Outpost24

Vulnerability Management made easy

Event Notifications

A Quick Start Guide

Version: 1.3

2018-05-07

Table of Contents

About This Guide

The purpose of this document to provide users with a comprehensive overview of how to setup and use the Event Notifications module in OUTSCAN and HIAB. This document has been elaborated under the assumption that the reader has access to the OUTSCAN /HIAB account and portal interface.

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

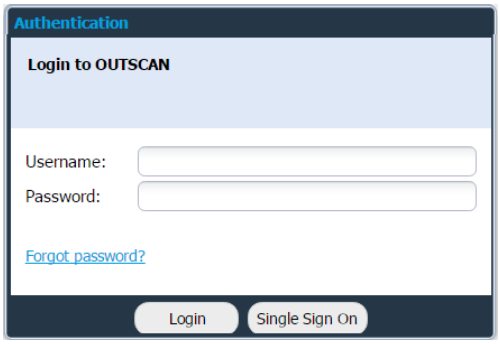
Copyright

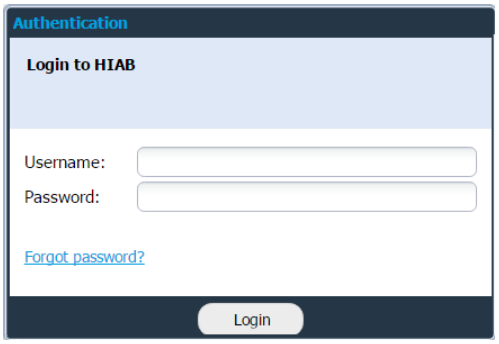
Trademark

1 Getting Started

To launch the OUTSCAN application, navigate to https://outscan.outpost24.com.
Users who have HIAB, connect to your HIAB by using its assigned network address.

***Note**: Use HTTPS protocol.*



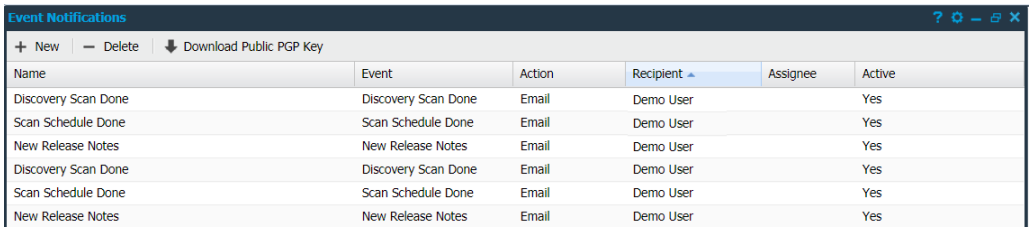


Log in using your credentials.

To set up Event Notifications, go to **Main Menu → Settings → Event Notifications**.

2 Introduction

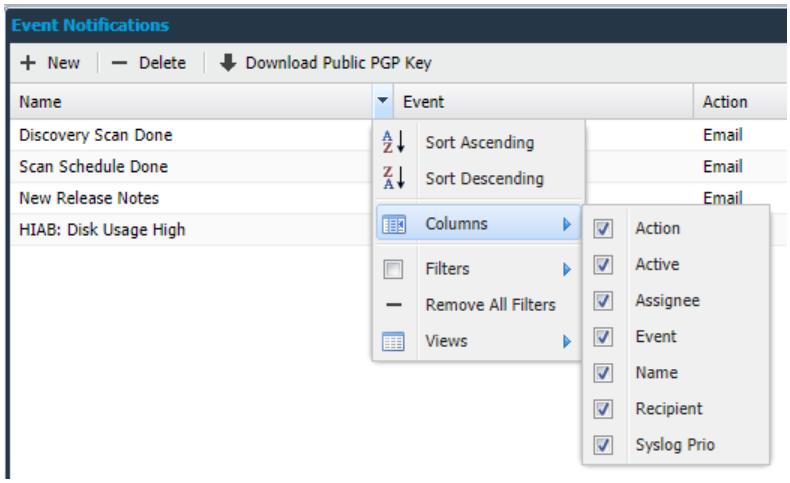
The event notifications area allows for actions to be performed upon certain events. The actions available are SNMP, syslog, creating a task, or sending an email. Default Event Notifications Settings are Discovery Scan Done, Scan Schedule Done, and New Release Notes



Option	Description
Discovery Scan Done	When a discovery scan is completed a notification will be sent out by email to the specified recipient (by default this will be the main user).
Scan Schedule Done	When a scan schedule is completed a notification will be sent out by email to the specified recipient (by default this will be the main user).
New Release Notes	When there are any release notes distributed, a notification will be sent out by email to the specified recipient, (by default this will be the main user).

To deactivate any of the default event notifications, right click on selected event and select **Disable**.

The event notifications window is configurable. Clicking the down arrow next to the name of any grid column allows you to customize which columns should be shown. The arrow becomes visible when hovering the mouse pointer over the column heading.



The available options are as follows:

Option	Description
Action	What to do when the event occurs
Active	Displays if the event is currently active.
Assignee	If the action is to create a ticket, the assignee is listed here.
Event	The type of the event to be notified.
Name	Displays the user specified name for the notification.
Recipient	If the action is to send an email, the recipient is listed here.
Syslog Prio	HIAB only. If the action is to send a syslog message, the priority is listed here.

You can further refine the search by enabling the filters.

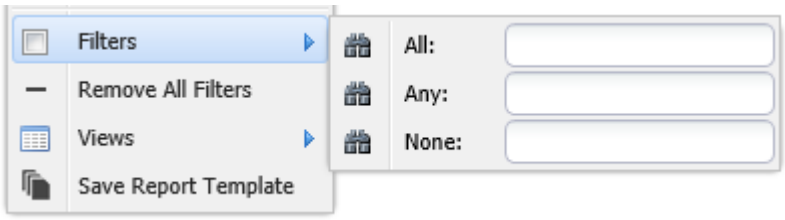
3 Filter

Most grid columns allow filtering, which lets you choose specific selection of data to be displayed. To enable filtering, click on the arrow next to the name of the grid column and go into **Filters**. The arrow is displayed when hovering the mouse pointer over the right end of the column heading.
Depending on the existing kind of data, you will be presented with various options. This section describes standard filter options found in most of the columns.
For specific filtering options, see each section below.

3.1 Textual

Displays 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.

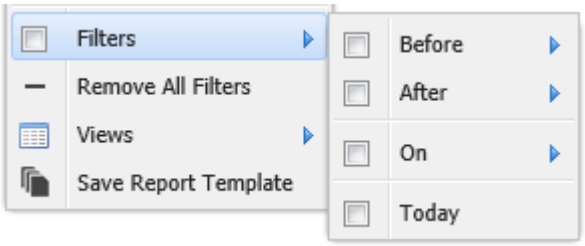
Ex.
`"Search entire phrase"`



Options	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.

3.2 Date

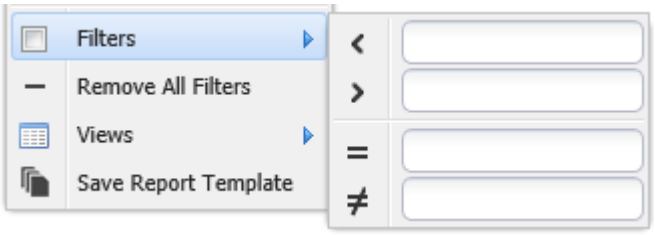
Displays few of the below options based on the column selection.



Options	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.
Today	Display all entries from today.
Never	Displays all entries missing a date.

3.3 Number

Include and/or exclude entries dependent on numbers.



Options	Description
<	Filter entries on values lesser than the provided value.
>	Filter entries on values greater than the provided value.
=	Filter entries that are equal to the provided value. This field allows you to enter both ranges and comma separated list of values.
≠	Filter entries that are not equal to the provided value, this field allows you to enter both ranges and comma separated list of values.

3.4 Remove All Filters

Select to remove all the applied filters.

3.5 Views

To save the current view of the Scan Scheduling, click on **Save View**. Provide a name while saving the view.

4 Creating and Editing Event Notifications

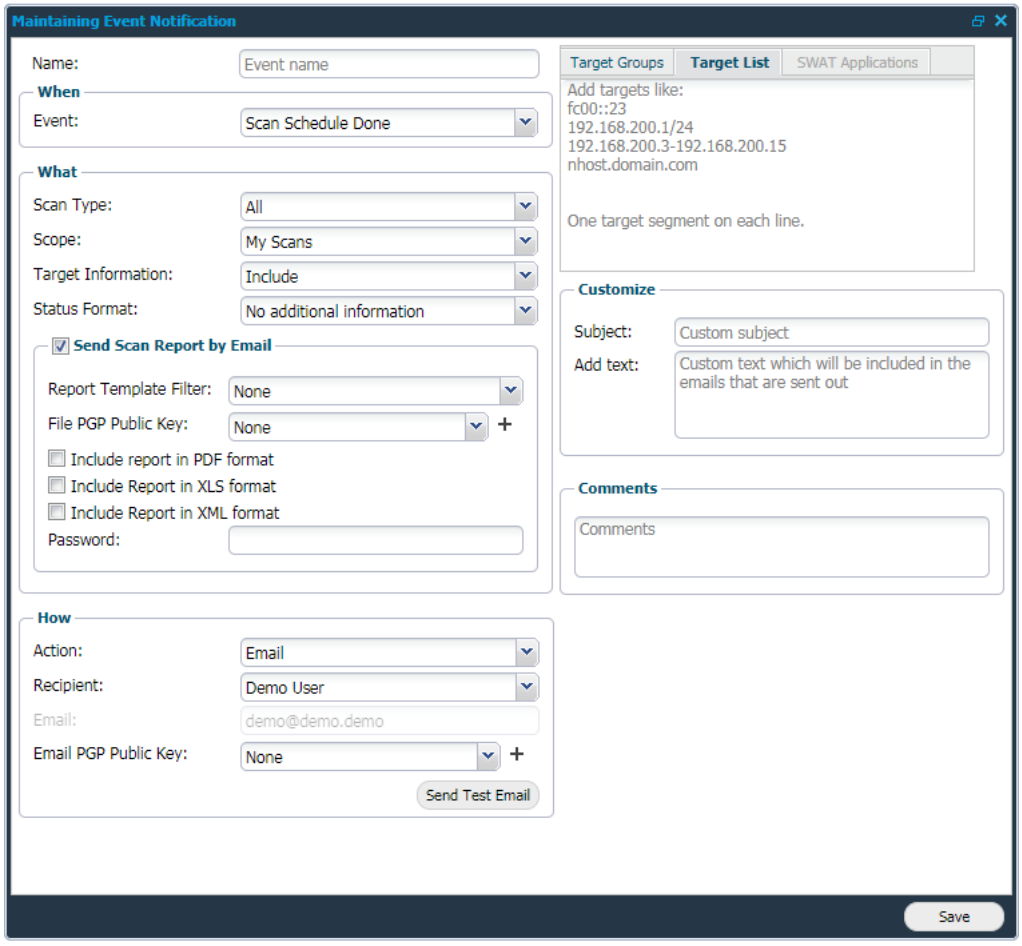
Create

To create a new event notification, click the **+ New** button in the top left corner of the window.

Configure

To configure one of the existing event notifications, right click on the selected event notification and choose **Edit**.

In any of the above cases, you will be prompted with the following window.



The elements of this window are described below:
***Note**: The **What** and **How** sections vary with the Event selected in the **When** section.*

Name

When creating a new event notification, provide a name in this field.

When

- **Event:** Select the event in the drop-down menu for which you want to be notified.

***Note**: Depending on your choice in the **When** section, you will be presented with various fields in the **What** and **How** sections.*

Option	Description
Scan Schedule Done	Sends a notification when a scan schedule has finished.
Discovery Scan Done	Sends a notification when a discovery scan has finished.
Discovery: Alive Target Found	Sends a notification when alive targets is discovered in a discovery scan.
Discovery: Alive Target Added	Sends a notification when alive targets are added from a discovery scan.
Discovery: Inactive Target Found (Each Scan)	Sends a notification when inactive targets are found. Only for Discovery scans.
Discovery: Inactive Target Found (Consecutive Scans)	Sends a notification when a target has been reported inactive for the number of consecutive discovery scans. The amount can be set in *Manage Targets* by accessing Settings the cogwheel in the upper right corner.
Target: Added	Send a notification when a new target is added.
Target: Removed	Sends a notification when a target is removed.
Target: Compliant	Sends a notification for each target that is compliant (if this is a compliance scan).
Target: Not Compliant	Sends a notification for each target that is not compliant (if this is a compliance scan).
Target: Report Finding Ready	Triggered when a scan has completed and a report has been created
Target: Large Report Found	Sends a notification when the report is too large.
Target: Host not reachable	Sends a notification when a host is not reachable during scanning.
Target: Authentication Failed	Sends a notification when the authentication fails for a target during a scan.
Target: Scan Scheduled	Sends a notification X day before the scan is scheduled for the targets. X can be set within the Send Before (Days) section.

Option	Description
Target: Scan Started	Sends a notification when the scan has started for the targets.
Target: Scan Timeout	Sends a notification when the scan timeouts for the targets.
Target: Scan Stopped	Sends a notification when the scan stops for the targets.
Target: Scan Failed	Sends a notification when the scan fails for the targets.
Target: Scan Results Updated	Sends a notification when the scan results are updated for the targets after an SLS-scan.
Scan: Could not start SLS	Sends a notification when scanning less scan could not start for the targets.
Scan: Schedule Scheduled	Sends a notification x days before the scan is scheduled to start. X can be set within the **Send Before (Days)** section.
Scan: Schedule Started	Sends a notification when the scan schedule has started.
Finding: High Risk Found	Sends a notification when a high risk has been detected.
Finding: Medium Risk Found	Sends a notification when a medium risk has been detected.
Finding: Low Risk Found	Sends a notification when a low risk has been found.
Finding: Information Found	Sends a notification when an informational finding has been reported.
Finding: Exploit Available	Sends a notification when a finding with an exploit available has been reported.
Finding: Ports Opened	Sends a notification when ports have been reported as opened.
Finding: Ports Closed	Sends a notification when ports have been reported as closed.
Finding: Comment Added	Sends a notification when a comment has been added for a finding. This is done by right clicking the finding within Reporting tools and choose **Add Comment**.
Finding: Risk Accepted	Sends a notification when a risk has been accepted.
Finding: Risk Acceptance Expired	Sends a notification when the acceptance for a risk has expired
Finding: Risk Acceptance Expiring	Sends a notification when the acceptance for a risk soon will expire.

Option	Description
Finding: Risk Acceptance Expired	Sends a notification when the acceptance for a risk expires.
Finding: Discussion Updated	OUTSCAN only. Sends a notification when the discussion for a SWAT finding has been updated.
Finding: Verify Done	OUTSCAN Only. Sends a notification when a verification has been performed in the SWAT report.
Finding: PCI failed	Sends a notification when a PCI report fails. This relates to the PCI preview policy, and the PCI module in OUTSCAN.
User: Logged In	Sends a notification when a user logs in.
New Release Notes	Sends a notification when there are new release notes available.
HIAB: Scanner Missing	Sends a notification when the current HIAB loses connection to any distributed HIAB.
HIAB: Update Done	Sends a notification when an update has finished successfully.
HIAB: Update Failed	Sends a notification when an update failed.
HIAB: Backup Done	Sends a notification when a backup has been performed.
HIAB: Backup Failed	Sends a notification when a backup has failed.
HIAB: Disk Usage High	Sends a notification when the Disk usage is too high.
HIAB: Server Rebooted	Sends a notification when the HIAB has restarted.
HIAB: Remote Support Notification	Sends a notification when remote support is enabled or disabled.
HIAB: Maintenance Plan Completed	Sends a notification when the maintenance plan has finished.

What

Option	Description
Scan Type	Select for which scan type you want to be notified.
Scope	Select the scope of the event. For events concerning schedule jobs and discovery jobs, you can set a Scope which determine if only your own jobs should be causing events or if any job that handles the targets shall be used (My Scans or All Scans).
Target Information	Select Include if you want to add the target information in the notification, else select Exclude.
Status Format	Set status format: ► No additional information ► Risk level summary information ► Risk level delta information
Send Scan Report by Email	Enable this feature if you want to send the scan report by email to a specified recipient. ► Report Template Filter: You can filter by selecting any of the saved report templates from the drop-down menu. ► File PGP Public Key: You can import a PGP key file by clicking the plus button to the right of the drop-down. Once you have imported a new key file, it will be added in the drop-down, available for you to use. ► Include report in PDF Format: Enable if you wish to send the report in PDF format. ► Include report in XLS Format: Enable if you wish to send the report in XLS format ► Include report in XML Format: Enable if you wish to send the report in XML format ► Password: Set a password to open the report.

How

Option	Description
Action	Select how do you want to send notification from the provided options. This could be adding an email recipient to be notified, creating a task on new findings, a SNMP trap, Splunk or sending a syslog message. ► **SNMP (**HIAB only): Send the notification to the configured SNMP server, these settings are available under: **Main Menu → Settings → Integrations → SNMP** (Tab). ► **Syslog** (HIAB only): Send the notification to the configured syslog server, these settings are available under: **Main Menu → Settings → Integrations → Syslog** (Tab). ► **Splunk** (HIAB only): Send the notification to the configured Splunk server, these settings are available under: **Main Menu → Settings → Integrations → Splunk** (Tab). ► **Email**: Send the notification by email to an already created user, or a custom email. Multiple emails can be entered, with a comma separator. ► **SMS**: OUTSCAN only. Send the notification by text message to an already created user ► **Task**: Create a task within the built-in ticketing system, and assign to an already created user ► **JIRA**: Create an issue within JIRA. These settings can be configured under: **Main Menu → Settings → Integrations → JIRA** (Tab) in OUTSCAN **Main Menu → Settings → Integrations → JIRA** (Tab) in the HIAB
Recipient	Provide a name to whom you want to send the notification. Custom is only available if you have super user privileges.
Email	If you want to send notification via email, please supply the email address in this field.
Email PGP Public Key	If desired, add a PGP Public Key to be used when emailing the notification.
Send Test Email	This allows you to send a test email to your account.
Send SMS Test	Sending a test SMS to a mobile phone is allowed for events like "High risk found". If an event like that is selected, the SMS option is available in *Action*. Select sms and the Test SMS button becommes visible.
Test SNMP	Sends a SNMP trap to the defined SNMP server.
Test Syslog	Sends a syslog message to the defined syslog server.

You can also filter out events by selecting a set of targets or target groups.
When setting up an event for "High risk found", it sends out an event for all high-risk

findings found on any target.
Selecting a target group for the event, the high-risk event is only sent to targets in that group limiting the events to specific targets.

Option	Description
Target Groups	Choose what target group the event notification will be assigned to.
Target List	Choose what IP range the event notification will be assigned to. You do not have to specify IP addresses that have been selected in the target groups tab.
SWAT Applications	Limit the event to specific SWAT applications.

Customize

Option	Description
Subject	Custom subject for email.
Add text	The added custom text will be included in the email that is sent out.

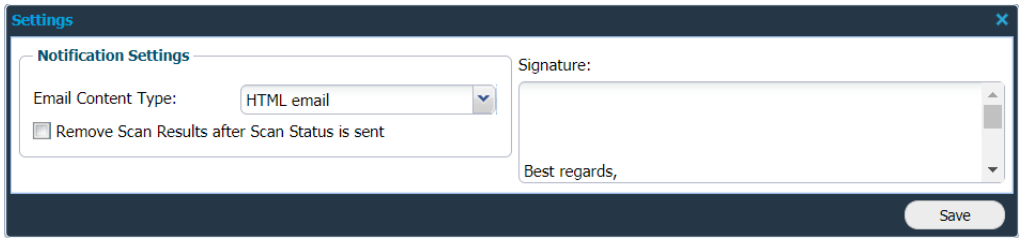
Comments

You can add any additional comments in this field.

5 Settings

5.1 OUTSCAN

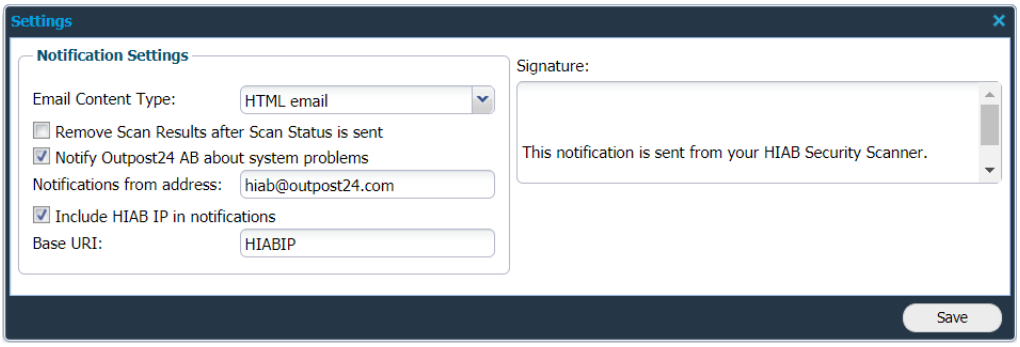
By clicking the Settings icon located on top right of the window, the notification settings can be changed.



Option	Description
Email Content Type	Allows you to choose the email format. ► HTML email ► Text only email
Remove Scan Results after Scan Status is sent	Remove the report from the system after the email is sent. It removes the report only after successfully sending the report to all the recipients.
Signature Section	Allows you to change the email signature from the system. If left empty, it will take the default signature.

5.2 HIAB

By clicking the Settings icon located on top right of the window, the notification settings can be changed.



Option	Description
Email Content Type	Allows you to choose the email format. ► HTML email ► Text only email
Remove Scan Results after Scan Status is sent	Remove the report from the system after the email is sent. It removes the report only after successfully sending the report to all the recipients.
Notify Outpost24 AB about system problems	Allows the system to send emails to Outpost24 regarding any system problem.
Notifications from address	Determines the sender address.
Include HIAB IP in notifications	Include a reference to the HIAB IP in system notifications.
Base URI	Allows you to define a domain name instead of the HIAB IP in the system notifications.
Signature	Section allows you to change the email signature from the system. If left empty, it will take the default signature.