Outpost24

Vulnerability Management made easy

PCI Compliance

User Guide

Version: 1.0
2018-04-27

Table of Contents

About This Document

This document provides users with a comprehensive overview of the PCI Scanning module for OUTSCAN. This document has been elaborated under the assumption the reader has access to the OUTSCAN Account, and Portal Interface.

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

Copyright

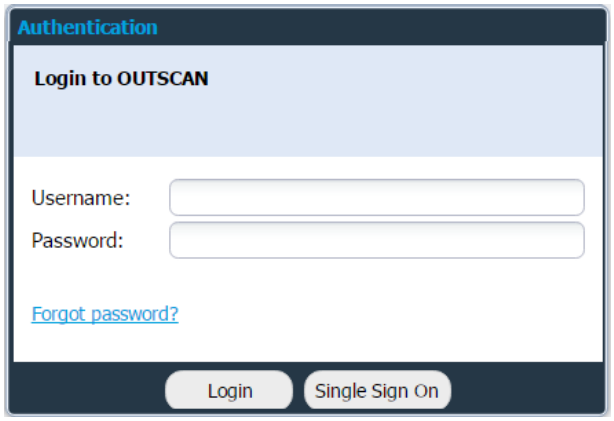
Trademark

1 Introduction

Outpost24 is a certified Approved Scanning Vendor (ASV) by the PCI Security Standards Council and offers OUTSCAN PCI, an extension of our OUTSCAN vulnerability management tool designed specifically to verify and prove PCI DSS compliance. OUTSCAN PCI examines network perimeters, identifies vulnerabilities and inventories actionable remedies, and can repeatedly scan until all criteria are met to effectively protect the integrity of cardholder data and verify compliance.

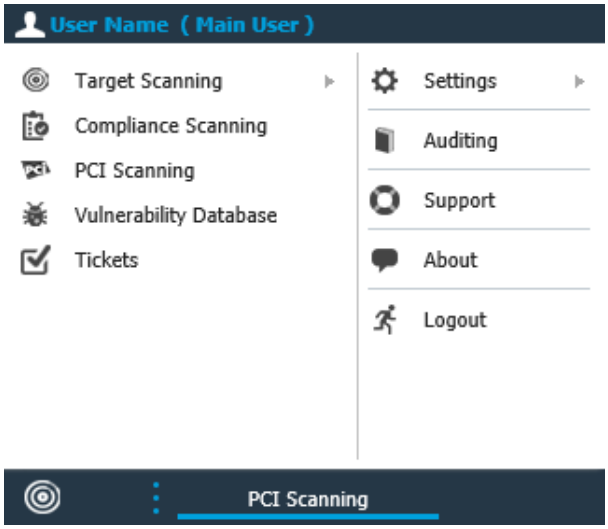
2 Getting Started with PCI Scanning

To launch the OUTSCAN application, navigate to https://outscan.outpost24.com.



Log on using your credentials.

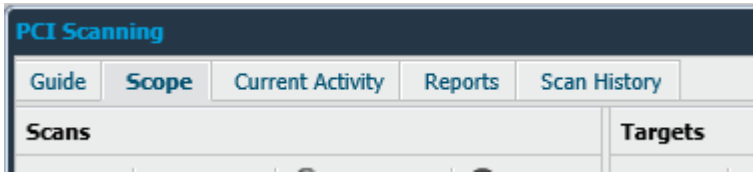
To access the PCI Scanning module, navigate to **Menu → PCI Scanning.**



3 Interface Sections

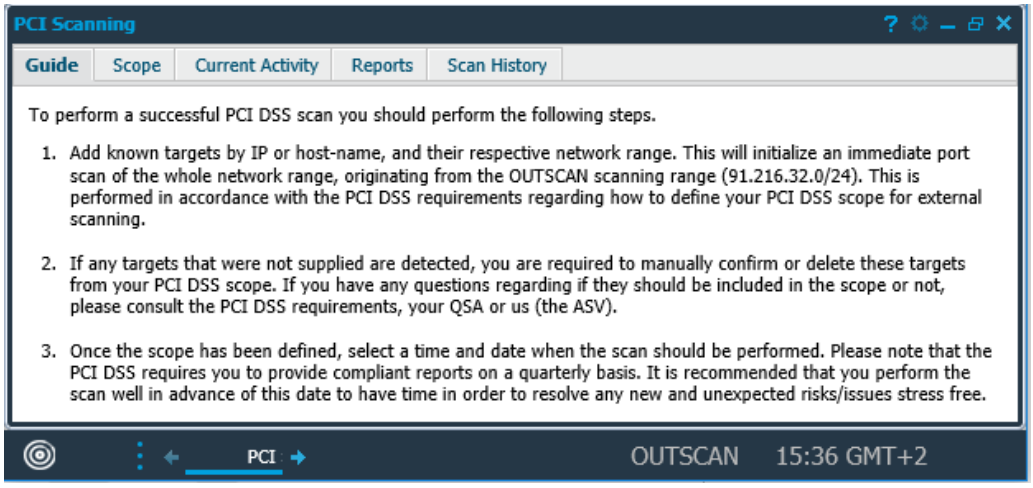
The PCI Compliance Scanning interface consist of five tabs.

- Guide
- Scope
- Current Activity
- Reports
- Scan History



3.1 Guide

The **Guide** tab is the welcoming page for the PCI Scanning and is displayed every time the PCI Compliance module is started. It provides a quick guide on how to set up and run scans.

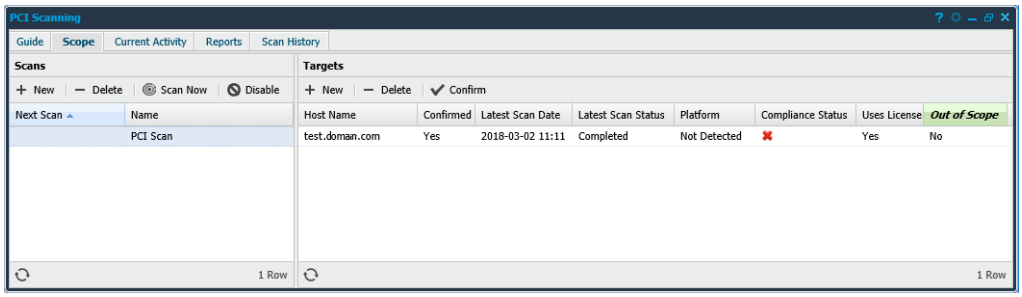


3.2 Scope

The **Scope** tab is used to set up the scope of the scans, the left Scans part is used to create schedules to run. These can either be scheduled to run at a specific time or be started manually.

The **Scope** tab consists of two sections:

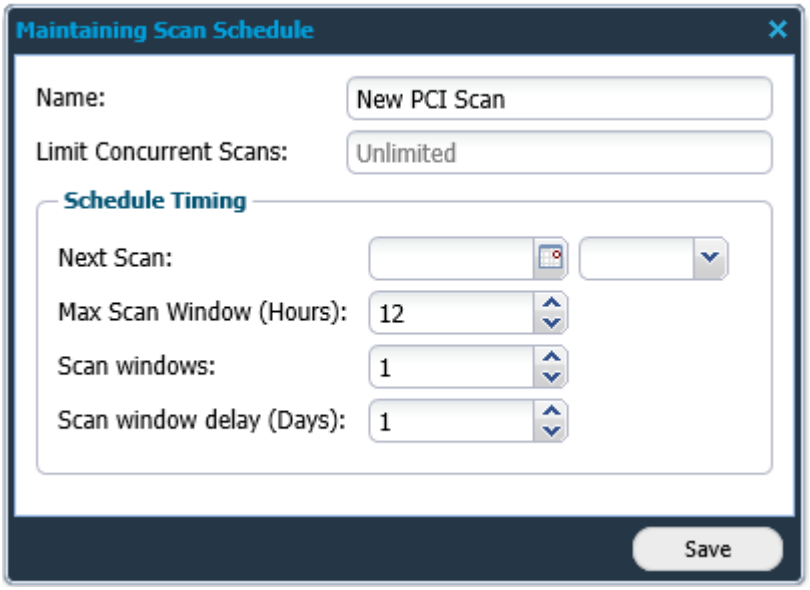
- Scans
- Targets



3.2.1 Scans

The **Scans** section consists of all defined scan schedules along with information about each schedule.

New	-	Displays the *Maintaining Scan Schedule* window where a new scan schedule can be set up.
Delete	-	Removes a scan schedule from the list.
Scan Now	-	Start the scan manually.
Disable	-	Stops the schedule from running a scan.



Edit - To edit a schedule object right-click on it and select Edit

Grid Window - The grid that shows the scan schedules is configurable. Clicking on the arrow next to the name of any grid column allows you to customize what columns that will be shown out of the following:

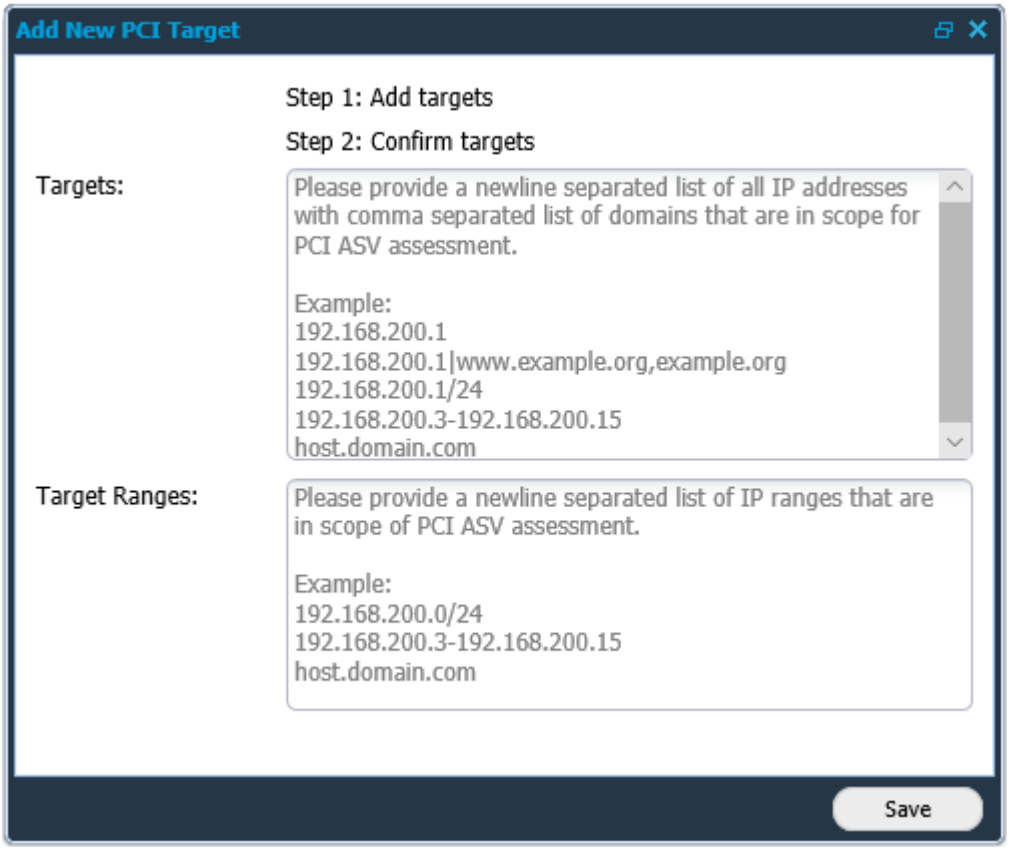
Option	Description
Latest Scan Date	The last time the schedule was executed.
Latest Scan Status	The status of the latest schedule execution.
Name	The name of the scan schedule.
Next Scan	The date when the next scan will occur, if empty it will not start automatically.

3.2.2 Target

In the **Target** section, targets can be selected for scanning. For each scan of a target, a compliance report is created.
In the Target Ranges field, you can enter a range of targets to be scanned.
When adding a target range, a discovery scan is performed to find all the alive targets in the range. These are added to the schedule as unconfirmed targets, and need to be confirmed or they should be deleted if they are not part of the PCI scanning scope.
A target can only exist in one PCI scan job.

New	-	Displays the *Add New PCI Target* window where new targets can be set up. When adding a domain or a network ranges, OUTSCAN scans for all hosts available automatically. All the found hosts are listed in the **Targets** section. ***Note**: The Add New PCI Target window is also displayed by default the first time PCI Scanning is started.*
Delete	-	Removes the hosts that should not be part of the scan.
Confirm	-	Selects and add found hosts to the scan.

***Note**: You are required to confirm or delete these targets from the PCI DSS scope. If you have any questions regarding if they should be included in the scope or not, refer to the PCI DSS requirements or your QSA.*



Edit - To edit a target right-click on it and select Edit

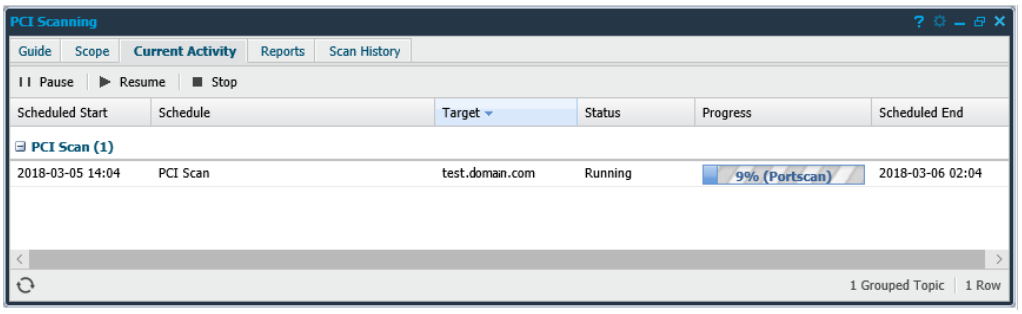
Grid Window - The grid that shows the targets is configurable. Clicking on the arrow next to the name of any grid column allows you to customize what columns will be shown out of the following:

Option	Description
IP Address	The IP address of the target.
Host Name	The targets host name.
Out of Scope	If the target is out of scope.
Confirmed	If the target is confirmed to be part of the PCI scanning scope or not.
Latest Scan Date	The most recent date that a scan was run.
Latest Scan Status	Status of the most recent scan.
Virtual Host Names	A list of virtual host names.
MAC Address	The targets MAC address.
Hidden URLs	A list of hidden URLs for the webappscanner to crawl. Hidden URLs are URLs that cannot be reached by crawling the default address.
Platform	The platform detected on this target.
Compliance Status	The latest compliance status for this target.

3.3 Current Activity

In the **Current Activity** tab, the progress of the current scans is monitored. The scans can be paused, resumed, and stopped at any time.

Pause - Pause the selected scan.
Resume - Resume the selected scan.
Stop - Stop the selected scan.



Export HTML: To export the currently visible data from the grid, right click on any entry and select Export HTML. This will give you an HTML page with data that you can save or copy data from.

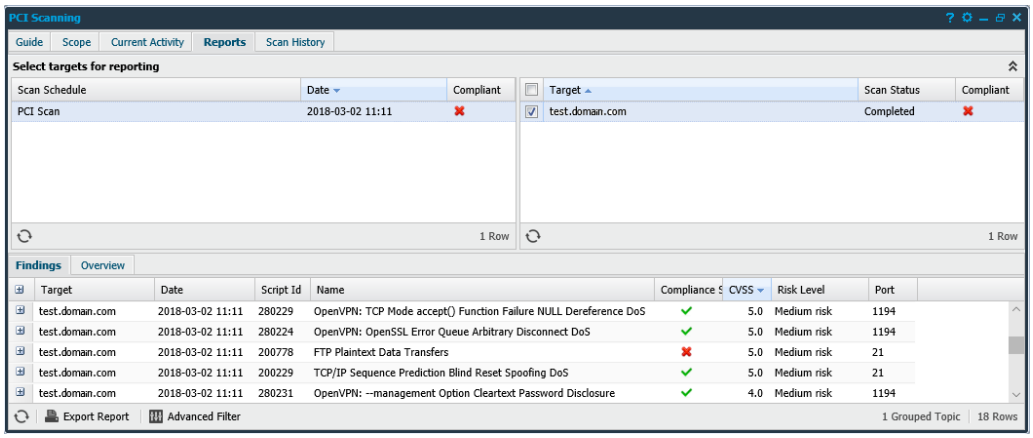
Grid Window: The grid that shows the status is configurable. Clicking on the arrow next to the name of any grid column allows you to customize what columns that will be shown out of the following:

Option	Description
Scheduled Start	The time the scan was scheduled to start at.
Schedule	The name of the schedule.
Target	The target IP.
Status	The current status.
Progress	The progress of the scan.
Scheduled End	When the scan will be terminated, unless already finished.
Service	The name of the service.

3.4 Reports

The **Reports** tab shows the results of the completed scans and consists of two parts.

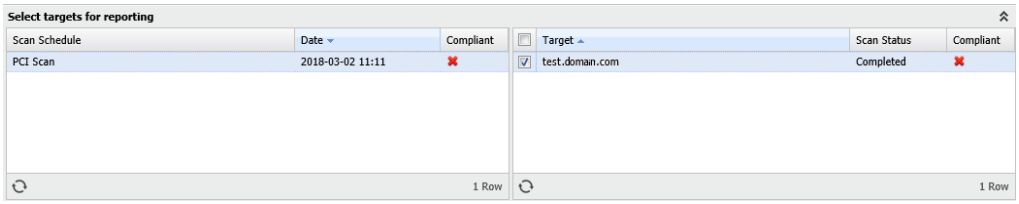
- Upper part – Listing the completed scans and targets with their results.
- Lower part – Showing the different findings for each scan and target.



3.4.1 Upper part

Consists of two fields where you can select the targets from the **Scope** tab for reporting.

- Scan Schedule
- Target



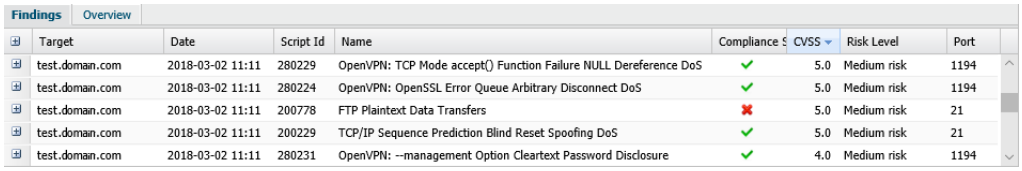
3.4.2 Lower part

Consists of two tabs

- Findings
- Overview

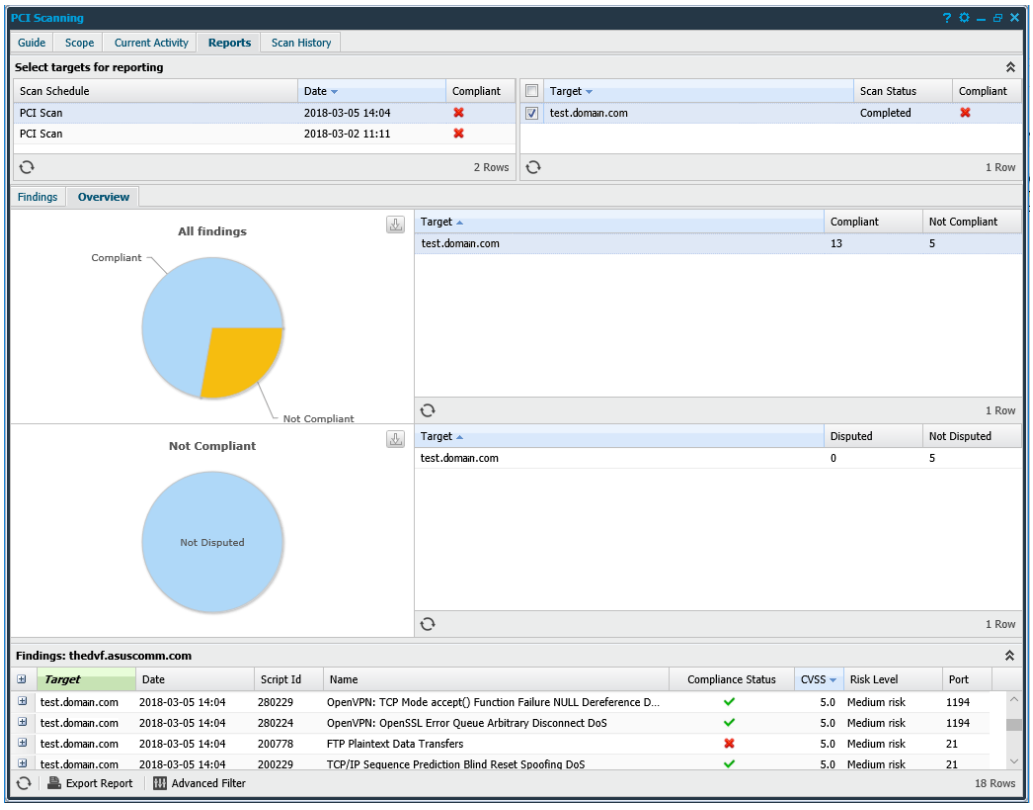
Findings tab

The **Findings** tab shows the specific findings for each target and whether it is compliant or not.



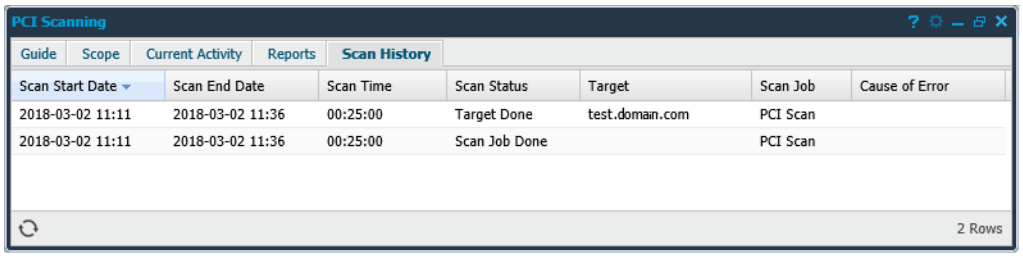
Overview tab

The overview tab provides charts together with the detailed findings. The charts can be exported as a PNG-file by clicking the download icon in the top right corner of the chart field.



3.5 Scan History

The **Scan History** tab shows all the PCI scans performed by the system.



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.

Export HTML: To export the currently visible data from the grid, right click on any entry and select Export HTML. This will give you an HTML page with data that you can save or copy data from.

Grid Window: The grid that shows the scan history is configurable. Clicking on the arrow next to the name of any grid column allows you to customize what columns that will be shown out of the following:

Option	Description
Scan start date	The time when the scan started.
Scan end date	The time when the scan finished.
Scan type	How the scan ended.
Target	This field can be a target IP, schedule name, or a discovery scan name.
Scan Job	The name of the scan job.
Scan Time	The total scan time for this job.
Cause of error	An additional information field which can show why a scan failed.

4 Performing a PCI DSS Scan

For a successful PCI DSS scan, perform the following steps.

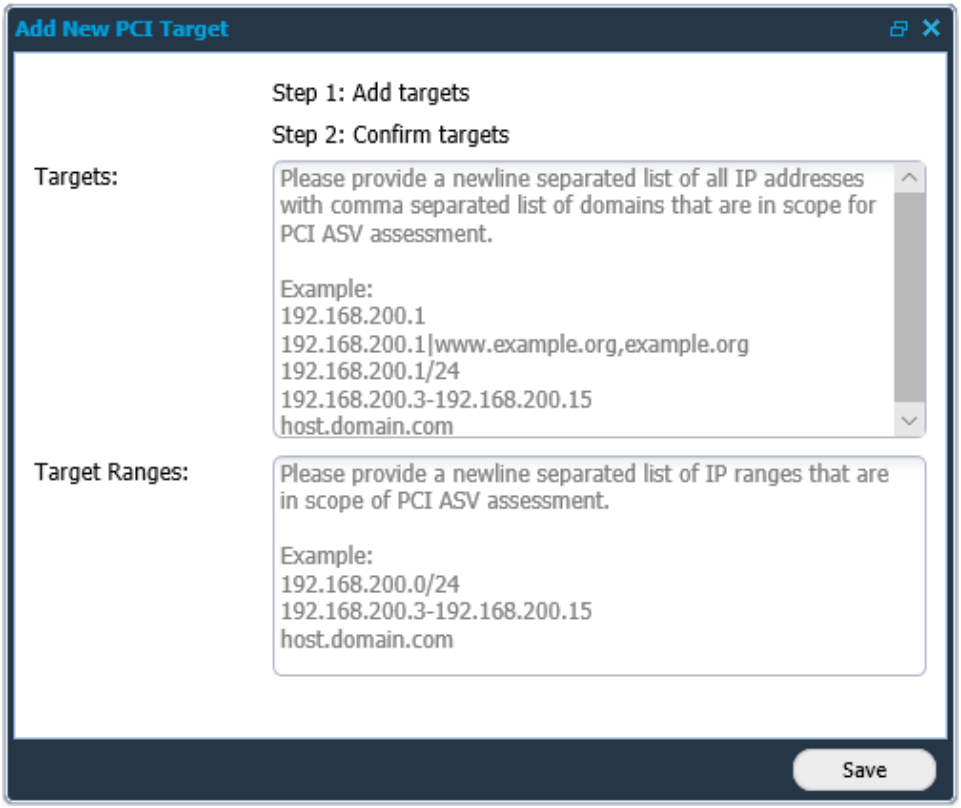
4.1 Add Targets

Caution!

Filling in IPs but not hostnames, causes VHOST lookups to fail during scanning causing SSL/TLS certificate validation errors.

---

1. Click on the **Scope** tab.
2. In the *Target* field, click **New** to open the *Add New PCI Target* window.
   ***Note**: If this is the first time the PCI scan is performed, the Add New PCI Target window opens automatically.*



3. Add known targets by IP or host-name, and their respective network range.
   This immediate initialize a port scan of the whole network range, originating from the OUTSCAN scanning range (91.216.32.0/24). This is performed in accordance with the PCI DSS requirements regarding how to define your PCI DSS scope for external scanning.

   Targets
   Provide a newline separated list of all IP addresses with comma separated list of domains that are in scope for PCI ASV assessment.

   Example:

   ```
   192.168.200.1
   192.168.200.1|www.example.org,example.org
   192.168.200.1/24
   192.168.200.3-192.168.200.15
   host.domain.com
   ```

   Target Ranges
   Provide a newline separated list of IP ranges that are in scope for PCI ASV assessment.

   Example:

   ```
   192.168.200.1/24
   192.168.200.3-192.168.200.15
   host.domain.com
   ```

4. Click **Save**.
5. Manually confirm or delete unsupplied targets from the PCI DSS scope that were detected.

   ***Note**: You are required to confirm or delete these targets from the PCI DSS scope. If you have any questions regarding if they should be included in the scope or not, refer to the Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2 April 2016 or your QSA.*
6. Once the scope of targets has been defined, Click **New** in the *Scans* field to open the **Maintaining Scan Schedule**.
7. Select a time and date when the scan should be performed and click **Save**, or click **Scan Now** to start the scan manually.

   ***Note**: The PCI DSS requires you to provide compliant reports on a quarterly basis. It is recommended to perform the scan well in advance of this date to have time to resolve any new and unexpected risks/issues.*

4.2 Report

Once the scan has finished, you receive an email notification and you can log in to see the report. The report states if you are compliant or not and this information is included in all the sections, so you can determine which issues are causing any compliance failure.

Address and resolve all vulnerabilities that are affecting the PCI DSS compliance.

Should a finding be incorrect or false positive, you can right click on the entry and select the option **Dispute**. To successfully dispute a finding, provide a full chain of evidence (when, where, and how) along with the documentation.

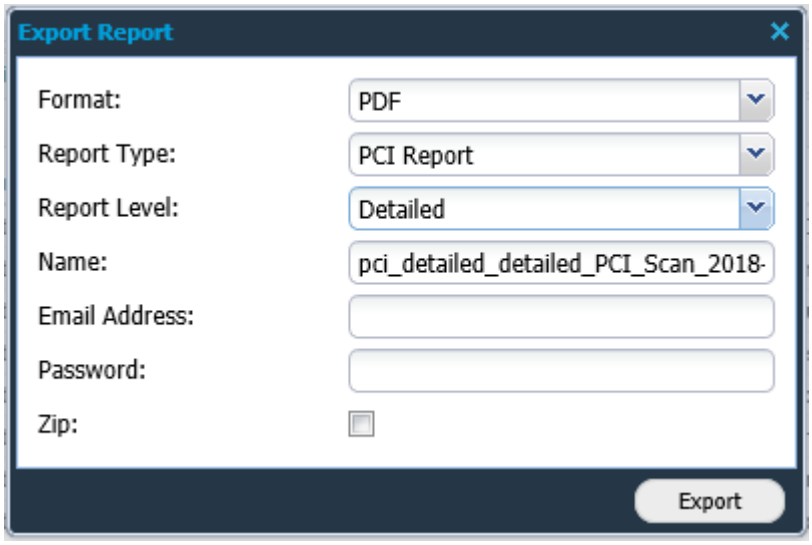
***Note**: That disputes are NOT to be submitted to the PCI SSC. Should you need help, such as what to present in the dispute, contact the Outpost24 Support.*

Any findings that cannot be re-mediated may be mitigated by having compensating controls put in place. Refer to the Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2 April 2016 (Appendix B and C) for further information regarding requirements for compensating controls.

***Note:** Some findings require a special note to be supplied where you justify the business need for the detected service. If any comments are required, you will have a dialog window open when you try to export the report. It is also possible to add the **Special Note** field to the reporting grid to determine their presence earlier, right clicking on the entry displays the option Comment special note in the context menu.*

4.2.1 Export Report

A report can be exported using the **Export Report** option visible on the bottom left of PCI Scanning window. Reports can be customized using different reporting formats, types and levels.



4.2.1.1 Format

A report can be exported in the most commonly and widely used document formats. The available reporting formats are as follows:

- **PDF:** This is the most commonly used reporting format. The reports generated in PDF format can be password protected.
- **Excel:** The reports generated using excel format, have a lot of tabular information, which can be useful when reporting information to IT/Security department or similar divisions.
- **XML:** This format is the default industry standard used for data exchange and integration. The reports generated in XML format are typically used for integration and automation.

4.2.1.2 Report Type

There are several report types, depending on the setup and license not all of them will be visible. Based on the type of scan and the type of information, select the corresponding report type.

- PCI Report
- Vulnerability
- Group Vulnerability
- Web App Discovery

4.2.1.3 Report Level

The report level helps you manage reports based on management hierarchy. It helps you generate the correct report based on how much information is needed and in which form. It can be observed that the information varies in the figures above, thus making each report exclusive depending on its functionality and audience.
There are three reporting levels:

- Detailed
- Summary
- Management

Detailed

The detailed report is the largest report that can be generated. It has in depth technical information about findings, targets, risk-levels, CVSS, report and additional information about the finding. As an example, the figure above displays the first page of a vulnerability report with level set to detailed. The report contains six chapters and has detailed information about all the vulnerabilities and targets. This report is mostly directed towards system administrators and security consultants in an organization.

Summary

The summary report is the ideal sized report with report information, executive summary and target summary. This report provides just about the right information required by the IT department of any organization.

Management

The management level report gives us a summary of the vulnerabilities and risks reported. It gives a good graphical overview of findings, risks and top solutions. This report is ideal while reporting to higher management.

4.2.1.4 Other Information

Name

You should provide the name of the report in this section. If you do not provide any specific name, it creates a name as per the selected options.

Email Address

If you wish to send the report via email instead of downloading, supply the email address in this field.

Password

If you want the report to be password protected, you can enter a password here.

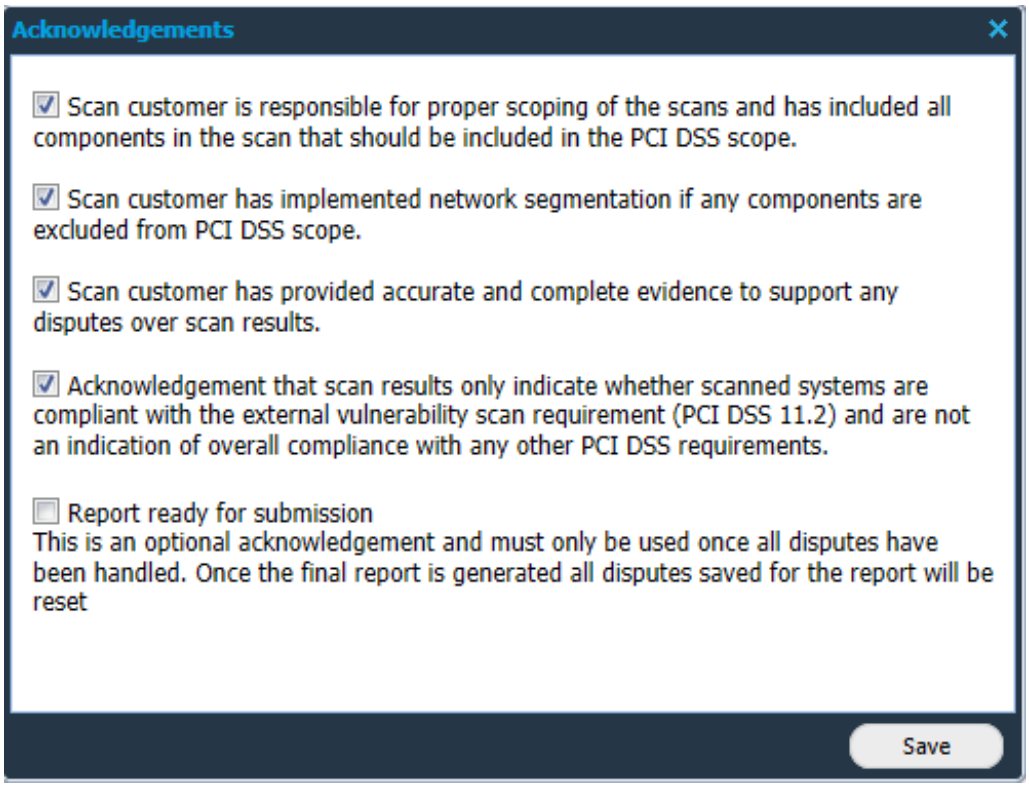
Include Attachments (Zip)

If ticked, the exported report will be compressed with zip compression as standard.

4.2.1.5 Acknowledgements

After clicking Export, the Acknowledgement window is displayed. Tick the boxes that apply and click save to complete the export.

***Note**: that the four first tick boxes need to be ticked before saving and committing the export.*



5 Glossary

Abbreviation	Description
ASV	Approved Scanning Vendor
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DSS	Data Security Standard
PCI	Payment Card Industry
QSA	Qualified Security Assessor

6 References

1) *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2 April 2016*