Outpost24

Vulnerability Management made easy

Auditing Guide

A Setup Guide to Manage Auditing in OUTSCAN/HIAB

Version: 1.7

2019-02-15

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.

Copyright

© 2020 Outpost24®. All rights reserved.
This document may only be redistributed unedited and unaltered. This document may be cited and referenced only if clearly crediting Outpost24® and this document as the source. Any other reproduction and redistribution in print or electronically is strictly prohibited without explicit permission.

Trademark

Outpost24® and OUTSCAN™ are trademarks of Outpost24® in Sweden and other countries.

1 Introduction

This document provides users with 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.

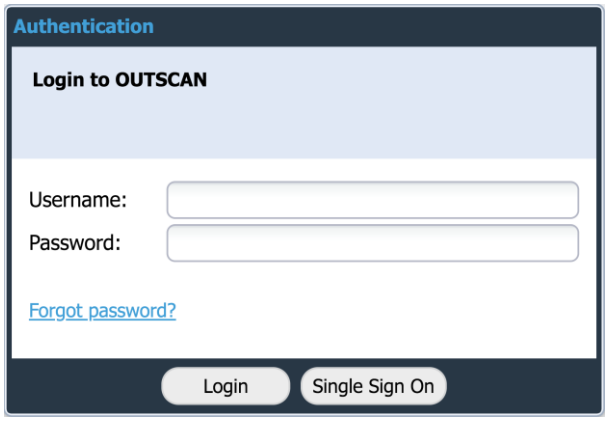
2 Getting Started

There are two ways of launching your applications.

- From OUTSCAN
- From a HIAB

2.1 OUTSCAN

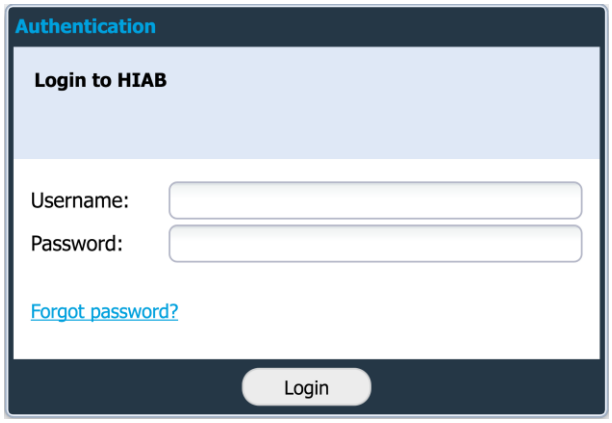
To launch the OUTSCAN application, navigate to https://outscan.outpost24.com.
***Note**: Use HTTPS protocol.*



Log in using your credentials.

2.2 HIAB

To connect to a HIAB, use the assigned network address.
***Note**: Use HTTPS protocol.*

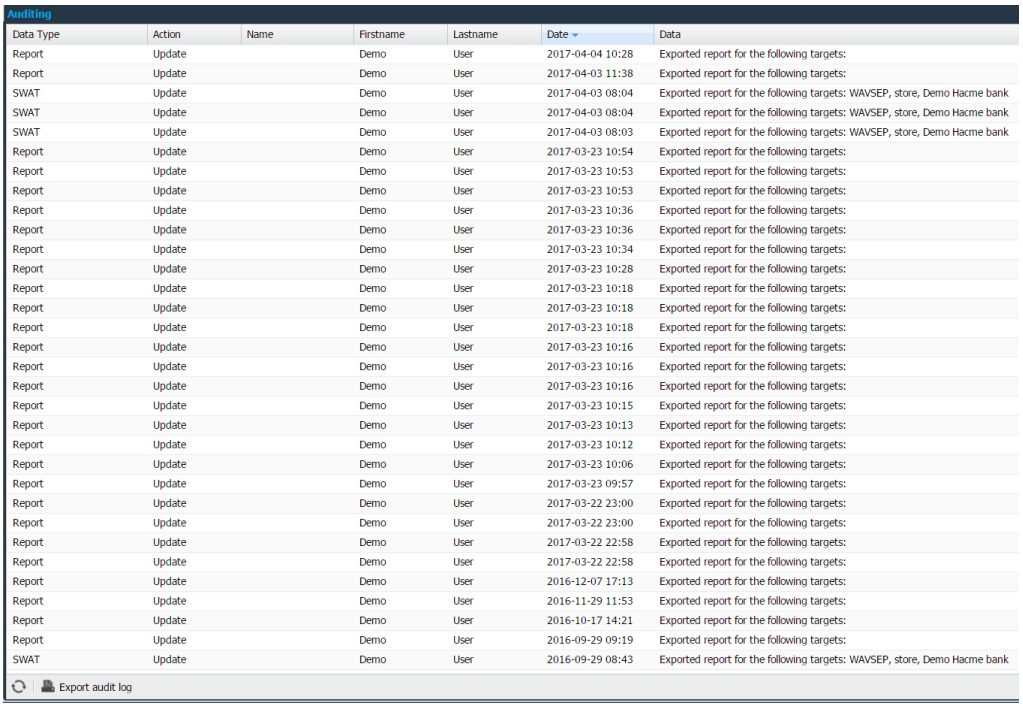


Log in using your credentials.

3 Auditing

To access the Auditing module, go to **Main Menu → 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.



Auditing

Data Type	Action	Name	Firstname	Lastname	Date	Data
Report	Update		Demo	User	2017-04-04 10:28	Exported report for the following targets:
Report	Update		Demo	User	2017-04-03 11:38	Exported report for the following targets:
SWAT	Update		Demo	User	2017-04-03 08:04	Exported report for the following targets: WAVSEP, store, Demo Hacme bank
SWAT	Update		Demo	User	2017-04-03 08:04	Exported report for the following targets: WAVSEP, store, Demo Hacme bank
SWAT	Update		Demo	User	2017-04-03 08:03	Exported report for the following targets: WAVSEP, store, Demo Hacme bank
Report	Update		Demo	User	2017-03-23 10:54	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:53	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:53	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:36	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:36	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:34	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:28	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:18	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:18	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:18	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:16	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:16	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:16	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:15	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:13	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:12	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 10:06	Exported report for the following targets:
Report	Update		Demo	User	2017-03-23 09:57	Exported report for the following targets:
Report	Update		Demo	User	2017-03-22 23:00	Exported report for the following targets:
Report	Update		Demo	User	2017-03-22 23:00	Exported report for the following targets:
Report	Update		Demo	User	2017-03-22 22:58	Exported report for the following targets:
Report	Update		Demo	User	2017-03-22 22:58	Exported report for the following targets:
Report	Update		Demo	User	2016-12-07 17:13	Exported report for the following targets:
Report	Update		Demo	User	2016-11-29 11:53	Exported report for the following targets:
Report	Update		Demo	User	2016-10-17 14:21	Exported report for the following targets:
Report	Update		Demo	User	2016-09-29 09:19	Exported report for the following targets:
SWAT	Update		Demo	User	2016-09-29 08:43	Exported report for the following targets: WAVSEP, store, Demo Hacme bank

Export audit log

4 Auditing Fields

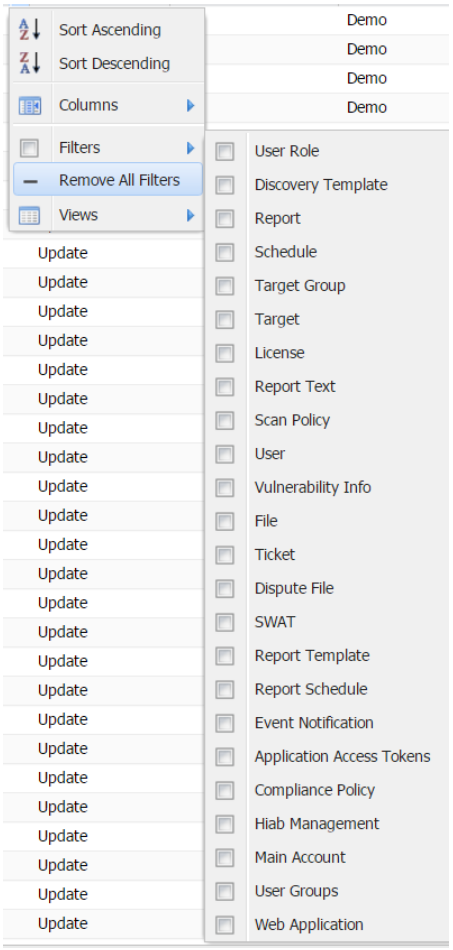
The **Auditing** window consists of nine columns, but not all may be visible. To add the extra columns, click on the arrow beside any column name and select the required columns.

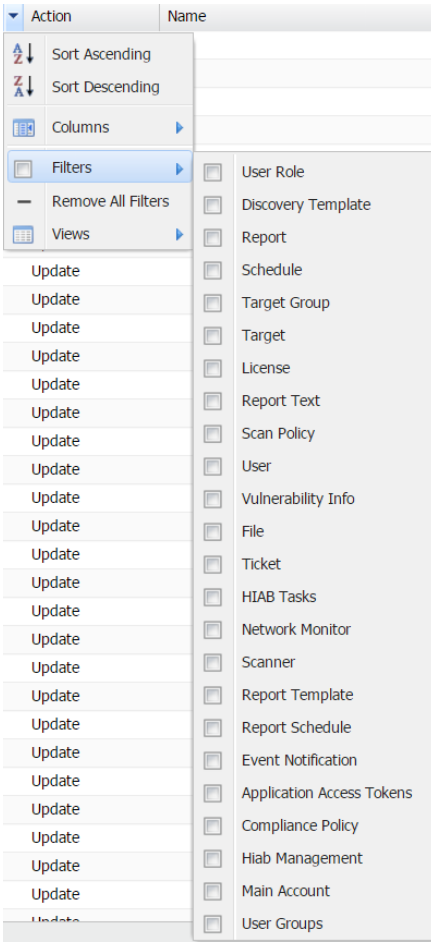
***Note**: Only seven columns are visible by default.*

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.

4.1 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 images below show the available filter options in OUTSCAN and HIAB.
Selecting different options displays all entries related to changes made to these options.
Note: *Note that the options differ between the OUTSCAN and HIAB.*





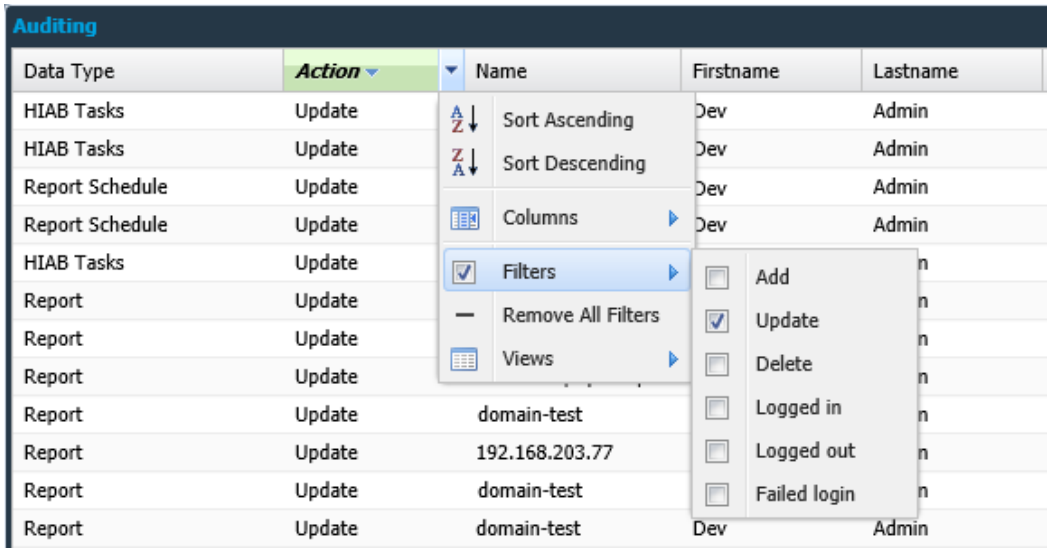
Note*: Main Account and User groups are only visible to Main User or Super User.*

4.2 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.

4.3 Other Columns

4.3.1 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, 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.

4.3.2 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.

4.3.3 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 **Main Menu → Settings → Manage Users**.*

4.3.4 Date

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

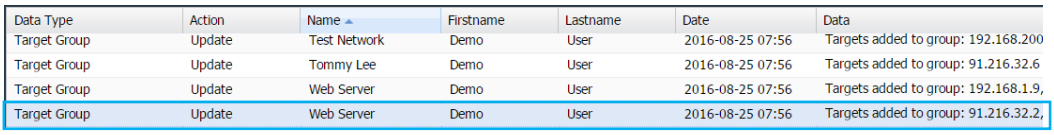
Option	Description
Before	Display all entries before the provided date.
After	Display all entries after the provided date.
On	Display all entries on the provided date.

4.3.5 Data

The **Data** column displays the additional information about the data type entries 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

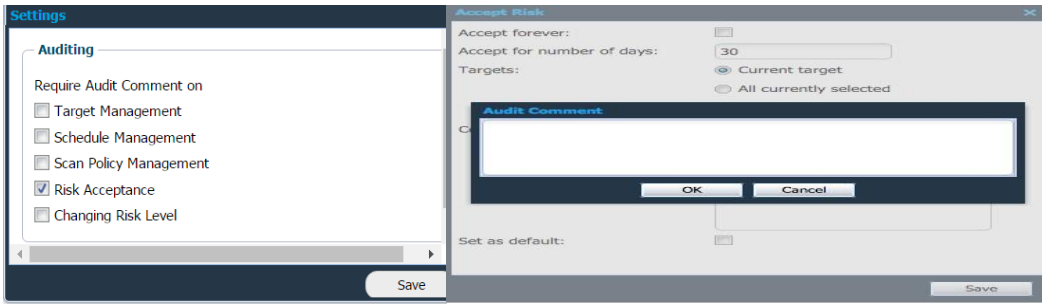
It is easy to filter using the name or action field, in case you are looking for the exact user or action.

---

5 Audit Settings

Note: *These options are 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 following options enforces an Audit Comment to be supplied by the user:

- **Target Management** - when adding, removing, or changing targets.
- **Schedule Management** - when adding, removing, or changing scan schedules.
- **Scan Policy Management** - when adding, removing, or changing a scan policy.
- **Risk Acceptance** - when accepting a risk in the reporting section.
- **Changing Risk Level** - when changing a risk level in the reporting section.

The comment can later be read in the audit log.

6 Export Audit Log

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