# Alerts Implementation Guide

## Contents

## *About This Document*

This document explains how to create alert and prevention rules for Windows, Mac, and Unix/Linux platforms to address your business needs. It describes the rule structure, syntax, and logic, and guides you through the steps of configuring both simple and advanced rules. It also provides tips and best practices.

This document focuses on the implementation of alert and prevention rules. It also provides a quick overview of the available alert review capabilities.

**This document was written for ObserveIT Enterprise version 7.10.x.**

## *Intended Audience*

This document is intended for security administrators and IT security personnel in charge of configuring the ObserveIT system to trigger alerts based on risky user activities. This document assumes familiarity with the ObserveIT Enterprise product.

## *Related Documentation*

**The latest ObserveIT product documentation is available at this URL.**

## *Support*

If you have any questions or require assistance, please visit the ObserveIT technical support portal at http://www.observeit.com/Support.

# 1   Overview of the Alerts Feature in ObserveIT

**ObserveIT Alerts provide a proactive, real-time detection, deterrence and prevention mechanism.** Alerts are user-defined notifications which are generated when suspicious login events or user activities occur during a session. When alerts are triggered, textual notifications can be displayed warning users about potential security violations so that they can take remedial action. In some cases, users can be "denied access" and hence prevented from continuing with their current activity. By highlighting and reporting suspicious user activity events in real-time, administrators, risk officers, and IT security personnel can respond quickly and effectively to any deliberate or inadvertent threats to system integrity, IT security, regulatory compliance, or company policy. ObserveIT's **Insider Threat Intelligence** detects behavioral irregularities, and alerts IT security staff in real-time using the **User Risk Dashboard** which provides a user-centric view of risky users in the system. For example, from the dashboard, security administrators can view and investigate alerts for risky users who violated company policy or security rules, quickly identifying users with the highest number of policy violations and those whose behavior did not improve with time.

ObserveIT administrators can configure fully customizable and flexible alert and prevention rules which define the conditions in which user actions will cause alerts to be generated. For each rule, a detection policy defines the conditions that will trigger an alert (based on robust combinations of **Who**, **Did What**, **On Which Computer**, **When**, and **From Which Client**), and additional actions to be taken when the alert is triggered. User warning notifications and blocking messages notify users in real-time about any out-of-policy behavior. Users can acknowledge a message, add a comment explaining their actions, and follow a link to view the company policy. If required, the security administrator can also select to start recording a user when a security violation is detected. Preventive actions, such as forced log off and forcibly closing applications/websites, enable security officers to stop users from breaching or violating company policies. On Linux systems, ObserveIT prevent rules can be configured to block unauthorized Linux commands, including SFTP commands, from being executed. For example, if a user attempts to run commands that manipulate sensitive protection policy files, the user will be denied access to the protection policy files. Video recording of user commands and terminal output can be activated on Linux prevent rules.

**The Rule Engine Service component on the Application Server processes the activity data and generates alerts based on rules which are active.**

The administrator can configure a notification policy which defines whom should be notified when an alert is generated, and how they will be notified.

For enhanced management and operation, alert rules can be assigned to one or more user groups (a.k.a "User Lists") such as Privileged Users, Everyday Users, Remote Vendors, Terminated Employees, Users in a Watch-List, Executives, Developers & DevOps. Privileged Users and Everyday Users lists are prepopulated based on common Active Directory groups. These lists can be modified, and other lists can be easily created or populated by assigning them individual users or Active Directory groups.

In addition, alert rules can be assigned to security Categories (such as, Data Exfiltration, Hiding Information and Covering Tracks, Running Malicious Software, Performing Unauthorized Admin Tasks, and more) in order to help navigation and facilitate rules operation and maintenance. Categories can be applied on Windows, Mac, or Unix/Linux operating systems. Some categories are relevant for all systems.

**ObserveIT comes with an extensive Insider Threat Library (ITL) that includes out-of-the-box rules configured to handle Insider Threat, detecting risky user activity across applications, operating systems, and users. These built-in rules are grouped by security categories and are already mapped to User Lists, each with a specific risk level.**

Alerts are integrated throughout the ObserveIT Web Console (in the User Risk Dashboard, User Diary, Endpoint Diary, Search pages, and video Session Player) with alert indications, risk level (severity), alert status, details, in video replays, session screenshots, and alert email notifications. The user-friendly graphical alert display allows the reviewer to quickly assess the threat and take immediate action if needed. Alerts can be assigned a status according to administrator assessment and assigned a risk level according to their severity.

Alerts can be viewed in various display modes. For example, Gallery mode provides a view of the user environment displaying the context of exactly what the user was doing when an alert was triggered. You can browse through the screenshots of each alert while viewing the full alert details next to each screen, and easily replay sessions in which alerts occurred, even opening the Session Player at the exact screen location where an alert was generated.

ObserveIT's enhanced alert review workflow enables Incident Response teams to drive incident investigation. Security and compliance officers can easily review generated alerts using powerful filters, flag alerts for follow up, mark them as issues or non-issues, delete false alerts, and print and export selected alerts. Comments can be added to alerts to help you provide feedback on findings and decisions regarding the triggered alerts. Alerts metadata can also be exported to PDF reports for sharing real-time information on risky user activity and specific incidents with other users in an organization who do not have access to ObserveIT.

Customized reports can also be configured, providing summary information about alerts on all monitored Windows and Unix-based servers.

Alerts can also be easily integrated into an organization's existing SIEM system via the ObserveIT Monitor Log.

## 1.1 Common Alert Scenarios

The following scenarios are some examples of risky user activities that might generate alerts in ObserveIT:

- Logging-in locally or remotely to unauthorized servers by unauthorized users or from unauthorized clients
- Sending sensitive documents to a local/network printer during irregular hours
- Copying files or folders that are either sensitive or located in a sensitive location during irregular hours
- Connecting a USB storage device (or mobile phone) in order to copy sensitive information
- Using Cloud storage backup or large file-sending sites that are not allowed by company policy
- Storing passwords in files that can be easily detected by password harvesting tools
- Clicking links within emails that open Phishing websites
- Browsing contaminating websites with high potential security risk
- Browsing websites with unauthorized content (gambling, adults, etc.)
- Being non-productive by wasting time on Social Networks, Chat, Gaming, Shopping sites, and so on
- Searching the Internet for information on malicious software, such as steganography tools (for hiding text-based information within images)
- Accessing the Darknet using TOR browsers
- Performing unauthorized activities on servers, such as, running webmail or Instant Messaging services
- Running malicious tools such as, password cracking, port scanning, hacking tools, or non-standard SETUID programs on Linux/Unix
- Hiding information and covering tracks by running secured/encrypted email clients, clearing browsing history, zipping files with passwords, or tampering with audit log files
- Attempting to gain higher user privileges (for example, via the su or sudo commands, running an application as Administrator)
- Performing copyright infringement by browsing copyright-violating websites or by running P2P tools
- Changing the root password by regular user or searching for directories with WRITE/EXECUTE permissions in preparation for an attack (on Linux/Unix)
- Performing IT sabotage by deleting local users or files in sensitive directories (on Linux/Unix)
- Creating backdoors by adding users/groups to be used later un-innocently
- Installing questionable or unauthorized software such as hacking/spoofing tools on either desktops or sensitive servers
- Accessing sensitive administration tools or configurations, such as Registry Editor, Microsoft Management Console, PowerShell, Firewall settings, etc.

# 2 Overview of the Steps for Creating Alert and Prevention Rules

Alert and prevention rules are created in the ObserveIT Web Console in the **Alert & Prevent Rules** tab. You can navigate to this tab via **Configuration > Alert & Prevent Rules**.

**Note: Prevent rules apply to Linux operating systems only.**

Before building your alert or prevention rules, consider the following points:

- What are the specific problems you are trying to solve? For which user activities would you want to receive alerts? For which users/groups might alerting be most valuable to you? Is it important to consider the day/date/time for these activities? Is it important to differentiate between host computers and/or client computers used for these activities?
- What actions do you want to take when an alert is triggered? Do you want to just warn the user about their actions so that they can take remedial action, block their screen forcing them to stop what they are doing, or "Prevent Execution" of the activity they were trying to perform?
- How frequently do you require alerts for each activity of interest?
- What is the status you want to assign to each alert (Active or Inactive)?
- What risk level (Critical, High, Medium, or Low) should be assigned to each alert?
- For which alerts do you want someone to receive email notifications, and how often?
- Consider creating reports that provide summary information about alerts on monitored Windows, Mac, or Unix-based endpoints.

The main steps for creating an alert or prevent rule are as follows:

1. In the **Alert & Prevent Rules** tab**,** click the **New Alert Rule** or **New Linux Prevent Rule** button depending on the type of rule you are creating.
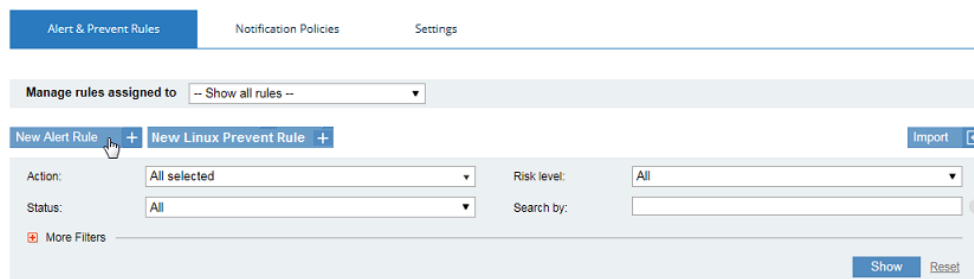


2. Define the rule details (name, description, category, OS type, notification policy, status, risk level, alert frequency for the rule). See General Rule Details.
3. If required, configure alert rule assignments to User Lists. See Assigning Alert Rules to User Lists.
4. If required, change the security category to which the rule is assigned. See Categorizing Alert Rules.
5. Define a detection policy for the rule. See Defining a Detection Policy for Alert Rules or Defining a Detection Policy for Prevention Rules.
6. Define actions to be taken when an alert is triggered from the rule. See Defining Actions for Alert Rules or Defining Actions for Prevention Rules.
7. Save the rule. See Saving Rules.
8. Activate the rule. See Activating Rules.
9. (Recommended) Test the rule, to see if alerts are triggered as you intended. See Viewing Generated Alerts in ObserveIT.

# 3 Rule Structure and Logic

This section describes the structure of alert or prevent rules, including rule details, flexible rule design, rule conditions, and the logic behind the rule conditions.

## 3.1 General Rule Details

For every rule (alert or prevent type), you can define the following general properties (note that some are mandatory):

- **Name** of the rule that briefly describes the activity, so that you can easily identify what happened when the alert is triggered. (Only unique names are allowed. When you try to create a rule with a name already in use, an error message appears, and the system does not allow you to save the rule. You can always edit and change the name of an existing rule, as needed.)
- **Description** of the rule (optional) that summarizes the details of the activity that will trigger an alert.
- **Category** – The category to which the rule is associated. The rule can also be associated with a category named "--UNCATEGORIZED--". To change the category or to add a new category, click the **Change** hyperlink. Note that when editing a System rule, you cannot change its category. For details, see Categorizing Alert Rules.
- **OS Type** – The operating system(s) for which you want to create the rule - **Windows**, **Unix**, or **Both** (i.e., Windows and Unix). Note that you can create prevention rules only on Unix systems.
- **Notification policy** (optional) to determine who receives email alert notifications and how frequently. See Managing Email Notifications and Viewing Alerts in Email Notifications.
- **Status** of the rule – **Active** or **Inactive**. See Activating Alert Rules.
- **Risk level** of the rule – **Critical**, **High**, **Medium**, or **Low** (color-coded dark red, red, orange, or gray) enabling you to quickly identify the risk level and respond accordingly. See Setting Alert Risk Level.
- **Alert frequency** – **Each time** or **Once per session**. See Alert Frequency.

- Alert Frequency.



> **After defining the general rule details, you can define a Detection Policy that comprises the conditions (Who?, Did What?, On Which Computer?, When?, From Which Client?) which will trigger an alert. See Rule Conditions.**

You can save the rule at any time and activate it once it is ready to be used (see Saving Rules and Activating Rules).

## 3.2 Flexible Rule Design

The configuration of alert and prevention rules is extremely flexible. You can merge several conditions and options into one rule to combine and detect a wide range of alert criteria (specific users, computer, URLs, applications, commands, and so on), or you can divide the criteria among several rules to maintain separate alert definitions.

You do not need separate rules, for example, to alert when a user browses different social media sites. You can combine the list of sites together into a single alert rule (for example, Facebook, Twitter, LinkedIn). An alert will be generated the first time the user visits each of these sites (if **Once per session** is the alert frequency).



When defining values by which to evaluate a condition of an alert rule (in the text box on the right), you can enter multiple values separated by commas either directly or by clicking the [...] icon to open a popup dialog that allows you to add and edit the long text strings and lists (such as URLs, IP addresses, user names, computer names, websites, and so on). This enables you to easily define your rule logic and criteria.

For example, you can enter a long list of URLs:



Since the list is long, it is truncated in the text box in the rule, for example: facebook, twitter, linked ....

> **Note: When Lists are supported (for details, see Assigning Alert Rules to User Lists), you can choose to select a predefined List instead of entering a set of values. By hovering over the values field, two icons appear that enable you to switch between the modes.**

## 3.3 Rule Conditions

ObserveIT rules comprise conditions that define the criteria for triggering an alert (**Who?**, **Did What?**, **On Which Computer?**, **When?**, **From Which Client?**). You can use these flexible conditions and options to define your rule to determine what activities and specific circumstances will trigger an alert. Alerts are generated on the activity defined in the **Did What?** section. By specifying the specific time, computer, client machine, or by which user an activity is performed, you can define the scope of the activity and limit the number of generated alerts. In other words, alert rules specify a particular activity that will generate an alert, along with optional conditions which limit the context in which that activity will generate an alert.

**By default, an alert is triggered each time an event/activity occurs during a session. For example, an alert is generated every time a particular application is run, a window opens displaying a particular title, a specific website URL is visited, a particular command is executed, and so on. You can also specify that an alert is generated just once per session.**

**Alert Frequency.**

The following table lists the conditions and related options for defining the scope of the alert. For in-depth explanations of each option and illustrative examples, click the specific links in the table below, or see Defining Alert Rules for the complete content.

| Condition | Description | |
|---|---|---|
| **Who?** | Who logged in to the computer? See Defining the "Who" Conditions | |
| | Login account [domain\]name | Use to alert according to the name (and optionally domain) of the account with which the user logged in. You can specify Active Directory group membership. |
| | Secondary user [domain\]name | Use to alert according to the name (and optionally domain) of the user used for secondary authentication (defined in the Active Directory or ObserveIT). You can specify Active Directory group membership. |
| | Login/secondary user [domain\]name | Use to alert according to the login account or secondary authentication user that logged in (as described above). You can specify Active Directory group membership. |
| **Did What?** | What particular activity triggered an alert? This condition has platform-specific options. See Defining the "Did What?" Conditions | |
| | **Logged In** | Use to alert when a user logs in to either a Windows or Unix/Linux computer. (The user may be, for example, any of the users defined in the Who? condition above.) You can restrict alert generation for "Logged in" events by specifying additional criteria, such as who logged in, when, on which computer the login took place, or from which client machine. |
| | **Ran Application (Windows)** | Use these options (Application name, Application full path, Process name, Window title, or Permission level) to generate an alert when a user runs one or more particular applications on a Windows computer. Running certain applications may signal, for example, that the user may be tampering with settings that may affect system security, user permissions, installed software/services, or accessing sensitive data. |
| | Application name | Use to alert when a user runs a specific application. |
| | Application full path | Use to alert according to the full path of the application the user is running. |
| | Process name | Use to alert when a user runs a specific process related to the active application—to detect the process name (for example, "regedit") rather than the application name ("Registry Editor"). |
| | Window title | Use to alert according to keywords that appear in the titles of windows with which the user interacts. |
| | Permission level | Use to alert according to the permissions level of the logged in user running the application (whether admin or not). |
| | **Visited URL (Windows)** | Use these options (Site, URL prefix, Any part of URL, or Website Category) to prevent users accessing sensitive or prohibited websites or webpages. |
| | Site | Use to alert when a user visits a specific website, regardless of specific pages opened in the site. |

| | URL prefix | Use to alert when a user visits a specific area of a website, according to the URL prefix that you define, which can be any portion of the URL (any substring). |
|---|---|---|
| | Any part of URL | Use to alert each time a user visits a unique website URL that contains the specified keyword (or string). No matter where in the URL the keyword appears, an alert is generated. |
| | Website Category | Use to generate an alert when a user browses a Website that belongs to a predefined list of categories that are forbidden for browsing or that require monitoring. A drop-down list includes 42 predefined Website categories. |
| | Website Category (detailed) | Use this option to generate an alert when a user browses a Website that belongs to any of the native categories defined in the NetSTAR cloud service. A drop-down list includes all the native categories available in the NetSTAR cloud service. |
| | **Exfiltrated File** | Use to alert when a tracked file is uploaded (copied or moved) to the default local sync folder of a cloud file sharing service that is supported by ObserveIT. Use to alert when a file is copied of downloaded to a USB-based device. |
| | To any destination | Use this option to alert when a file is exfiltrated to any destination, such as any website, cloud sync folder, webmail, social media sites and file sharing sites. |
| | To website/web-application (Upload) | Use this option to alert when a file is uploaded to any website or web-application, including webmail, social media sites and file sharing sites. Uploads can be detected on any file, whether tracked or non-tracked. An uploaded file is not subsequently tracked by ObserveIT. |
| | To cloud storage sync folder | Use this option to alert when a tracked file is moved or copied to a local cloud storage sync folder, such as Dropbox and Box. |
| | To USB device | Use this option to alert when a tracked file is copied or downloaded to a USB device. |
| | By attaching it to an email client | Use this option to alert when a file is attached to an email client. |
| | By sending it via email | Use this option to alert when an email is sent from an email client. |
| | **Brought in a File** | Use to alert when a file is downloaded or saved from a sensitive website or web application (such as, Salesforce, Sharepoint, CRM, ERP). |
| | By downloading from website/web-application | Use to alert when a file is downloaded or saved from a sensitive website or web application. |
| | By saving attachments from an email client | Use this option to alert when an attached file saved from an email. |
| | By taking a file from cloud storage sync file | Use this to alert when a tracked file is moved or copied from a local cloud storage sync folder, such as Box. |
| | **Email** | Use to alert when a file is sent from an email client, a file is attached to an email or a file attachment is saved from an email |

| | | Sent an email using an email client | Use this option to alert when an email is sent from an email client. |
|---|---|---|---|
| | | Exfiltrated file by sending it via email | Use this option to alert when an attached file is sent via email. |
| | | Exfiltrated file by attaching it to an email client | Use this option to alert when a file is attached to an email whether or not the email is sent. |
| | | Saved file from an email client | Use this option to alert when an attached file from email client is save. |
| | | **Used Keyboard (Key Logging)** | Use to alert on captured key logger data, such as when users type blacklisted commands (within CMD, Powershell, Putty, or Terminal), blacklisted phrases in an email, or sensitive words while browsing social media websites. |
| | | Typed text | Use this to alert when a user types blacklisted commands (within CMD, Powershell, Putty, or Terminal), blacklisted phrases in an email, or sensitive words while browsing social media websites. |
| | | Pressed special key/combination | Use this to alert when a user presses one of the special keys, which are PrtScr, Backspace, Insert, Enter, Clear, Return, Delete, End, Esc, Home, Page Up, Page Down, Tab and F1 to F12. |
| | | | Use this to alert when a user Presses any combination keys, which are Alt, Ctrl, Shift and Win with other keys (Windows) and Cmd, Control, Option, and Shift with other keys (Mac). |
| | | **Copied Text** | Use to alert on text with sensitive or confidential content is copied to the clipboard. |
| | | **Interacted with In-App Elements (Windows)** | Use to define Alert Rules based on specific user interactions with application sensitive elements (In-App Elements). A submenu will display all applications/websites in which In-App elements were marked. |
| | | **Executed SQL Command (Windows)** | Use this option to generate an alert when a user executes a particular SQL command against a database (in Windows). An alert can be generated if a user accesses a database in order to perform harmful activity. |
| | | **Executed Command (Unix/Linux)** | Use these options (Command name, Parent command, Top level command, Setuid mode, Full path, Argument, Switch, Permissions) to generate an alert when a user executes a particular Unix/Linux command. This is useful to track when a user performs some action on sensitive data, files, directories, paths, user permissions, or system configuration settings. |
| | | Command Name | Use to alert when a user executed a Unix/Linux command. |
| | | Parent Command | Use to alert if a command is run from another command using its name, or when a command is not run by a specific command. |
| | | Top Level Command | Use to alert upon the execution of commands run from within an application running under the shell, such as sudo (top level). |
| | | Setuid Mode | Use to alert if an unauthorized `setuid` program is run, as this program runs as `root` and the commands it runs internally will also run as `root`. |
| | | Full path | Use to alert according to the explicit path of the command. |

| | | | |
|---|---|---|---|
| | Argument | Use to alert when a user uses specific command line parameters in a command. | |
| | Switch | Use to alert when you need more search combinations than the "Argument" option, in order to find exactly what you need.<br><br>For example, if you are looking in an alert rule for the argument "–r", the switch option allows you to use: "–rf" or "–fr" which extends the range of your search options. | |
| | Permissions | Use these options to alert if a user tries to switch identity or run commands under a different identity (privileged escalation). For example, running commands under 'root'.<br><br>Alerts are based on the permissions used to run the command, whether the user's own permissions (those granted during login), root permissions, or other permissions. For further details, see Permissions are own, Permissions other than own, Permissions are root, and Permissions are root (other than own). | |
| | **Performed Paste** | Use this option to generate an alert when a user pastes text, file, folders, or images with sensitive or confidential content. Alerts are triggered by keyboard and point-click paste actions. Paste can be of any type, of text, of files/folders and of images. | |
| | **Detect Connected USB** | Use this option to generate an alert when a any USB device is connected, when any white listed USB device is connected, when any unlisted USB device is connected or when a specific USB device is connected. Options are To which USB, USB model, USB vendor, USB label and USB S/N. | |
| **On Which Computer?** | On which computer (or within which group of computers/servers) did the activity occur?<br>See Defining the "On Which Computer?" Conditions | | |
| | Computer [domain\]name | Use to alert according to the name (and optionally domain) of the computer on which an activity occurred. | |
| | ObserveIT server group name | Use to alert according to the name of the server group on which an activity occurred. (The server group is defined in the ObserveIT Web Console **Server Groups** page.) | |
| | Computer IP address | Use to alert according to the IP address of the computer on which an activity occurred.<br><br>**Note**: When alert rules are based on IP address ranges, you can specify the IP address range using the CIDR notation format: aaa.bbb.ccc,ddd/N, where N in an integer between 0-32.<br>For example: 192.158.2.0/24<br><br>You can click the link Check CIDR syntax to check if your format is permitted. | |
| | OS name | Use to alert according to the name of the operating system on which an activity occurred. (Use the OS names and details that are displayed in the ObserveIT Web Console **Servers** page.) You must include the *full* OS name when using the "is/is not" operators. | |
| | Agent version number | Use to alert according to the version number of the ObserveIT Agent under which an activity occurred. | |
| **When?** | On what day and/or at what time was the activity performed?<br>See Defining the "When?" Conditions | | |
| | Day of week | Use to alert according to particular days of the week. | |
| | Time of day | Use to alert according to particular times. | |

| | Specific date | Use to alert according to particular dates. |
|---|---|---|
| | Specific date and time | Use to alert according to a particular range of dates and times. |
| **From Which Client?** | From which client computer did the user connect to the monitored computer (on which the activity occurred)? | |
| | Client name | Use to alert according to the name (and optionally domain) of the client computer from which the user connected to the monitored computer (as described in **On Which Computer?**). |
| | Client IP address | Use to alert according to the IP address of the client computer from which the user connected to the monitored computer. IPv4 and IPv6 formats are supported.<br><br>**Note**: When alert rules are based on client IP address ranges, you can specify the IP address range using the CIDR notation format: aaa.bbb.ccc,ddd/N, where N in an integer between 0-32.<br>For example: 192.158.2.0/24<br><br>You can click the link Check CIDR syntax to check if your format is permitted. |

## 3.4 Alert Frequency

What is the frequency of the alert generation? How often do you want to generate alerts for serious events which may impact the system?

> **The first instance of every event/activity in a session always triggers an alert. For example, an alert is generated the first time a particular application is run, a window opens displaying a particular title, a specific website URL is visited, a particular command is executed, and so on.**

An alert can be triggered by a specific event (for example, a Window title containing "host"), which may repeat itself for succeeding screenshots (for example, if the user keeps working in Notepad the word "hosts" is triggered from almost every recorded screen). In this case, generating an alert for every screen is not feasible, and it would probably be sufficient to generate an alert only once in a user session. To prevent too many alerts from being generated for the same event, ObserveIT lets you control the number of times an alert can be triggered.

When defining the details for an alert or prevention rule, the **Alert frequency** option enables you to define how often an alert should be generated upon recurrence of an activity–whether each time the alert occurs (the default) or just once per session.

### Each Time

(This is the default option) Allow alerts to be generated each time the defined criteria are met. For example, you might select this option to generate an alert each time that an unauthorized user accesses a specific sensitive file (such as, `regedit.exe` or `mmc`) during a session. The user risk score can be significantly affected by using this option.

> **When** Each time **is the selected alert frequency, the alerts mechanism intelligently avoids generating alerts for every mouse click or keystroke in the same window. This also applies if you change focus to another window and then revert back to the window for which an alert was already generated.**

For example, the following conditions would generate an alert every time the `mmc` process is rerun (upon every new process ID) and the window title "Network Connection" is displayed:

### Once Per Session

Prevents alerts from being generated more than once per user session. For example, you might select this option if you do not want to be alerted every time the user browses an illegal Website, but only once during a session (which by default lasts 15 minutes, and can be configured in the **Configuration > Server Policies** page).

An alert is generated only the first time a user runs an application in a session—such as when a user runs the Internet Information Services (IIS) Worker Process (`w3wp`) to stop system services:

> When more than one application is specified in the rule, the alert is triggered the first time *each application* is used in the session (for example, `cmd` or `services`).

## 3.5 Rule Logic

The underlying rule logic determines how conditions and criteria correlate. The validity of the alert criteria is tested by the rule engine, and only when an activity meets all the criteria will an alert be generated.

- The rule conditions relate to each other logically using "AND" logic (for example, **Who**, **Did What**, **On Which Computer**, *and* **When**).

- The criteria specified within each condition section (**Who?**, **Did What?**, **On Which Computer?**, **When?**, **From Which Client?**) relate to each other logically using either "AND" or "OR" logic. You can specify within the condition whether *all* the criteria must be met ("AND" logic), or whether *any* of the conditions may apply ("OR" logic). For example, one rule can alert when a certain process is run *and* when certain text is displayed in the window title. Another rule can alert when either "this command" *or* "that command" is executed.

- You can define multiple values for a condition using a comma to separate the values to indicate "OR" logic, such as "reboot, shutdown" to denote "reboot *or* shutdown"– .

- You can combine "OR" and "AND" logic by using a combination of comma-separated values and options— such as in the following rule which generates an alert when a user opens either an Excel *or* Word file containing sensitive company data, *and* the keywords, "budget", "finance", or "strategy," appear in the window title:

# 4 Defining Alert Rules

This section walks you through the process of defining alert rules, including in-depth explanations of the alert rule criteria and what conditions and scenarios to consider when creating your rules for triggering alerts. It also includes a description of the actions that you can take when an alert is triggered. The ObserveIT installation package includes an extensive library of out-of-the-box alert rules which you can use as they are, or customize. These rules have built-in policy notifications designed to increase the security awareness of users, and reduce overall company risk. If you want to customize these rules, it is recommended that you first copy, then edit, and activate these rules to match your organization's security needs. For details about how to enhance your use of the ObserveIT out-of-the-box alert rules, see **Insider Threat Library (ITL) Tuning**.

Alert rules are described in detail the ObserveIT online help. Click here for the latest version.

## 4.1 Assigning Alert Rules to User Lists

For which types of users or groups are your rules most relevant? Are there specific users or groups to which you want to assign your rules?

ObserveIT allows you to map alert rules to user groups (known as "User Lists" of type Users) that can be created and fully-customized. This version includes the following built-in User Lists: Privileged Users, Everyday Users, Remote Vendors, Terminated Employees, Users in a Watch-List, Executives, Developers & DevOps. Alert rules can be easily assigned to multiple Lists each with a specific risk level. The alert rules in the Insider Threat Library are already assigned to the relevant User Lists each with a specific risk level.

You can view and manage alert rule assignments to User Lists from the **Manage rules assigned to** drop-down list at the top of the **Alert & Prevent Rules** page.

## 4.2 Categorizing Alert Rules

Categorization facilitates the operation and maintenance of rules and enables them to be grouped within similar security topics. Each alert rule in the ObserveIT Insider Threat Library is associated with one Category. A rule that does not fit into one of the predefined categories can be associated with a special built-in category named "--UNCATEGORIZED--".

To which security category do you want to assign your rules?

**The ObserveIT** Website Categorization **module automatically detects categories of Websites that end users are browsing, enabling alerts to be generated on browsing categories such as Gaming, Adults, Infected or Malicious Websites, Phishing Websites, and more.**

In the **Alert & Prevent Rules** page of the ObserveIT Web Console, you can view and manage the categories to which rules are associated. In this page, you can create new categories, and change the categories to which the rules are associated.
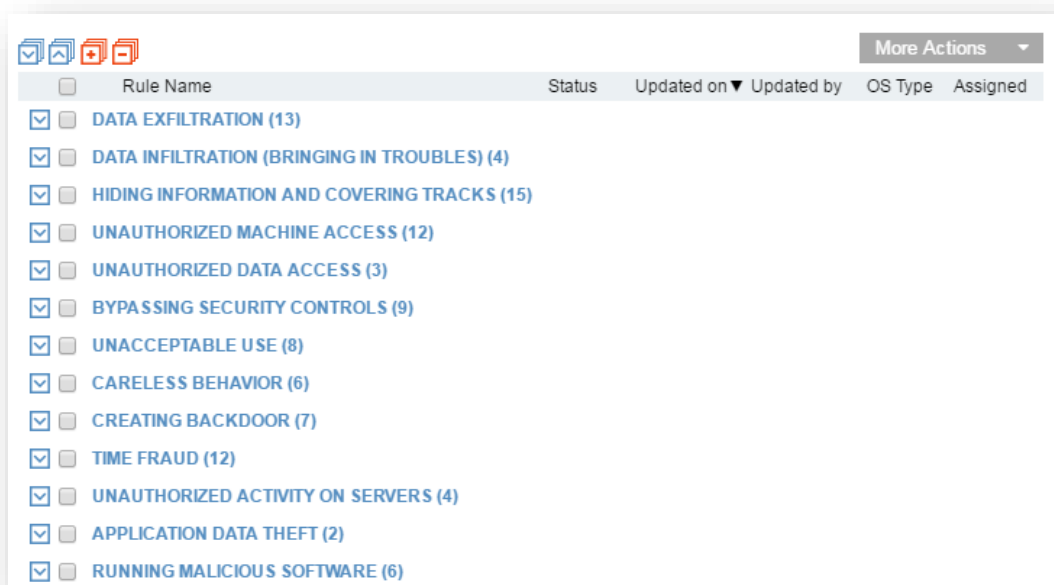


## 4.3 Defining a Detection Policy for Alert Rules

The core part of creating rules is defining the criteria (Who?, Did What?, On Which Computer?, When?, From Which Client?) that when met, will trigger an alert. A detection policy comprises the criteria that you configure for your rule. By specifying where, when, and by whom an activity is performed, you can define the scope of the activity and limit the number of generated alerts.

All the conditions, except for specific Did What? activities, can be used in both Windows and Unix environments. Each condition has its own set of parameters for which you can choose from a list of available options (fields and operators) and specify input values.

### 4.3.1 Who Performs the Activities that Trigger Alerts?

Which user triggered the alert? Who are the risky users in your organization? You can specify the **Who?** criteria to create a rule to generate an alert only when specific individuals or groups of users perform an activity. For example, you can limit the scope of the alert rule to *who* was logged in or *who* ran an application, visited a website URL, executed a command, and so forth. (For details about the many user activities you can monitor, see What Activities Trigger Alerts?)

## Options for Defining the "Who?" Conditions

What are the user's credentials? Users may be specified by login account name and/or secondary login account name:

- **Login account [domain\]name**: Use this option to generate an alert based on one or more login account names (optionally including a domain) with which the user(s) logged in. You can specify Active Directory group membership by using the "is member of group" operator. The user may be a member of a user group—such as "Employees\Joe" in the following rule:



- **Secondary user [domain\]name**: (This option is similar to the **Login account** option described above.) Use this option to generate an alert based on the user accounts used for secondary authentication. (Secondary authentication accounts are defined in the Active Directory or directly in ObserveIT.) Secondary authentication is typically used to differentiate between various admin users who log in using the same shared admin-level account (for example, administrator or root).

- **Login/secondary user [domain\]name**: Use this option to generate an alert based on *either* the login account name or secondary login account name used, and you can specify Active Directory group membership (as described above)—such as when a member of the remote vendors group logs in:



## 4.3.2 What Activities Trigger Alerts?

For what particular activities do you want to receive real-time alerts? What are the suspicious, dangerous, malicious, or out-of-policy user activities that may threaten your systems or data? Which sensitive application data did users interact with?

You can specify Did What? criteria to create a rule to generate an alert when a particular activity is performed.

On Windows and Mac systems for example, you can search for users that logged in, ran a specific application, viewed a specific window title, visited a URL, downloaded a sensitive file from a website and moved it to a cloud sync folder, uploaded a file to any website or web application, typed a blacklisted command/phrase, copied text with sensitive content to the clipboard, executed an SQL command containing keywords (Windows only), and so on. On Unix systems, you can search for users who logged in, executed a specific command (based on command name, parent command, top level command, setuid mode, full path, arguments, command switches) or acted under a different user's permissions.

You can also specify the maximum frequency that each defined alert will trigger (for example, whether once per session, or on every occurrence). See Alert Frequency.

## Options for Defining the "Did What?" Conditions

All the **Did What?** activities are either Windows or Unix-specific, except for login which is relevant for both platforms. For details about each of the **Did What?** options, see Logged In, Ran Application, Visited URL, Exfiltrated Tracked File, Downloaded/Exported File, Typed Text (Key Logging), Copied Text, Interacted with in-app elements, Executed SQL Command, and Executed Command (Unix).

### Logged In (Windows and Unix/Linux)

Use this option to generate an alert when a user logs in to either a Windows or Unix/Linux computer. Note that "Logged in" is the default activity that appears when creating a new alert rule, and that it cannot be combined with any other activity. You can restrict alert generation for "Logged in" events by specifying additional criteria, such as who logged in, when, on which computer the login took place, or from which client machine.

*Considerations and Tips*

> **Note: Without specifying some additional criteria related to this activity, many alerts will be generated—in fact *every time* someone logs in to any monitored computer! Therefore, it is important to specify particular users, endpoints, days/times, and so forth—so that you receive only relevant alerts.**

## *Ran Application (Windows)*

Use the **Ran Application** options to generate an alert when a user runs one or more particular applications on a Windows computer (see Application name, Application full path, Process name, Window title, Permission level). Running certain applications may signal, for example, that the user may be tampering with settings that may affect system security, user permissions, installed software/services, or accessing sensitive data.

### *Application Name*

Use this option to generate an alert when a user runs a specific application—such as when a user opens an Excel file containing sensitive company data, and the keywords, "budget, fiscal, or transactions," appear in the window title:



An alert is generated for every unique window title that displays these keywords (in Excel). An alert will not be generated the second time the same window title reappears within the session.

The Application Name option may be useful, for example, when someone renames the executable name of a program, the application name will still be the same, but the process name will be different. For example, if you search for the application name "Registry Editor", then even if someone renamed the "regedit" executable to "xyz", although the process will be named "xyz" (and not "regedit"), the application name will still be "Registry Editor", so the alert rule will fire.

**Note: It is recommended to use the operator "contains" (rather than "is") to detect all versions of an application (since the application name may change among the various versions of the product).**

### *Application Full Path*

Use this option to generate an alert according to the full path of the application the user is running. (For example, "`C:\Program Files\OpenVPN\bin\openvpn.exe`".) This may be useful to alert when a command is run from a specific location.

### *Process Name*

Use this option to generate an alert when a user runs a specific process related to the active application—to detect the process name (for example, "regedit") rather than the application name (for example, "Registry Editor"). Oftentimes, the process name is more consistent among the many versions and configurations of the same product, whereas the application name may change for marketing or deployment reasons. Therefore, by specifying the process name in the rule, the system will better detect all versions.

**Note: The service name must be entered *without* its file extension—for example, "`regedit`" and not "`regedit.exe`".**

### *Window Title*

Use this option to alert according to keywords that appear in the titles of windows with which the user interacts—such as when a user opens "Notepad – **host**s" and "Notepad – my**host**s"—where the keyword "host" appears in the window title:

This rule triggers an alert for every unique (different) window title that displays the keyword "**host**" (in the same session). In the above example, two separate alerts will be generated when the two different window titles, "Notepad – **host**s" and "Notepad – my**host**s", appear for the first time in the session.

You can specify multiple keywords in the rule to trigger an alert when any of the keywords appear in the window title (to detect a broader range of user activity). For example, if you specify the keywords, "host" or "security", an alert is generated when either "host" or "security" appear in the window title (for every unique window title that contains these keywords, as described above).

*Permission Level*

Use this option to generate an alert according to the permissions level of the user that is running the application (whether admin or not). This may be valuable to detect when a user runs a particular application, one which may possibly signal malicious intent—such as when a user attempts to access the `hosts` file without admin permissions:



*Considerations and Tips*

- Determine the applications and sensitive data files that you want to monitor, and the users who are accessing them. For example, only administrators have permissions to use certain system applications, such as `cmd.exe`, so you may want to alert when non-admin users run `cmd` or when admins managed to run `cmd` at unusual hours (they obtained UAC permissions somehow).

- Wildcards are not supported. For partial searches, use the operator "contains" instead of "is". (For example, "Window title *contains* budget, fiscal, transactions".)

### Visited URL (Windows)

Use the **Visited URL** options (Site, URL prefix, Any part of URL, Website Category) to generate an alert when a user visits a particular website, webpage, area of a website, or a Website category that employees are forbidden to browse or that require monitoring. Is the user accessing sensitive or prohibited websites or webpages? This is useful to prevent possible hacking attempts or data theft.

*Site*

Use this option to generate an alert when a user visits a specific website, regardless of which pages were opened in the site. This is useful to track users accessing unauthorized or inappropriate sites (during work hours)—such as when a user browses social media sites (Facebook, Twitter, or LinkedIn):



According to the above rule:

- An alert will be triggered the *first time* in the session the user visits *any one* of these sites (when the URL domain contains the matching text: "facebook" or "twitter" or "linked in"). For example, when the user visits the Facebook login page: www.facebook.com/login?.... or the Linked In login page: www.linkedin.com/company/login.
- Because "Alert" is set to "only once per session", an alert will *not* be triggered when any other pages or areas within the website are visited within the same session. For example, when the user visits a friend's page after logging in to Facebook (www.facebook.com/friend?....).

*URL Prefix*

Use this option to generate an alert when a user visits a specific area of a website, according to the URL prefix that you define. This is very useful if you want to be alerted when someone visited a particular area of a Web application, for example, the "Leads" section in the Salesforce website, but you do not want to be alerted on each and every individual lead that they are reviewing (which if you want, can be achieved using Any part of URL described below).

What is a URL prefix? In ObserveIT, "prefix" in this context can be any portion of the URL (any substring), and does not necessarily have to start at the very beginning of the URL. The "URL prefix" is thus the text (string) that you specify, which can start and end at any point in the URL. For example, you can specify "google.com/accounts" to generate an alert when a user visits the Google Accounts page versus alerting when a user visits the home page of the site, "https://www.google.com/".

The following rule generates an alert when a user visits the Admin Users page of ObserveIT (a sensitive area of the ObserveIT Web application):
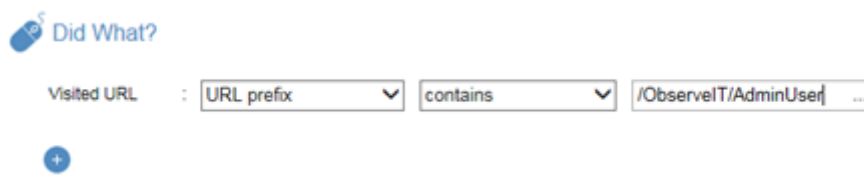


According to the above rule:

- An alert will be triggered the first time in the session the user visits the Admin Users page of the ObserveIT website, matching the URL prefix: **/ObserveIT/AdminUser**. For example:
  https://111/222/333/444:4884**/ObserveIT/AdminUser**View.aspx?GroupINdex=**3**&TabIndex=1&lang=en
- After visiting the above page, an alert will *not* be triggered when the user visits the following page, since it is in the *same URL prefix,* which is "*https://111/222/333/444:4884/ObserveIT/AdminUser*":
  https://111/222/333/444:4884**/ObserveIT/AdminUser**View.aspx?GroupINdex=**2**&TabIndex=1&lang=en
- An alert *would be triggered* when the user visits the following page since it is in a *different website* (because now the URL prefix is "*https://111/222/333/555:5995/ObserveIT/AdminUser*" which is different than "*https://111/222/333/444:4884/ObserveIT/AdminUser*"):
  https://111/222/333/**555:5995/ObserveIT/AdminUser**View.aspx?GroupINdex=**3**&TabIndex=1&lang=en
  The alert rule engine detects URL prefix matches for each unique site.

By including more of the text from the beginning of the URL address, you can limit the scope of the alert rule to a particular site (such as "https://twitter.com/settings/accounts/" or from whatever point in your site that would best identify your website's address). Otherwise, alerts may be generated for each site that shares a common "URL prefix".

*Any Part of URL*

Use this option to generate an alert when a user visits a website URL containing the specified keyword (or string). This option alerts for *every unique* URL that matches the criteria, even when only one character is different. For example, "Visited URL: Any part of URL contains game" would generate alerts for the unique URLs in the following Google searches:
https://www.google.com/?gfe_rd=cr&ei=jG2NVIKEBcrH8gfo6IC4Bw&gws_rd=cr#q=*game*
https://www.google.com/?gfe_rd=cr&ei=jG2NVIKEBcrH8gfo6IC4Bw&gws_rd=cr#q=*arcadegames*

Use this option carefully and *sparingly* to prevent generating too many alerts!

This option is useful to track "dangerous" URL keywords (for example, "hack" or "crack") or out-of-policy keywords (for example, "porn" or "gambling").

The following rule generates an alert when a user attempts to access Salesforce reports which may contain sensitive customer data. The keyword "reports" in the browser's window title limits the scope of alerts to the reports pages of the Salesforce website:

**Did What?**

| Visited URL | : | Any part of URL ▾ | contains ▾ | salesforce.com ... |
| and Ran Application | : | Window title ▾ | contains ▾ | reports| ... |

*Website Category*

This option provides high visibility into your employees' web browsing habits. Use this option to generate alerts when browsing phishing, harmful, counter-productive websites, or websites that are not allowed by policy or are suspicious for specific individuals. ObserveIT has over 28 billion indexed URLs that are updated on a daily basis to keep you up-to-date with new websites and new security risks.

A drop-down list includes all the predefined Website categories:



*Website Category (detailed)*

ObserveIT's Website Categorization module supports direct access to the NetSTAR cloud service. Use this option to generate an alert when a user browses a Website that belongs to any of the native categories defined in the NetSTAR cloud service.

A drop-down list includes all the native categories available in the NetSTAR cloud service.

## Exfiltrated Tracked File (Windows/Mac)

When File Activity Monitoring is enabled, files downloaded from any web application or website are tracked by the ObserveIT Agent. You can use the **Exfiltrated Tracked File** option to generate an alert when a tracked file is uploaded (copied or moved) to the default local sync folder of a cloud file sharing service that is currently supported by ObserveIT.

Following is an example of a rule that will alert when an image file (.png) that was downloaded/exported from Salesforce or Sharepoint is exfiltrated to the sync folder of any of the cloud file sharing services supported by ObserveIT:



In the Alerts page, the alert details show that a medium severity alert was generated when a user copied the `servlet.png` file from Salesforce and exfiltrated it to the sync folder of the Dropbox cloud storage.

## *Exfiltrated Any File (Windows/Mac)*

This option is available for alert type rules on Windows and Mac-based operating systems. Note that this feature is a Beta version.

When File Activity Monitoring is enabled in the System Policy settings, an alert can be configured when any file, tracked or non-tracked, is exfiltrated to the following destinations:

- **To any destination**: An alert is triggered when a file is exfiltrated to any destination, such as any website, cloud sync folder, webmail, social media sites and file sharing sites.
- **To website/web-application (Upload)**: An alert is triggered when a file is uploaded to any website or web-application, including webmail, social media sites and file sharing sites. Uploads can be detected on any file, whether tracked or non-tracked. An uploaded file is not subsequently tracked by ObserveIT.
- **To cloud storage sync folder**: An alert is triggered when a tracked file is moved or copied to a local cloud storage sync folder, such as Dropbox and Box.

## *Downloaded/Exported File (Windows/Mac)*

Use the Downloaded/Exported File option to alert when a tracked file is downloaded or exported from a sensitive website or web application (such as, Salesforce, Sharepoint, CRM, ERP).

Following is an example of a rule that will alert when an image file (.png or .jpg) is downloaded/exported from Salesforce or Sharepoint:



In the Alerts page, the alert details show that a medium severity alert was generated when a user downloaded/exported the `kupon.jpg` image from Salesforce



## *Typed Text (Key Logging) (Windows/Mac)*

The **Typed Text (Key Logging)** option enables you to alert on captured key logger data. Use this option to be alerted when the user types blacklisted commands (within CMD, Powershell, Putty, or Terminal), blacklisted phrases in an email, or sensitive words while browsing social media websites.

## Copied Text (Windows/Mac)

Use the **Copied Text** option to alert on text that was copied to the clipboard, such as, text that has sensitive or confidential content.

Following is an example of a rule that will trigger an alert when confidential text such as a project name "voyager or VYG" is copied to the clipboard while Microsoft Word is running:



After the alert is generated, in the Alerts page, you can view the alert details showing the conditions that triggered the alert:



## Interacted with In-App Elements (Windows)

Use the **Interacted with Application** option to generate an alert when a user interacts by clicking ("Clicked") or by viewing ("Displayed") predefined application sensitive elements (known as **In-App Elements**). By marking sensitive data at element level within applications/websites, you can expose risky user activity and subsequently generate alerts which can be viewed in the ObserveIT Web Console (Activity Alerts, Session Player) and the **Insider Threat Intelligence** dashboard.

The following example shows a typical condition you might define for alerting when a user interacts with an element in the Registry Editor. By changing a value in the registry, severe issues could result with the operating system or the installed software/services.



### Additional Points to Consider

- Upon selecting the **Interacted with Application** option, a submenu displays all applications/websites in which at least one element was marked using the ObserveIT Marking Tool.
- The header of the **Did What?** section displays two unique fields:
- **Interacted application** – The name of the application selected in the submenu. Each **Did What?** condition relates to a single application/website.

- **Identifier** – A dropdown list displaying all pre-marked In-App elements in the selected application/website, from which the user can choose one. The goal of the identifier is to help the security person that reviews the triggered alerts (in the **Alerts** page) to quickly understand the context of the triggered alert. The value of the identifier field in runtime is documented and displayed together with the triggered alert. For example, an alert can be defined to be triggered each time a record of a patient whose doctor is "John Medic" is viewed by any user (in a Health system). By choosing the pre-marked field Patient Name as identifier, this name of the patient will be displayed to the security person together with the triggered alert.

- A single element or multiple elements can be chosen from the multiple-selection dropdown list opened upon clicking the first field in the row. Multiple selection is available only for elements that were marked for the same interaction type (**Clicked**, **Displayed**). Upon selecting the first element, all elements that do not have the same interaction in common are automatically disabled for selection.

- Upon selecting the interaction type **Clicked**, there will be no more options in the conditions. When selecting the interaction type **Displayed**, additional options enable evaluation of the value of the element in runtime against a specific condition (such as, a value that starts with "super").

### Executed SQL Command (Windows)

Use the **Executed SQL Command** option to generate an alert when a user executes a particular SQL command against a database (in Windows). This option is very important since it can help track when a user accesses a database and performs a potentially harmful activity, or even when a DBA performs certain actions at unusual hours or on particularly sensitive data. (For example, when a user runs the "SELECT" statement in the middle of the night in an attempt to steal company data.)

#### Statement

Use this option to generate an alert when a user executes an SQL statement or command that matches specific keywords—such as when a user runs "UPDATE" and "DROP" to tamper with credit card data:



An alert is generated when each command is used uniquely the first time in a session (for example, DROP TABLE CREDIT_CARD). The rule recognizes exact usage of the command and will not generate an alert upon a second execution in the same session.

However, if any values change, a separate alert is generated upon each unique instance. For example, this rule will trigger two separate alerts for the following two instances where the UPDATE CREDIT_CARD command is executed in the same session but with different values assigned:

```
UPDATE  CREDIT_CARD

SET     Blocked = 1

WHERE   CreditCardNumber = 6542789512345614


UPDATE  CREDIT_CARD

SET     Blocked = 1

WHERE   CreditCardNumber = 1234561234561234
```

#### Considerations and Tips

- Executing SQL commands could seriously impact the database. Therefore, it is important to create a rule with this criteria to alert whenever any changes are made to the database.

## *Executed Command (Unix/Linux)*

When safeguarding your system against Unix/Linux commands, your privileged users are the group that are the most risky. Privileged users such as admins who have the access and expertise into the Unix operating system, are the user group that have the know-how to use the commands to steal data, destroy systems, and get away with it. Thus it is extremely important to monitor and alert on Unix commands and privileged users who may want to perform unauthorized or malicious activities that could adversely affect system security or data.

Use the **Executed Command** options to generate an alert when a user executes a particular Unix/Linux command. This is useful to track when a user performs some action on sensitive data, files, directories, paths, user permissions, or system configuration settings. Are they performing some unauthorized or malicious activities that will adversely affect system security or data?

### *Command Name*

Use this option to generate an alert when a user executes a Unix/Linux command. For example, this is useful to track when a user executes "`vi`" to update system configuration files stored under the `/etc` directory (such as `/etc/hosts, /etc/profile`), or executes "`rm`" to remove certain files, or executes "`sudo`" to perform an activity with superuser permissions. The "`sudo`" command is frequently used by system administrators (and infrequently by regular users). Therefore, you may want to refine the rule to include arguments so that you can detect when regular users use the "`sudo`" command to assume root permissions, for example:



### *Parent Command*

Use this option to be alerted if a command is run from another command using its name, or when a command is not run by a specific command.

Following is an example of the conditions you could define to be alerted if the root shell command is opened from unauthorized commands.



### *Top Level Command*

Use this option to be alerted upon the execution of commands run from within an application running under the shell, such as sudo (top level). For example, alert upon the execution of external commands from within a text editor run via sudo.

Following is an example of the conditions you could define to generate an alert if `sudo` is used to run a script.

# Did What?

| | Executed Com... : | Top level command ⌄ | is ⌄ | sudo ... |
|---|---|---|---|---|
| and | Executed Com... : | Parent command ⌄ | is not ⌄ | sudo, sh, bash, dash, ksh ... |
| and | Executed Com... : | Command name ⌄ | is not empty ⌄ | |

➕

*Setuid Mode*

Use this option to be alerted if an unauthorized `setuid` program is run, as this program runs as `root` and the commands it runs internally will also run as `root`.

To ensure that only authorized `setuid` programs are running on the system, you could define the following condition:



*Full Path*

Use this option to generate an alert according to the full path of the command. This may be useful to detect when a command is run from a specific location. For example, you can specify "`/bin/rm`" to generate an alert when a user runs the `rm` command from the native operating system.

*Argument*

Use this option to generate an alert based on specific command line arguments provided by the user. The Argument option is useful to alert when a user attempts to execute some action on sensitive file names, directory names, paths, and so on—such as in the following rule which generates an alert when a user might be maliciously removing a user's profile:



*Switch*

Use this option to alert when a user uses specific command line switches in a command. (A switch is a command line argument that starts with a minus sign "−", for example,
"`rm −r`", "`rm −rf`".) The Switch option provides an easy way to alert on specific command line switches in a way that the Argument option cannot. The reason is that the Switch option detects all variations of the switch flags regardless of syntax order, or whether separated or combined in the alert rule definition, as long as the switch flag group or single switch flag start with "−". For example, if you define: "Command name is ps" and "Switch is −e, -l, -f", an alert will be generated for all variations ("ps −elf" and "ps −fle" and "ps −fe" and "ps −e −l −f", and so on).

To detect a command such as "`rm −rf`", you have to define the rule as "switch is −r, -f" and the system will detect all combinations such as "`rm −fr`", "`rm −rf`", "`rm −r −f`":

*Permissions*

Use the following options to alert when a user uses particular permissions. A user can log in with regular credentials, their own or someone else's, and then assumes root permissions via the `sudo/su` command, or by running any "`setuid`" program that grants root permissions. The system compares the permissions of the original logged-in user with those of the current effective user running the action.

- **Permissions are own**: Use this option to generate an alert when a user logged in with his/her own credentials and ran the specified commands under his/her original permissions (granted at the time of login).

- **Permissions other than own**: Use this option to generate an alert when a user runs the specified commands with permissions that are different from the logged-in user:



- **Permissions are root**: Use this option to generate an alert when a user runs a specific scenario using root permissions (regardless of whether the user logged in originally as root or changed permissions after login):



- **Permissions are root (other than own)**: Use this option to generate an alert when a user logs in with non-root credentials, assumes root permissions using the `sudo/su` command, and then runs the specified commands as root user (or runs any "`setuid`" program that grants root permissions):

## 4.3.3 On Which Computers do the Activities Occur?

On which computer (or within which group of computers/servers) did the activity occur? Use the **On Which Computer?** options to limit the scope of the specified activities to one or more particular computers. This may be useful to generate alerts for activities that are performed on critical computers or sensitive servers.

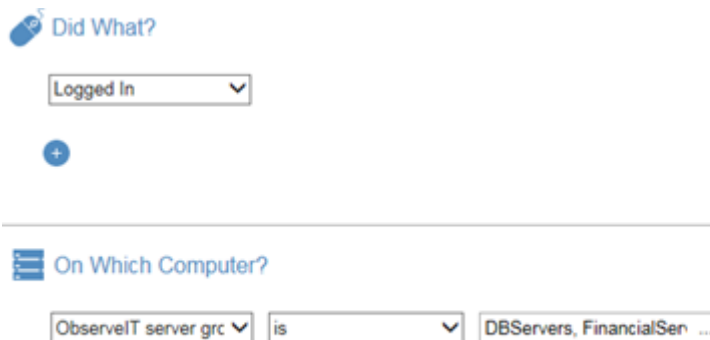### Options for Defining the "On Which Computer?" Conditions

#### Computer [Domain\] Name

Use this option to generate an alert according to the name (and optionally domain) of the computer on which an activity occurred (for example, "LOCAL\DB, DomainA\FIN"). This option is useful if it is critical know when the activity is being performed on a particular computer—such as one with "SQL" in its name:
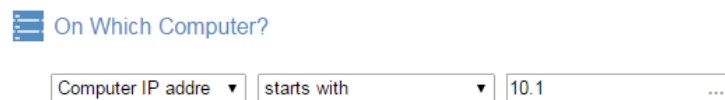


#### ObserveIT Server Group Name

Use this option to limit the scope of the alert to particular server groups defined within ObserveIT—such as when a user tries to log in to sensitive database servers ("DBServers" or "FinancialServers"):



The server groups are defined in the **Configuration > Server Group** page in the Web Console.

#### Computer IP Address

Use this option to limit the scope of the alert to computers with one or more particular IP addresses—such as when a user performs an activity from a computer within an organization where the IPs begin with "10.1":



> **When alert rules are based on IP address ranges, you can specify the IP address range using the CIDR notation format: aaa.bbb.ccc,ddd/N, where N in an integer between 0-32. For example: 192.158.2.0/24**

#### OS Name

Use this option to limit the scope of the alert to computers running a particular operating system (for example, "Windows Server 2012 R2, Ubuntu, Solaris 11"). (Use the OS names and details that are displayed in the **OS Version** list in the **Configuration > Servers** page in the Web Console.) This option may be useful, for example, if you want to catch Windows users accessing Unix Ubuntu machines.

> **Note: You must include the *full* OS name when using the "is/is not" operators. Therefore, it is recommended instead to use the operators "contains" or "starts with" so that you can specify partial searches for OS names (such as "Windows" or "Win").**

*Agent Version Number*

Use this option to limit the scope of the alert to computers running a particular version number of the ObserveIT Agent under which an activity occurred (for example, "5.5, 5.6.9").

### Considerations and Tips

- You may want to know when users perform activities on particular critical computers. Therefore, specifying the computer alert criteria can be very helpful.

## 4.3.4 When do the Activities Occur?

On what day and/or at what time was the activity performed? Use the **When?** options to limit the scope of the alert to particular days/dates/times. This may be useful to generate alerts for activities that are performed during suspicious times, such as outside regular business hours.

### Options for Defining the "When?" Conditions

- **Day(s) of Week**: Use this option to limit the scope of the alert to particular days of the week. For example, "Day of week is Saturday, Sunday" or "Day or week is not Tuesday".
- **Time(s) of Day**: Use this option to limit the scope of the alert to particular times. For example, "Time of day is before 10:59" or "Time of day is between 08:00 and 18:00".
- **Specific Date(s)**: Use this option to limit the scope of the alert to particular dates. For example, "Specific date is 25/12/2014" or "Specific date is not between 15/09/2014 and 30/09/2014". You can use this option to include a list of holiday dates throughout the year.
- **Specific Date(s) and Time(s)**: Use this option to limit the scope of the alert to a particular range of dates and times—such as when activities are performed outside regular business hours, during weekends or holidays, not during the month of August:



Note that the date format is: dd/mm/yyyy and the time format is: hh:mm:ss.

### Considerations and Tips

- Consider what activities are relevant for your organization to track during regular work hours and those important to track when they occur outside business hours. Note also the exceptions which should not be monitored, such as when specific IT administrators perform maintenance work over the weekend.

## 4.3.5 From Which Client Computers?

From which client computer did the user connect to the monitored computer (on which the activity occurred, as described in On Which Computer?)? Use the **From Which Client?** options to limit the scope of the alert to cases where a user connected to a monitored computer from one or more particular client computers.

### Options for Defining the "From Which Client?" Conditions

- **Client Name**: Use this option to alert according to the name (and optionally domain) of the client computer from which the user connected to the monitored computer. For example, "Client name *is* OITLAP, OITPC" or "Client name *does not start with* OIT" or "Client name *contains* LOCAL\LAPTOP".

- **Client IP Address**: Use this option to alert according to the IP address of the client computer from which the user connected to the monitored computer. IPv4 and IPv6 formats are supported. For example, "Client IP address *is* 10.1.0.16, 10.1.2.100" or "Client IP address *is not* fe80:0000:0000:0000:c033:d38d:88d7:de73"—or "Client IP address *does not start with* 10.1" to alert when a user tries to log in to a monitored computer from an IP address outside the organization:



> When alert rules are based on IP address ranges, you can specify the client IP address range using the CIDR notation format: aaa.bbb.ccc,ddd/N, where N in an integer between 0-32. For example: 192.158.2.0/24

### Considerations and Tips

- It may be valuable to specify IP addresses of particular external or internal client machines to track from where particular users (such as remote vendors or employees) are accessing your system, or from where they are performing particular activities that may affect system security.

## 4.4 Defining Actions for Alert Rules

After defining a detection policy for a rule that will trigger an alert, you can specify actions to be taken when the alert is triggered.

ObserveIT preventive actions enable security and compliance officers to stop users from breaching security or violating company policies. On Windows, Mac, or Unix endpoints, users can be forcibly logged off from machines that they are not authorized to access or to prevent them from continuing with activities that are risky or malicious. On Windows or Mac endpoints, applications or Web browsers that users should not be running can be forcibly closed, including "triggering" applications (for example, when users browse forbidden websites or website categories, or execute potentially harmful SQL commands).

ObserveIT enables you to configure **Warning Notifications** or **Blocking Messages** to notify end users in real-time about any violation of an organization's security policy, so that they can take remedial action. On Windows and Mac endpoints, users can acknowledge a message, add a comment explaining their actions, and open a link to view the company policy. If required, you can also select to start recording screenshots of the user activity from the point at which the alert was generated. Configured actions identified by specific icons are displayed throughout the ObserveIT Web Console and the User Risk Dashboard.

End-user messages appear on the screen after a risky activity has occurred and an alert was generated.

In the **Action** area of the **Create/Edit Alert Rule** page, depending on your operating system, you can define the following actions that will be taken when an alert is triggered:

- No Action
- Warning Notification
- Blocking Message
- Start Video Recording
- Start Standard Recording
- Log Off
- Close Application

### 4.4.1 No Action

(Windows/Mac or Unix systems). This is the default action that is automatically selected when creating a rule.

### 4.4.2 Warning Notification

(Windows/Mac or Unix systems). Notify users in real-time about potential out-of-policy behavior, in order to raise their awareness of the organization's security policy. On Windows, users can add a comment explaining their actions, and open a link to view the company policy. On Unix, users can only see the warning notification, but cannot respond to it with feedback, and cannot open a link to a company policy. On both operating systems, while configuring a warning notification, you can select to start recording screenshots of the user activity from that point. By default, every time a warning notification is displayed to the user, a predefined sound will be played. You can also display a company logo or image with each Warning Notification (not configured by default).

Following is an example of an end user warning notification on Windows OS:
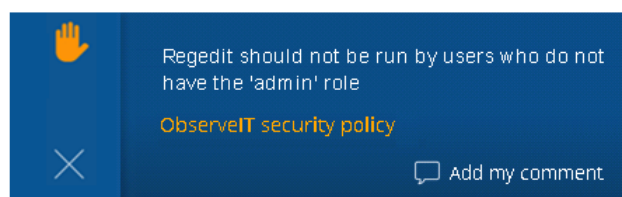
Following is an example of an end user warning notification on Unix OS:
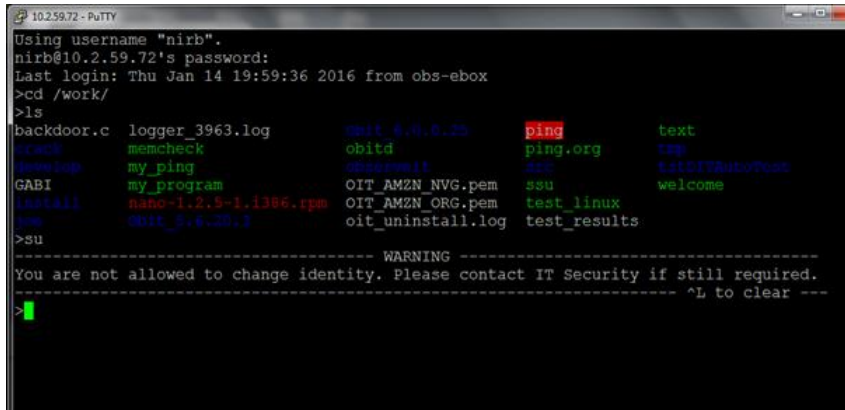


## 4.4.3 Blocking Message

(Windows/Mac systems). Blocking messages, which open after a user has performed a risky activity, block the screen with a message forcing users to stop what they are currently doing. Users can be required to acknowledge the message, provide feedback explaining their actions (forcing text feedback), and open a link to view the company policy. While configuring Blocking Messages for a rule, you can also select to start recording the screenshots of every user activity from that point onwards.

Following is an example of an end-user blocking message on Windows OS:
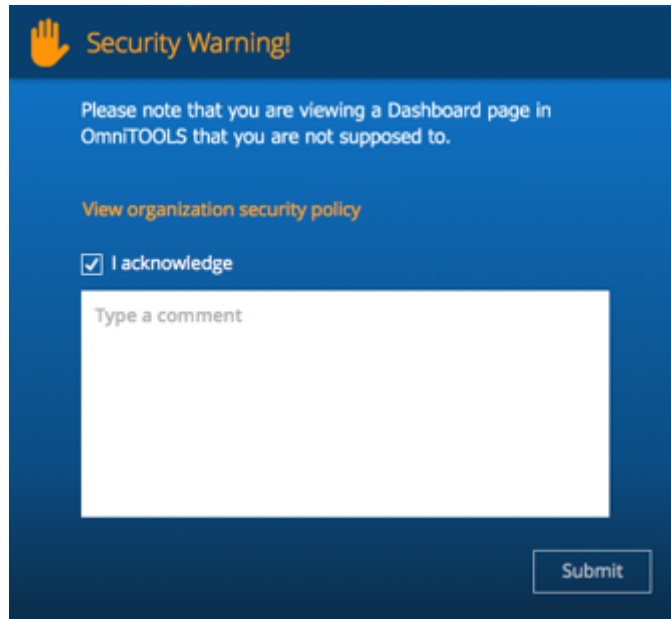


## 4.4.4 Start Video Recording

(Windows/Mac systems). While configuring alert rules on Windows systems, when the conditions of a specific detection policy are met, the security administrator can select to start recording screenshots of user activities from that point onwards, by clicking the **Start Video Recording** action option. This option is relevant only for users for which the currently applied recording policy is to capture metadata-only without screenshots; for these users, the rest of the session will be fully recorded including the capturing of screenshots.

## 4.4.5 Start Standard Recording

(Unix systems). When the conditions of a specific detection policy are met, the security administrator can select to record user activity in standard mode while configuring alert rules on Unix systems as a standalone action, by clicking the **Start Standard Rec.** action option. This option is relevant only for users for which the currently applied data recording policy is Commands-only mode; for these users, the rest of the session will be recorded in the extended Standard mode (that is, commands and terminal output).

### 4.4.6 Log Off

(Windows/Mac or Unix systems). The **Log Off** action enables you to block users that log in to machines which they are not authorized to access or prevent users from continuing with activities that are risky or malicious. This action blocks the user's screen with a message asking them to log off or they will be automatically logged off within a specified period of time which is configurable (by default 30 seconds). Users have an option to provide an explanation for their activity within this time period.

### 4.4.7 Close Application

(Windows/Mac systems). The **Close Application** action block users that are running harmful applications by forcing their closure. The force closing of applications can also be applied on "triggering" applications (such as, browsers or SSMS) when users browse forbidden websites or website categories, or execute potentially harmful SQL commands. The user's screen is blocked with a message asking them to close the application or it will be automatically closed within a specified period of time which is configurable (by default 30 seconds). Users have an option to provide an explanation for their activity within this time period.

## 4.5 Assigning Alert Status

Alerts can be assigned one of the following statuses according to administrator assessment:

- **New**: Newly-configured alerts that have not yet been assigned any other status.
- **Reviewing**: Alerts that are currently being reviewed by the administrator for follow-up action.
- **Issue**: High risk alerts that require attention by the administrator and contribute to the user risk score during user risk analysis. User risk score is a value attributed to user actions, which depend on risk severity levels.
- **Non-Issue**: Alerts that have been reviewed by the administrator and are considered low risk. These alerts will not contribute to the user risk score during user risk analysis.

In the **Alerts** page, an administrator can change the status of a selected alert(s) by clicking the **Change status** link. A popup enables you to select the required status. You can select multiple alerts for changing their status at the same time.

> If you change the status to Non-Issue, **the alert score will be reset to zero and the risk score of the user for whom the alert was defined will be reduced. In the User Risk Dashboard, you will be able to see the change in the user's risk score and a reduction in the number of alerts assigned to the user. If any warning notifications or blocking messages were assigned to the user, these indications will also be reduced; these changes will also be reflected in the User Risk Dashboard.**
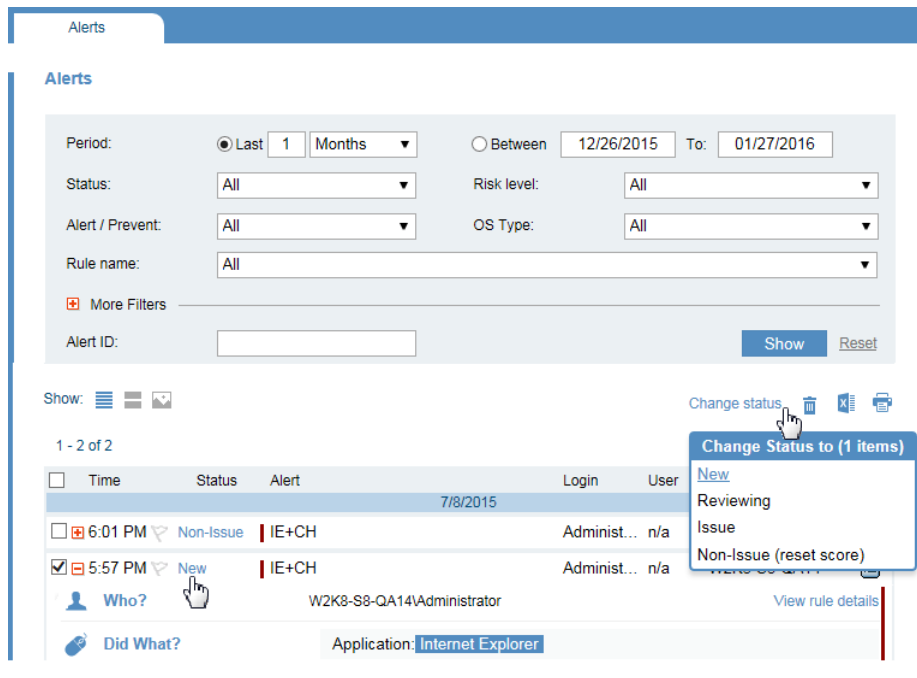
## 4.6 Setting Alert Risk Level

Administrators can assign a risk level to each alert or prevention rule according to the severity of the alert (based on their organization's needs). The alert risk levels are Critical, High, Medium, and Low, and are color-coded in ObserveIT (as Dark Red, Red, Orange, and Gray). This makes it easier to review generated alerts, generate reports, and in particular, this enables ObserveIT administrators to quickly identify the risk level and respond accordingly (see Viewing Generated Alerts in ObserveIT). Administrators can decide according to the severity how often email alert notifications are received (see Managing Email Notifications).

## 4.7 Managing Alert Email Notifications

Administrators can assign a notification policy to each alert or prevent rule to designate who gets notified by email and at what frequency (whether immediate notification with separate emails upon each alert, digest emails of alert activity per specified number of minutes, or digest emails on a daily basis at a fixed time). This enables IT security officers to receive immediate warnings of high-risk activities, while reducing email overhead for those of low risk.

When an alert is triggered, and an email notification is received (per the rule's policy), the ObserveIT user/administrator can click a link in the email to open the alert in the **Alerts** page of the Web Console for further investigation (see Viewing Alerts in Email Notifications).

Administrators configure alert notification policies in the **Alert Notification Policies** page of the ObserveIT Web Console and assign a notification policy to an alert rule in the **Create Alert Rule** page.

## 4.8 Saving Alert Rules

When you have completed configuring each rule, remember to save the settings. You can save a rule that is not activated and activate it later, when needed. (For example, you may want to complete the rule at a later stage or modify it further before activating it.)

You can save the alert rule by clicking **Save** Save at the bottom of the **Create Alert Rule** page.

## 4.9 Activating Alert Rules

Rules are inactive by default and must be activated to trigger alerts. (Inactive rules are ignored by the rule engine.) You can edit a rule and save it multiple times before you activate it.

To activate the rule, in the **Edit** (or **Create**) **Alert Rule** page, set the **Status** to **Active**, and click **Save** at the bottom of the page.



After you have activated the rule, your rule creation is complete. It is recommended to test the rule to see if an alert is triggered. For further details, see Viewing Generated Alerts in ObserveIT.

# 5 Defining Prevention Rules

**You can create prevention rules on Linux operating systems only.**

ObserveIT can prevent unauthorized Linux commands from being executed based on flexible prevention rules that you can define. For example, if you attempt to run commands that manipulate sensitive files, the commands will be blocked from execution, preventing access to the files.

Prevention rules are configured by ObserveIT administrators to define the conditions under which an alert will be triggered. As opposed to alert rules for which you can warn the user about any out-of-policy behavior, prevention rules are designed to prevent the user from continuing with their current activity. When a prevention rule is triggered, the current activity will be blocked and the standard operating system `Permission denied` message will be displayed together with a customized text message (if configured). End users cannot acknowledge the message, explain their actions, nor view a security related policy.

Prevention rules are displayed in the **Alert & Prevent Rules** page in the ObserveIT Web Console. From this page, you can create new prevention rules or edit existing rules. You can navigate to this page via **Configuration > Alert & Prevent Rules**.

The following steps are required to define a prevention rule:

1. In the Alert & Prevent Rules page in the ObserveIT Web Console (Configuration > Alert & Prevent Rules), click the **New Linux Prevent Rule** button.
2. Specify the rule details. See General Rule Details.
3. Configure a detection policy for the rule that will trigger the alert. See Defining a Detection Policy for Prevention Rules.
4. Specify the action to take. The only action you can apply to the end user for a prevention rule is to "Prevent Execution". See Defining Actions for Prevention Rules.
5. When you have finished creating your rule, click **Save** to save your settings.

## 5.1 Defining a Detection Policy for Prevention Rules

When creating (or editing) a prevention rule, you can configure a detection policy that answers the following questions:

- **Who?** – Who was logged in to the session when the alert was triggered? See Options for Defining the "Who?" Conditions.
- **Did what?** - What was the user doing when the alert was triggered? Note that the only **Did What?** condition that you can configure for a prevention rule is **Executed Command** (based on **Command name** and/or **Arguments**). See Executed Command (Unix/Linux).
- **On which computer?** - On which computer was the user logged in? See Options for Defining the "On Which Computer?" Conditions.

## 5.2 Defining Actions for Prevention Rules

After defining a detection policy for a prevention rule, the only action you can apply to the end user if an alert is triggered is to "**Prevent Execution**" of the activity they were trying to perform. You can choose to display a message to the user, but the user cannot acknowledge the message, explain their actions, nor view the company policy. However, while configuring the **Prevent Execution** action, you can also select to switch the recording mode to **Standard** mode until the end of the session, which means that all user commands and terminal output will be recorded.

# 6 Alert and Prevention Rules – Sample Walkthrough

This section guides you through the process of building alert or prevention rules, from simple rules to more advanced ones. Its goal is to convey the power and flexibility of the rules so that you can better understand how to build and customize your own rules according to your organization's needs.

The sample scenarios demonstrate how the rule logic is expressed in ObserveIT. For details about the rule structure and logic, conditions, and strategy for building rules, see Rule Structure and Logic.

Alert and prevention rules are created in the ObserveIT Web Console in the **Alert & Prevent Rules** tab. You can navigate to it via **Configuration > Alert & Prevent Rules**.

## 6.1 Sample 1: User Logs in After Hours

This simple example creates a rule to generate an alert when a user logs in to any computer outside business hours. Why are employees logging in after work? What are they up to?

This rule defines *after working hours* as:

- On weekends (Saturday or Sunday), *or*
- Before or after business hours (not between 08:00 and 18:00)

In ObserveIT, this rule looks like this:



In the **Alerts** page, the details of an alert triggered by this rule looks like this:

In slideshow mode, the same alert looks like this:
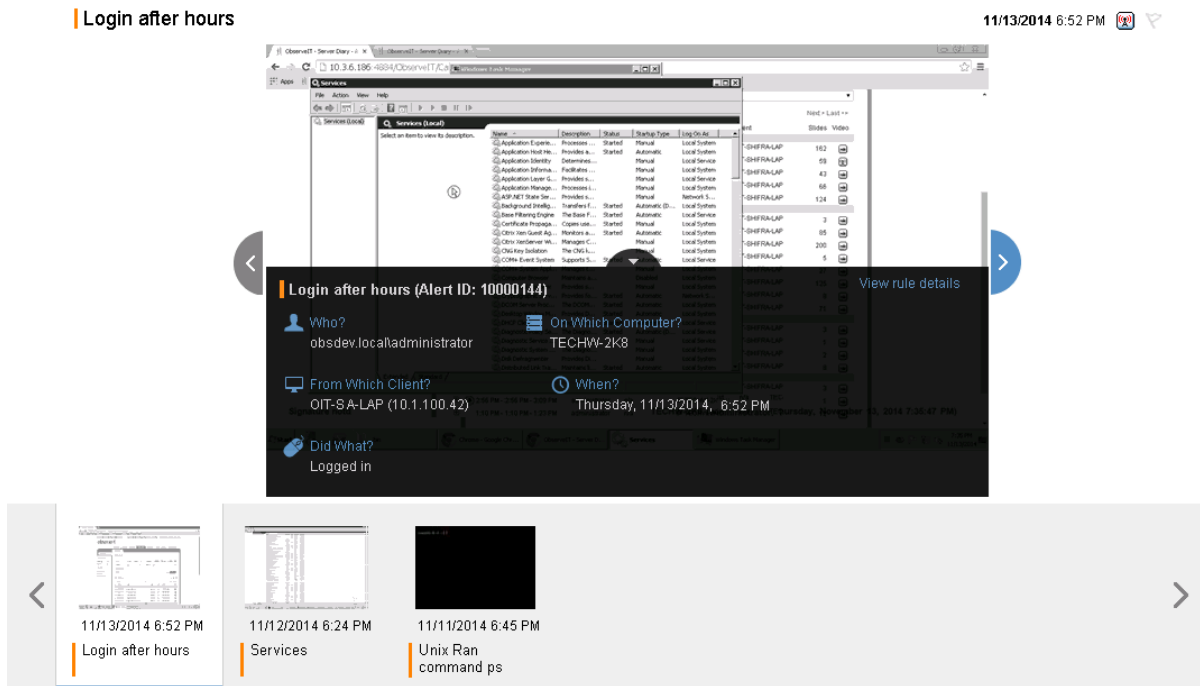


## Additional Points to Consider

Beyond the basic options presented in this scenario, you can:

- Specify additional criteria to alert when a certain user or user group logs in, at what time, on what target computer, and on which client machine. For further details, see Rule Conditions.
- Check the date/time of activity, whether before, after, between certain days or hours, or not on certain days by using any of the available operators. For further details, see When do the Activities Occur?
- Configure general settings for every alert rule. For further details, see General Rule Details.
- View the generated alerts in the ObserveIT Web Console. For further details, see Viewing Generated Alerts in ObserveIT.

# 6.2 Sample 2: User Transfers Large Files Using a Cloud Application

This example demonstrates how to create a rule to alert when a user attempts to transfer large company files using a cloud service instead of via a platform which is authorized by the company policy. This rule could be crucial for alerting when company data may be at risk of being exposed to the public.

> By alerting when a user copies or moves sensitive company files, security and risk analysts can quickly pinpoint users who are putting a business at risk. The risk score of these users would be increased and displayed in the ObserveIT User Risk Dashboard.

For purposes of this example, WeTransfer is the online file-transferring platform.

In ObserveIT, the rule might look like this:
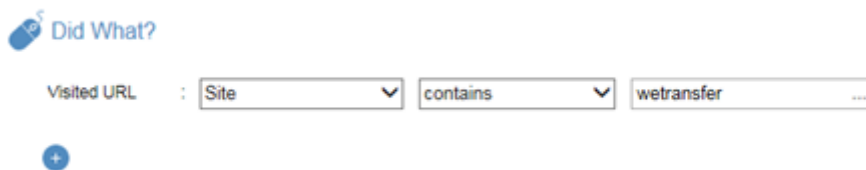
An alert is generated only once per session—the first time that the user visits www.wetransfer.com (and not for subsequent pages visited in this site). This helps you identify that this site was accessed, and that the user may be attempting to transfer company data over the cloud, in an unsecured manner to unknown outside parties. You can always track additional uses of WeTransfer in the session by using the ObserveIT **Search** and **Session Player** functionalities.

### *Additional Points to Consider*

You can define rules to alert when:

- A user visits any unique webpage in the WeTransfer site. For example, "Visited URL: Any part of URL contains wetransfer" would generate two separate alerts when a user accesses the following two pages on this site: www.wetransfer.com/mobile and www.wetransfer.com/plus. For further details, see Any Part of URL.

- A user visits a specific area of the WeTransfer site. For example, "Visited URL: URL prefix contains wetransfer.com/plus" would generate an alert when a user accesses the WeTransfer Plus area (which enables users to transfer very large files, up to 10GB). For further details, see URL Prefix.

## *6.3 Sample 3: Remote Vendor Potentially Changes Registry Values on a Sensitive Server*

This more advanced example demonstrates how to create a rule to alert when a specific user potentially changes a value in the Windows Registry on critical servers while connected from a non-recognized (external) IP address. Changing a value in the Registry Editor could cause severe problems with the operating system or the installed software or services.

This rule also specifies that the user is a remote vendor using his credentials for login or secondary authentication. (You can check the user by Active Directory group, name of the gateway machine they are using, specific user names, or domain.)

Note: In this example, the rule is assigned to all users.

The configuration of this rule might look like this:



In the above example, an alert will be generated when a remote vendor connects from an external IP (that does not start with the company's local prefix "**10.2**"), logs on to servers belonging to the specified groups (**DBServers** or **FinancialServers**), runs Windows Registry Editor, and opens the dialog box that allows changing the value of a registry key.

Due to the severity of this rule, after an alert is triggered, the user's screen will be blocked with a message forcing the user to stop the current activity and read the message. According to the above configuration, the user must acknowledge the message and provide feedback explaining his actions. In addition, the user can open a link to view the company policy about accessing sensitive servers. For details, see Blocking Message.

## Additional Points to Consider

A wide variety of user activity can be monitored and alerted, such as when:

- Specific applications or processes are run, when URLs in Web browsers are visited, and when certain text is displayed in window titles. For further details, see Rule Conditions.
- Groups of users and/or users that are part of a certain domain perform a suspicious activity. This is the typical use-case, rather than tracking a specific user. This enables tracking users more easily, when you may not know specific user names. For further details, see Who Performs the Activities that Trigger Alerts?
- You can assign rules to specific User Lists, each with their specific risk level. For example:

| Add user list to this rule | | ✖ |
| --- | --- | --- |
| **User List Name** | | **Risk Level** |
| ☑ Admin Users | | Medium ▼ |
| ☐ Regular Users | | Medium ▼ |
| ☑ Remote Vendors | | Critical ▼ |
| ☐ Users in Watch-List | | Medium ▼ |
| | | Add   Cancel |

For further details, see Assigning Alert Rules to User Lists.

You can also define rules to:

- Include AND/OR logic. For example, to alert when an administrator adds or removes a user, you can define: "Command name is useradd, userdel". For further details, see Rule Logic.
- Check for various parameters, users, domains, servers, computers, client machines, and so on. You can use naming conventions in the rule, such as the "Computer name starts with LAP". For further details, see On Which Computers do the Activities Occur? and From Which Client Computers?).
- Check for users by login name, secondary identification, or both. For further details, see Who Performs the Activities that Trigger Alerts?
- Check for users by permissions. For example, only users who have Administrator permissions (and therefore may do harm), or non-admin users who have NO admin rights and may be performing unauthorized activities—*Why are they trying to use Regedit?* For further details, see Permission Level.
- Set the scope of the alert frequency–how often to generate an alert for a recurring activity. The default alert frequency is **Each time** (for example, every time someone runs the `Regedit` application even if it happens multiple times within a session) or just **Once per session**.  For further details, see Alert Frequency.

# 6.4 Sample 4: Preventing the Abuse of Privileged Permissions to Create a Backdoor User

Now that you understand how to build advanced rules, this example proceeds to create an alert rule specific to a Linux environment.

This example demonstrates how to create a prevention type rule that will trigger a high risk alert when someone creates a local admin user (with `root` permissions) that could be a potential security risk to the system. The new admin user would then be able to log in undetected (unmonitored by the system) and perform malicious actions. For example, a user who obtains temporary `root` permissions in order to accomplish a specific task could abuse it to add a backdoor user that can be used in the future.

In this example, the security administrator configures a prevention rule to block a non **Admin** user attempt to run the `su` (switch user) command to switch identity even with `root` permissions.

In ObserveIT, the configured rule might look like this:



When the alert is triggered, the `su` command will be blocked from execution, disabling the user from changing the identity. The end user will receive the standard operating system `Permissions denied` message together with the configured text message:

```
$ su
-sh: 1: su: Permission denied
$
-------------------------------------- WARNING --------------------------------------
Non admin users should not be allowed to su to root even if they have the root password
---------------------------------------------------------------- ^L to clear ---
```

**Security administrators will be able to view a recording of the user activities in standard mode (all commands and terminal output).**

## *Additional Points to Consider*

You can define rules:

- To alert when a user uses specific command line arguments in a Unix/Linux command to execute some action on sensitive file names, directory names, paths, add users, change permissions, and so on, by using arguments in the rule. Arguments can be used in cases that require detecting exact matches of the syntax order. Switches can be used for cases that require more flexibility, to detect switch flags regardless of syntax order or how they are combined in the alert rule definition (as long as the switch flag group or single switch flag start with a minus sign "−"). For further details, see Executed Command (Unix/Linux), Argument, and Switch.

- To alert when a user runs commands as a root user, regardless of how root permissions were obtained (by running, for example, `su`, `sudo`, or any `setuid` program). For further details, see Permissions.

- To alert when a user runs any commands on Unix/Linux systems, such as when a user attempts to copy, rename, modify, or delete certain system configuration files or folders. For further details, see Command Name.

# 7 Viewing Generated Alerts in ObserveIT

When an alert is generated, alert indicators and details appear throughout the ObserveIT system, as described in the following sections:

- Viewing Alerts in Email Notifications: Email notifications provide summary information about alerts and include links to the Web Console for viewing session details and screenshots in slideshow or video mode.
- Viewing a List of Alerts: The **Alerts** page displays a list of all the alerts and related details.
- Viewing Alerts in Gallery Mode: Browse through screenshots of each alert while viewing the full alert details.
- Viewing Alerts in Session Diaries: Recorded sessions that contain alerts are marked with appropriate alert indications that are displayed in the relevant **Server Diary**, **User Diary**, and **Search** results page.
- Viewing Alerts in the Session Player: View and replay the recorded sessions in which alerts were triggered.
- Viewing Alerts in the User Risk Dashboard: View and investigate details about the highest risky alerts that were triggered against risky users.
- Generating Custom Reports about Alerts: Create customized reports with summary information about alerts on monitored Windows and/or Unix-based servers.

The user-friendly graphical display of the generated alerts enables you to quickly assess the threat and take immediate action if needed.
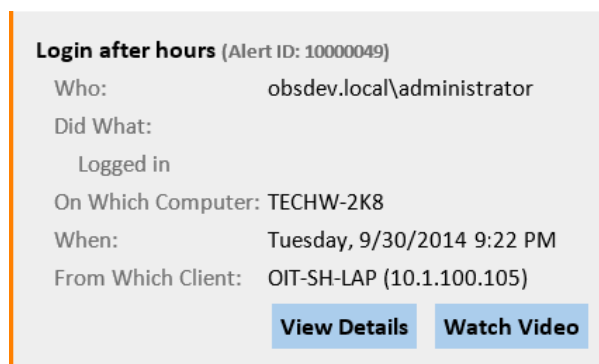
## 7.1 Viewing Alerts in Email Notifications

Alerts can be sent to one or more email addresses as defined in the Notification Policy associated with each alert rule. For further details about notification policies, see Managing Email Notifications.

Alert emails display the following details:

- Colored severity bar (on the left) indicating the alert severity level (Dark Red=Critical, Red=High, Orange=Medium, Gray=Low)
- Alert rule name (in bold)
- Alert ID
- Conditions that triggered the alert (Who, Did What, On Which Computer, When, From Which Client)
- **View Details** and **Watch Video** buttons for accessing the Web Console to view details in either a maximized view of the alert in slideshow mode, or in a video of the recorded session to view what the user was doing when the alert was triggered.

### 7.1.1 Individual Alert Email Notifications

Individual email notifications display details of the alert:

## 7.1.2 Alert Digest Emails

Digest emails (as shown below) display some additional details and links:

- **Alert Summary**: lists the number of alerts per severity
- **Alert Details**: displays information about each alert, grouped by severity

You can click any of the links to access the Web Console to view session details and screenshots in slideshow mode (in addition to the **View Details** and **Watch Video** buttons).

## 7.2 Viewing a List of Alerts

In the **Alerts** page, you can view the names, user risk level, applied action (if defined in the alert rule), and status of all triggered alerts, with the newest alerts at the top (organized by date/time and color-coded per risk level).

You can monitor the number of alerts generated for each rule, and if required, you can modify the rule criteria by clicking an alert rule name to open its edit page.

> **You can view the generated alerts in Gallery mode, to view screenshots and slides showing exactly what the user was doing when the alert was triggered (see Viewing Alerts in Gallery Mode). In addition, you can launch the Session Player to view a video replay of the session in which the alert occurred (see Viewing Alerts in the Session Player).**

Navigate to the **Alerts** page by selecting **Configuration > Alerts** in the Web Console.

**Alerts**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Period: | ⦿ Last 1 Months ▼ | ○ Between | 01/02/2016 | To: | 02/03/2016 | | |
| Status: | All ▼ | | Risk level: | All ▼ | | | |
| Alert / Prevent: | All ▼ | | OS Type: | All ▼ | | | |
| Rule name: | All ▼ | | | | | | |
| ⊞ More Filters | | | | | | | |
| Alert ID: | | | | | | Show | Reset |

Show: ≡ ▬ ⤓            Change status 🗑 📄 🖨

1 - 20 of 551                    1 2 . . . 27 28                    Next > Last >>

| | Time | Status | Alert | Login | User | Server | Video |
|---|---|---|---|---|---|---|---|
| | | | **2/2/2016** | | | | |
| ☐ ⊞ | 4:31 PM | ▽ New | Unauthorized USB drive Accessed | administ... | ilan | OITSRV | 📹 |
| ☐ ⊞ 💬 | 4:31 PM | ▽ New | USB or similar device inserted - autopl... | administ... | ilan | OITSRV | 📹 |
| ☐ ⊞ ⊠ | 4:30 PM | ▽ New | Remote Desktop Connection | administ... | ilan | OITSRV | 📹 |
| ☐ ⊞ ⊠ | 4:30 PM | ▽ New | Remote Desktop Connection | administ... | ilan | OITSRV | 📹 |
| ☐ ⊞ ⊠ | 4:30 PM | ▽ New | Remote Desktop Connection | administ... | ilan | OITSRV | 📹 |
| ☐ ⊞ | 3:44 PM | ▽ Non-Issue | Windows Title contains "Services" | administ... | ilan | OITSRV | 🖥 |
| ☐ ⊞ 💬 | 1:13 PM | ▽ Non-Issue | user started Putty Session | administ... | ilan | OITSRV | 🖥 |
| ☐ ⊞ ⊠ | 1:13 PM | ▽ Non-Issue | Remote Desktop Connection | administ... | ilan | OITSRV | 🖥 |
| ☐ ⊞ ⊠ | 1:13 PM | ▽ Non-Issue | Remote Desktop Connection | administ... | ilan | OITSRV | 🖥 |
| ☐ ⊞ ⊠ | 1:13 PM | ▽ New | Remote Desktop Connection | administ... | ilan | OITSRV | 🖥 |
| ☐ ⊞ | 11:03 AM | ▽ New | Unauthorized USB drive Accessed | administ... | ilan | OITSRV | 🖥 |
| ☐ ⊞ 💬 | 11:03 AM | ▽ New | USB or similar device inserted - autopl... | administ... | ilan | OITSRV | 🖥 |
| ☐ ⊞ | 11:03 AM | ▽ New | Windows Title contains "Services" | administ... | ilan | OITSRV | 🖥 |
| | | | **2/1/2016** | | | | |
| ☐ ⊞ | 4:18 PM | ▽ New | Windows Title contains "Services" | administ... | ilan | OITSRV | 🖥 |
| ☐ ⊞ | 2:14 PM | ▽ Non-Issue | Windows Title contains "Services" | lior | n/a | OITSRV | 🖥 |
| ☐ ⊞ | 2:14 PM | ▽ Non-Issue | Edit application file in C:\Program Files... | lior | n/a | OITSRV | 🖥 |
| ☐ ⊞ | 2:13 PM | ▽ Non-Issue | Unauthorized USB drive Accessed | administ... | ilan | OITSRV | 🖥 |

You can filter the alerts list per criteria, such as time, status, risk level, alert rule type (alert/prevent), OS type, flagged alerts, and/or alerts associated with a certain rule, user, server, or client, and so on.

In the **Alerts** page, you can also:

- Flag important alerts for follow-up.
- Change the status of specific alerts.
- Expand an alert row to view more details, including the conditions (**Who?**, **Did What?**, etc.) which triggered the alert, and any action (for example, **Warning Notification**) that was configured for the alert.

The following example shows the details for a medium risk level severity alert (indicated by an orange indicator next to the alert rule name and to the right of the details). Note that in this example, a warning notification was configured to be displayed to the risky user. For further details, see Warning Notification.

## 7.3 Viewing Alerts in Gallery Mode

In **Gallery** mode, you can browse through the screenshots of each alert while viewing the full alert details next to each screen. Viewing alerts in Gallery mode provides a view of the user environment, enabling you to see the context of exactly what the user was doing when an alert was triggered.

You can open the Gallery mode by clicking the ▣ icon in the **Show** area of the Alerts page.

In Gallery mode, you can:

- Browse through the screenshots by clicking the Next ▶ or Previous ◀ buttons. The alert details change accordingly.

  Note that if an action was configured for the alert, the details show the action type (for example, **Warning Notification**) as the header, as shown in the above screenshot.

- Click the Video 🎞 icon to open the Session Player at the screen location where the alert was generated.

- Click the ⬈ icon to maximize the screenshots view, as shown in the following example:
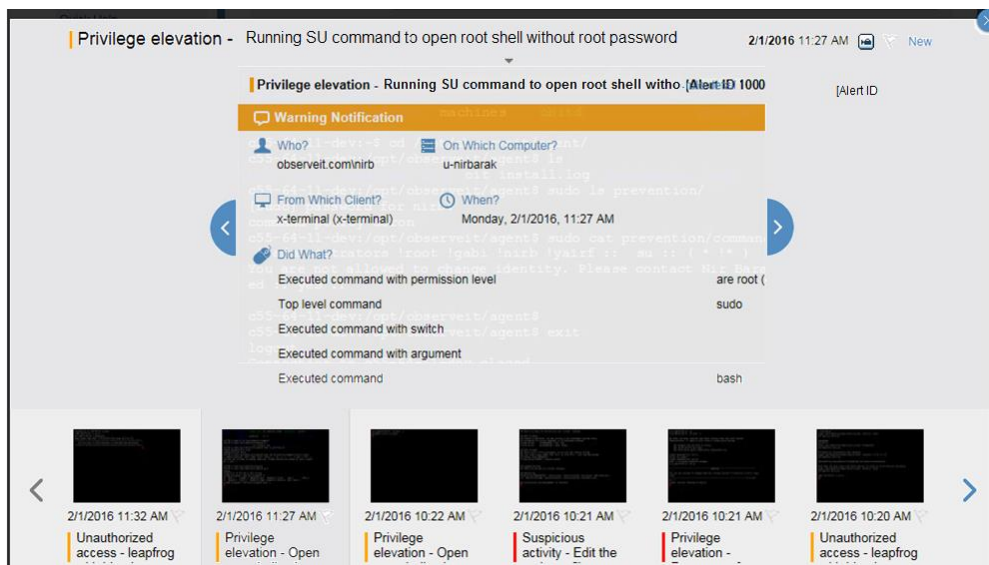


In maximized view, you can:

- See a slideshow of the alert screenshots, with alert details emphasized.

- Use the ▶ and ◀ buttons to move through the slideshow.

- Select a slide in the slideshow to see the details of an alert maximized.

- Click the Video 🎞 icon to open the Session Player at the screen location where the alert was generated.

The following example displays a video replay of the above session showing exactly when the alert occurred. Note that the color of the ring around an alert icon shows the alert risk level; in this case, medium (orange).
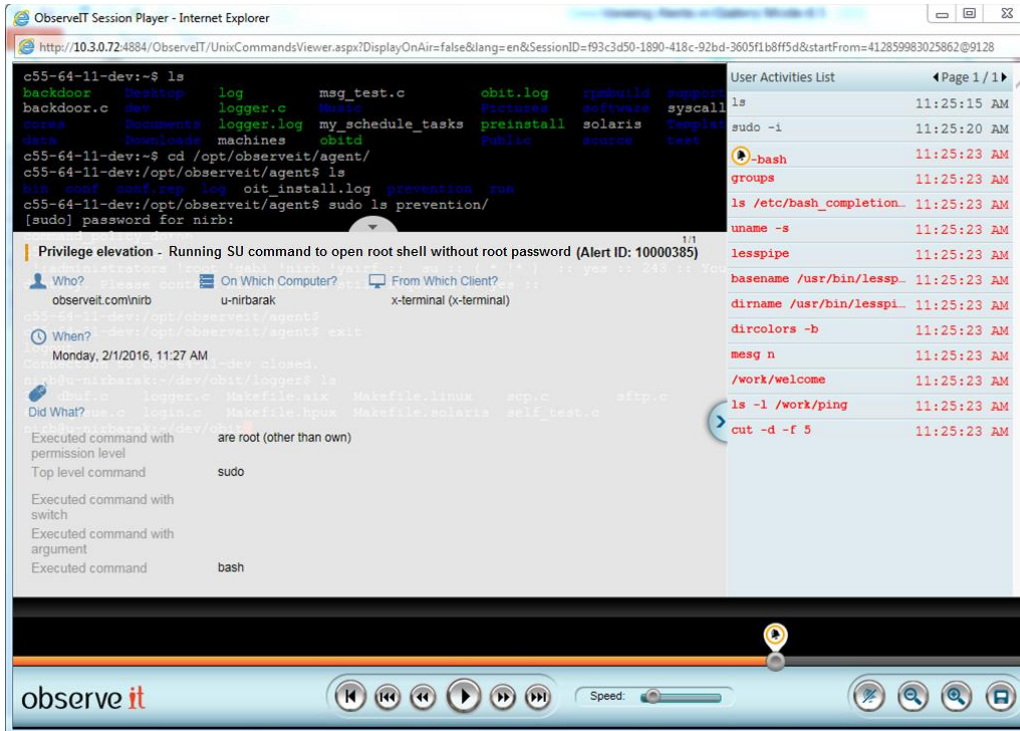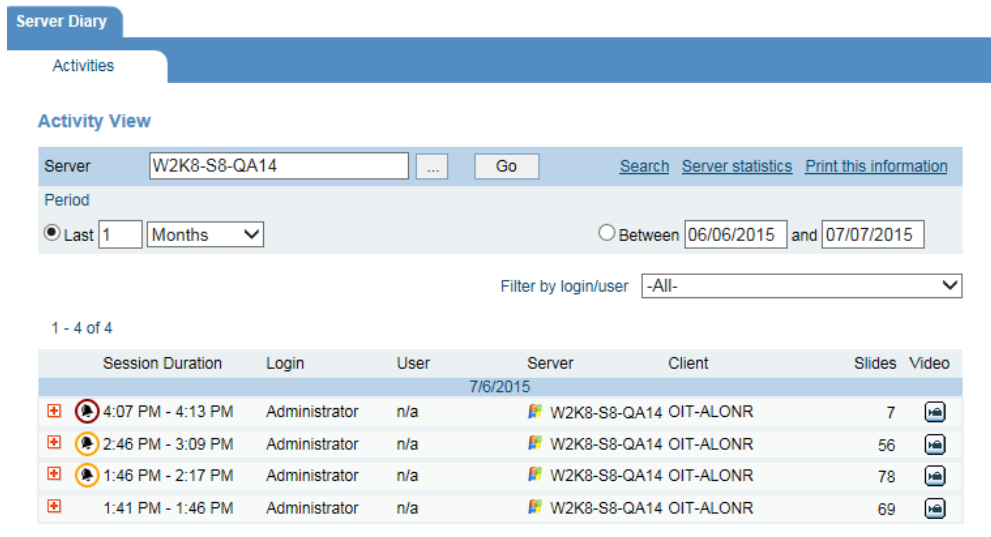
## 7.4 Viewing Alerts in Session Diaries

Recorded sessions that contain alerts display alert indications in the relevant **Server Diary**, **User Diary**, and **Search** results (you can search according to alert IDs).

Following is an example of the **Server Diary** showing high and medium risk level alert indications next to some sessions.
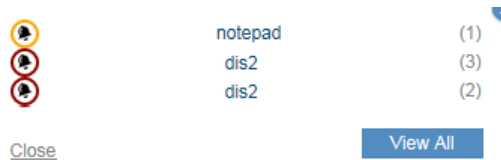


**You can click a Video**  **icon to open the Session Player at the screen location where the alert was generated.**
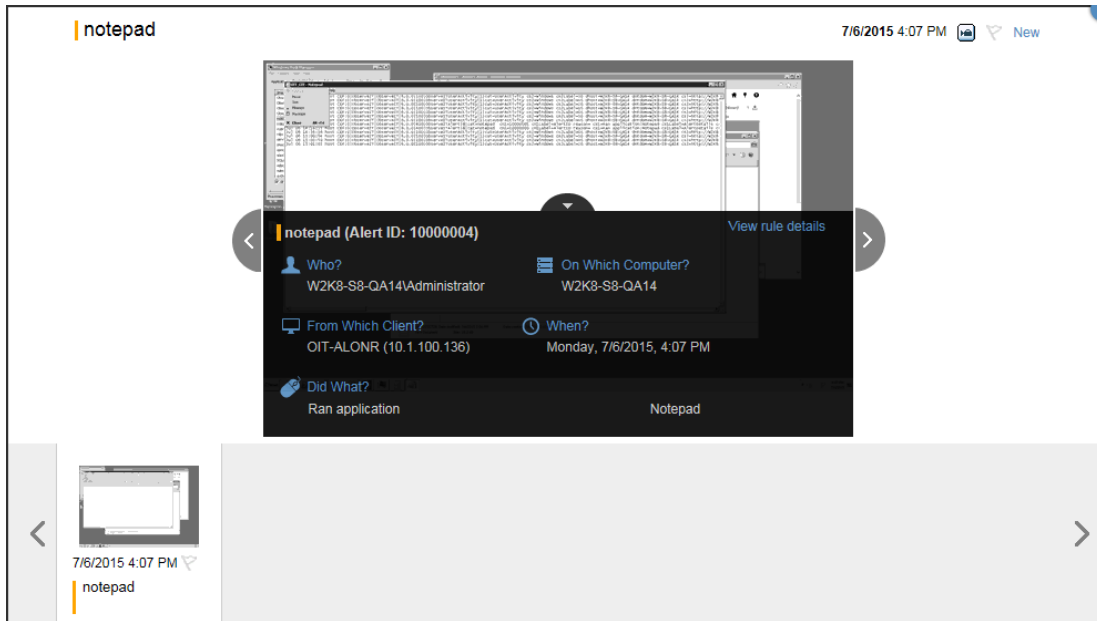
Clicking an alert  icon next to a session opens a popup displaying a list of the alerts (and number of alert instances) that were generated during that session.

For example:

| notepad | (1) |
| dis2 | (3) |
| dis2 | (2) |

Close                    View All

In the popup window, click an alert to open a maximized screenshot displaying the alert's details.



notepad                                          7/6/2015 4:07 PM      New

notepad (Alert ID: 10000004)                              View rule details

Who?                          On Which Computer?
W2K8-S8-QA14\Administrator         W2K8-S8-QA14

From Which Client?            When?
OIT-ALONR (10.1.100.136)           Monday, 7/6/2015, 4:07 PM

Did What?
Ran application                    Notepad

7/6/2015 4:07 PM
notepad

You can also click **View All** in the popup window in order to see a slideshow of screenshots for all the alerts. For details, see Viewing Alerts in Gallery Mode.

## 7.5 Viewing Alerts in the Session Player

In the **Session Player**, you can view and replay the recorded sessions in which alerts were triggered. Alert details are displayed for each alert, as the replay progresses. The alert risk severities are indicated by the color of the ring around the alert icon–critical (dark red), high (red), medium (orange), or low (gray).

Following is an example of a video replay of an ObserveIT session on which a number of alerts with different risk level severities were generated.
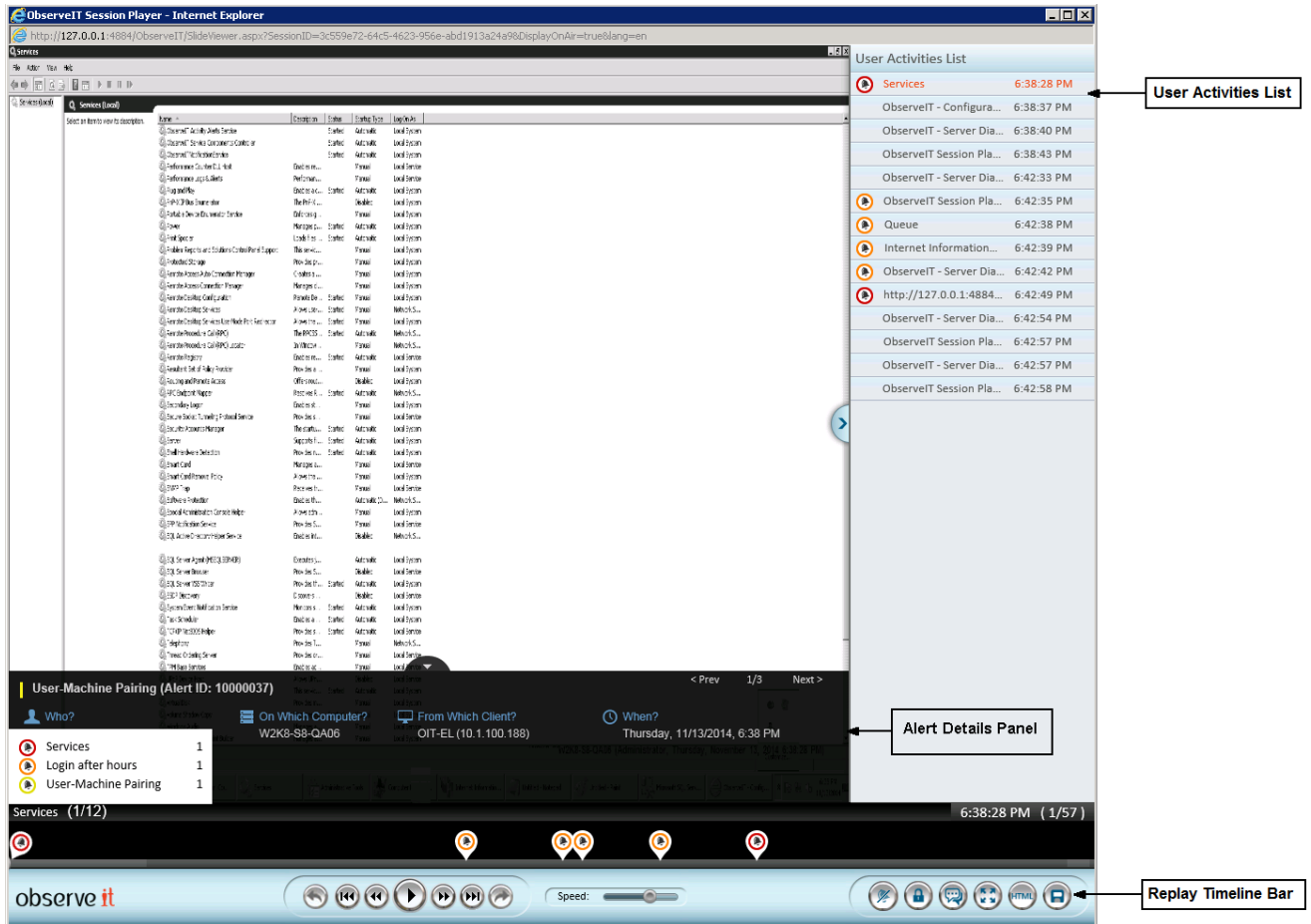
In the **User Activities List**, you can view alert indications on the suspicious activities.

The **Alert Details Panel** displays a summary of the alert activity including alert name, severity, conditions, and the number of alerts in the session (in the upper right corner—1/3 in the example below). You can click the Bell icon 🔔 in the **Replay Timeline Bar** to toggle between showing or hiding the alert details, as required.

Alert indicators appear on the **Replay Timeline Bar** and in the **User Activities Lis**t. You can click an alert icon on the **Replay Timeline Bar** to view the names of the alert rules and number of instances. The icon (ring) is colored per the highest severity alert in the session. For example, the red alert icon shown on the bottom left of the below screenshot represents the highest severity of the three alerts triggered in the session.

## 7.6 Viewing Alerts in the User Risk Dashboard

In the ObserveIT **User Risk Dashboard**, you can see the highest risky alerts that were triggered against risky users. The risky applications that the user accessed and the alerts that were triggered in response, are displayed alongside the User Risk Score graphic for each risky user. For each alert, the number of alert instances triggered by the specific alert rule appears next to the "bell" icon.
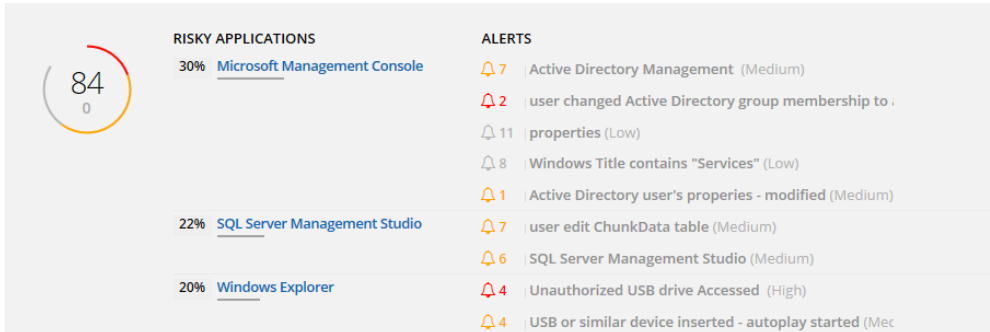


From the User Risk Dashboard, you can further investigate alerts that were attributed to a risky user, in order to determine exactly what caused the alerts to be triggered.

For example, if you click the alert **Adding a local user (High)** as shown in the following example:
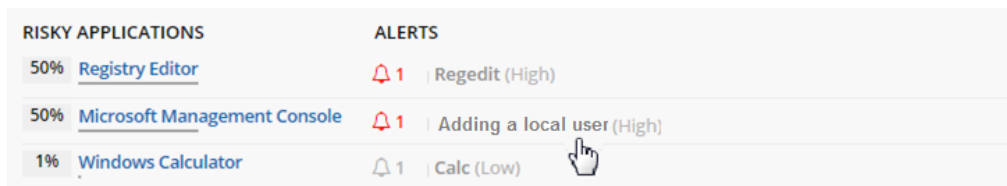


a new browser tab opens the **Alerts** page in the **Management Console**, displaying the alert. By clicking the alert, the exact alert details are displayed, as shown below:
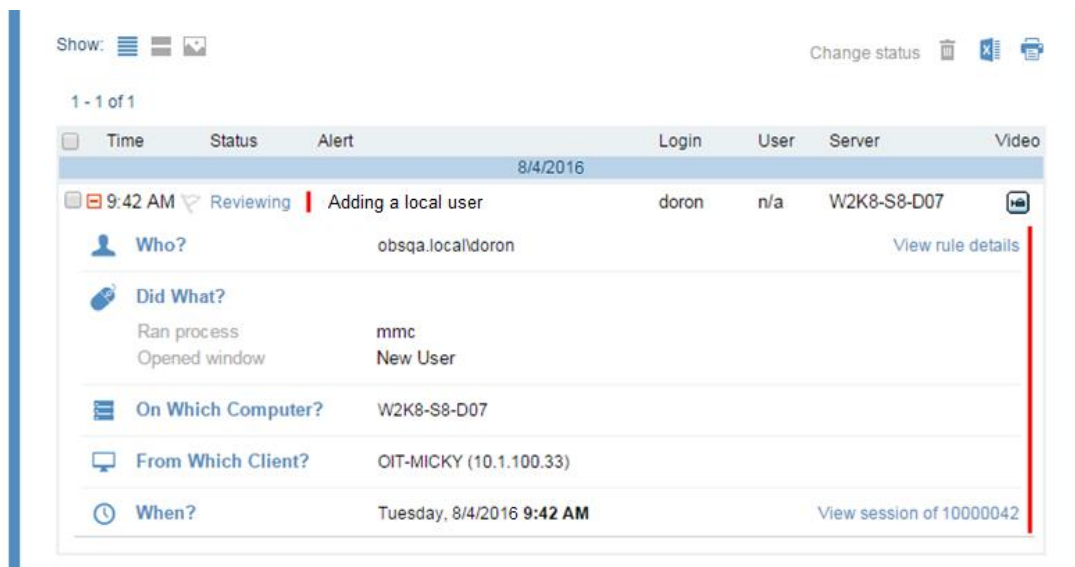


The alert details show exactly who, did what, on which computer, from which client, and when the action(s) occurred.

> **Any changes that you make to an alert might affect the user score. For example, if you delete an alert, or change the alert status from Issue to Non-Issue, the alert score will be reduced, and this will affect the overall user risk score. For details, see Assigning Alert Status.**

## 7.7 Generating Custom Reports about Alerts

ObserveIT enables you to create customized reports that provide summary information about alerts on monitored Windows and/or Unix-based servers.

Following are some examples of reports you might want to create:

- Report on alerts that were generated on the detection of user actions to copy files or insert USB storage devices with the intent to exfiltrate data.
- Report on alerts based on specific (user-defined) interactions with sensitive application (In-App) elements.
- Report all critical alerts on Windows or Unix machines grouped by risk level that were deleted during the last year.

For details on how to configure and view customized alert reports, please refer to Configuring Custom Reports in the ObserveIT product documentation.

# 8 Insider Threat Library (ITL) Tuning

In order to enhance your use of the ObserveIT Insider Threat Library, some fine-tuning of the rules and referenced lists is advised.

After the successful installation or upgrade of ObserveIT, the following steps are recommended:

1. Built-in User lists, **Everyday Users**, **Privileged Users**, **Remote Vendors**, **Developers & DevOps** and **Executives**, should be populated according to the organization's structure (at least those that are relevant to the organization).
2. Built-in User lists, **Termination List** and **Users in Watch List** can be populated with sensitive high risk users, and these Lists can be made Private (for confidentiality reasons).
3. Empty built-in Windows and Linux/Unix lists should be populated with relevant information, such as, production server IPs, authorized Social Network sites, sensitive desktop applications, sensitive files/folders, and so on.
4. Already populated built-in Windows and Linux/Unix lists can be reviewed to check whether more items should be added.
5. Regular working hours should be defined in the relevant rules, if the default of Mon-Fri 07:00-19:00 does not apply to the organization's policy.
6. Actions can be added to rules for notifying end users that they violated the organization's policy.
7. The system should run for a couple of days before reviewing it to perform further adjustment of list content, activation/deactivation of rules, changing assignment of rules or their risk level, and additional fine-tuning.

> **Note that all the rules included in the ObserveIT Insider Threat Library are defined as System Rules (an indication of this is presented when opening the Edit Alert Rule page). Some properties of system rules cannot be edited; they include, Name, Category, OS Type, and the DETECTION POLICY conditions. System Rules are maintained by ObserveIT and these properties will be upgraded automatically upon upgrading the ITL package.**