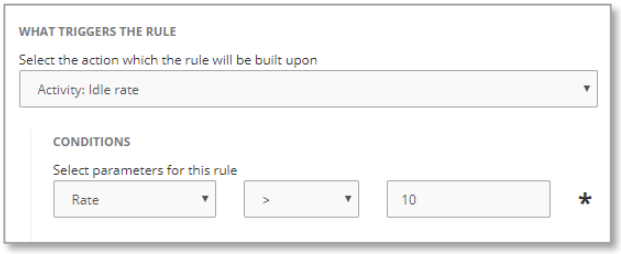


Productivity

Detects the productivity level (in percent) of a user. To learn more about how productivity is measured in Teramind, check out the BI Reports > Productivity section on the Teramind User Guide.

Enter a percent value and use the '<', '>' or '>=' logic for the condition.

This condition is only supported in the *Activity: Productivity* action.

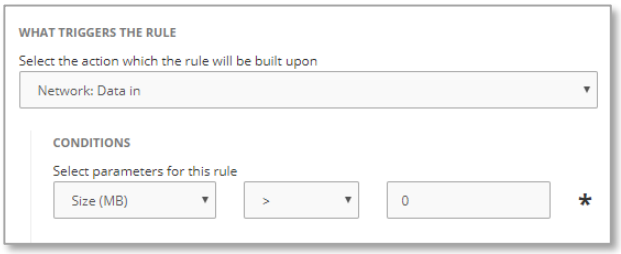


Rate

Detects the idle rate (in percent) of a user. To learn more about how idle rate is measured in Teramind, check out the BI Reports > Productivity section on the Teramind User Guide.

Enter a percent value and use the '>' or '>=' logic for the condition.

This condition is only supported in the *Activity: Idle Rate* action.

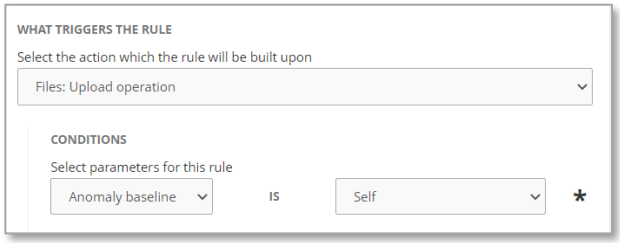


Size

Detects the size (in Mega Bytes) of data in a network operation.

Enter a value in Mega Bytes and use the '>' or '>=' logic for the condition.

This condition is only supported in the *Network: Data In* and *Network: Data Out* actions.



Anomaly Baseline

Anomaly Baseline uses algorithm to determine if certain user behavior is outside a baseline. 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 the baseline of the entire organization. Using a baseline lets you, for example, set an anomaly rule to notify you when a user uploads an unusual number of files than they normally do in a day-to-day basis.

A special formula is used to check for anomaly baseline. The formula is:

```
Anomaly Score = (Current
Activity Value - Mean) /
Standard Deviation
```

The Current Activity Value is the amount of activity. For example, the number of File Uploads by a user. The score is measured automatically every hour to determine if it crossed the baseline. The default value of this is 3.5.

As an example, consider a user uploaded [1, 2, 3, 4, 1, 1, 1, 1, 1, 1, 1, 1, 1, 30] times every day for 15 days. And on the 16th day, the uploaded for 80 times.

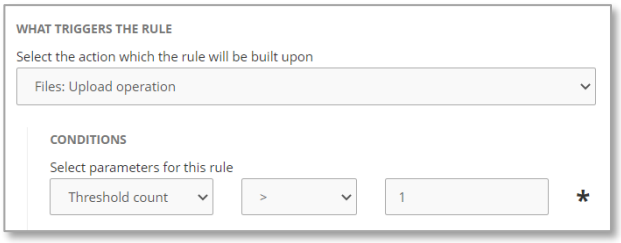
In this case, their anomaly score will be:

3.62 = (80-8.125) / 19.82

Which is greater than the default value of 3.5. So, this means the user exceeded the anomaly baseline on the 16th day.

The anomaly baseline can be applied to a user's own activities (Self), the activities compared to a department (Department) or the entire organization. If you choose anything

other than Self, then the Anomaly Score of the user activities will be compared against the Score of the Department/Organization for the same period.



Threshold Count

The anomaly threshold is like the threshold value available in a regular rule action (Advanced Mode). It will trigger the rule action if the total count of Anomaly Baseline violation crosses the set number of threshold. For example:

If you set the threshold to >0 then the rule will be triggered immediately (as soon as the anomaly baseline crosses the first time). As an example, consider a user uploaded [1, 2, 3, 4, 1, 1, 1, 1, 1, 1, 1, 1, 1, 30] times every day for 15 days. And on the 16th day, the uploaded for 80 times. In this case, the user will cross the Anomaly Baseline on the 16th day (see Anomaly Baseline above). And as soon as the baseline is crossed, the rule action will be triggered.

However, say, you set the threshold to >1 then the baseline has to be crossed twice before the rule action is triggered. In the above example, if the user keeps uploading the file at the similar rate, the rule action will be triggered in about 32 days or so.

Note that, anomaly threshold works for a user's own activities (Self) and not for any department or entire organization.

This condition is supported in all actions except for *Applications* and *Webpages*.

11 Defining Rule Actions

Actions let 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.

You can assign actions to a rule from the **Actions** tab on the Rules Editor for regular rules. Or, from the **RULE ACTIONS** section on the Anomaly Rules Editor for anomaly rules.

Note that, not all rule categories support all actions. For example, the Agent Schedule only supports the NOTIFY action for most of its schedule violation types except for the *Login* and *Idle* activities. Same way, different Types of Activity / Types of Content may also have their own special actions. For example, Webpages have an action called REDIRECT which is not available for other activity. Also, not all actions are available on all the operation systems. For example, the COMMAND action does not work on the macOS at the moment.

Note that only the following actions are supported on Teramind Starter: WARN, BLOCK, NOTIFY, and REDIRECT.

On Mac, only the following actions are supported: NOTIFY, BLOCK, WARN, LOCK OUT USER, and RECORD VIDEO. Some actions might not be supported for all rule criteria. Actions may also behave slightly differently than Windows. Please see this article on our Knowledge Base to learn more about what rules and features are supported on Mac.

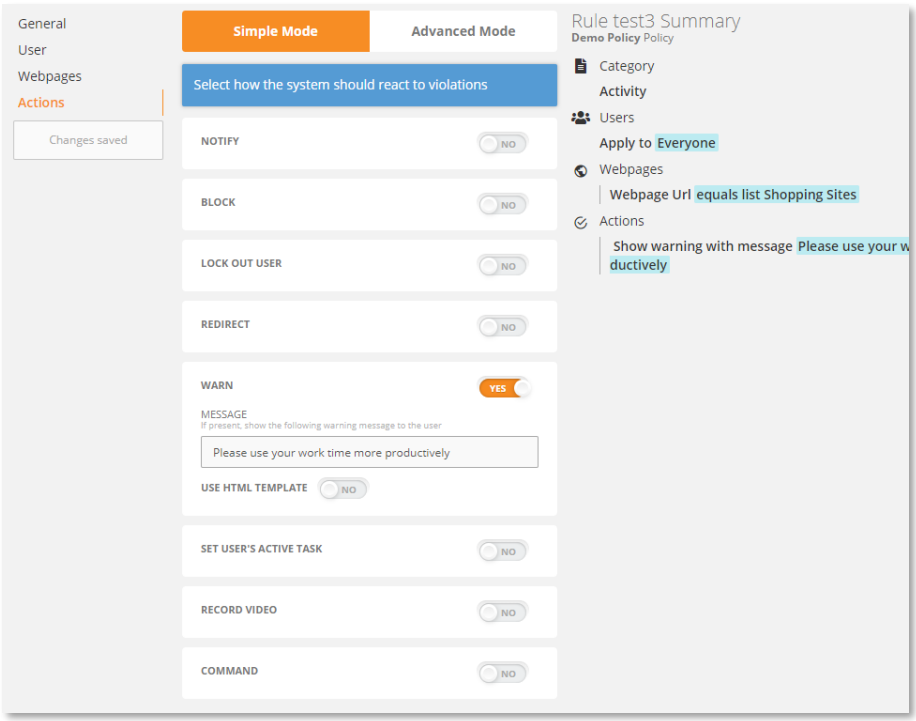
Note that, Anomaly Rules only support the Notify action.

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 completing an activity. The Rules Editor will automatically disable actions that conflict with the currently selected action(s).

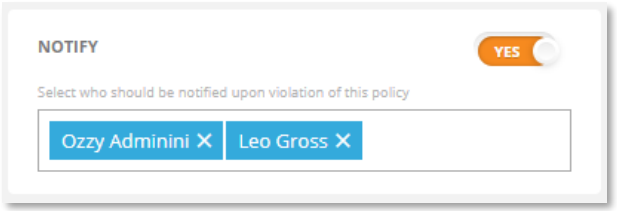
There are two ways you can setup actions: Simple Mode and Advanced Mode.

11.1 Simple Mode Actions

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 the actions you can use:



11.1.1 Notify (Windows & Mac)

Teramind will send an email notification to the specified email accounts whenever any user violates the rule.

The ALERT EMAILS LIMIT option (under *Settings* > *Alerts*) lets you specify how the notification emails should be handled.

Note 1:
You can send the notification to up to 15 email addresses.

Note 2:
You can send the notification to up to 15 email addresses.

Note 3 (for the Mac users):

On the Mac, the Notify action is supported for all rules (that are available on Mac) except for the Keystrokes rules.

Notes About Notification Emails

You can send the notification to up to 15 email addresses

Notes for the OCR Rules

By default, the OCR notify alerts are limited to 1 per rule, app, agent and computer in a 4-minute window. But On-Premise customers can change this default behavior by adding the following line to their `teramind.config` file:

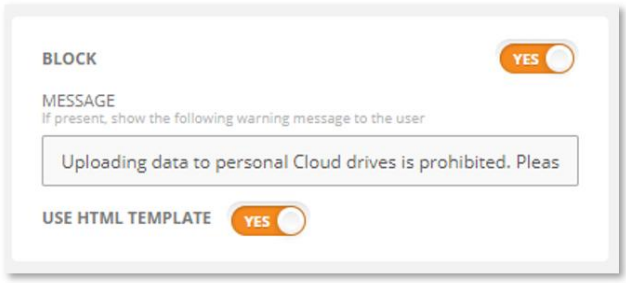
```
web_instances_disable_ocr_alert_throttling = onsite
```

When this feature is enabled, all violations will be emailed (unless you have the *Settings* > *Alerts* > *ALERT EMAIL LIMIT* option set) and recorded in the Behavior Alerts report.

Note that after editing the config file, you will need to restart your `teraweb` container for the changes to take effect.

Notes for the Mac Users

On the Mac, the Notify action is supported for all rules (that are available on Mac) except for the Keystrokes rules.



11.1.2 Block (Windows & Mac)

Blocks the user activity and shows a message.

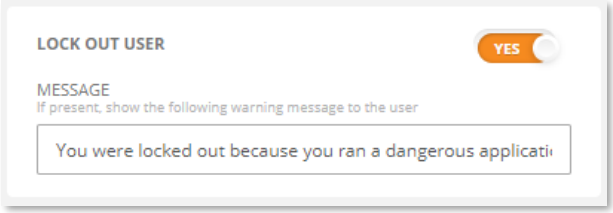
You can use a HTML template to display the message. See the Customizing the Rule Messages and Alerts section to learn more.

The USER ALERTS THRESHOLD option (under *Settings* > *Alerts*) lets you specify how long Teramind should wait between multiple alert messages that the user sees.

Note 1:
The MESSAGE option isn't available for *Content Sharing* rules.

Note 2:
In most cases, if you use this action with a *Webpages* rule, then the browser tab for the webpage/URL will be closed immediately after showing the MESSAGE. However, if a rule criterion (e.g., *Idle Time*) causes the rule to trigger after some delay, then the tab will not be closed but the webpage will be replaced by a blank page showing the MESSAGE (if any present).

Note 3:
If you use this action with an *Emails* rule, such as block a user from sending an email, then the email will not be sent, and it will be deleted.



11.1.3 Lock Out User (Windows & Mac)

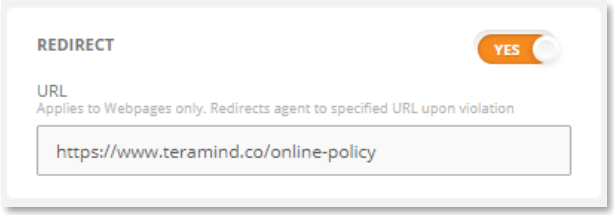
Shows a warning message to the user and then when they press the OK button, they are locked out of the system. If the user logs back in, they will be logged out automatically. An administrator has to unlock the user for them to be able login again. Check out the Employee Action Menu section on the Teramind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

Note 1:
This action works on the Hidden Agent only. By design, it will not be enforced on the Revealed Agent. Please also note that the lock out feature isn't a full protection from user tampering. It has the following limitations:

- Only the selected user account will be locked out. If there are other users on the computer, they will be able to log in.
- If the user may be able to log in using the Windows Recovery mode.

- The user may be able to take out the disk and connect with another computer and access data.

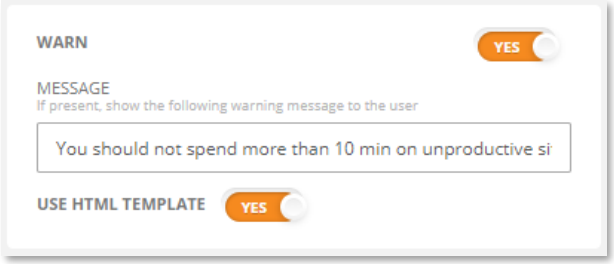
Note 2 (for the Mac users):
On the Mac, when the rule is triggered, the user is locked out only once and taken to the login screen. They can log back in. In case the action is configured with an *Applications* condition, then the last active application specified in the condition will be terminated and the user will be locked out. In case the action is used with a *Network*-based rule, the network connection that triggered the rule will be closed.



11.1.4 Redirect (Windows)

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

This action is available to Websites-based rules only.

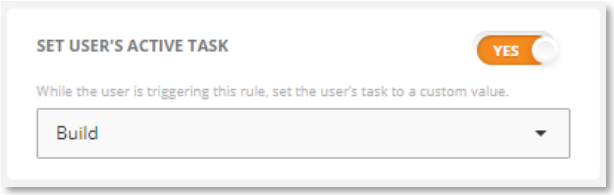


11.1.5 Warn (Windows & Mac)

Warns a user with a message.

You can use a HTML template to display the warning message. See the Customizing the Rule Messages and Alerts section to learn more.

The USER ALERTS THRESHOLD option (under *Settings* > *Alerts*) lets you specify how long Teramind should wait between multiple alert messages that the user sees.

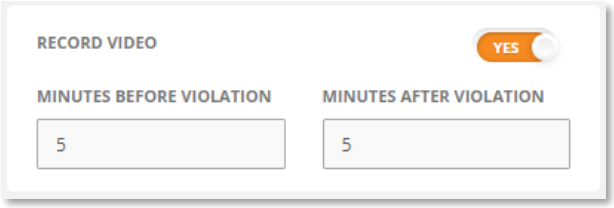


11.1.6 Set User's Active Task (Windows)

You can automatically assign the user a task based on their activities.

The RULE TASK SELECTION ACTION TIMEOUT option (under *Settings* > *Alerts*) lets you specify how long Teramind will wait before assigning a new task to a user.

Applicable only if the user is using a Hidden Agent.



11.1.7 Record Video (Windows & Mac)

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.

If you don't want to record screen all the time but just before and after a rule violation incident, you can use this action and then turn on the RECORD ONLY WHEN BEHAVIOR RULE WAS VIOLATED option under *Monitoring Settings* > *Monitoring Profile* > *Screen* window.



11.1.8 Command (Windows)

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

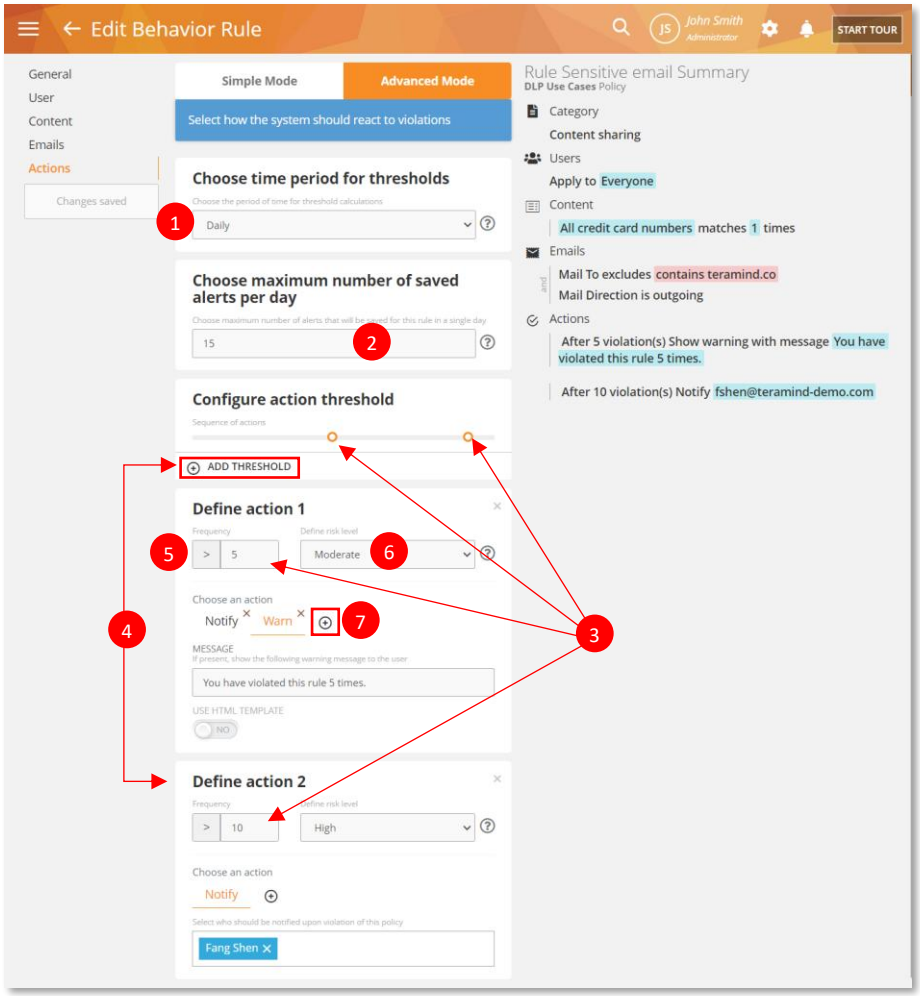
This is a powerful action as it allows you to run any application or script on the user's computer. For example, you can force shutdown the pc (`shutdown /s /f /t`

0), kill a task (`taskkill -im ixplore.exe`) and do much more.

11.2 Advanced Mode Actions

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 Using the Risk Report section to learn more about risk analysis) and can also be used to filter other reports (e.g., BI Reports > Behavior Alerts).



1. You can choose the time period for the thresholds such as *Hourly*, *Daily*, *Monthly* etc.
2. Select/enter the maximum number of alerts that can be triggered for this rule in a day. If more than the specified number of alerts are triggered for this rule in a single day, Teramind will not save further alerts and the alerts will not appear on the BI Reports > Behavior Alerts or other

alert logs. If you leave the field empty or use an invalid value (entering a string, a negative number, etc.) then no daily limit will be applied. If you set it to 0, then no alerts for the rule will be generated (the rule will still trigger). Note that, you can set the global maximum alerts per alert type in the Settings > Alerts > MAXIMUM DAILY ALERTS COUNT field.

3. The threshold slider lets you adjust the frequency once you have added one or more thresholds. Note that, each small dot on the slider is connected to a *Frequency* field of an action. Changing one will update the other.
4. 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). For each threshold, you can set frequency, risk level and action. Note that, the actions (e.g., *Notify*, *Warn*) are same as the Simple Mode actions.
5. You can use the *Frequency* field to set a frequency.
6. Use the *Define a risk level* field to set a risk level. You can choose from: *No Risk*, *Low*, *Moderate*, *High* or *Critical*.
7. Use the small ⊕ button (under the *Choose an action* text) to add an action.

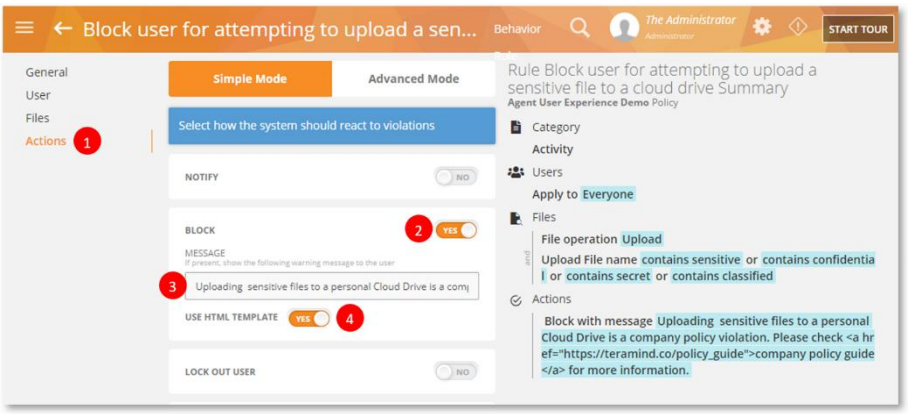
12 Customizing the Rule Messages and Alerts

You can display a customized alert message to an employee or user in case of a policy/rule violation incident. Warn, Block, and Lock Out User rule actions support displaying custom user messages.

By default, alerts appear on the top-right corner of the user's desktop in a small white box. You can format the alert message using HTML codes. You can also change the default alert template to change the look and feel of the alert box. For example, to match the brand of your company, or to link to your company policy.

12.1 The USE HTML TEMPLATE Option

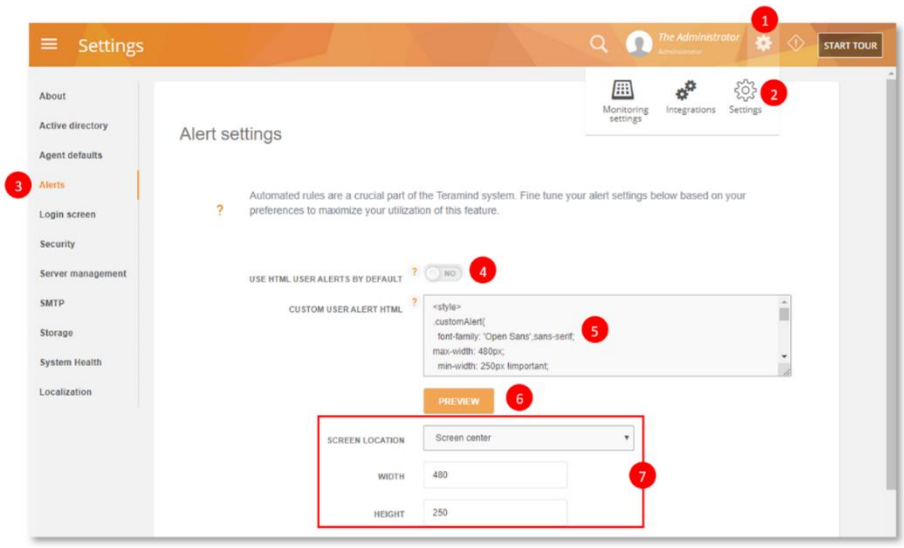
To enable the use of HTML template, create or edit a rule then follow these steps:



1. Go to the rule's **Action** tab.
2. Select a rule action, such as **Warn/Block/Lock Out User**.
3. Enter your alert message in the **MESSAGE** field.
4. Turn on the **USE HTML TEMPLATE** option and save the rule. You can also make the HTML template the default option from the alert setting. Check the section below to learn how to do that.

12.2 Customizing the HTML Alert Template

Before using the HTML template, it is a good idea to customize it so that the Alerts messages are visually distinctive and match with any company branding you might have. You can customize the look and feel of your message box by editing the HTML Alert template:



1. Click the **Gear** icon on the top-right corner.
2. Select **Settings**.
3. Select the **Alerts** tab.
4. To make this template default option for the rules, turn the **USE HTML USER ALERTS BY DEFAULT** option on.
5. Enter the HTML code in the **CUSTOM USER ALERT HTML** field.
6. Click the **PREVIEW** button to see how the alert will look.
7. You can change the **SCREEN LOCATION**, **WIDTH**, **HEIGHT**, etc.

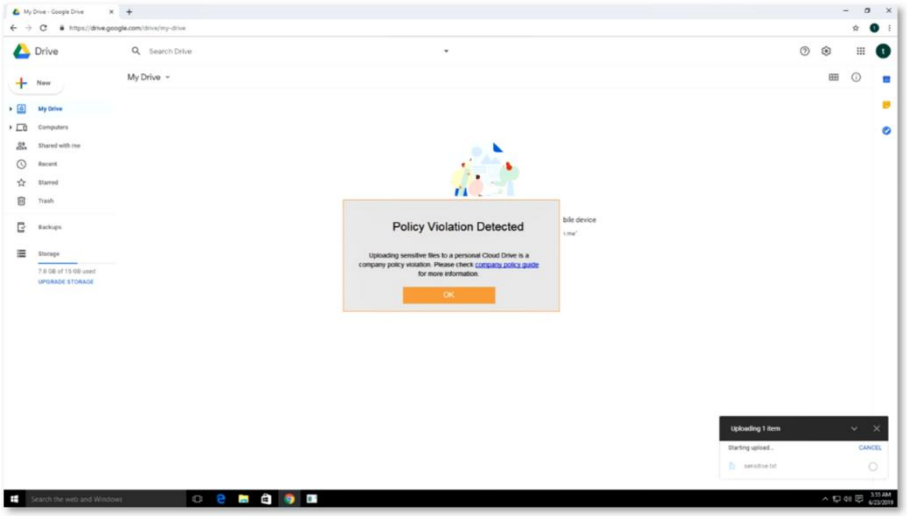
There are two dynamic variables: `%ALERT%`, `%DETAIL%` you can use in your message. These variables will then be replaced with the actual alert message and details when triggered. Also, the alert can have HTML buttons such as, the `OK` and `CANCEL` buttons.

Here is a sample HTML code:

```
<style>
.customAlert{
font-family: 'Open Sans',sans-serif;
max-width: 480px;
min-width: 250px !important;
min-height: 100px;
padding: 10px;
box-sizing: border-box;
background: #088A68;
background-color: #ddd;
padding: 16px 38px 16px 28px;
box-shadow: 0 3px 6px 0 rgba(0,0,0,.1);
border-radius: 4px;
border: 1px solid #f78d24;
}
.message{
font-size: 14px;
```

```
padding: 5px;
color: #000;
font-size: 14px;
line-height: 20px;
text-align: center;
}
.okButton {
top: 100%;
left: 50%;
width: 50%;
height: 36px;
outline: 0;
border: 0;
background: #f2a654;
color: white;
text-align:center;
}
.okButton:hover{
transition: 0.3s;
cursor: pointer;
}
.alert-title {
clear: both;
font-size: 25px;
padding: 20px 0;
text-align: center;
}
</style>
<div class='customAlert'>
<div class="alert-title">
Policy Violation Detected
</div>
<p class='message'>
%ALERT%
</p>
<div style="text-align:center;">
<button class='okButton' >OK</button>
</div>
</div>
```

And this is how it will look on the user's desktop:



Sometimes the alert might not show exactly on the user's computer as it's displayed on the alert Preview. This is due to how the HTML text is rendered by the Teramind Agent. For security reasons, we have restricted the use of some tags and others are rendered a bit differently than a typical browser.

12.2.1 Using Images / Icons in the HTML Alert Template

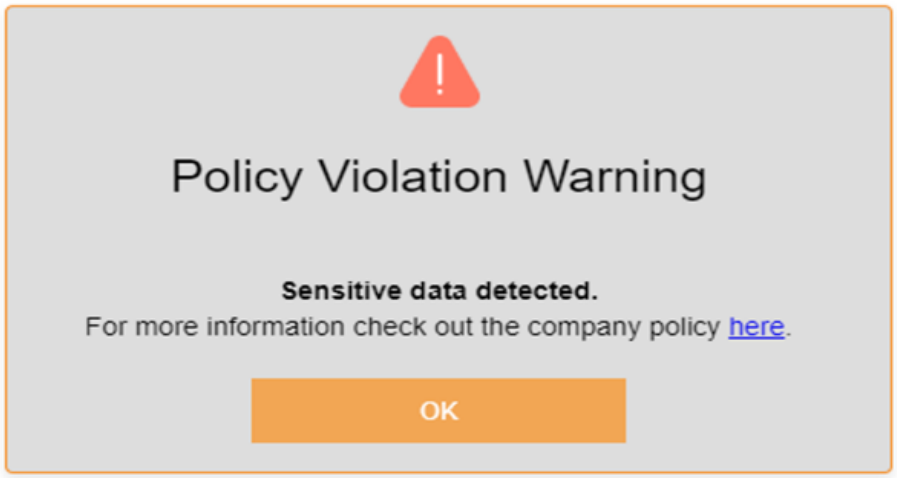
You can use Base64 encoded images in your HTML, for example, to show your company logo, a warning sign, etc. You can, of course, use the <img> tag to load external image files too. But be warned this might not work if the user is offline or the image resource is not accessible from the user's domain. Base64 is better as it will directly inject the image information in the HTML itself without requiring an external file.

Here is an example HTML code for using a warning icon on the alert message (insert it just before the `<div class="alert-title">` line from the previous example):

```
<img style="width:40px; height:40px;"
src="
+Z//+ZzP+Zmf+ZZv+ZM/+ZAP9m//9mzP9mmf9mZv9mM/9mAP8z//8zzP8zmf8zZv8zM/8zAP8A//8AzP8Amf8AZv8AM/8
AAMz//8z/zMz/mcz/Zsz/M8z/AMzM/8zMzMzMmczMZszMM8zMAMyZ/8yZzMyZmcyZZsyZM8yZAMxm/8xmzMxmmcxmZsxm
M8xmAMwz/8wzzMwzmcwzZswzM8wzAMwA/8wAzMwAmcwAZswAM8wAAJn//5n/zJn/mZn/Zpn/M5n/AJnM/5nMzJnMmZnMZ
pnMM5nMAJmZ/5mZzJmZmZmZZpmZM5mZAJlm/5lmzJlmmZlmZplmM5lmAJkz/5kzzJkzmZkzZpkzM5kzAJkA/5kAzJkAmZ
kAZpkAM5kAAGb//2b/zGb/mWb/Zmb/M2b/AGbM/2bMzGbMmWbMZmbMM2bMAGaZ/2aZzGaZmWaZZmaZM2aZAGZm/2ZmzGZ
mmWZmZmZmM2ZmAGYz/2YzzGYzmWYzZmYzM2YzAGYA/2YAzGYAmWYAZmYAM2YAADP//zP/zDP/mTP/ZjP/MzP/ADPM/zPM
zDPMmTPMZjPMMzPMADOZ/zOZzDOZmTOZZjOZMzOZADNm/zNmzDNmmTNmZjNmMzNmADMz/zMzzDMzmTMzZjMzMzMzADMA/
zMAzDMAmTMAZjMAMzMAAAD//wD/zAD/mQD/ZgD/MwD/AADM/wDMzADMmQDMZgDMMwDMAACZ/wCZzACZmQCZZgCZMwCZAA
Bm/wBmzABmmQBmZgBmMwBmAAAz/wAzzAAzmQAzZgAzMwAzAAAA/wAAzAAAmQAAZgAAMwAAAP93Yf/29P/6+f93YP94Yf9
7Zf9/av+IdP+Rfv+ypf+6rv/Mw//q5v/t6v/u6/94Yv93Yv99aP+AbP+Bbf+EcP+Lef+Whf+ll/+toP+1qf+4rf+7sf/B
t//Hvv/Sy//Z0//j3//m4v/r6P/s6f/y8P/9/f/+/v///yH/C05FVFNDQVBFMi4wAwEAAAAh+QQFAAD/ACwAAAAAAAIAA
gAI/wD/CRxIsKDBgwgTKlzIsKHDhxAjSpxIsWLEbduwocOmkWNHj9ywWRxJsqTJkyhTqlzJsqXLlzBjRtzosabNmzg5bp
PJs6fPn0CDCh1KtChBdDRzKl2KE6nRp1CjSp1KtapRplizLrXKtavXr2DDAs2otaxZm2LTql3Lti3Xs3Dj1nRLt67du3g
hyt3LN6/fv4ADWz3Ht/BeboITK17M+CRhw5DlnmtMubLlyiEja5a787Lnz6DXJt1MGm7o06hTPy3Neq/q17BjqyTbuvZZ
dLJz69690LbvuLyDC4/9uzjw4ciTVzbO/Kzy59D9Np9uNrr162qpa9eKGLv371K3i//Hihu8+fM/x6tnir69e5br4yt9T
78+Rfn4c9rfzz9h/v839SdgfwAWONeACLpHm4EFJuggeAxGyNGDFFonoYQVZojchRdq6KFuHHL44YiqhRgiiSh+ZmKI5a
Xo4mIrmvjijInFKCONOOJlo4kt5ujjWjuu2NmPRIYV5IpFJunVkTEq6eRUozEp4pNUFiVlk1VmCVSUV0o4pJZgvsRllxi
GaWZLZMb45ZlskvRYmje2KadFcNo4550SZVZnnHj22dueWPopqEF6AnrioIgOZKidiQ5a6KJTNuonpIxKeuejlHZo6Z2Z
```

```
VrrpmZh2WuanZ4rqKalZhmpqhKiGueqprSr/qeqrDMZaJa2w2urjrLgaqKuSveb664u8BtvgsD4aKyyyIxarLIDM0vjss
tFW6Oy0/1WbIrbUaovgtdzm5+2H4XY77n7glovfuRWqay677qXrrnzwJjjvu/WCJ++98eVLIL+B+vvevgCvJ3B9BeN7sH
IEJ6zewu05rDDEwTUs8XgUQ3hxwBlDZ/HG4nV8HcgTi6zaxyRvZ/JzKZe8Mmgot6zdy8PJ7DLNmNnMMc6w6Xwzz4rF7DN
1QBM39M5Ffyb00dMlnRrTPzt919JQNyc1aFVHfXVbVGfN3NaWea012GJ1LbZxZDN29thpd2X22sW1LRjcbMs91dt0/2a3
dHkj/733Wnj37dvfdgleN+FCBW64bYi3tfjhjfek+OO1RZ4W5ZBb/tLkmLem+VedZ/65SqGLPjpKpZt+Okmpq746na37/
Xp6scs+e0+1u367Q7nrvjtDvfv+O0LBCz+8QcUbf7xAySu/fPPO/w599LtPT/3r1l+/evbaf85995p/D37jBbMDjz3kaA
MAANngM8476QC8fEr8umNPP+vnrz8A2tTzDb/zM8m91DEOf+zvgPnTxjzeVK4AlmRe7SAHAieYv3uoY14OhJ263JENCno
QAPr4n7oyWBF3taODH/QgObzhLhJKxF3q0EcKU3gPBmLLhRFxlz1mOMNwtBCHDXGXO/94OMNsXLCBQASeuu5BxBnO44dJ
JJ66vmHAJn6QHzacVhT9o65wWHGG7oDiFhWlwy+mUB5iHOM/5mUOM37QHhhU4xrddY4qunGC+IijGufljTuq8F57nNc6/
EjBcgByjPcaJCERaMhDJpFfilzk/hqpRyBCUpIHpGQlSQiwSGJyfZpMYwY7+Un9hVKU8yuYJz95yhG6UJWlzF8rXenAhK
0Sk7NEYi1hGUsA5FKXz7NlL33psF3yMpa/BKb0HHZLSSYzXKlk5jCfCc3hXayZi6Qmt453zWlubJkSwyYhtbnN6nWzl+Q
sJ/Y2Jk4/pvOGswNZO+/4TniejmTzdGM9tbj/PXl6k2T3xOc/QRZQf6KzZd5LWT7NuE97Rq5lC/1iQx1KOJlF1IoT5Sf5
IDrQlG2UoweV2UcV2lGP/o1znbpoEzNK0bbpTKVEZGlLwYbSlJbUpHLzGUx5KNOZSq2mNg2pznKq05silGxADSoyj5a2o
+10hj1V50+datSjXo1pT01hVKVatKSKKqsf3KpPaQY1sHpQrGM1mVe/WlWRJq1qZi1k1roK17a6lWdZi+sE0cpVtebVrn
d9mdf0ykix0WytqyJsJg0r2MEC1mYrQ2xiHxvYjJ1NsZNcm8gkO1mhek1ka8OsKeGWMc52dqmapRjcRCtLukHMtKctJV9
RCS+6/7EWlHk7GGxjy8rcCixvtyWmb+u1W97ism/+6ltwZ+vIcxXXuM4UXL0Et1zDseu50M2mdc9luOpuV1vYze44Fzeu
xXn3u8wKr3jd+ThtPe686P2VetdLT8pFi3LwjW+s5ktffWIOWZjLr35Jxd/+MrRzv+qcgAdsqQIbWKKhs1XoFszgRDn4w
RgtXatKR+EKC+rCGF5p6kiVug57GE8gDnFMW7ep1pn4xHJKsYp5GjtJxe7FMAbVjSmLXETVDsc5BpOMXwVk6Qoqd0U2Mo
qRzGMlc4rJnq3xpXqXZCe3KXhVtrKZipflHl8Zy00mL5uS12Uvb5nLYRazq8ic5iD/qP95Zdbyk6AXZzPfCs5tVjOVpld
nOzuJz3nWM7AAHeXi3ZnOgRY0kbLXZzkny3qNdrS0GJ1oReeIe5GWtIu+l2k/T5rShYbemzld6fY+GtOlNvWnUR1qUeNI
fNjotJsdBOtYp1rVm4a1rGc9oFrbutXTe5Gvd81r/vj616it9baGfev/jujYyJYttEkEbWJbmtbVbrazNQTtaPe229zut
rWv3WtxaxvBFOo2R8ZNbmOrm93tRpi6vX3ceT9o3vSOLr7thW94x9s9+M63dgNe7n6fW8MCCrjAx6vwfwXc37iW98MPPm
L7KHzdFEe4xCcO7GnT5+IY7/ixN87xZF/8PSD/D7nJGw7wlEMc3edJucqlLfOIyfzlMP+OzGf+7ZqbZ+cLZy/QNbZznOd
8ZEA3+tGhA3Se13vo2Gl60OsrdaQ3XelLT47Up+7frUdn61w/sNeZvnWsR1g5YA87hMHOMrCb/ezDGdPNM548raf97XDn
jdznLnKQ1yztas8w4EWi98HjPe+5GXzgRaz43ey96HR3deIVf3iNw+bxkO+7z41G+cgH+/KKd7q+Q8/5zmt+56/BfNI9/
/mnhV70A3894U+j+tWfHvWokT3sGa572ut+8Sv+/Wl+D3waEx80tb8667OHNeJXPneeSb7yb990zxB/90K/vmWkP/2V93
451y8+/1TDP6HGcL/7NA8/Zcgvfq2yf/aJOT/6e65+GLH/+YaO//vxHzzFvL/9YfV/8OcX8id1/Nd/gSGAB4iABKiAy+d
rgCGA2KAOw7QPEjiAdVGAW9cNw5QPF8g3Eqg+sXQPF4iBbaGBYIcPvVQPJagjJVgPvfQOJWiCaoGCYPcOsdQP7DCDhTOD
3YBCmESCM0iDYWGDaScOpRRGQ0gXQ8gR6sAPmARHTUiEXmGEgIeDi6QN7TCFVNgVXMgR9LBI8PCFXVgVVjh458BEd0QPZ
FiGVNGG2NAN4+BGCwSHaXGGrxcP+ENE2SCDcOiGUfGHHgEOavhB2kAP6yCI5fcVePh77v8wDkC4P+ZADyKkiIB4FZZYE+
cADu8wD/RAD/LwDluYiQfSFY1IilMIOqi4ilphiqz4iuzxFrA4i/phhrR4i2hRFbi4ix5BFafIixL4hsDIi1Lxi8MogOF
xjMT4FMaojP8HFc4IjEbRjNH4fphYjbtIFNgojUOxjdwIFN74jbQTjtk4juSIi+B4jsvIE+oojjHRju7oEvAYj2gyj+so
j/Z4j/WYj+W4j/yIjvj4j/1IOgKpj6hTkAb5QAiZkKwzi+kgDhAZkRI5kRRZkRHpQ7RIP7S4gCmnkbPIkR0pQLcIkn4nk
hv5gN83ErtIkiWpkrjIki15HyuJkikpky9JkzX/mUO8CJMxqZMzSX2KOBHDyJM9yTvASJRFuRALcpNAGZR6MZQ4eXwOQY
0O2JROGUTHiJQhqZTKqJVJiTxdGZXa9ydZKZZSyUVhaZWZqBDR6JVbeRBtaZZnCZbO6JZvSRDVaJdfmZdyOZdkFJdqmYk
9wjx8GZhrWRDYqJc9uY2KeXJ4mZh9OZaEWZjep4yPWY3dEA+auZmc2Zme+ZmbOYbbOBBUuZCwOBBDZpr19w+pqZpj6Zqm
OZmwKZCyOZv8WJu2aY//kEW5CY+s2Zv/+A+lCZxBSZy3aZz5OEfI6ZvLOY/K2Zzn+JzQGY7SOZ2jaZ3RiZ3kWJ3a6Yzc2
Z3H+J3g/ymN44mN4lme6Iie0Xie6jmLuNmet/ie8Ome7DmfpNgZ9rmM+YmL+LmfGfmX/smKlxmgqzigBCqYBnqgVwmgCi
qIdNmgDoqYELqgArGUE8qFUnShZJihGoqhB9GaHVpxHBqiLYiWJFqiJnqiz0iWKrqibNmiLsqiMCqZCzGcM/o9D3GjNMo
QNqqjzbMmSuSjpOeTQgp43UGkRTp2L5SkbFdCTFp1TvqkuKdBUvqVSFql9lYSFoqlI3cSXDpvQOqSX9qlHjmm4gMfZgpr
/pimrYembCp5AfmmDAgTcjqnMMGbdbptPAGieQopQdGnlucTfAqoaTKY5kiodBOmh4qoYoVjqELBqKmVjJAKNVYxqUzjh
ZZqM4pajJlqVarYqQ7jqF6xpaBKSzVYqs3lOKgaLpsKJKv6LIDRo69aIK2agbNqKqL6F7J6q9uRq3PDq3sSGrsKrLUxGS
VCrDFypKWHrAbiq8vKrOrhrLxBqtD6G7X6HNRarZGBIOigJ9wwrF/KJcbKFgEBADs="/>
```


And here is how it will look:



There are many online resources available that can convert an image to Base64. You can search for the term 'base64 encoder' to find these resources.

12.2.2 Configuring Other Alert Options

You can configure other settings such as alert delay, the maximum number of alerts shown, alert time out, etc. from the Alert settings screen. The table below explains what those settings mean and when to use them:

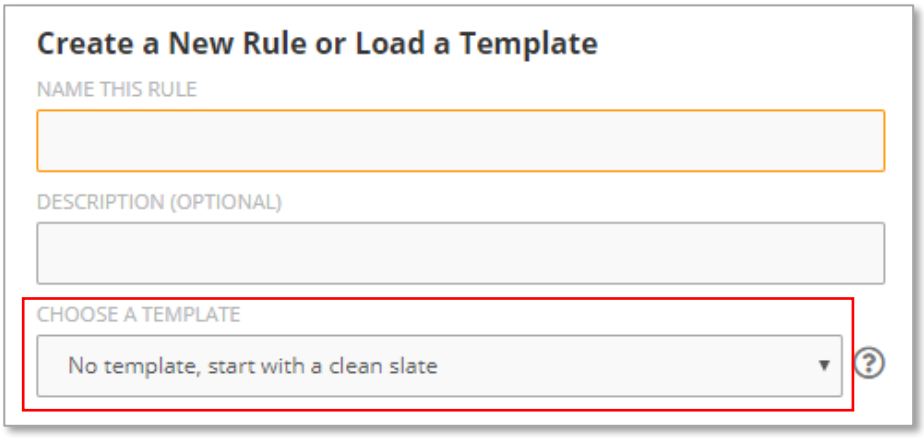
ALERT EMAILS LIMIT	The Notify action sends out an email notification to the selected user(s) when a rule is violated. This setting defines the threshold where the system will group these notification alerts into a single email. The system will send these many identical alert emails, and then it will group them into an email digest. If set to 0, Teramind will send each notification alert as a separate email.
USER ALERTS THRESHOLD	This setting 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.
LOG ALERTS THRESHOLD	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.
MAXIMUM DAILY ALERTS COUNT	MAXIMUM DAILY ALERTS COUNT limits the total number of alerts that get logged by Teramind on a daily basis per alert type. You can also set the alert limit at the rule level from the rule's

	Advanced Mode action panel (*Choose maximum number of saved alerts per day*).
ULE TASK SELECTION ACTION TIMEOUT	You can build rules in Teramind to set a user's task based on their activity. RULE TASK SELECTION ACTION TIMEOUT (SECONDS) defines the time out when switching tasks. If the user switches activity and remains in the new activity for the defined seconds, the rule will be re-evaluated.

13 Using the Prebuilt Rule-Templates

13.1.1 Using the Regular Rule Templates

When creating a new rule, you can choose from a list of pre-built templates. Click the **CHOOSE A TEMPLATE** pull-down menu to choose a template on the Rules Editor's *General* tab.

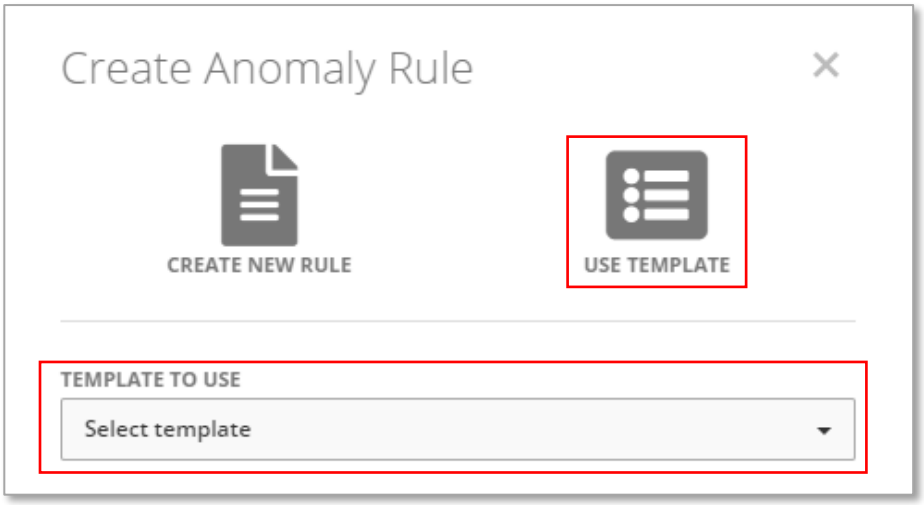


Teramind has many templates for Data Loss Prevention, Email, Applications, Websites, File Operations etc. Once you select a template, the rest of the rule's tabs will be automatically populated with pre-configured settings and sample data. You can, of course, change them to meet your needs.

Check out the Appendix section for a list of all the prebuilt regular rule templates available in Teramind.

13.1.2 Using Anomaly Rule Templates

When creating a new anomaly rule, you can choose from a list of pre-built templates. Click the **USE TEMPLATE** button, then choose a template from the **TEMPLATE TO USE** pull-down menu to choose a template.



Teramind comes with many anomaly rules templates. You can choose from a list of types such as: Applications, Emails, File Operations etc.

Check out the Appendix section for a list of all the prebuilt anomaly rule templates available in Teramind.

14 Enforcing the Rules

14.1 Automatic Enforcement

When you create a new rule, by default it's automatically turned on. You can edit a rule even when it's running. Any changes you make to the rule will be enforced immediately if the user is online and connected to the Teramind server or as soon as they connect.

> It's always a good idea to test a rule when you create or edit it to see if it's working as intended. You can do so by checking the Alerts Report.

Rules are enforced depending on what type of Teramind Agent is installed on the user's computer:

If the user is using a Stealth Agent:

- **Regular Rules:** The rule will be enforced according to any Rule Schedule you have setup or for 24/7 if no such schedule exists. The rule will be enforced even if the user is offline or disconnected from the Teramind server.
- **Anomaly Rules:** Since an anomaly rule does not have a schedule, it will run for 24/7.

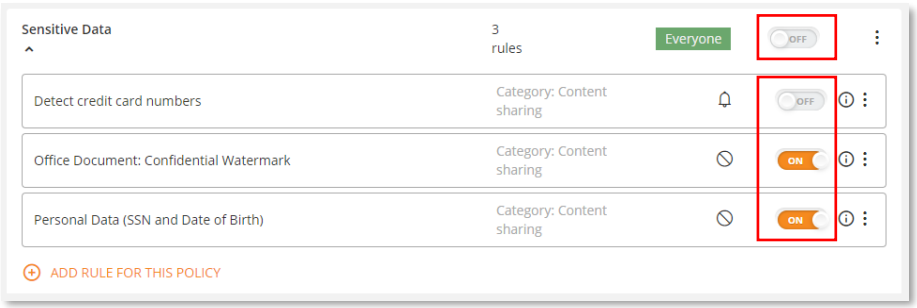
If the user is using a Revealed Agent:

- **Regular Rules:** The rule will only be enforced when the user has logged in to the Agent and clicked the **Start** button to begin their shift. The rule will still follow any Rule Schedule you have setup. The rule will continue to be enforced until the user clicks the **Stop** button to end their shift or as soon as the rule schedule has ended – whichever comes first.
- **Anomaly Rules:** Since an anomaly rule does not have a schedule, it will run until the user clicks the **Stop** button on the Revealed Agent.

14.2 Manual Enforcement

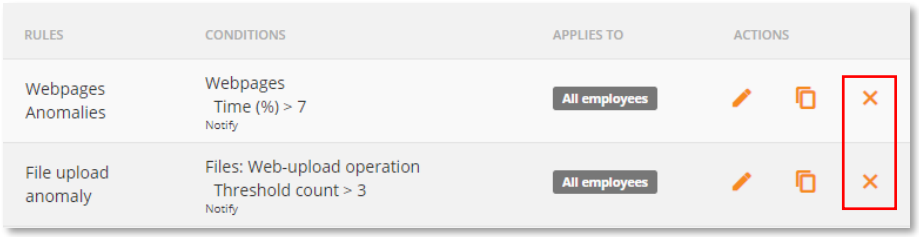
You can manually turn a rule on/off from the Teramind Dashboard. To do so:

- **Regular Rules:** You can manually control the rules from the *Behavior Policies* screen. To access the *Behavior Policies* screen, click the **BEHAVIOR** > **Policies** menu.



Use the ON/OFF button next to a rule's name to turn it on or off. You can also use the ON/OFF button next to the Policy's name for which the rule is a part of. If you turn off the policy, all rules under the policy will be deactivated even if the individual rules are turned on. If the policy is turned on, the rules that has the ON status will be activated and the OFF rules will remain inactive.

- **Anomaly Rules**: The only way to turn off an anomaly rule is to remove it from the *Anomaly rules* screen. To access the *Anomaly rules* screen, click the **BEHAVIOR** > **Anomaly rules** menu.



Click the **X** button besides an anomaly rule to remove it.

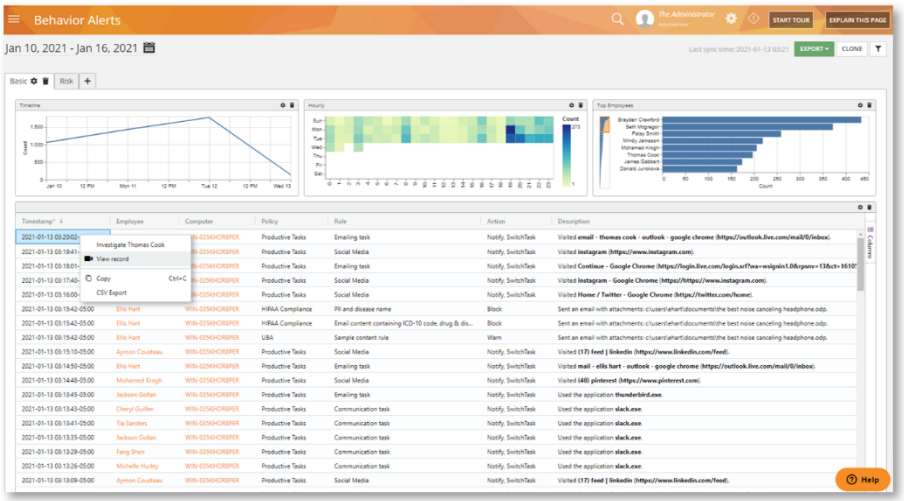
15 Investigating the Rule Violation Incidents

There are multiple ways you can investigate rule violation incidents on Teramind.

15.1 Using the Behavioral Alerts Report

This is your primary source to view all rule violation incidents. You can use the Alerts report to view a list of rule violation incidents with all the necessary details, such as: the date/time the incident happened, the user or activity involved and other pertinent information. You can also view a session recording of an alert, export the alerts report or schedule it for auto delivery to selected email addresses.

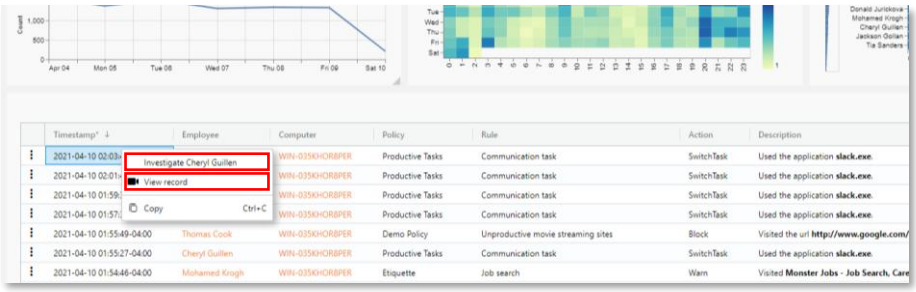
You can access the Alerts report from the **BI Reports** > **Behavior Alerts** menu, under the **Basic** tab.



For more information on the Alerts report and to learn how to use its different features, check out the BI Reports > Behavior Alerts section on the Teramind User Guide.

15.1.1 Using the BI Report's Investigate / View Record Feature

On the Behavior Alerts screen, you will see a table/grid widget. If you right-click on row, you will see a pop-up menu:



1. Click the **Investigate** option from the pop-up menu to view the Employee's Activity Monitoring Report report. From that report, you can see all the alerts for the employee under the *Alerts* tab.

2. Click the **View record** option to view the Session Recording of the employee at the selected timestamp.

15.2 Using the Alerts Log Widget

You can also add an Alerts Log widget to your dashboard. The widget allows you to view the most recent alerts in real-time or for the selected date range. You can add the Alerts Log widget to a dashboard by clicking the **ADD WIDGETS** button on the **Dashboard**'s screen.



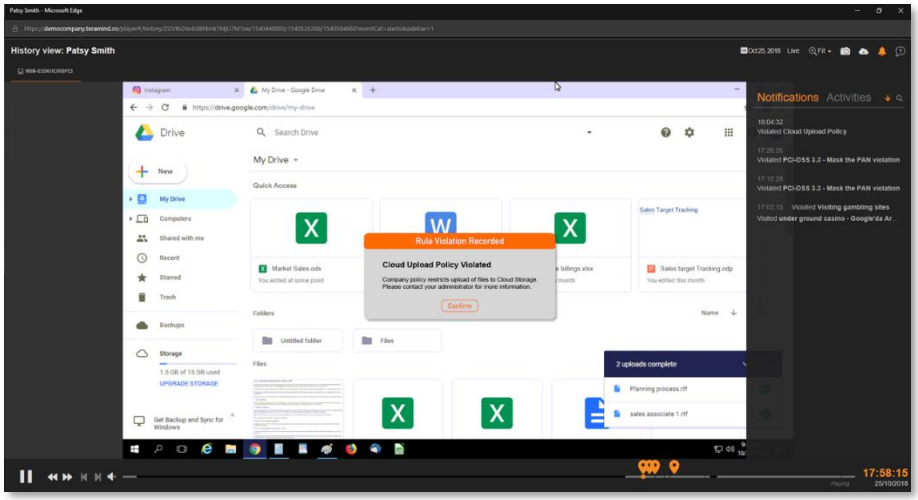
For more information on the Widgets and to learn how to use them, check out the Dashboard Widgets sections on the Teramind User Guide.

15.3 Using the Session Player

Session Player allows you to view a user's desktop in live view or history playback mode. You can precisely locate when a rule violation incident occurred, check out all the alert notifications the user received and investigate the trail of user activities leading up to the incident. If the user is online, you can take remote control of their computer or freeze their inputs to prevent further incidents.

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 take snapshots of the user's desktop, forward the recordings to select email addresses or download them as MP4 files.

You can access the Session Player from the BI Reports, from the Employee's Activity Monitoring Report or even from the Dashboards. Click the **Movie Camera** icon, wherever you see it, to access the Session Player.

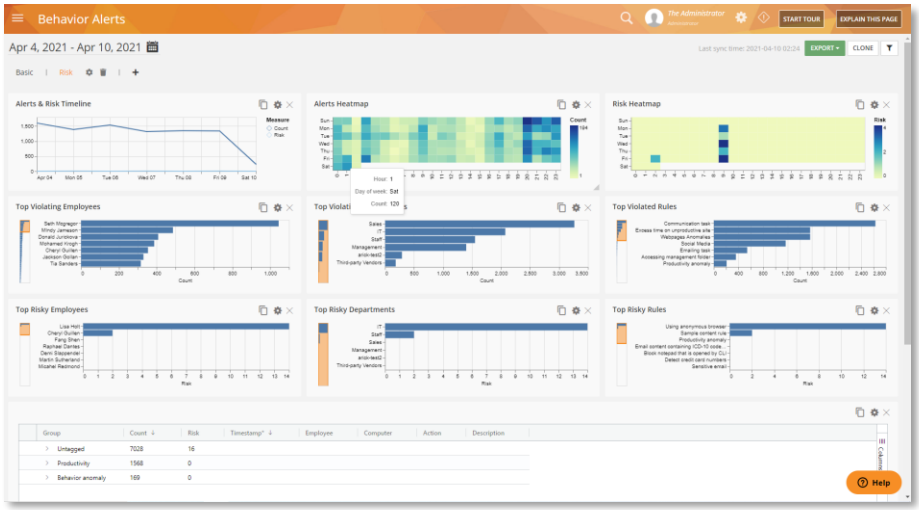


For more information on the Session Player and to learn how to use its different features, check out the Session Player section on the Teramind User Guide.

15.4 Using the Risk Report

The Risk report allows you to analyze the impact of rule violation incidents and the risks they pose to your organization. The report shows top risky rules, users, applications and websites. You can drill-down each risk category to further investigate what caused the risk level to change. You can also plot the risk trend by department, severity, number of violations, tag etc. Unique risk scores help you identify high-risk rules or users so that plans can be developed for treating the risks.

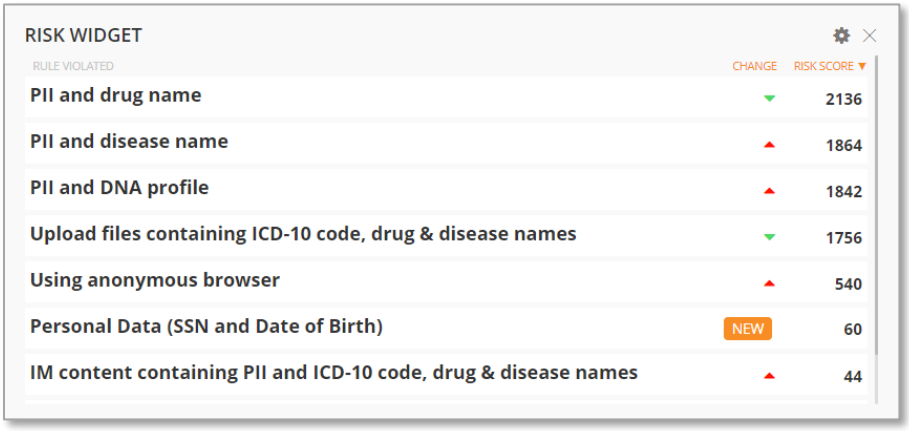
You can access the Alerts report from the **BI Reports** > **Behavior Alerts** menu, under the **Risk** tab.



For more information on the Risk report and to learn how to use its different features, check out the BI Reports > Behavior Alerts section on the Teramind User Guide.

15.5 Using the Risk Widget

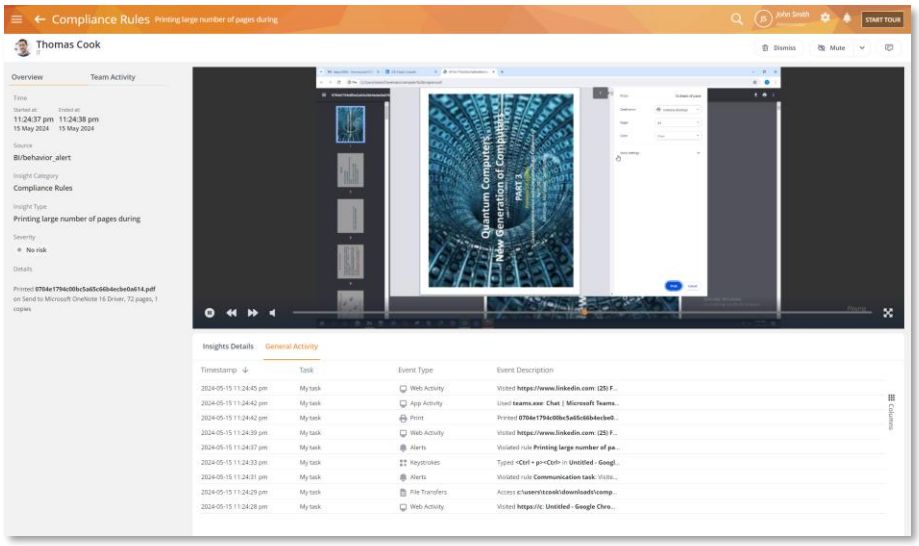
You can also add a Risk widget to your dashboard. The widget allows you to view the most recent risk trend and risk scores for users, activities or rules in real-time or for the selected date range. You can add the Risk widget to a dashboard by clicking the **ADD WIDGETS** button on the **Dashboard**'s screen.



For more information on the Widgets and to learn how to use them, check out the Dashboard Widgets sections on the Teramind User Guide.

15.6 Using OMNI

You can use the OMNI dashboard to have a snapshot view of the most critical insights and incidents about your organization in a social media-like interface. You can view behavior alerts and drill down to investigate what activity caused the rule to trigger.

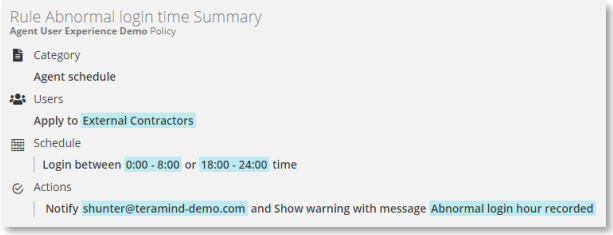


OMNI also features threat detection and abnormalities identification. To learn more about OMNI, please check out the OMNI section on Teramind User Guide.

16 Sample Rules Walkthrough

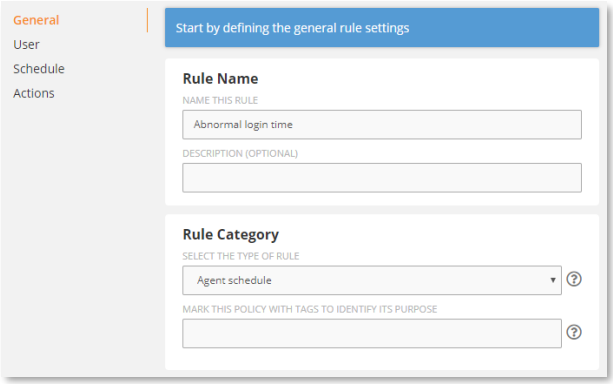
16.1 Rule Sample 1: User logs in during off hours

16.1.1 Rule Summary



This example shows how you can create an Agent Schedule rule to detect a user attempting to login during off hours.

16.1.2 Setting up the Rule



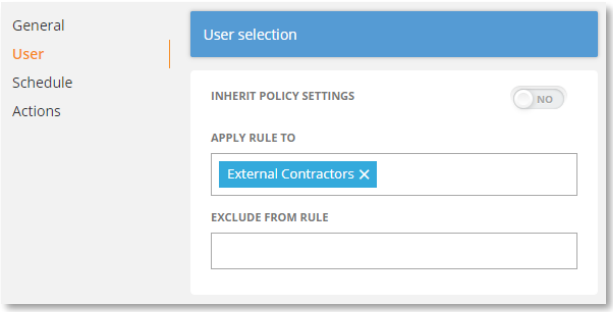
General

On the first tab, General, we assigned a name for the rule and a description.

We have chosen an Agent Schedule rule type since we are looking to detect a user's login time.

To learn more:

- Agent Schedule Rules: What Schedule Violations Can You Detect?
- Understanding Common Rule Elements - names, description, tags, schedule etc.



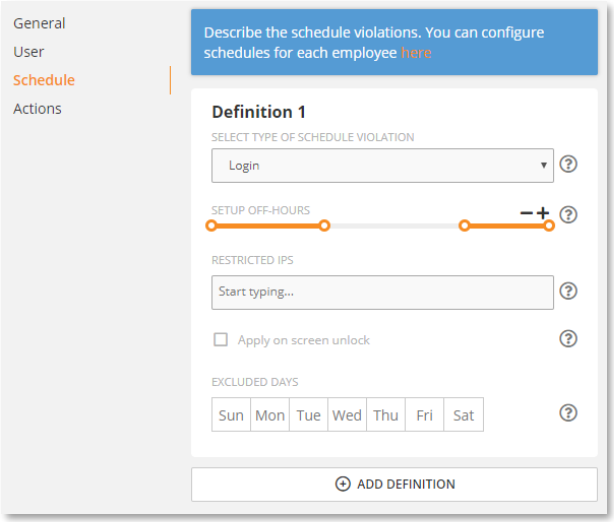
User

For the users, we choose to manually add the users (by turning off the INHERIT POLICY SETTINGS). We also decided to apply this rule to external contractors only. To do so, we first created a department named 'External Contractors' and then edited the selected users' profiles and assigned them to this department.

To learn more:

- Defining Users

- Creating/Editing Departments
- Creating/Editing Employee Profiles



Schedule

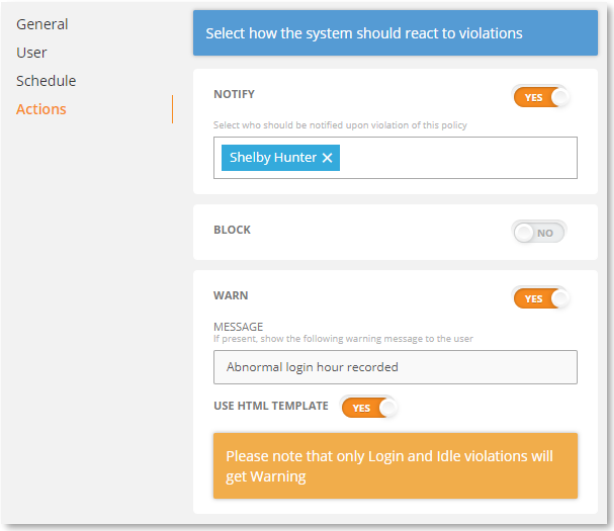
We have selected the Login schedule violation type so that we can monitor the login attempts.

We have also setup two time slots that will be considered as off-hours (12am-8am and 6pm-12am). Any attempt to login in these two periods will trigger the rule.

If you wanted, you could setup additional options such as restricted IPs or exclude any days you don't want to monitor.

To learn more:

- Rule Criteria – for Agent Schedule rules



Actions

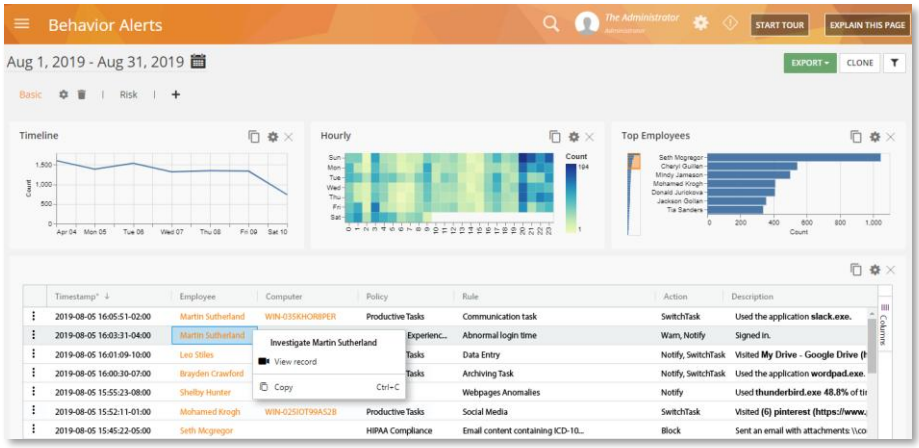
Finally, for the last tab, 'Actions', we have selected to use a NOTIFY action to notify the security admin and WARN action to show a warning to the offending user. For this last action, we decided to use the HTML template option to make the alert prominent to the user.

To learn more:

- Defining Rule Actions
- Customizing the Rules Messages and Alerts

16.1.3 Viewing the Rule Alerts

Click **BI Reports** > **Behavior Alerts** then select the **Basic** tab to view a report of all rule violation alerts and trends. The 'Grid Widget' located below the screen shows a list of all the alerts:

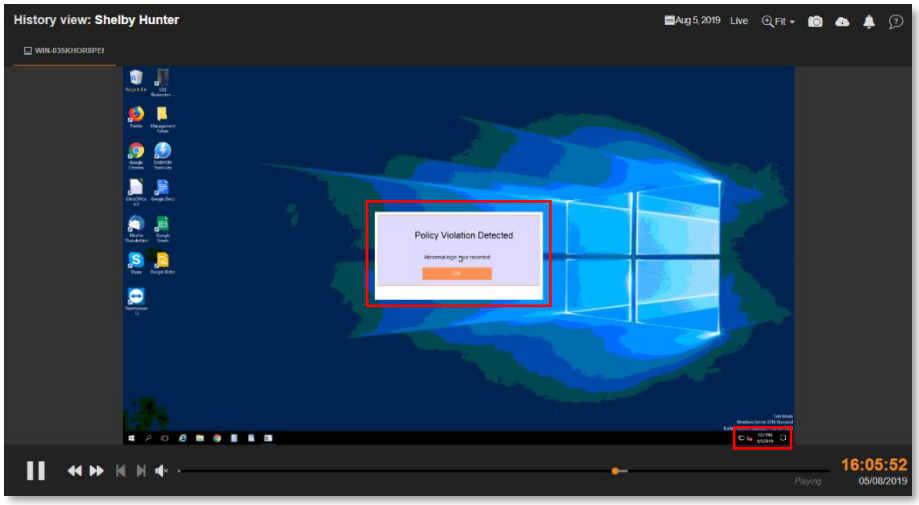


You can see that, on 2019-08-05 at 16:03:31, employee Martin Sutherland signed in. Since the action meets the rule criteria (Login: between 12am – 8am and 6pm – 12am), it is triggered.

*Right-click on that row and then select **View record** to view the Session Recording of the alert.*

16.1.4 Viewing the Session Recording

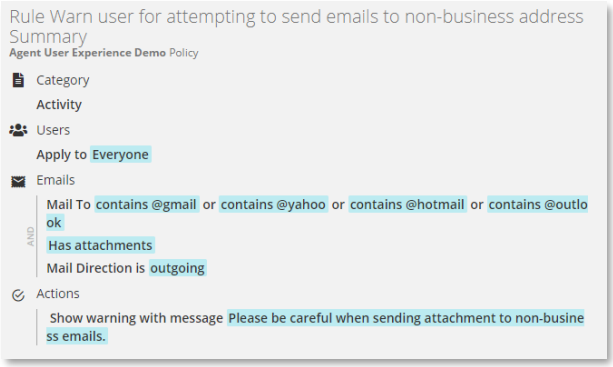
Here you can see the Session Recording of how the rule message will look on the user's desktop:



When a user logs in outside our set schedule, they will see a warning message. Note that, the login time is based on the user's local time.

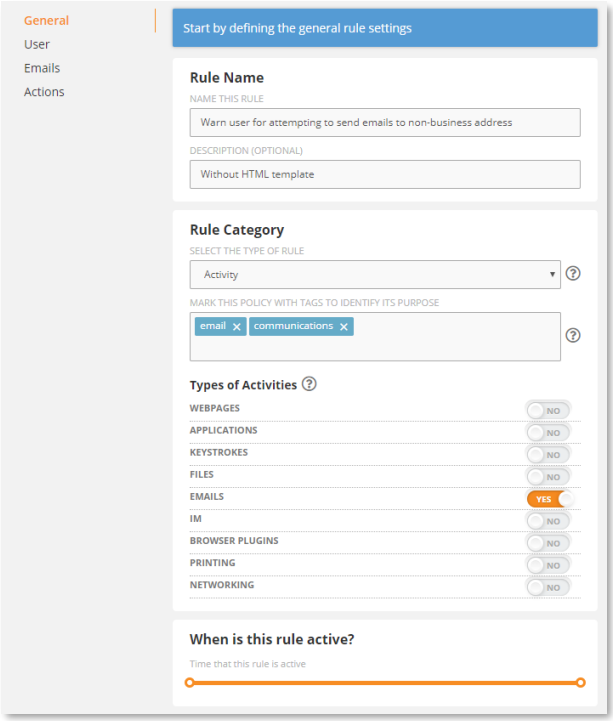
16.2 Rule Sample 2: User sending emails with attachments to non-business address

16.2.1 Rule Summary



This example shows how you can create a simple Activity rule to warn a user when they send an email with attachment(s) to a non-business email address.

16.2.2 Setting up the Rule



General

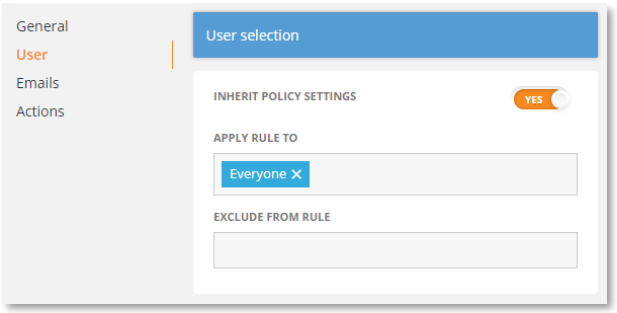
On the first tab, General, we assigned a name for the rule and a description. We also used some tags to identify the rule easily.

We have chosen an Activity rule type since we are looking to detect a user action (the act of sending an email) and not any content. We have selected **Emails** as the *Types of Activities*.

We left the rule schedule to its default 24-hour setting.

To learn more:

- Activity Rules: What Activities Can You Detect?
- Emails– emails activity rule
- Understanding Common Rule Elements - names, description, tags, schedule etc.

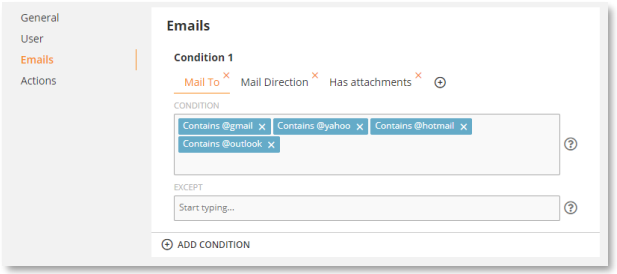


User

For the users, we used the default policy settings (by leaving the INHERIT POLICY SETTINGS option turned on).

To learn more:

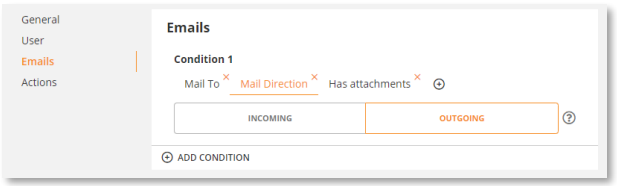
- Defining Users



Emails

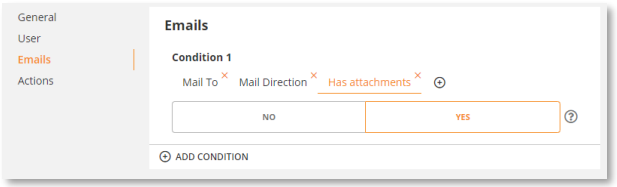
Mail To

We have added three criteria to the Emails activity. For the first criterion, 'Mail to', we have specified several email domains that we would consider as 'non-business' addresses and used a *contains* logic to detect even a partial match.



Mail Direction

For the second criterion, 'Mail Direction', we have selected OUTGOING to detect only the outgoing emails.

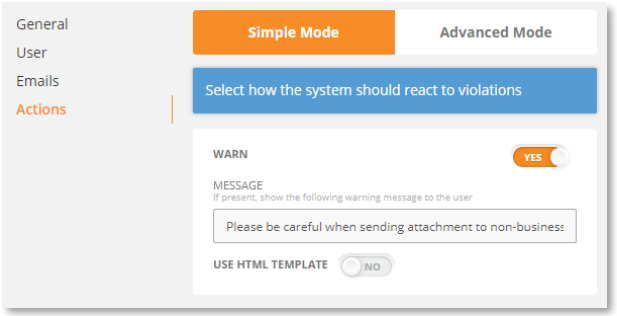


Has Attachments

For the second criterion, 'Mail Direction', we have selected OUTGOING to detect only the outgoing emails.

To learn more:

- Rule Conditions
- Rule Logic



Actions

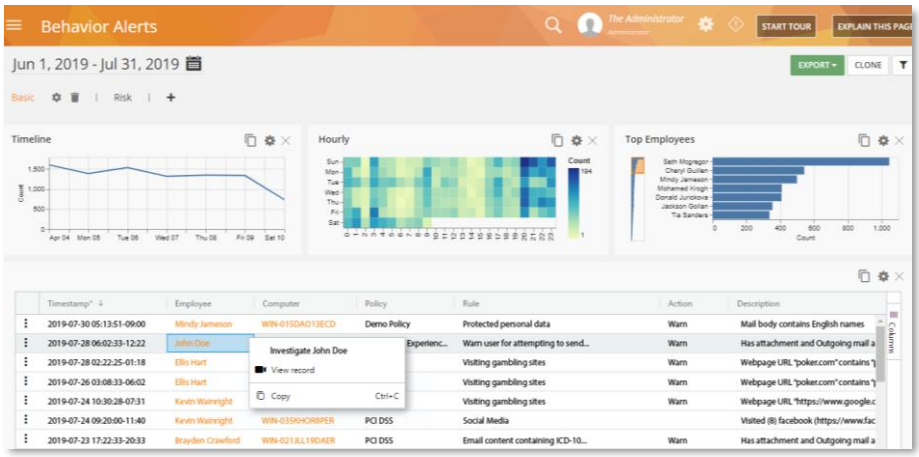
Finally, for the last tab, 'Actions', we have selected to use a WARN action to just show a simple warning to the user.

To learn more:

- Defining Rule Actions

16.2.3 Viewing the Rule Alerts

Click **BI Reports** > **Behavior Alerts** then select the **Basic** tab to view a report of all rule violation alerts and trends. The 'Grid Widget' located below the screen shows a list of all the alerts:

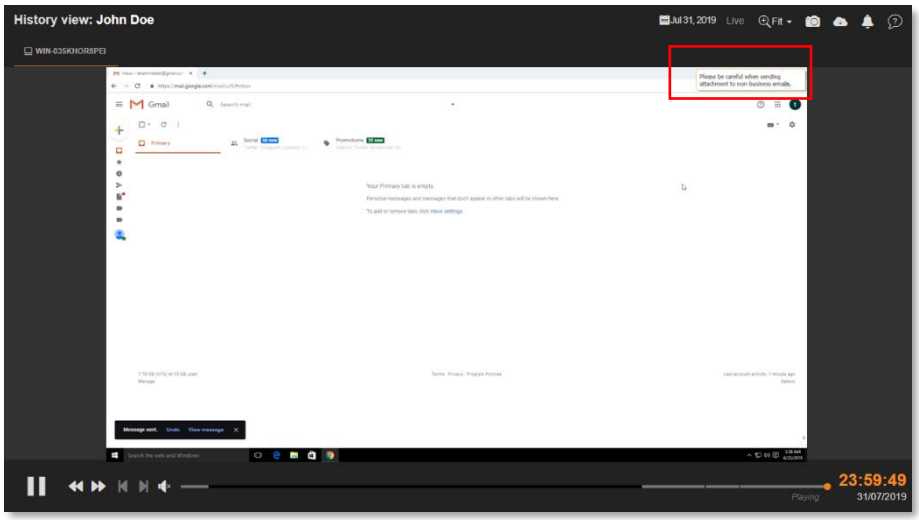


You can see that, on 2019-07-28 at 06:02:33, employee John Doe sent an outgoing email to a non-business email account and the rule gets triggered.

*Right-click on that row and then select **View record** to view the Session Recording of the alert.*

16.2.4 Viewing the Session Recording

Here you can see the Session Recording of how the rule message will look on the user's desktop:

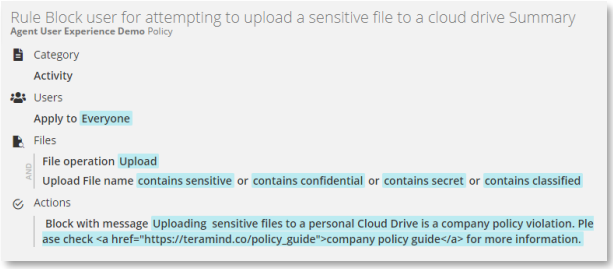


You can see that, as soon as the user sends an email to a non-business address, the rule's warning message is shown on the top-right corner of their screen.

You will notice that the message is very bare-bone and may fail to attract any attention. You can change that by customizing the rule messages and alert.

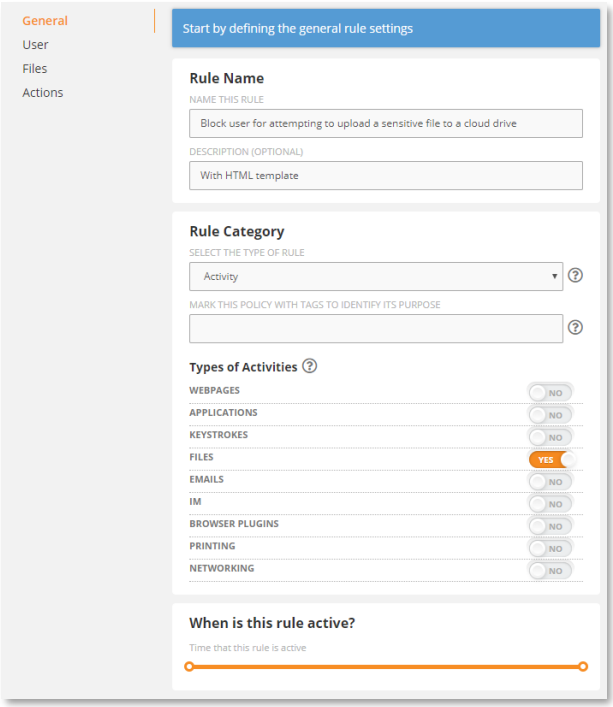
16.3 Rule Sample 3: User attempting to upload a sensitive file to a cloud drive

16.3.1 Rule Summary



This example shows how you can create an Activity rule to block a user and display a message for attempting to upload certain files to a cloud drive.

16.3.2 Setting up the Rule



General

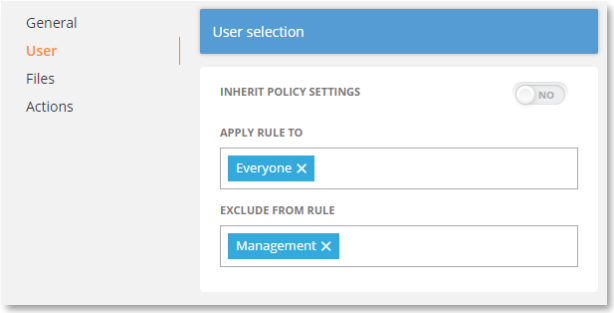
On the first tab, General, we assigned a name for the rule and a description.

We have chosen an Activity rule type since we are looking to detect a user action (the act of uploading a file) and not any content. And we have selected **Files** as the *Types of Activities*.

We left the rule schedule to its default 24-hour setting.

To learn more:

- Activity Rules: What Activities Can You Detect?
- Files– files activity rule
- Understanding Common Rule Elements - names, description, tags, schedule etc.

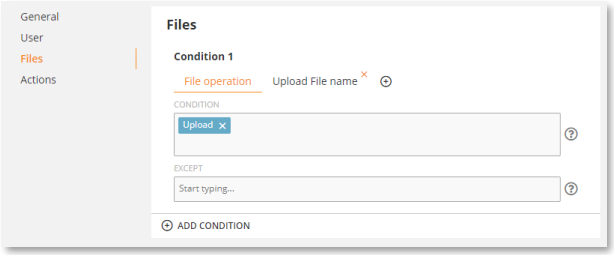


User

For the users, we choose to manually add the users (by turning off the INHERIT POLICY SETTINGS). We have also excluded the Management department from the rule's scope.

To learn more:

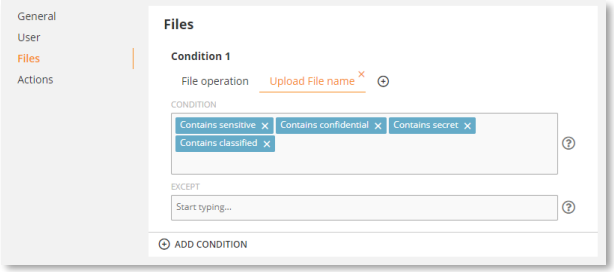
- Defining Users



Files

File Operation

We have added two criteria to the Files activity. For the first criterion, 'File Operation', we have selected the *Upload* operation.

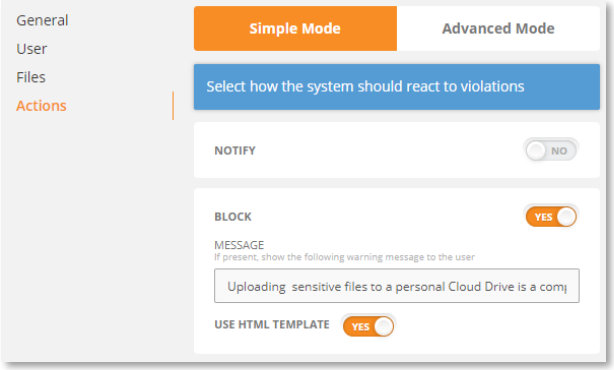


Upload File Name

For the second criterion, 'Upload File Name', we have specified some keywords that we would like to detect in the file names.

To learn more:

- Rule Conditions
- Rule Logic



Actions

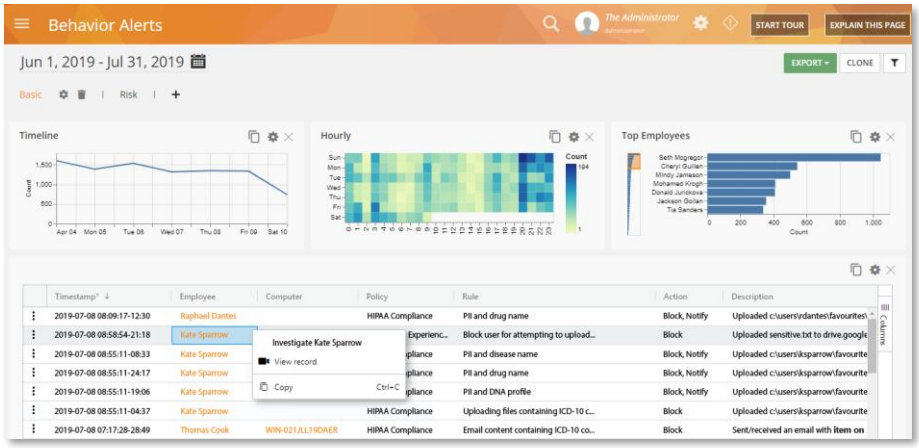
Finally, for the last tab, 'Actions', we have selected a BLOCK action to block the activity and at the same time show a message to the user. For this demonstration, we used a HTML template.

To learn more:

- Defining Rule Actions
- Customizing the Rules Messages and Alerts

16.3.3 Viewing the Rule Alerts

Click **BI Reports** > **Behavior Alerts** then select the **Basic** tab to view a report of all rule violation alerts and trends. The 'Grid Widget' located below the screen shows a list of all the alerts:

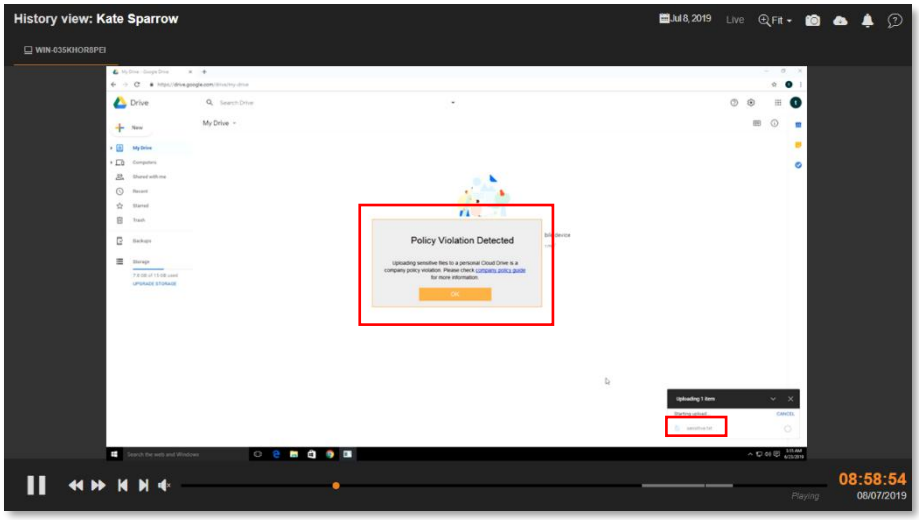


You can see that, on 2019-07-08 at 08:58:54, employee Kate Sparrow tried to upload a file to Google Drive and the rule blocked her action.

*Right-click on that row and then select **View record** to view the Session Recording of the alert.*

16.3.4 Viewing the Session Recording

Here you can see the Session Recording of how the rule message will look on the user's desktop:

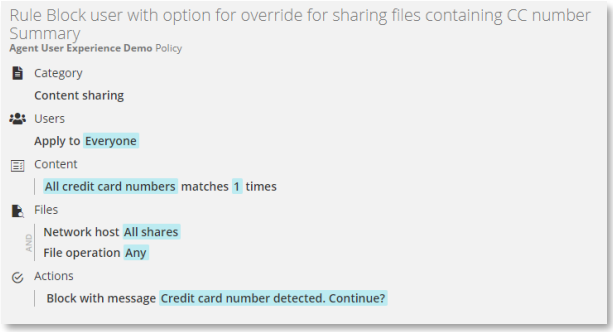


You can see that, as soon as the user attempts to uploads a file named `'sensitive.txt'` the rule is triggered as the filename contains one of our specified keywords, 'sensitive'.

The rule shows the message we specified, and the upload operation is blocked.

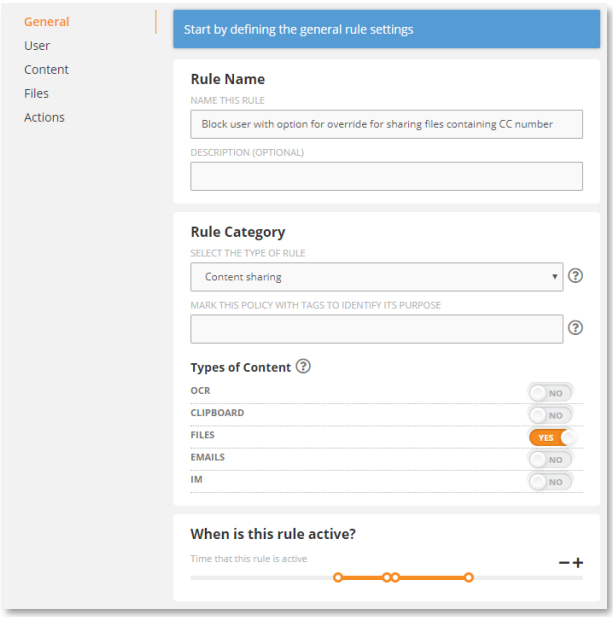
16.4 Sample Rule 4: User attempting to share files containing sensitive content

16.4.1 Rule Summary



This example shows how you can create a Content rule to block a user and display a message for attempting to upload a file containing credit card numbers. The user will be able to override the block action by clicking a 'Yes' button or cancel the operation by clicking a 'No' button. In any case, a rule alert will be recorded.

16.4.2 Setting up the Rule



General

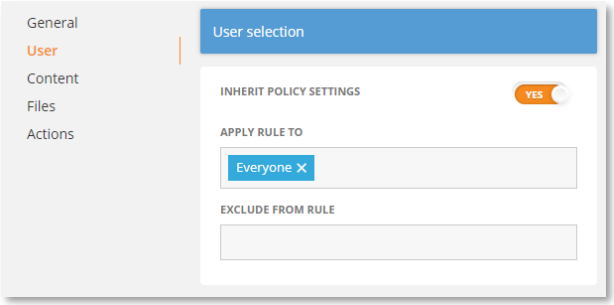
On the first tab, General, we assigned a name for the rule and a description.

We have chosen a Content Sharing rule type since we are interested in detecting sensitive content. We have selected **Files** as the *Types of Content*.

We changed the rule schedule so that it will monitor 9am-12pm and 12:30pm-5:00pm, a typical worktime taking into account a 30-minute launch break.

To learn more:

- Content Sharing Rules: What Contents Trigger the Rules?
- Files– files content sharing rule
- Understanding Common Rule Elements - names, description, tags, schedule etc.

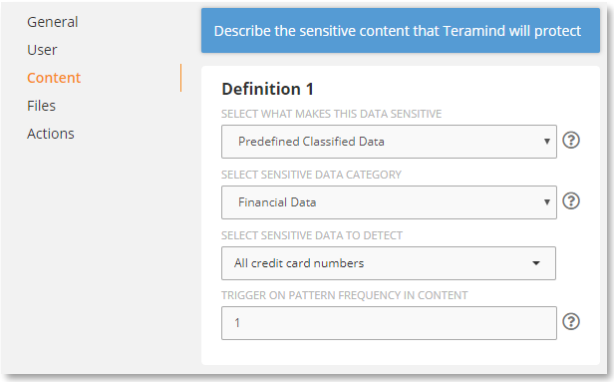


User

For the users, we used the default policy settings (by leaving the INHERIT POLICY SETTINGS option turned on).

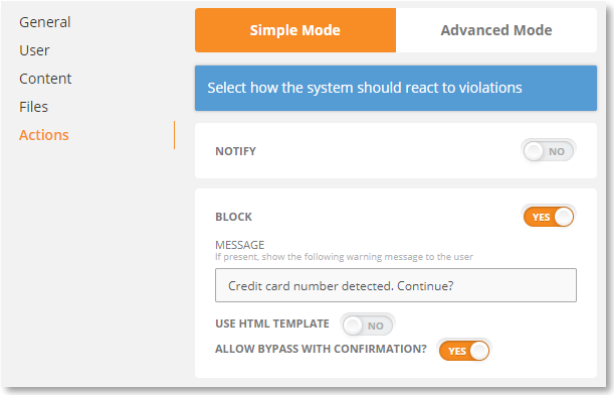
To learn more:

- Defining Users



Content

For content, we used a built-in template, 'Predefined Classified Data' and then sleeted the 'Financial Data' category to detect 'All credit card numbers'. The rule will trigger even if there's only one credit card number detected in a file. We did so by entering a value of '1' in the TRIGGER ON PATTERN FREQUENCY IN CONTENT field.



Actions

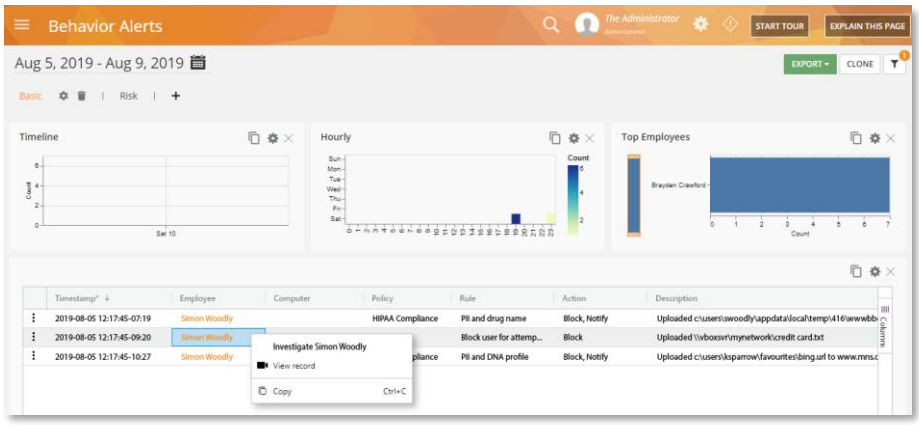
Finally, for the last tab, 'Actions', we have selected a BLOCK action. This will show a warning to the user and block the action.

To learn more:

- Defining Rule Actions

16.4.3 Viewing the Rule Alerts

Click **BI Reports** > **Behavior Alerts** then select the **Basic** tab to view a report of all rule violation alerts and trends. The 'Grid Widget' located below the screen shows a list of all the alerts:

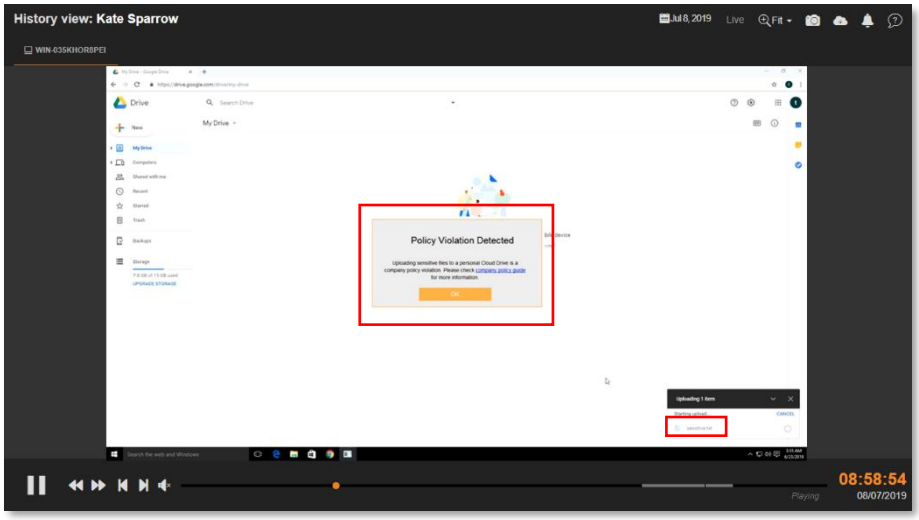


You can see that, on 2019-08-05 at 12:17:45, employee Simon Woodly tried to upload a file containing credit card data to a Box drive and the rule got triggered.

*Right-click on that row and then select **View record** to view the Session Recording of the alert.*

16.4.4 Viewing the Session Recording

Here you can see the Session Recording of how the rule message will look on the user's desktop:



You can see that, as soon as the user attempts to uploads a file named `'sensitive.txt'` the rule is triggered as the filename contains one of our specified keywords, 'sensitive'.

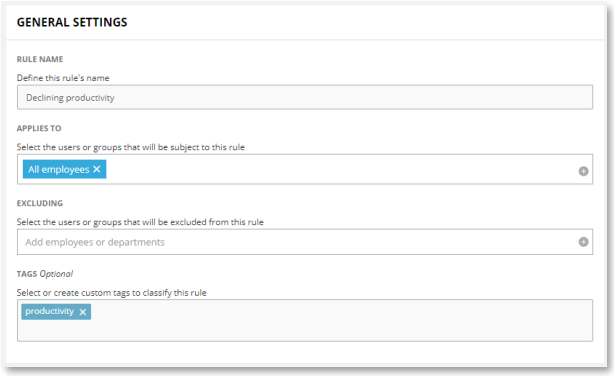
The rule shows the message we specified, and the upload operation is blocked.

16.5 Sample Rule 5: Employee productivity anomaly

16.5.1 Rule Summary

This example shows how you can create an Anomaly rule to monitor the productivity level of employees and receive a notification when it goes below a certain threshold. You will also be able to compare this against their Departmental and Organizational average.

16.5.2 Setting up the Rule



General Settings

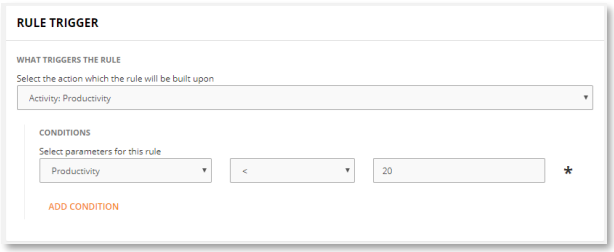
On the first section, General Settings, we assigned a name for the rule and a description.

For the users, we have selected All employees.

We have also used a tag to find the rule easily.

To learn more:

- Creating Anomaly Rules
- Setting Up the Rule Basics - names, description, user, tags etc.



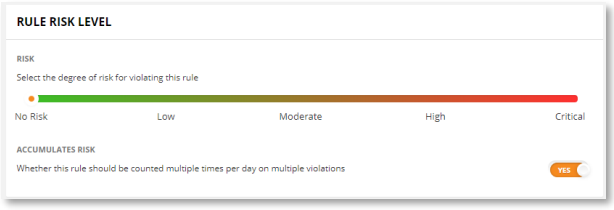
Rule Trigger

We chose the 'Activity: Productivity' as the rule trigger.

For the rule's condition, we selected the *Productivity* criterion and chose a less than '<' logic to detect when the productivity goes below 20%.

To learn more:

- Detection Criteria - What Behavioral Anomalies Trigger the Rules?
- List of Prebuilt Anomaly Rule Templates

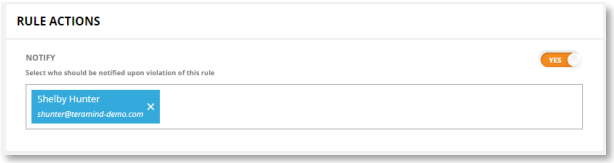


Risk Level

We left the risk level's default settings (No Risk) and ACCUMULATES RISK option turned on so that multiple violations of the rule will add up towards the risk score for this rule.

To learn more:

- Setting the Risk Level in an Anomaly Rule



Actions

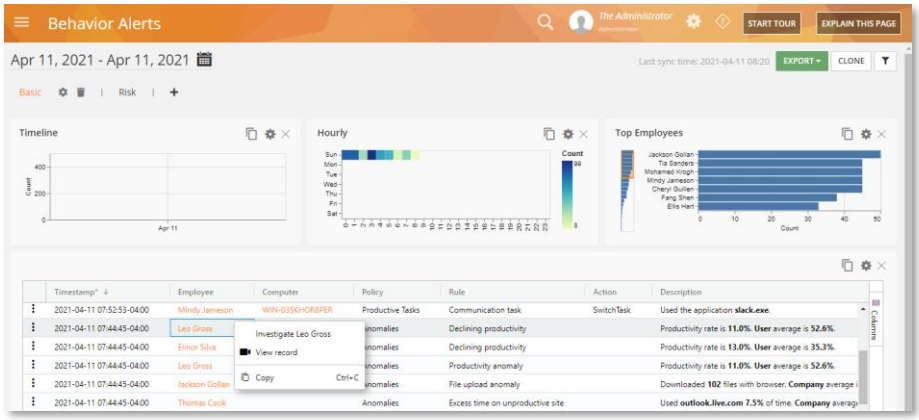
Finally, for the last section, 'Actions', we have turned on the NOTIFY action to inform a manager about the productivity loss.

To learn more:

- Defining Rule Actions

16.5.3 Viewing the Rule Alerts

Click **BI Reports** > **Behavior Alerts** then select the **Basic** tab to view a report of all rule violation alerts and trends. The 'Grid Widget' located below the screen shows a list of all the alerts:

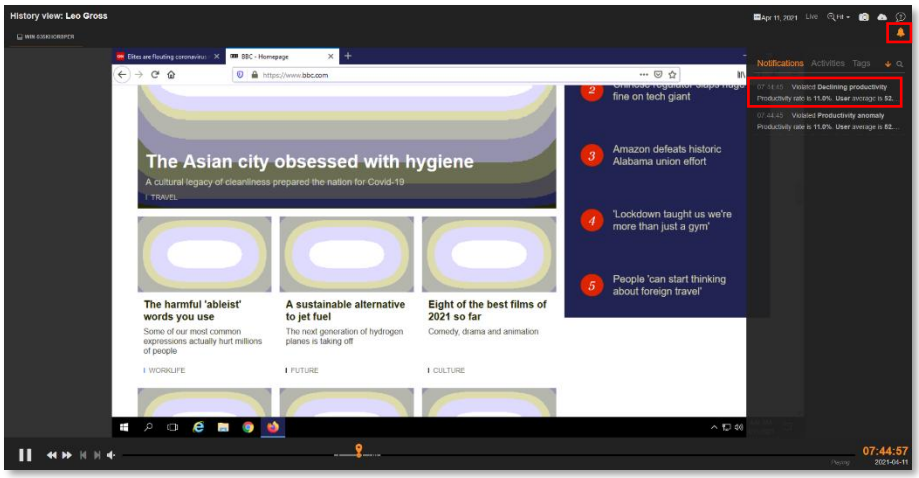


You can see that, on 2021-04-11 at 04:44:45, employee Leo Gross triggered an anomaly rule due to his productivity dropping to 11% where his usual productivity was above 52% before.

*Right-click on that row and then select **View record** to view the Session Recording of the alert.*

16.5.4 Viewing the Session Recording

Here you can see the Session Recording of how the rule message will look on the user's desktop:



*You can click the **Notification** 🔔 icon near the top-right corner of the Session Player to see all the alerts/notifications.*

*Click a **Notification** to see what the user was during when the rule was triggered.*

17 Appendix

17.1 List of Prebuilt Rule Templates

Data Loss Prevention
Credit Card Number: Wide
Credit Card Number: Narrow
Credit Card Number: At least 50 numbers
Credit Card Magnetic Strip Data: Wide
Credit Card Magnetic Strip Data: Narrow
Credit Card Magnetic Strip Data: 50 Track1 entities
Office Document: Confidential Watermark
Credit Card Magnetic Strip Data: 50 entities
Health Data: Disease or Drug names
Health Data: Drug names or NDC identifiers
Personal Data: US SSN and Date of Birth
Health Data: US SSN with Health Information
Health Data: UK NHS Numbers and Medical Information

Emails
Outbound email with social security number
Outgoing email to non-business address
Email contains a CV
Outgoing email w-attachment to non-business address
Email contains accusative sentiment
Email contains angry sentiment
Email contains discouraged sentiment
Email contains dissatisfied sentiment
Email contains lawsuit threat
Email contains profanity
Email contains sexual harassment content
Email contains unresponsive complaint
Incoming email from competitors
Outbound email with attachment
Outbound email with credit card number
Outbound email with sensitive keywords

Keystrokes
Screenshot taken

Printer
Large print job

Application
Anonymous browser detected
MSIExec program installation or removal
Network sniffer launched
Non-whitelisted application executed
Registry editor launched
Running peer-to-peer file sharing applications
Running screen sharing applications
Snipping tool used

File Operations
Access sensitive files
Driver tampering
Hosts file edited
Program installation
Write to cloud drive (native)
Write to config file
Write to removable media
Copy file from RDP
Copy file from RDP to removable media

Websites
Non-whitelisted website accessed
Adult websites
Excessive time on job search websites
Excessive usage of social media
Gaming or gambling sites
Streaming movies

IMs
IM contains accusative sentiment
IM contains angry sentiment
IM contains discouraged sentiment
IM contains dissatisfied sentiment
IM contains lawsuit threat
IM contains sexual harassment content
IM contains unresponsive complaint

17.2 List of Prebuilt Anomaly Rule Templates

Applications
Application usage anomaly

Emails
Outgoing email anomaly
Outgoing email attachments anomaly

File Operations
External storage insertion anomaly
File copy anomaly
File creation anomaly
File delete anomaly
File rename anomaly
Files downloaded by browser anomaly
Files downloaded by cloud client anomaly
Files uploaded by browser anomaly
Files uploaded by cloud client anomaly

Instant Messages
Instant messages count anomaly

Networking
Network connection count (no https) anomaly
Network connection count anomaly
Network data in (no https) anomaly
Network data in anomaly
Network data out (no https) anomaly
Network data out anomaly

Printers
Documents printed count anomaly

User Activity
Idle time anomaly
User productivity rate anomaly

Websites
Website usage anomaly

17.3 List of Pre-Defined Classified Data

Financial Data

All Credit Card Numbers
Magnetic Data
Magnetic Data (Track 1)
Magnetic Data (Track 2)
Swift Code
ABA Route Numbers

By Type
Visa
Mastercard
American Express
Bankcard
Dinners International
Dinners USA & Canada
Discover
En Route
JCB
Maestro
Switch

USA
Visa
Mastercard
American Express
Bankcard
Dinners International
Dinners USA & Canada
Discover
En Route
JCB
Maestro

Japan
Visa
Mastercard
American Express
JCB
Maestro

Europe
Visa
Mastercard
American Express
Discover
Maestro
Switch
Solo

United Kingdom
Visa
Mastercard
American Express
Discover
Maestro
Switch
Solo

Canada

Solo RuPay **By Country** USA Japan Israel Europe United Kingdom Canada	**Israel** Visa Mastercard American Express JCB Maestro	Visa Mastercard American Express Dinners Discover Maestro

Health Data

Common Drug Names Common Disease Names DNA Profiles	NDC Number HICN	NHS Number ICD10 Code

Personally Identifiable Data

USA Zip Code and Address UK Postal Code and Address USA Cities SSN English Names	Dates Phone Numbers IPv4 Addresses IPv6 Addresses Email Addresses	URL VIN Personal Cryptographic Keys USA Vehicle License Plates USA Driver License Number (All States)

Code Snippets

Clang C++ C# Go	Haskell Java JavaScript Objective-C	PHP Python Ruby SQL