Outpost24

Vulnerability Management made easy

Event Notifications

Quick Start Guide

Last update:

9 February 2017

Table of Contents

1. Executive Summary 3

2. Event Notifications in Graphical User Interface 4

   2.1. Default Event Notification Settings 4

   2.2. Editing and Creating Event Notifications 5

3. Technical Support 8

About This Guide

1. Executive Summary

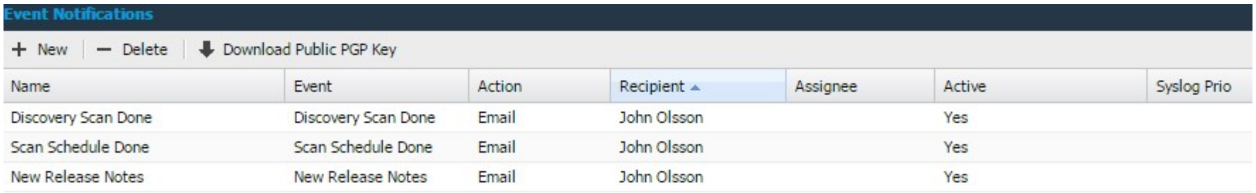
This document is meant to provide users a comprehensive overview of how to setup and how to use Event Notifications for Outscan and HIAB. This document has been elaborated under the assumption that the reader has access to the Outscan/HIAB Account and Graphical User Interface.

Information in this document is subject to change without prior notice.

2. Event Notifications in Graphical User Interface

To get into Event Notifications click on the main menu button at the bottom-left corner of your screen and select “Settings >> Event notifications”.

2.1. Default Event Notification Settings



Name	Event	Action	Recipient ▲	Assignee	Active	Syslog Prio
Discovery Scan Done	Discovery Scan Done	Email	John Olsson		Yes	
Scan Schedule Done	Scan Schedule Done	Email	John Olsson		Yes	
New Release Notes	New Release Notes	Email	John Olsson		Yes	

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).

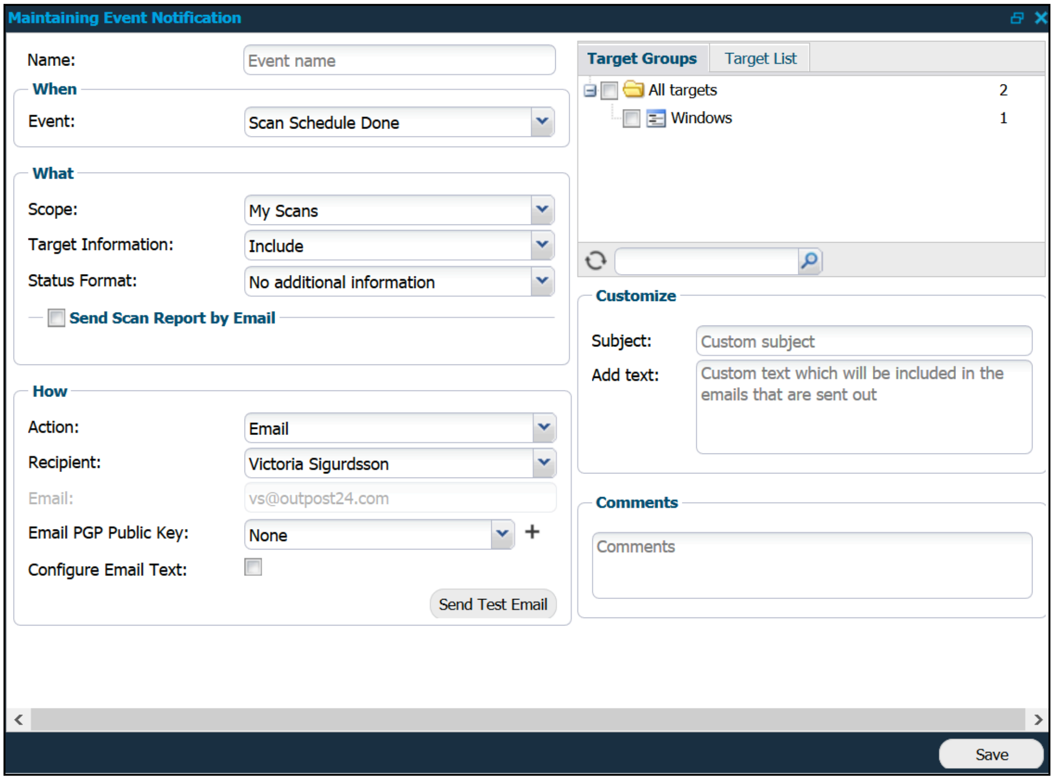
Scan Schedule Done – When a scan schedule is completed a notification will be sent out by email to the specified recipient (by default this will be the main user).

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”.

2.2. Editing and Creating Event Notifications

To configure one of the existing event notifications, right click on the selected event notification and choose “Edit”. If you want to create a new event notification click the “New” button in the top left corner. Whether you create a new event notification or editing an existing one you will then be prompted with the following window.



Maintaining Event Notification

Name: Event name

When

Event: Scan Schedule Done

What

Scope: My Scans

Target Information: Include

Status Format: No additional information

□ **Send Scan Report by Email**

How

Action: Email

Recipient: Victoria Sigurdsson

Email: vs@outpost24.com

Email PGP Public Key: None

Configure Email Text: □

□ All targets	2
□ Windows	1

Customize

Subject: Custom subject

Add text: Custom text which will be included in the emails that are sent out

Comments

Comments

Name – Name the event notification that you created or rename an existing notification.

Event – This dropdown will present you with multiple events that may occur when using the tool. Choose for which event you want to receive the notification. Depending on your choice here you will be presented with various fields in the “What” and “How” frames.

- **Scan Schedule Done** – Will send a notification whenever a scan schedule has finished
- **Discovery Scan Done -** Will send a notification whenever a discovery scan has finished
- **Discovery: Alive Target Found -** Will send a notification whenever alive targets is discovered in a discovery scan
- **Discovery: Alive Target Added -** Will send a notification whenever alive targets are added from a discovery scan
- **Discovery: Inactive Target Found (Each Scan) -** Will send a notification whenever inactive targets are found

- **Discovery: Inactive Target Found (Consecutive Scans)** - Will send a notification whenever a target has been reported inactive for the number of consecutive discovery scans. The amount can be set in Manage Targets by accessing the cogwheel in the upper right corner.
- **Target: Added -** Will send a notification whenever a new target is added
- **Target: Removed -** Will send a notification whenever a target is removed
- **Target: Report Finding Ready -**
- **Target: Large Report Found -** Will send a notification whenever the report is too large

Target: Host not reachable - Will send a notification whenever a host is not reachable during scanning

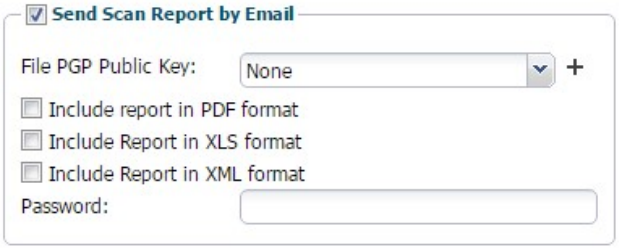
- **Target: Authentication Failed -** Will send a notification whenever the authentication fails for a target during a scan
- **Target: Scan Scheduled -** Will send a notification X days before the scan is scheduled for the targets. X can be set within the Send Before (Days) section
- **Target: Scan Started -** Will send a notification whenever the scan has started for the targets
- **Target: Scan Timeout -** Will send a notification whenever the scan timeouts for the targets
- **Target: Scan Stopped -** Will send a notification whenever the scan stops for the targets
- **Target: Scan Failed -** Will send a notification whenever the scan fails for the targets
- **Target: Scan Results Updated -** Will send a notification whenever the scan results are updated for the targets
- **Scan: Could not start SLS -** Will send a notification whenever scanning less scan could not start for the targets
- **Scan: Schedule Scheduled -** Will send a notification x days before the scan is scheduled to start. X can be set within the Send Before (Days) section
- **Scan: Schedule Started -** Will send a notification whenever the scan schedule has started
- **Finding: High Risk Found** - Will send a notification whenever a high risk has been detected
- **Finding: Medium Risk Found -** Will send a notification whenever a medium risk has been detected
- **Finding: Low Risk Found -** Will send a notification whenever a low risk has been found
- **Finding: Information Found -** Will send a notification whenever an informational finding has been reported
- **Finding: Exploit Available -** Will send a notification whenever a finding with an exploit available has been reported
- **Finding: Ports Opened -** Will send a notification whenever ports has been reported as opened
- **Finding: Ports Closed -** Will send a notification whenever ports has been reported as closed
- **Finding: Comment Added -** Will send a notification whenever 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 -** Will send a notification whenever a risk has been accepted
- **Finding: Risk Acceptance Expired -** Will send a notification whenever the acceptance for a risk has expired

- **Finding: Risk Acceptance Expiring -** Will send a notification whenever the acceptance for a risk soon will expire
- **Finding: Discussion Updated –** Outscan only. Will send a notification whenever the discussion for a SWAT finding has been updated
- **Finding: Verify Done –** Outscan Only. Will send a notification whenever a verification has been performed in the SWAT report
- **Finding: PCI failed** – Will send a notification whenever a PCI report fails. This relates to the PCI preview policy, and also the PCI module in Outscan
- **User: Logged In -** Will send a notification whenever a user logs in
- **New Release Notes -** Will send a notification whenever there are new release notes available
- **HIAB: Scanner Missing -** Will send a notification whenever the current HIAB loses connection to any distributed HIAB
- **HIAB: Update Done -** Will send a notification whenever an update has finished successfully
- **HIAB: Update Failed -** Will send a notification whenever an update failed
- **HIAB: Backup Done -** Will send a notification whenever a backup has been performed
- **HIAB: Server Rebooted -** Will send a notification whenever the HIAB has restarted
- **HIAB: Remote Support Notification -** Will send a notification whenever remote support is enabled or disabled
- **HIAB: Maintenance Plan Completed -** Will send a notification whenever the maintenance plan has finished

Scope – This field allows you to specify if the event should trigger a notification on specific schedules only, or on scans or other events.

Target Information – Will let you include or exclude what you specified in the Scope field.

Send Report by Email – Check this if you want the scan report to be sent by email to the specified recipient. Checking this box will give you access to the fields to the right. **File PGP Public Key -** You can import a PGP key file by clicking the plus button to the right of the dropdown. Once you have imported a new key file it will be added in the dropdown, available for you to use.



☑ Send Scan Report by Email

File PGP Public Key: None +

□ Include report in PDF format

□ Include Report in XLS format

□ Include Report in XML format

Password:

Password – Set a password to open the report.

Action – Specifies how the notification will be performed.

- **SNMP** – HIAB only. Send the notification to the configured SNMP server, these settings are available under Main Menu >> Settings >> Server >> Servers (Tab)
- **Syslog** - HIAB only. Send the notification to the configured syslog server, these settings are available under Main Menu >> Settings >> Server >> Servers (Tab)
- **Splunk –** HIAB only. Send the notification to the configured splunk server, these settings are available under Main Menu >> Settings >> Server >> Servers (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 >> Account >> Features in Outscan, and under Main Menu >> Settings >> Server >> JIRA (Tab) in the HIAB.

Recipient – Choose what recipient the notification will be sent to. The "Custom" option will unlock the Email field below were you can add an email address as recipient.

Email PGP Public Key - You can choose whether you want the notification email to be encrypted or not. You may import a PGP key file by clicking the plus button to the right of the dropdown. Once you have imported a new key file it will be added in the dropdown available for you to use.

Configure Email Text – Enable to configure the fields that are included in the email

Send Test Email Button – Sends a notification email to the specified recipient.

Target Groups Tab – Choose what target group the event notification will be assigned to. **Target List Tab** - 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.

Subject – Choose the subject of the notification email. This can be left blank to use default subject.

Add Text – Add what text that you would like to be included in the notification email.

3. Technical Support

Contact our 24/7 support team by email or telephone:

Email support@outpost24.com

Tel (from the UK): +44 20 7193 6094

Tel (from the US): +1 (800) 69 13 150

Outpost24

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