Outpost24

Vulnerability Management made easy

HIAB/OUTSCAN Audit Guide

A Setup Guide to Manage Auditing in HIAB/Outscan

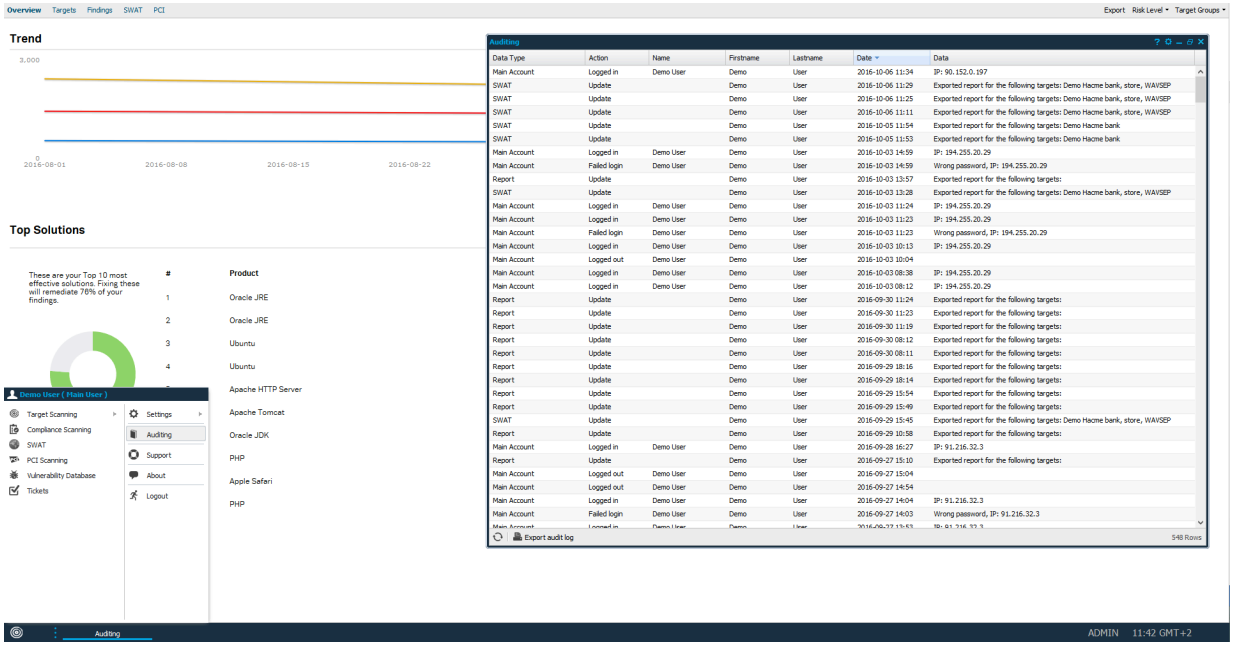
Last update:
2 March 2017

TABLE OF CONTENT

1 Purpose Of Document

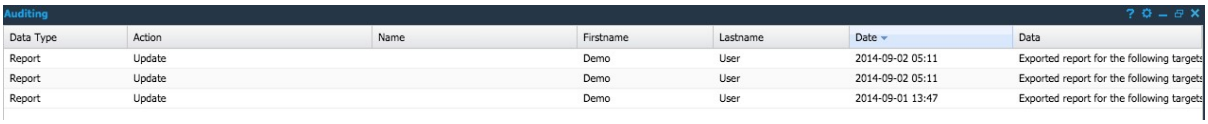
This document gives the reader an understanding of how to setup Audit features for HIAB and Outscan user roles. This document assumes that the reader has basic access to the HIAB/Outscan Account and Graphical User Interface.

2 Introduction



The “Auditing” window lets you see what changes has been made in the system, such as; users logging in and out, targets created, scans started, and more. You are only allowed to see changes made by yourself and users that you administrate.

3 Auditing Fields



The Auditing window consists of nine columns:

- **Data Type:** Indicates what type 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:** Indicates the name of the support personal that made changes
- **Comment:** The comment given by the user if required

3.1 Data Type

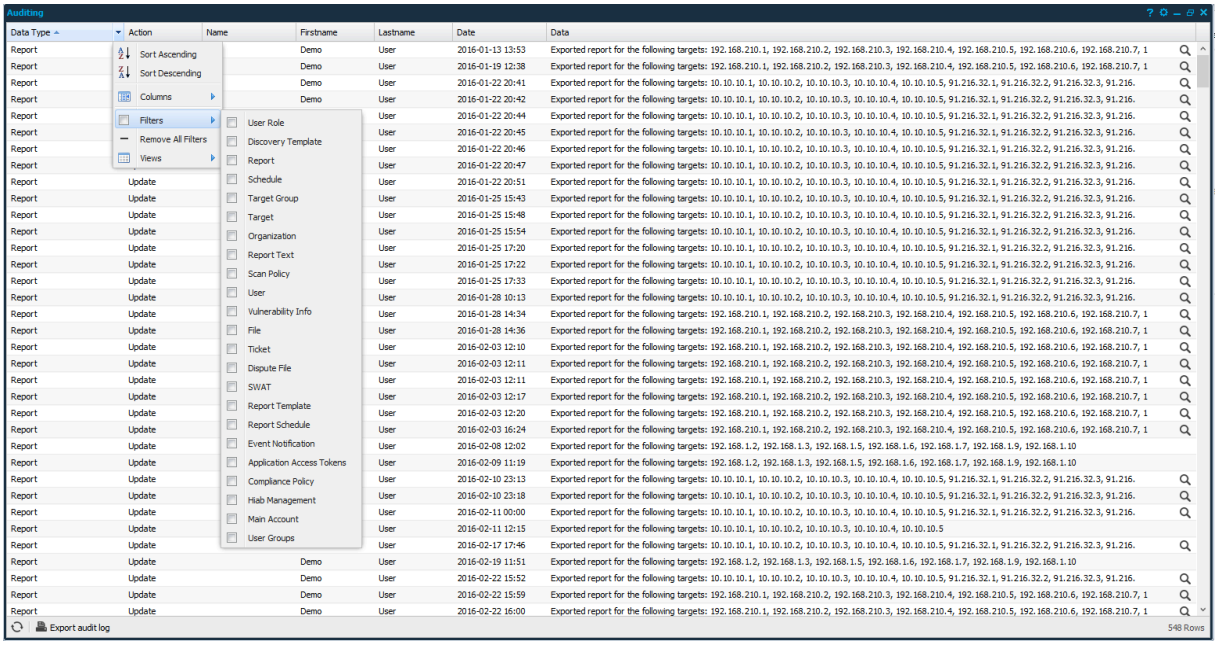
The “Data Type” column can take different values depending on the type of entry that is being changed.

The data type field can take any one of these values:

- **User Role:** Indicates that the change is made to the User Role
- **Discovery Template:** Indicates that the change is made to the Discovery Template
- **Report:** Indicates that the change is made to the Report
- **Schedule:** Indicates that the change is made to the Schedule
- **Target Group:** Indicates that the change is made to the Target Group
- **Target:** Indicates that the change is made to the Target
- **Organization:** Indicates that the change is made to the Organization
- **Report Text:** Indicates that the change is made to the Report Text
- **Scan Policy:** Indicates that the change is made to the Scan Policy
- **User:** Indicates that the change is made to the User
- **Vulnerabilty Info:** Indicates that the change is made to the Vulnerability Info
- **File:** Indicates that the change is made to the file
- **Ticket:** Indicates that the change is made to the Ticket
- **Dispute file:** Indicates that the change is made to the Dispute File.
- **SWAT:** Indicates that the change is made to SWAT.
- **Report Template:** Indicates that the change is made to the Report Template
- **Report Schedule:** Indicates that the change is made to the Report Schedule
- **Event Notification:** Indicates that the change is made to the Event Notification
- **Application Access Token:** Indicates that the change is made to the Application Access Token

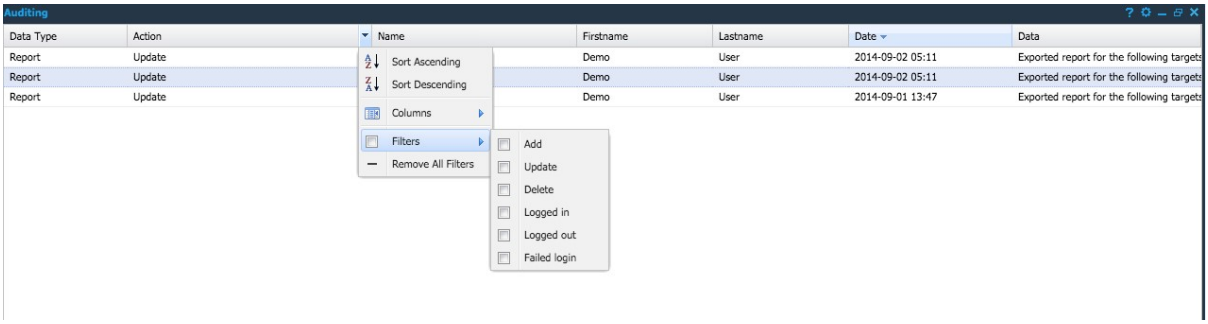
- **Compliance Policy:** Indicates that the change is made to the Compliance Policy
- **Hiab Management:** Indicates that the change is made to the HIAB Management
- **Main Account:** Indicates that the change is made to the Main Account
- **User Groups:** Indicates that the change is made to the User Group

Filtering Using Data Type Field.



The most effective and time saving way to search Audit logs is by setting filters. Filter settings can be set on the column 'Data Type' with the options mentioned above.

3.2 Action



The “Action” column reflects upon the type of action performed. This column is widely used during auditing to filter for the specific user action.

This column can contain the following values.

- **Add:** When an entry is added
- **Update:** When an entry is updated or a report is exported
- **Delete:** When an entry is deleted.
- **Logged In:** When a user logs in
- **Logged Out:** When a user logs out.

This column can be used to filter user actions. For example if you are trying to check who has deleted targets, setting the filter in the action column to delete, will display all the deletion actions performed. Results can further be narrowed down using filtering on multiple columns.

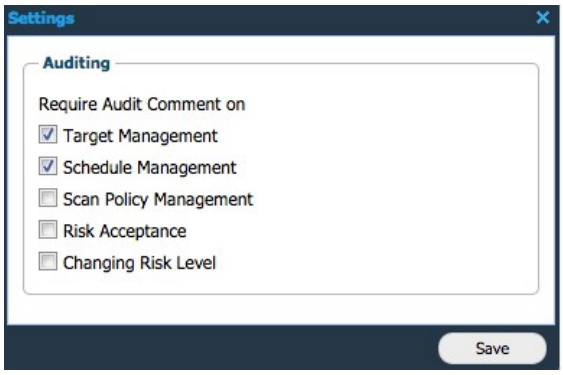
3.3 Other Columns.

The other columns are fairly self-explanatory and similar filters can be applied to narrow down on required entry.

Important Note – Consultancy User
Whenever a support technician accesses or makes changes to the settings, the name of the technician will appear in this column.

Important Note – Searching by Name
It is easiest to filter using the name or action field, in case you are looking for the exact user or action

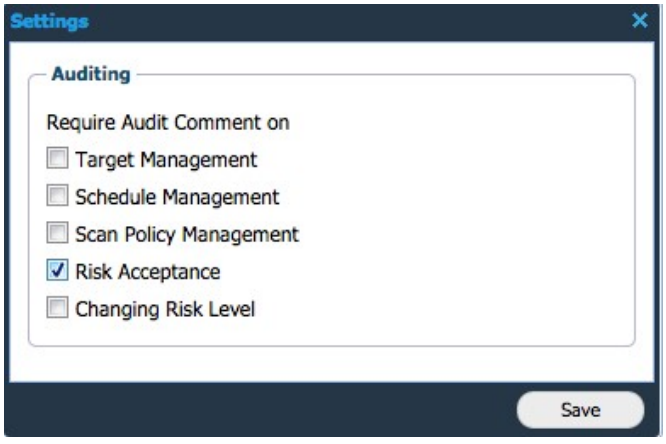
4 Audit Settings



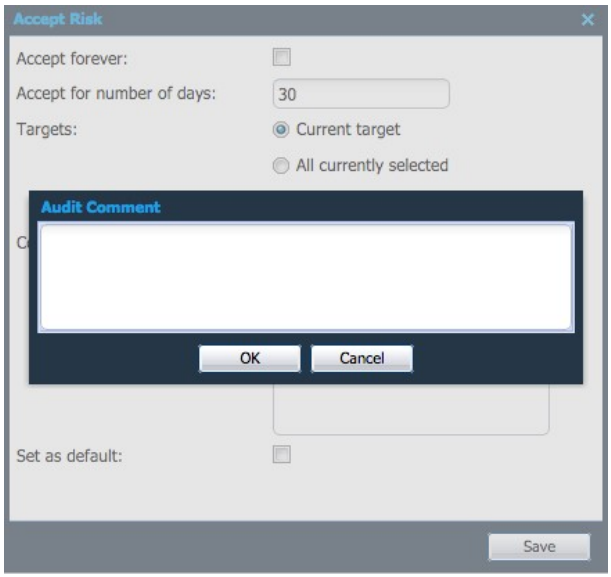
The audit settings help us define the actions, which will require an audit comment. It has the following options:

- Target Management
- Schedule Management
- Scan Policy Management
- Risk Acceptance
- Changing Risk Level

In case of any of these options are checked. The corresponding actions will require a comment before they are implemented.



For example in the figure you can see that “Risk Acceptance” has been checked. When any authorized user tries to accept risk, he is prompted to enter an audit comment (figure below). These comments are very helpful during later audits.



5 Additional Information

For any additional help during Auditing, please contact support at Outpost24.

Email support@outpost24.com

Tel (from the UK): +44 20 7193 8410
Tel (from the US): +1 (800) 69 13 150
Tel (from Spain): +34 91 188 08 15
Tel (from Mexico): +52 55 8421 4503
Tel (from Hong Kong): +852 8175 8310
Tel (from Malaysia): +603 2035 5931
Tel (from Singapore): +65 3151 8310
Tel (from Thailand): +662 642 7258
Tel (all other countries): +46 455 612 310