

Tickets

Quick Start Guide

Table of Contents

| | | |
|----------|---------------------------|----------|
| 1 | TICKETS | 4 |
| 1.1 | TICKETS GRID WINDOW | 5 |
| 1.2 | MANAGE TICKETS | 8 |
| 1.3 | TICKETS SETTINGS | 9 |

About This Document

This document provides users with a comprehensive overview of the Tickets for OUTSCAN and HIAB. This document has been elaborated under the assumption the reader has access to the OUTSCAN/HIAB Account and Graphical User Interface.

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

Copyright

© 2018 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.

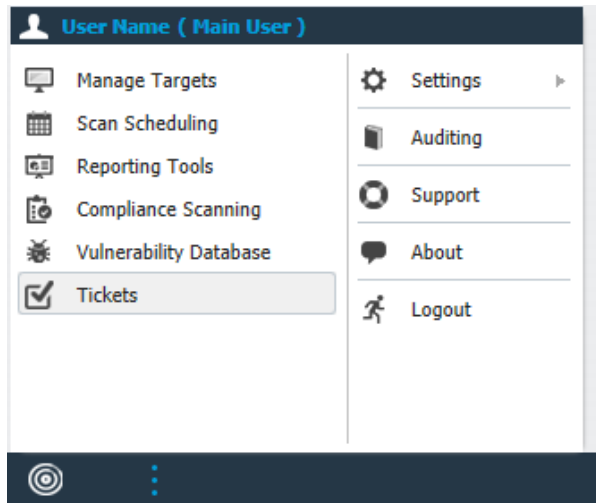
Trademark

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

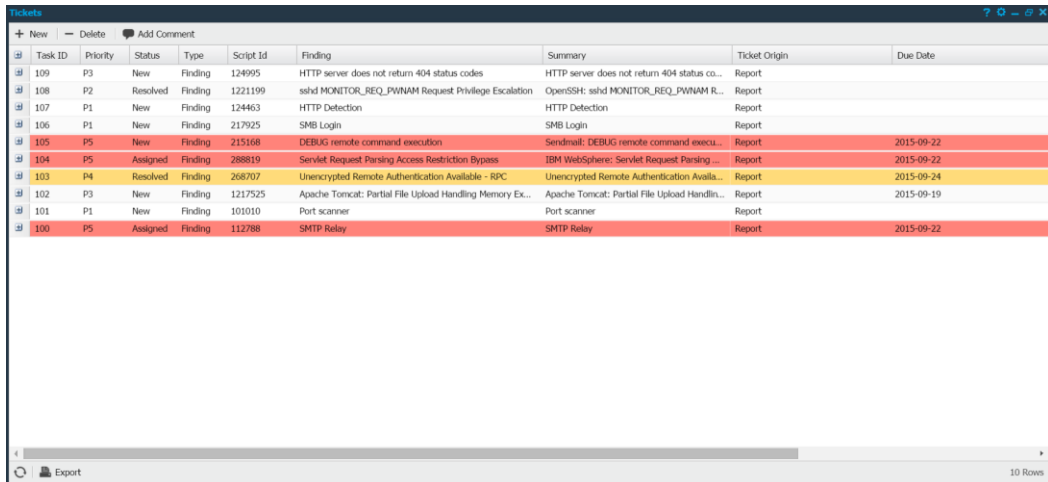
1 Tickets

The **Tickets** module is used to manage different assignments with individual users that have access to the ticketing module. Access to the **Tickets** module can be managed under the **Roles** tab in the **Manage Users** module.

To access **Tickets**, open the main menu located in the lower left corner.

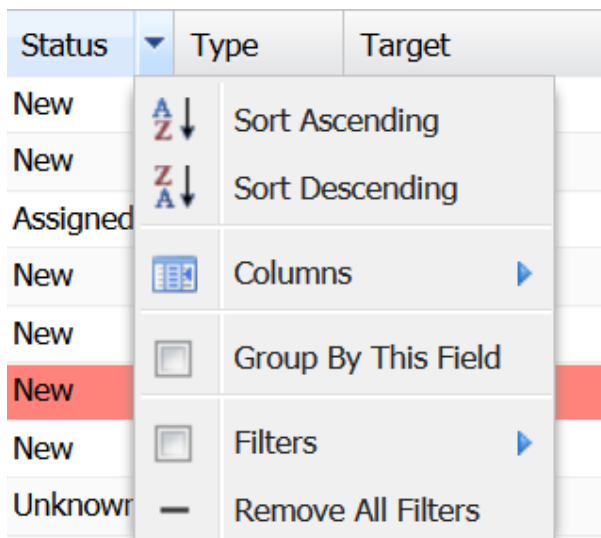


1.1 Tickets Grid Window



| Task ID | Priority | Status | Type | Script ID | Finding | Summary | Ticket Origin | Due Date |
|---------|----------|----------|---------|-----------|--|---|---------------|------------|
| 109 | P3 | New | Finding | 124995 | HTTP server does not return 404 status codes | HTTP server does not return 404 status co... | Report | |
| 108 | P2 | Resolved | Finding | 1221199 | sahd MONITOR_REQ_PWNAM Request Privilege Escalation | OpenSSH: sah d MONITOR_REQ_PWNAM R... | Report | |
| 107 | P1 | New | Finding | 124463 | HTTP Detection | HTTP Detection | Report | |
| 106 | P1 | New | Finding | 217925 | SMB Login | SMB Login | Report | |
| 105 | P5 | New | Finding | 215168 | DEBUG remote command execution | Sendmail: DEBUG remote command execu... | Report | 2015-09-22 |
| 104 | P5 | Assigned | Finding | 288819 | Servlet Request Parsing Access Restriction Bypass | IBM WebSphere: Servlet Request Parsing ... | Report | 2015-09-22 |
| 103 | P4 | Resolved | Finding | 268707 | Unencrypted Remote Authentication Available - RPC | Unencrypted Remote Authentication Availa... | Report | 2015-09-24 |
| 102 | P3 | New | Finding | 1217525 | Apache Tomcat: Partial File Upload Handling Memory Ex... | Apache Tomcat: Partial File Upload Handlin... | Report | 2015-09-19 |
| 101 | P1 | New | Finding | 101010 | Port scanner | Port scanner | Report | |
| 100 | P5 | Assigned | Finding | 112788 | SMTP Relay | SMTP Relay | Report | 2015-09-22 |

The *Tickets* grid includes different columns. To enable or disable a column click the arrow next to the name of any column. In the displayed drop-down menu there is a field called **Columns** which lists the available columns. Most of these columns allow filtering, this provides the option to display a subsection of all available data. To enable filtering, access the same drop-down menu as for columns and click **Filters**.



The available columns for the *Tickets* grids are:

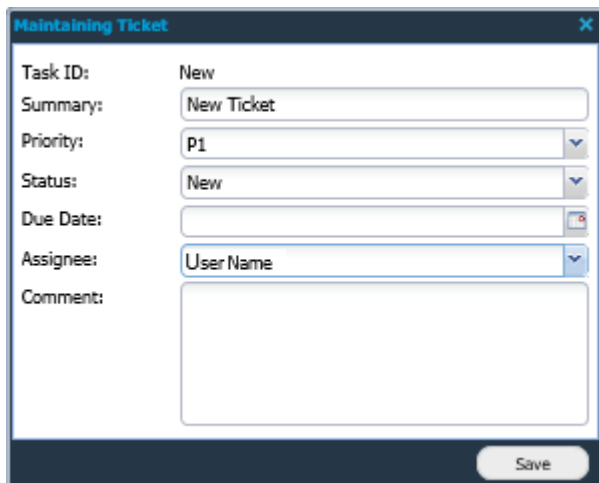
| Option | Description |
|----------------------|---|
| Assignee | Whom the ticket has been assigned to. |
| Due Date | Due date of the ticket. |
| Finding | The name of finding for which this ticket was created for. This will be empty if the ticket concerns with multiple findings or origin is Custom type. |
| Host name | Name of the host affected. (Empty for custom type.) |
| Priority | Displays the priority of the ticket where P5 is the highest. <ul style="list-style-type: none"> ▶ P1 ▶ P2 ▶ P3 ▶ P4 ▶ P5 |
| Report Date | The date of the report which the ticket was created from. (Empty for custom type.) |
| Script ID | Script ID of the finding which the ticket will trigger for. (Empty for custom type.) |
| Status | Status of the ticket. <ul style="list-style-type: none"> ▶ New ▶ Assigned ▶ Resolved ▶ Reopened ▶ Verified ▶ Rejected |
| Summary | Summary of the ticket. |
| Target | The target which the finding/report was reported/created for. |
| Task ID | ID of the ticket. |
| Ticket Origin | Where the ticket originated from: <ul style="list-style-type: none"> ▶ WAS ▶ PCI ▶ Report ▶ Custom |
| Type | The type of the ticket: <ul style="list-style-type: none"> ▶ Finding: when a ticket is related to a single finding. ▶ Report: when a ticket is related to the whole report of the target. |

| Option | Description |
|-----------------|---|
| | <ul style="list-style-type: none">▶ Custom: if the ticket was manually created by the user. |
| Verified | Displays the status of the finding which this ticket is created for: <ul style="list-style-type: none">▶ Not verified▶ No longer present▶ Still present |

1.2 Manage Tickets

Assigning new tickets is performed from either **Reporting Tools**, **PCI Reports**, or from **Tickets**.

To create and assign a new ticket from the *Tickets* grid window press **New** in the upper left corner. This displays the *Maintaining Ticket* window where you can edit the Summary, Priority, Status, Due Date, Assignee, and add comment for the ticket.



Right clicking a ticket in the *Tickets* grid provides different actions to choose between:

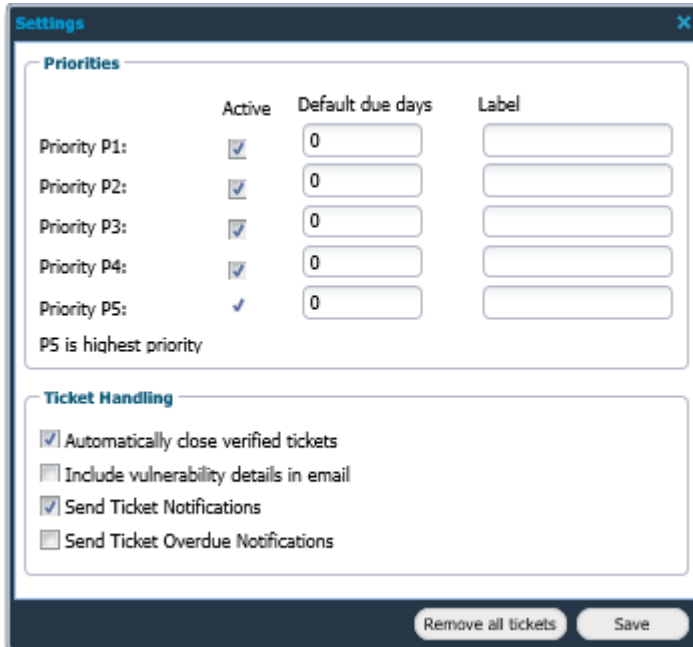
| Option | Description |
|--------------------|-------------------------------------|
| Add Comment | Add comment for the specific ticket |
| New | Create a new ticket |
| Delete | Delete the specific ticket |
| Edit | Edit the specific ticket |

Marking multiple entries by holding CTRL and left click makes it possible to either use **Delete** to delete multiple tickets or **Add Comment** to add comments to multiple tickets. These two options are available in the top menu bar of the grid.

Exporting a report from the *Tickets* grid is done by clicking **Export** in the lower left corner of the window. The available formats are PDF and Excel. This report includes information about all tickets in the *Tickets* grid.

1.3 Tickets Settings

Clicking the **Settings** icon in the upper right corner of the window toolbar provides access to the tickets settings:



The screenshot shows a 'Settings' window with two main sections: 'Priorities' and 'Ticket Handling'.

Priorities Section:

| | Active | Default due days | Label |
|--------------|-------------------------------------|--------------------------------|----------------------|
| Priority P1: | <input checked="" type="checkbox"/> | <input type="text" value="0"/> | <input type="text"/> |
| Priority P2: | <input checked="" type="checkbox"/> | <input type="text" value="0"/> | <input type="text"/> |
| Priority P3: | <input checked="" type="checkbox"/> | <input type="text" value="0"/> | <input type="text"/> |
| Priority P4: | <input checked="" type="checkbox"/> | <input type="text" value="0"/> | <input type="text"/> |
| Priority P5: | <input checked="" type="checkbox"/> | <input type="text" value="0"/> | <input type="text"/> |

P5 is highest priority

Ticket Handling Section:

- Automatically close verified tickets
- Include vulnerability details in email
- Send Ticket Notifications
- Send Ticket Overdue Notifications

Buttons at the bottom: Remove all tickets, Save

The priority list can be used to select fewer ticket levels than the original 5 and/or the order can be reversed.

When a *Label* is defined on a priority level, it will be displayed instead of the default *P1* name in the drop-down throughout the system.

Default due days is a configuration option that automatically will set the due date based on the setting here and the selected priority upon creation of the original ticket.

| Options | Description |
|---|--|
| Priority P1-P5 | Able to mark it as active or not, set a value for default due days and rename it. <i>Note: P5 is checked as default and cannot be unchecked.</i> |
| Automatically close verified tickets | It enables the system to close tickets when it has been verified. |
| Include vulnerability details in email | Include the details of the vulnerability found in the email for the ticket. This is the default setting for "Include vulnerability details in email" checkbox, where you create tickets for the finding. The check box "Include vulnerability details in email" in Create Ticket window in Reporting Tools, PCI, WAS will be loaded with the default value you set here. |
| Send Ticket Notifications | Enable this option to allow the system to send email notifications when a ticket is created, changes status, and is closed. |
| Send Ticket Overdue Notifications | Send a notification to the assignee once a ticket is overdue. |
| Remove all tickets | Removes all tickets that are visible in the <i>Tickets</i> grid. |