Outpost24

Vulnerability Management made easy

Auditing Guide

A Setup Guide to Manage Auditing in OUTSCAN/HIAB

Version: 1.6

2018-06-18

Table of Contents

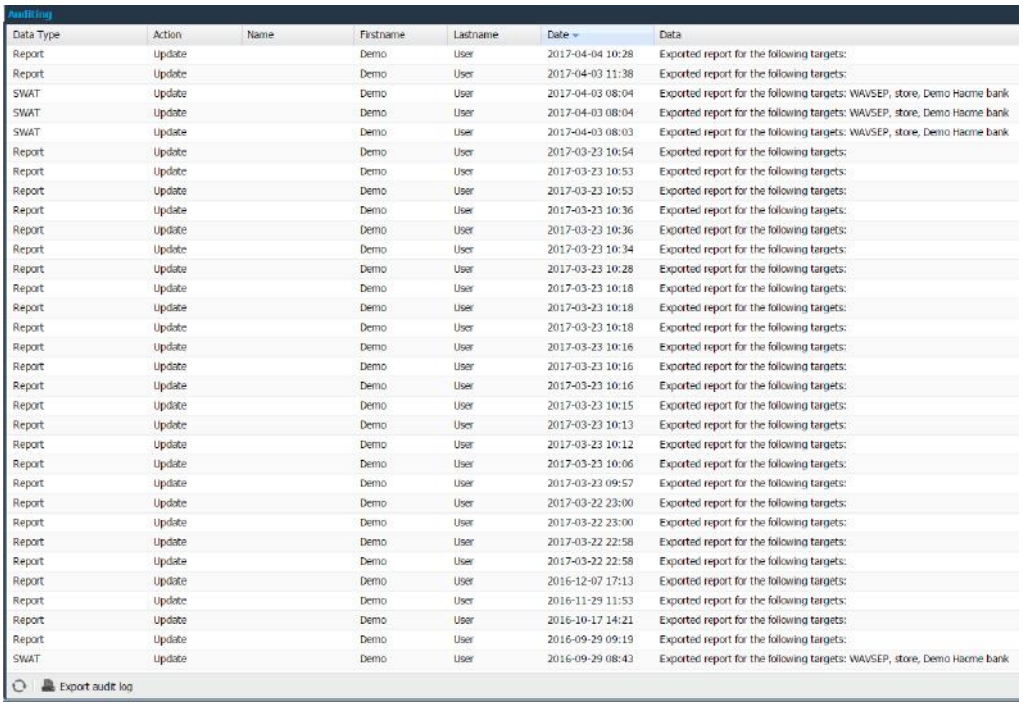
About This Guide

The purpose of this document is to provide users a comprehensive overview of Auditing setup for OUTSCAN and HIAB user roles. This document assumes that the reader has basic access to the OUTSCAN/HIAB account and Portal Interface.

For support information, visit https://www.outpost24.com/support.

1 Introduction

To access the Auditing window, click the **Main Menu** button in the lower left corner and select **Auditing**. The **Auditing** window displays a detailed user activity information such as login and log out, targets created, scans initiated, and many more. You are only allowed to see changes made by yourself and users that you administrate.



2 Auditing Fields

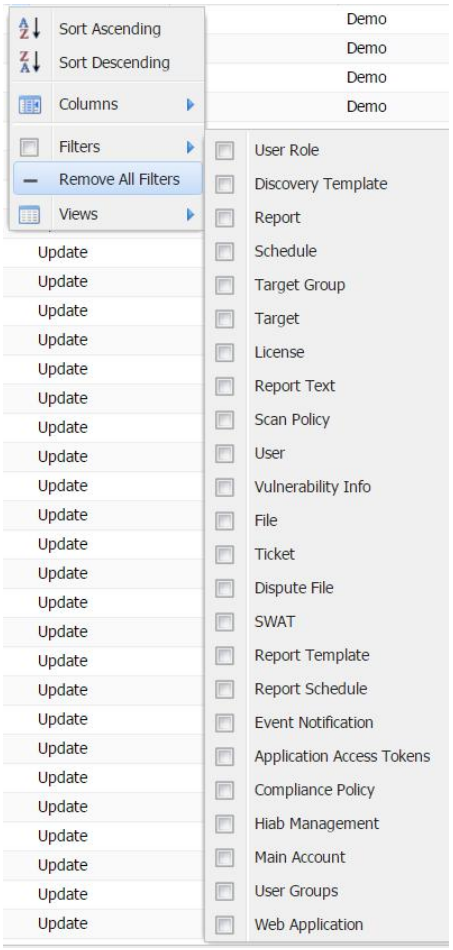
The **Auditing** window consists of nine columns, but not all may be visible. To add the extra columns, click on the arrow beside any column name and select the required columns.

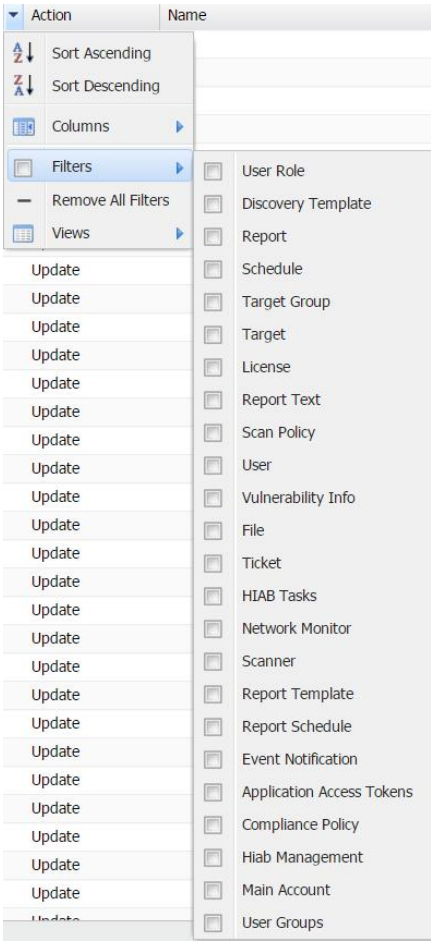
***Note**: Only seven columns are visible by default.*

Option	Description
Data Type	Indicates what type of entry has been changed.
Action	Indicates what type of action is being performed.
Name	Indicates the name of the edited/ added entity.
First Name	First name of the user making the change.
Last Name	Last name of the user making the change.
Date	Date when the change was made.
Data	Additional information about the audit entry.
Consultancy User	OUTSCAN only. Indicates the name of the support personnel who made changes.
Comment	The comments entered by the user are displayed here.

2.1 Data Type

The **Data Type** column can vary depending on the type of entry that is being changed. The most effective way to search Audit logs is by setting filters. The screenshots below show the available filter settings in OUTSCAN and HIAB.





Option	Description
User Role	Displays all entries related to changes made to the User Role.
Discovery Template	Displays all entries related to changes made to the Discovery Template.
Report	Displays all entries related to changes made to the Report.
Schedule	Displays all entries related to changes made to the Schedule.
Target Group	Displays all entries related to changes made to the Target Group.
Target	Displays all entries related to changes made to the Target.

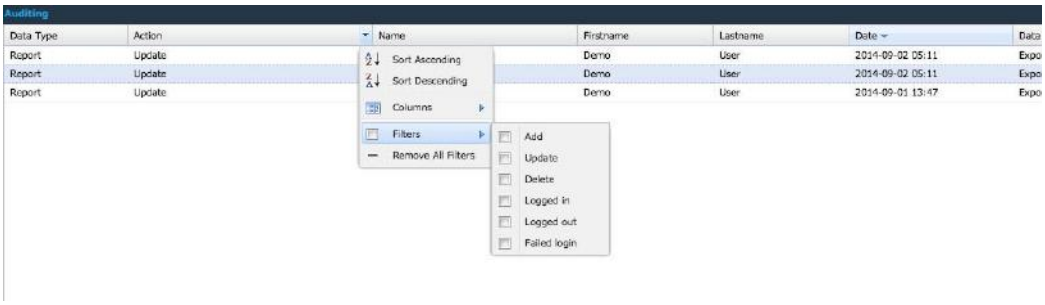
Option	Description
License	Displays all entries related to changes made to the License policy.
Report Text	Displays all entries related to changes made to the Report Text.
Scan Policy	Indicates that the change is made to the Scan Policy.
User	Displays all entries related to changes made to a User.
Vulnerability Info	Displays all entries related to changes made to the Vulnerability Info.
File	Displays all entries related to changes made to a file uploaded by the user in various sections. Example: Password files in scan policies, encryption keys for emails etc.,
Ticket	Displays all entries related to changes made to the Ticket.
Dispute file	OUTSCAN only. Displays all entries related to changes made to the PCI Dispute File.
SWAT	OUTSCAN only. Displays all entries related to changes made to SWAT.
HIAB Tasks	HIAB only. Displays all entries related to changes made in HIAB settings.
Network Monitor	HIAB only. Displays all entries related to changes made in network monitoring.
Scanner	HIAB only. Displays all entries related to changes made for a scanner or scheduler.
Report Template	Displays all entries related to changes made to the Report Template.
Report Schedule	Displays all entries related to changes made to the Report Schedule.
Event Notification	Displays all entries related to changes made to the Event Notification.
Application Access Token	Displays all entries related to changes made to the Application Access Token.
Compliance Policy	Displays all entries related to changes made to the Compliance Policy.
HIAB Management	Displays all entries related to changes made to the HIAB Management.
Main Account	Displays all entries related to changes made to the Main Account.
User Groups	Displays all entries related to changes made to the User Group. ***Note**: Main Account and User groups are only available for Main user or Super user.*
Web Application	OUTSCAN only. Displays all entries related to changes made to the Web Applications.

2.2 Action

The **Action** column shows the type of action performed. This column is used to filter the specific user action during auditing.

Example:
If you are trying to check who deleted targets, setting the filter in the action column to delete will display all the deletion actions performed. Results can further be narrowed using filtering on multiple columns.

Filter settings can be set on the column **Action** with the options mentioned below.



Option	Description
Add	Displays when an entry is added to the system.
Update	Displays when an entry is updated or a report is exported.
Delete	Displays when an entry is deleted from the system.
Logged In	Displays when a user logs in.
Logged Out	Displays when a user logs out.
Failed Login	Displays when a user fails to login.

2.3 Other Columns

2.3.1 Name

The **Name** column indicates the name of the corresponding entry in **Data Type** column. It can be filtered by three text fields. It is possible to use all three at once to limit the results, but you can also use quotes to match an entire phrase.

Option	Description
All	Displays records that contain all the search words.
Any	Filters on records that contain any of the search words.
None	Excludes all records that contain any of the search words.

2.3.2 First Name

The **First Name** of the user who made the changes. It can be filtered by three text fields. It is possible to use all three at once to limit the results, but you can also use quotes to match an entire phrase.

Option	Description
All	Displays records that contain all the search words.
Any	Filters on records that contain any of the search words.
None	Excludes all records that contain any of the search words.

2.3.3 Last Name

The **Last Name** of the user who made the changes. It can be filtered by three text fields. It is possible to use all three at once to limit the results, but you can also use quotes to match an entire phrase.

Option	Description
All	Displays records that contain all the search words.
Any	Filters on records that contain any of the search words.
None	Excludes all records that contain any of the search words.

***Note**: The first name and last name of a user should be set using user account under Settings/Manage Users.*

2.3.4 Date

The **Date** column indicates the date and time of the performed action. It can be filtered by three types.

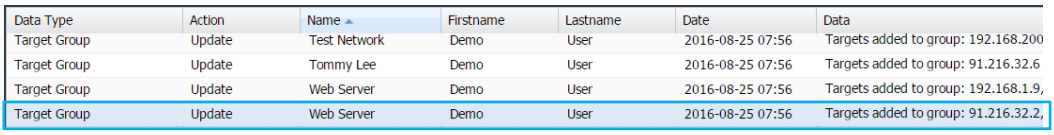
Option	Description
Before	Display all entries before the provided date.
After	Display all entries after the provided date.
On	Display all entries on the provided date.

2.3.5 Data

The Data column displays the additional information about the data type entry's action. It can be filtered by three text fields. It is possible to use all three at once to limit the results, but you can also use quotes to match an entire phrase.

Option	Description
All	Displays records that contain all the search words.
Any	Filters on records that contain any of the search words.
None	Excludes all records that contain any of the search words.

Example:



Data Type	Action	Name	Firstname	Lastname	Date	Data
Target Group	Update	Test Network	Demo	User	2016-08-25 07:56	Targets added to group: 192.168.200
Target Group	Update	Tommy Lee	Demo	User	2016-08-25 07:56	Targets added to group: 91.216.32.6
Target Group	Update	Web Server	Demo	User	2016-08-25 07:56	Targets added to group: 192.168.1.9,
Target Group	Update	Web Server	Demo	User	2016-08-25 07:56	Targets added to group: 91.216.32.2,

In the above figure, Action column displays Update and Data column displays the additional details regarding the change that occurred on the selected object.

Important Note – Consultancy User

Available on a super user account on OUTSCAN. Whenever a support technician makes changes to the settings, the name of the technician will appear in this column. This feature is not enabled by default.

Important Note – Searching by Name

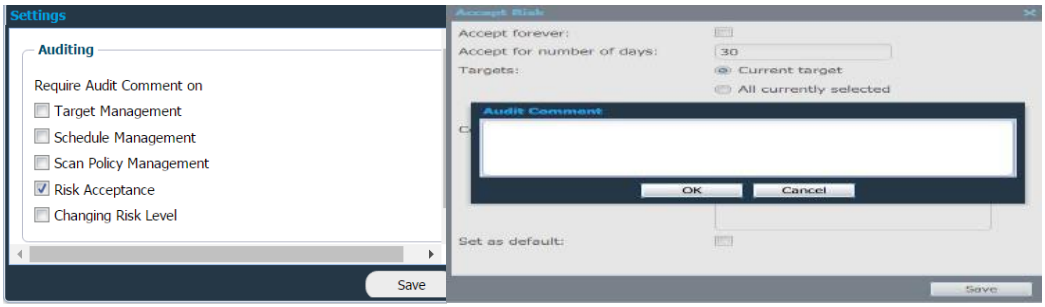
It is easy to filter using the name or action field, in case you are looking for the exact user or action.

---

3 Audit Settings

Note: *This Setting is only available for a Main User or Super User*

By clicking the Settings icon in the top right corner of the window, the Audit settings can be changed. This helps the user to define the actions, which will require an audit comment. The available options are as follows:



3.1 Require Audit Comment on

- **Target Management** when enabled, enforces a note to be supplied by the user when adding or removing targets. The note can later be read in the audit log. This option is only available for the main user.
- **Schedule Management** when enabled, enforces a note to be supplied by the user when adding or removing scan schedules. The note can later be read in the audit log. This option is only available for the main user.
- **Scan Policy Management** when enabled, enforces a note to be supplied by the user when adding or removing a scan policy. The note can later be read in the audit log. This option is only available for the main user.
- **Risk Acceptance** when enabled, enforces a note to be supplied by the user when accepting a risk in the reporting section. The note can later be read in the audit log. This option is only available for the main user.
- **Changing Risk Level** when enabled, enforces a note to be supplied by the user when changing a risk level in the reporting section. The note can later be read in the audit log. This option is only available for the main user.

4 Export Audit Log

You can export the audit log to Excel format by pressing the Export audit log button on the left bottom of the window.