



Vulnerability Management *made easy*

Scan Scheduling

Quick Start Guide

Last update:
9 February 2017

Table of Contents

1. Executive Summary.....	3
2. Scan Scheduling in Graphical User Interface.....	4
2.1. Scan Scheduling Main Page.....	4
2.2. Scan Policy Tab.....	5
2.3. Scan Status tab.....	7
2.4. Scan History Tab.....	7
3. Technical Support.....	9



About This Guide

1. Executive Summary

This document is meant to provide users a comprehensive overview of the feature Scan Scheduling 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.

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

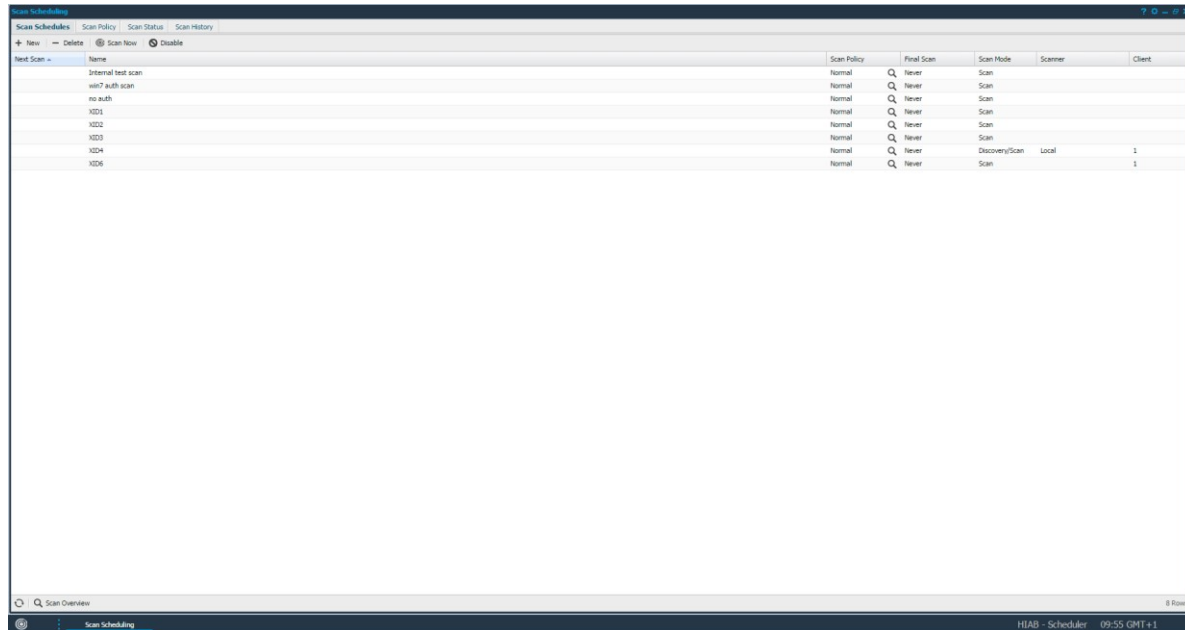
Reproduction of any part of the document without prior permission is strictly prohibited.

© Outpost24. All Rights Reserved.

2. Scan Scheduling in Graphical User Interface

To get into Scan Scheduling click on the main menu button at the bottom-left corner of your screen and select “Target Scanning -> Scan Scheduling” or just “Scan scheduling”.

2.1. Scan Scheduling Main Page



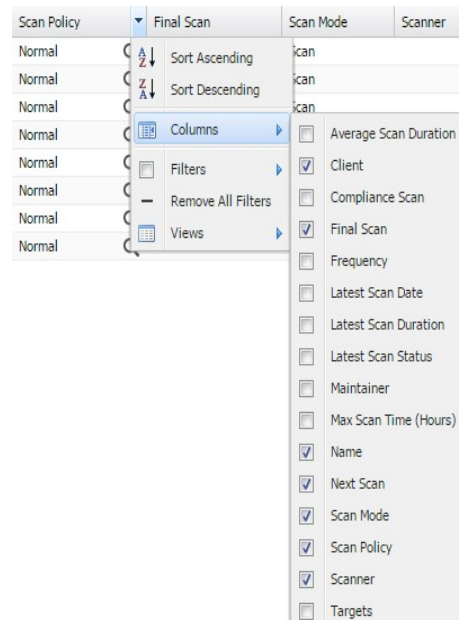
Name	Scan Policy	Final Scan	Scan Mode	Scanner	Client
Internal test scan	Normal	Q Never	Scan		
win7 auth scan	Normal	Q Never	Scan		
no auth	Normal	Q Never	Scan		
X02	Normal	Q Never	Scan		
X022	Normal	Q Never	Scan		
X03	Normal	Q Never	Scan		
X04	Normal	Q Never	Discovery/Scan	Local	1
X06	Normal	Q Never	Scan		1

In the main Scan Scheduling page you will see all your defined scan schedules along with information about each schedule. The information shown is configurable by the user by selecting which columns he or she wants to show.

To add or remove a column, hover your mouse over the column name and click on the down pointing arrow and select “Columns”.

You can choose between the following columns:

- **Average Scan Duration:** Shows the average scan duration for each scan schedule.
- **Client:** This is a custom attribute defined by the user and is not available by default. The user may add custom made columns to be able to add any information he or she wishes.
- **Compliance Scan:** Shows if the scan schedule is a compliance scan or not.
- **Final Scan:** Displays a date at which the scan schedule’s final scan will take place.
- **Frequency:** Frequency of the scans in the scan schedule.
- **Latest Scan Date:** Displays the date of the latest performed scan.



Scan Policy	Final Scan	Scan Mode	Scanner
Normal	Sort Ascending	Scan	
Normal	Sort Descending	Scan	
Normal	Columns	Scan	
Normal	Filters		
Normal	Remove All Filters		
Normal	Views		

- Average Scan Duration
- Client
- Compliance Scan
- Final Scan
- Frequency
- Latest Scan Date
- Latest Scan Duration
- Latest Scan Status
- Maintainer
- Max Scan Time (Hours)
- Name
- Next Scan
- Scan Mode
- Scan Policy
- Scanner
- Targets



- **Latest Scan Duration:** Displays the duration of the latest scan.
- **Latest Scan Status:** Displays the status of the latest scan.
- **Maintainer:** Displays which user is the maintainer of the scan schedule.
- **Max Scan Time:** Displays for how many hours the scan will run before it shuts down.
- **Name:** The name of the scan schedule.
- **Next Scan:** Displays the date of the next scan (if scheduled).
- **Scan Mode:** Displays what kind of scanning mode the scan schedule is using.
- **Scan Policy:** Displays which scan policy is used during the scans.
- **Scanner (HIAB Only):** Displays which scanner the HIAB is using during the scans.
- **Targets:** Displays the number of targets in the specific scan schedule.

Paging: If a grid contains a lot of information then all of the data will not be loaded at once. When the scrollbar reaches an end position it will automatically load the next section. You can also enter a number in the toolbar to immediately jump to a specific entry.

Refresh: The refresh icon will perform a reload of the currently shown data.

Filtering: Most grid columns allow filtering, this lets you specify to only show a sub-selection of all data. To enable filtering, click on the arrow next to the name of the grid column and go into **Filters**. Depending on the type of data, this may display different things.

The 4 buttons in the top allows you to perform following actions with your scan schedules:

- **New:** Create a new scan schedule.
- **Delete:** Delete the selected scan schedule.
- **Scan Now:** Immediately initiates the selected scan schedule.
- **Disable:** Disables the selected scan schedule.

To see the changes made to a certain entry, right click on it and select **Audit log**. This will show a dialog with all the changes made to the object that were made by you or one of the users that you administrate.

To export data from the grid, right click on any entry and select either to export it as HTML or CSV (comma separated values) in the sub menu. This will give you either a HTML page or a CSV file that you can save or copy data from.

2.2. Scan Policy Tab

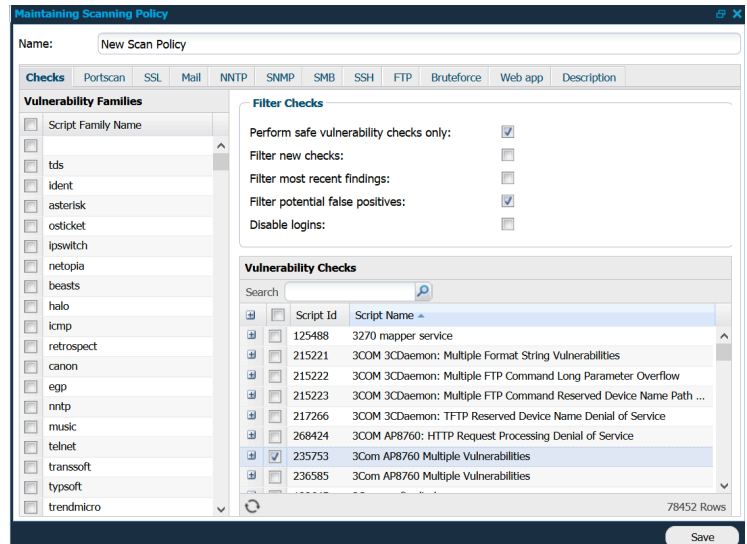
In the Scan Policy tab you can customize your scanner to perform the scans that you wish or configure each scan to suit your network. The scan policies with type: "System" are predefined and available by default. These scan policies cannot be edited. If you try to edit a predefined scan policy the additional changes will be saved along with the predefined policy under a custom name, set by the user. The initial predefined policy will stay the same as

Scan Scheduling			
Scan Schedules	Scan Policy	Scan Status	Scan History
+ New - Delete			
+	Name ▾	Type	
+	Unsafe	System	
+	Test Credentials	System	
+	Port scan	System	
+	PCI (preview)	System	
+	Normal with webapp	System	
+	Normal	System	
+	New checks and most recent findings	User defined	
+	New checks and most recent findings	System	
+	New checks	System	
+	John test	User defined	

before editing. The policies with the type “User Defined” are defined by a user. By pressing the button with the plus-sign to the left of the policy name will expand the policy and reveal all information.

To create, edit and maintaining a scan policy, click on the “New” button or right click on any of the existing scan policies and you will be prompted with following window:

- Checks:** All vulnerability checks are divided into families. In the vulnerability families section you can select which script families you want to have included in the policy. You can select/deselect all families at once by clicking the top checkbox. Here you can select if the policy should only include **safe checks**, which are checks that do not try to exploit vulnerabilities in order to find them. Unchecking **safe checks** can exploit a vulnerable target. **Filter new checks** is used to only include new checks since the last time the scan ran. **Filter most recent findings** adds all checks that were found during the last scan. Checking **Filter Potential False Positives** will enable the scan policy to exclude all the potential false positive. Checking **Disable Logins** will enable the scan policy to disable certain kinds of login attempts.



In the **Vulnerability checks** you can select individual checks to be executed when running your scan. The search bar at the top allows you to search the vulnerabilities to easily find the checks you are looking for.

- Portscan:** Contains the setup for the port scanner which is used to scan the targets for open ports. Warning: scheduling more than 10.000 ports in UDP scanning will have an effect on the overall scan time. Roughly it will take an hour per 20.000 ports in best case.
- SL:** Contains the settings for any SSL service found when scanning targets with this policy.
- Mail:** Contains the settings for the different mail protocols available when scanning targets with this policy.
- NNTP:** Contains the settings for any news server found when scanning targets with this policy.
- SNMP:** Contains the settings for any SNMP server found when scanning targets with this policy.
- SMB:** Tab which contains the authentication settings and credentials used to enable **Authenticated Scanning**.
- SSH:** Contains the authentication settings and credentials used to enable **Authenticated Scanning**.
- FTP:** Contains the settings for any FTP server found when scanning targets with this policy.
- Brute force:** Contains the settings for the brute force and the different protocols which the brute force can operate on.
- Web App:** Allows to enable or disable web app scanning.
- Description:** Contains a small description of the scan policy. If you create your own scanning policy it's possible to write a small text here which describes its use.

2.3. Scan Status tab

In the Scan status tab you will see the progress of all active scans. You're also able to pause, resume and stop all the active scans.

Scan Scheduling							
Scan Schedules		Scan Policy		Scan Status		Scan History	
 Pause ▶ Resume ■ Stop ■ Stop All Scans							
Scheduled Start	Schedule	Target	Status	Progress	Scheduled End	Priority	Scanner
Internal test scan (2)							
2016-01-11 14:08	Internal test scan	10.216.11.1	Waiting for con...	0%	2016-01-15 18:08	Normal	Local
2016-01-11 14:08	Internal test scan	10.216.11.121	Waiting for con...	0%	2016-01-15 18:08	Normal	Local

If you right click on any active scan you will be able to set priority on the scan. Choose between low, medium or high priority. Most grid columns allow filtering, this lets you specify to only show a subselection of all data. To enable filtering, click on the arrow next to the name of the grid column and go into **Filters**. Depending on the type of data this can show different things.

2.4. Scan History Tab

Scan Scheduling											
Scan Schedules		Scan Policy		Scan Status		Scan History					
Scan Start Date	Scan End Date	Scan Time	Scan Type	Target	Target Group	Scan Policy	Scan Schedule	Scanner	Download State	Cause of Error	
2016-01-11 15:03	2016-01-11 15:04	00:01:00	Target Stopped	10.216.11.1	asd	Normal	Internal test scan	Local	Not Downloaded		
2016-01-11 15:03	2016-01-11 15:04	00:01:00	Target Stopped	10.216.11.121	asd	Normal	Internal test scan	Local	Not Downloaded		
2016-01-11 15:03	2016-01-11 15:04	00:01:00	Scan Job Done	Internal test scan		Normal	Internal test scan	Local	Not Downloaded		
2016-01-11 14:22	2016-01-11 14:29	00:07:00	Target Done	10.216.11.1	asd	Normal	Internal test scan	Local	Not Downloaded		
2016-01-11 14:09	2016-01-11 14:21	00:12:00	Target Done	10.216.11.121	asd	Normal	Internal test scan	Local	Not Downloaded		
2016-01-11 14:08	2016-01-11 14:30	00:22:00	Scan Job Done	Internal test scan		Normal	Internal test scan	Local	Not Downloaded		
2015-12-22 08:04	2015-12-22 08:05	00:01:00	Target Stopped	10.216.11.48	no auth	Normal	XID4	Local	Not Downloaded		
2015-12-22 08:04	2015-12-22 08:04	00:00:00	Discovery Done	XID4		Discovery	XID4	Local	Not Downloaded		
2015-12-22 08:03	2015-12-22 08:05	00:02:00	Scan Job Done	XID4		Normal	XID4	Local	Not Downloaded		
2015-12-15 11:44	2015-12-15 11:44	00:00:00	Target Stopped	10.216.11.81	win7 Auth scan	Normal	XID4	Local	Not Downloaded		
2015-12-15 11:44	2015-12-15 11:44	00:00:00	Target Stopped	10.216.11.48	no auth	Normal	XID4	Local	Not Downloaded		
2015-12-15 11:44	2015-12-15 11:44	00:00:00	Scan Job Done	XID4		Normal	XID4	Local	Not Downloaded		
2015-12-10 11:02	2015-12-10 11:03	00:01:00	Target Stopped	10.216.11.81	win7 Auth scan	Normal	XID4	Local	Not Downloaded		
2015-12-10 11:02	2015-12-10 11:03	00:01:00	Target Stopped	10.216.11.48	no auth	Normal	XID4	Local	Not Downloaded		
2015-12-10 11:02	2015-12-10 11:03	00:01:00	Scan Job Done	XID4		Normal	XID4	Local	Not Downloaded		
2015-12-02 06:48	2015-12-02 06:48	00:00:00	Target Stopped	10.216.11.81	win7 Auth scan	Normal	XID6	Local	Not Downloaded		
2015-12-02 06:47	2015-12-02 06:48	00:01:00	Target Stopped	10.216.11.48	no auth	Normal	XID4	Local	Not Downloaded		
2015-12-02 06:47	2015-12-02 06:48	00:01:00	Scan Job Done	XID6		Normal	XID6	Local	Not Downloaded		
2015-12-02 06:47	2015-12-02 06:48	00:01:00	Scan Job Done	XID4		Normal	XID4	Local	Not Downloaded		
2015-12-02 06:45	2015-12-02 06:45	00:00:00	Scan Job Failed	XID2		Normal	XID2	Local	Not Downloaded	The scan sche...	
2015-12-02 06:44	2015-12-02 06:44	00:00:00	Target Stopped	10.216.11.90		Normal	XID1	Local	Not Downloaded		
2015-12-02 06:44	2015-12-02 06:44	00:00:00	Target Stopped	10.216.11.61		Normal	XID1	Local	Not Downloaded		
2015-12-02 06:44	2015-12-02 06:44	00:00:00	Target Stopped	10.216.11.46		Normal	XID1	Local	Not Downloaded		
2015-12-02 06:44	2015-12-02 06:44	00:00:00	Target Stopped	10.216.11.42		Normal	XID1	Local	Not Downloaded		
2015-12-02 06:44	2015-12-02 06:44	00:00:00	Target Stopped	10.216.11.26		Normal	XID1	Local	Not Downloaded		

In the Scan History tab you will find a history over all scans performed along with information about each scan. Use the columns to customize the information to show the information that you want to see. If the scan for some reason fails you will find a descriptive explanation in the "Cause of Error" column - this is extremely valuable information when troubleshooting.

Most grid columns allow filtering, this lets you adjust the column to only show a sub-selection of all data. To enable filtering, click on the arrow next to the name of the grid column and go into **Filters**.

Depending on the type of data this can show different things.



If you right click on any entry in the scan history list, depending on what scan it was, you will get some or all of the following options:

- **Show Scan Results:** If you right click on a scan that ended successfully you have the option to show the report for this scan. This can be done both on individual targets and on complete scan schedules.
- **Scan:** Will start a scan against the same target(s).
- **Audit log:** To see the changes made to a certain entry, right click on it and select **Audit log**. This will show a dialogue with all the changes made to the object that were made by you or one of the users that you administrate.
- **Export:** To export data from the grid, right click on any entry and select either to export it as HTML or CSV (comma separated values) in the sub menu. This will give you either a HTML page or a CSV file with data that you can save or copy data from.
- **Download Blueprint (HIAB Only):** By clicking on this options you will automatically download the blueprint of that specific scan. The blueprints are encrypted and can only be decrypted and used by Outpost24 to troubleshoot and investigate. If the specific scan was performed by another scanner than local one, the "Download Blueprint" option must be pressed twice for the download to begin, once for the scanner to send the blueprint to the scheduler and once for downloading the blueprint from the scheduler.



3. Technical Support

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

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