Outpost24

Vulnerability Management made easy

Reporting Tools

Quick Start Guide

Last update:
9 February 2017

Table of Contents

About This Guide

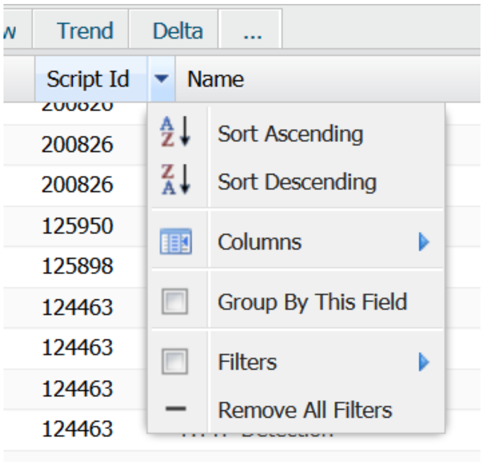
1. Executive Summary

This document is meant to provide users a comprehensive overview of the Reporting Tools Section in 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 notice.
Reproduction of any part of the document without prior permission is strictly prohibited.

2. Reporting Tools Graphical User Interface

The Graphical User Interface for Reporting Tools consists of several grids, each created for building specific, informational and customized reports.



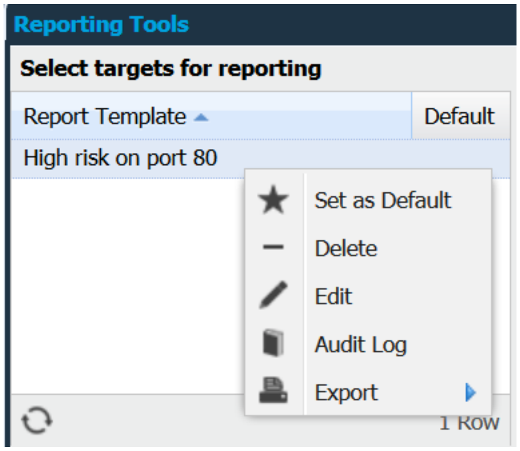
In each grid you will see different columns. To enable or disable a column you click the arrow next to the name of the column. In this dropdown menu there is a field called *Columns* which displays all of the columns available. Most of these columns allow filtering, which gives you the option to display a subsection of all data available. Enabling filtering is done by opening the same dropdown menu as for columns and then access *Filters*.

Depending on the existing kind of data within the column which you attempt to filter, you will be presented with various options:

- Textual – Displays three text fields. It is possible to use all three at once to limit your results, but you can also use quotes to match an entire phrase
  - All – Displays records that contain all of 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
- Date – Displays four options;
  - Before – Filter to display all entries before the provided date
  - After – Filter to display all entries after the provided date
  - On – Filter to display all entries on the provided date
  - Today – Display all entries from today
- Values – If the field only contains a small set of values, they will be listed in the filtering menu. Select those that you wish to include
- Number – Include and/or exclude entries dependent on numbers
  - < - Filter entries on values lesser of 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
- Yes/No – Choose to filter on either “Yes” or “No”

2.1. Report Template Grid

The Report Template grid is used to filter your targets by defined templates and is only visible if there are already templates created.



Reporting Tools

Select targets for reporting

Report Template ▲	Default
High risk on port 80	

A template is a saved setup which includes targets, target groups, scan schedules, filters, grouping and columns. This setup will be applied to the findings tab when a template is selected. A template can also be marked as default which means that it will be applied by default when the reporting section is opened.
Changing the default status of a template is made by right clicking the entry and select *Set as Default* or *Clear Default*.
Creating a report template is done by right clicking any finding in the finding grid after that you have filtered on desired columns and thereafter chosen *Save Report Template*.

2.2. Scan Schedule Grid

The Scan Schedule grid allows you to select and display a specific Scan Schedule that has been executed. If scan schedules has been executed multiple times these are listed within the Scan Schedule grid, allowing you to choose the specific scan which you want to display. To deselect a scan schedule, click the selected entry again.
The Scan Schedule grid is configurable and includes the following columns:

- Scan Schedule – The name of the scan schedule that was executed
- Scan Policy – The name of the scan policy that was used for that scan
- Date – The time and date that the scan started
- Last Update – Last time this report was updated using the SLS feature

2.3. Target Group Grid

The Target Group grid allows you to select the target group for which you wish to display found vulnerabilities within the Findings Tab. You can select multiple target groups by holding Shift and Ctrl while clicking in the target group tree.
It is possible to filter target groups based on names. Enter parts of the name that you wish to use in the search field below the grid. The tree will be filtered to only show target groups that have names which are matching the entered string.
Right clicking a Target Group will give you the option to choose *Scan*, which creates a Scan Schedule for those targets. This will be visible under Scan Scheduling.
The Target Group grid is configurable and has the following columns:

- **Target Group** – Displays all currently existing target groups
- **Targets** – Displays the number of targets in each target group

2.4. Target Grid

The Target grid lets you determine which targets you want to include in your report. In order to display any results at all, at least one target must be selected.

By right clicking a target in the target grid you can choose between the following actions:

- **Delete Report** – This will delete the entire report, even if you have filtered the report based on some criteria. This deletion is permanent and specific user role privileges are required to execute
- **Export** – Exports currently visible data as HTML or CSV
- **Update Scan Results** – HIAB only. Execute a Scanning less scan (SLS) against the targets selected
- **Scan** – Outscan only. Start a scan against the selected targets in the Target Grid. **Note:** Only available if the “Force target groups in schedule” option is disabled. This is available in the reporting grid under the cogwheel in the upper right corner.
- **Grant Support** – Outscan only. This option will allow you to define a time window during which the support team are able to view your report. Please note that no alert will be sent to the team so you will have to notify them once you’ve performed this task.

The Target grid is configurable and includes the following columns:

- **High Risk** – The number of high risks detected on the specific target
- **Host Name** – Host name of the target
- **Instance ID** – The AWS instance ID of the target
- **Low Risk** – Number of low risks detected on the specific target
- **Medium Risk** – Number of medium risks detected on the specific target
- **NetBIOS** – HIAB only. The NetBIOS name of the target
- **Platform** – Detected platform of the target
- **Scan Status** – Displays how the scan ended. In order to find any vulnerabilities the scan status should state Complete
- **Scanner** – HIAB only. Which scanner the scan was executed on. Only visible if at least one scanner is already registered
- **Status** – Shows if target were live or not reachable during the scan
- **Target** – IP address of the target

2.5. Findings Tab

The Findings Tab lists all findings found based on what you have selected within the Remote Template Grid, Scan Schedule Grid, Target Group Grid and/or Target Grid.

When right clicking a finding in the findings grid you will have the following options:

- **Mark As False Positive** – Marks this finding as a false positive. You can send additional information to the Technical Service Team if you select to inform us about the problem. This information will be use to further improve the vulnerability database. To unmark an entry as a false positive, select *Unmark as False Positive*. A finding marked as a false positive will still be listed in your results but in exported reports it will be marked as a false positive
- **Request Clarification** – Request clarification from the Technical Service Team regarding the finding
- **Assign Ticket** – Assign a ticket to this finding. You will be able to set the priority, with P5 being the highest priority, include a due date, add an assignee, and also supply additional comments
- **Verify** – Starts a verification scan that checks if the finding is still existing on the target
- **Add Comment** - Allows you to add a comment to the vulnerability which will be included in all findings of this specific vulnerability. The "show comment on future findings" option adds the comment to the vulnerability database. This will make it visible in future reports
- **Accept Risk** - This allows you to set a number of days that you accept the risk of this vulnerability. The accepted risks will show up in the finding information and in the exported reports. You can set it to allow the risk up to forever and you can also add a comment explaining why it has been accepted. Select the *For all targets* option to accept the risk of this vulnerability for all your targets. If this finding is still present during your next scan it will automatically get the same acceptance setting as it did last time
- **Change Risk** – Modify the risk level for the specific finding or vulnerability. Once selected, a window is displayed which allows you to select the risk level in a dropdown menu. Any updated risk levels will be displayed in italic font
- **Save Report Template** – Save current setup as a report template
- **Create Dynamic Group** – Create a dynamic group based on scan results. The currently applied filtering is used and any target in the latest scan that has findings matching these filters will be included in the group. When a new scan finishes for a target the group will be updated based on the previously set dynamic group rules
- **Export** – Export currently visible data from the grid to either HTML or CSV format

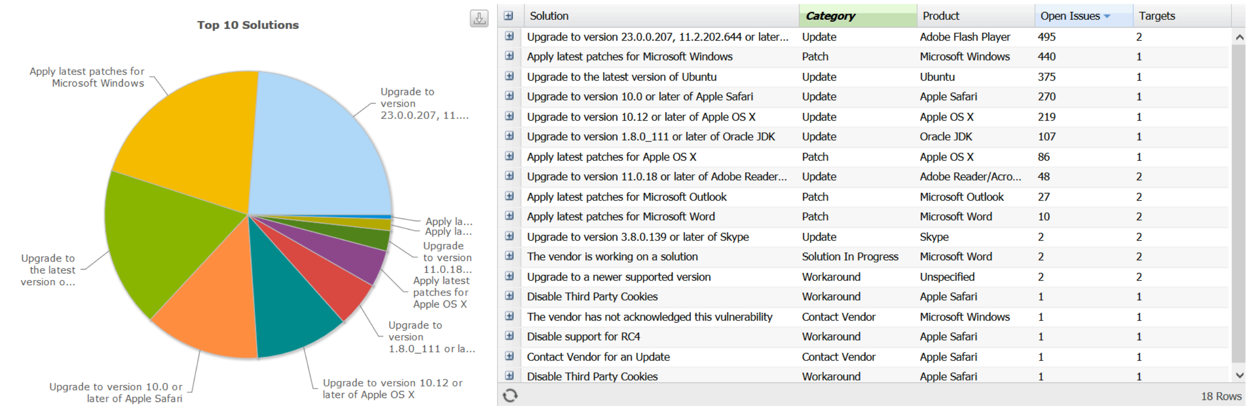
The findings tab is configurable and these options are available:

- **Accept Date** – Date when the risk were marked as accepted
- **Acceptance Expires** - The date when the risk will not be considered accepted anymore
- **Accepted –** Displays if the risk is accepted or not
- **Accepted By** – Informs you of which user it was that accepted the risk
- **Added –** Flags if this entry was added after the time of the scan
- **Age (Days)** - How old the vulnerability is
- **ARN** – Only available if AWS has been enabled. The AWS ARN for the target
- **Bugtraq –** Bugtraq ID of the vulnerability

- CVE – CVE entry of the vulnerability
- CVSS – CVSS score of the vulnerability
- Date – The date of when the vulnerability was found
- Date Added – The date of when the specific entry was added
- Exploit Available – Determines if the detected vulnerability is exploitable
- False Positive – Shows if the vulnerability has been marked as a false positive
- Family – The name of the family which the vulnerability belongs to
- First Seen – When the vulnerability was first discovered on the specific target
- Has FP Comment – Flags if the finding has a false positive comment
- Host Name – The configured host name for the target
- ID – Outscan only. Serial number for the entry in the database
- Instance ID – Only available if AWS has been enabled. The AWS instance ID of the target
- Last Seen – When the vulnerability was last seen
- Name – Name of the vulnerability
- NetBIOS – HIAB only. The NetBIOS name of the target
- New – Flags if the vulnerability is new and has not been found in previous scans
- Platform – Detected platform of the target
- Port – Displays on which port the vulnerability was found
- Potential – Flags if this finding has been marked as a potential false positive by the system
- Previously detected – Shows if this vulnerability was detected in previous scan
- Product – Shows the vulnerable product
- Protocol – What protocol is used (ICMP, IGMP, TCP, UDP)
- Risk Level – Displays the risk level of the vulnerability (High, Medium, Low, Informational)
- Scanner – HIAB Only. Which scanner the scan was executed on
- Script ID – ID of the script which detected the vulnerability
- Service – Which service that was found on the port
- Target – IP address of the target
- Ticket Assignee – Name of the assigned ticket holder
- Type – Displays the type of the finding (Port, Information, Vulnerability)
- Verified – Shows if the vulnerability has been verified
- Virtual Hosts – The virtual hosts for which the vulnerability has been reported
- Vulnerability Type – Displays what kind of vulnerability the finding is

2.6. Solutions Tab

The Solutions tab provides a graphical overview of the top 10 solutions for the vulnerabilities listed in the Findings Tab. The information presented can be of aid when an organization is to identify solutions that resolves multiple vulnerabilities and thus it will aid in the matter of planning and prioritizing tasks.


Top 10 Solutions
Apply latest patches for Microsoft Windows
Upgrade to version 23.0.0.207, 11....
Apply la...
Apply la...
Upgrade to version 11.0.18...
Apply latest patches for Apple OS X
Upgrade to version 1.8.0_111 or la...
Upgrade to version 10.12 or later of Apple OS X
Upgrade to version 10.0 or later of Apple Safari
Upgrade to the latest version o...

Solution	Category	Product	Open Issues	Targets
Upgrade to version 23.0.0.207, 11.2.202.644 or later...	Update	Adobe Flash Player	495	2
Apply latest patches for Microsoft Windows	Patch	Microsoft Windows	440	1
Upgrade to the latest version of Ubuntu	Update	Ubuntu	375	1
Upgrade to version 10.0 or later of Apple Safari	Update	Apple Safari	270	1
Upgrade to version 10.12 or later of Apple OS X	Update	Apple OS X	219	1
Upgrade to version 1.8.0_111 or later of Oracle JDK	Update	Oracle JDK	107	1
Apply latest patches for Apple OS X	Patch	Apple OS X	86	1
Upgrade to version 11.0.18 or later of Adobe Reader...	Update	Adobe Reader/Acro...	48	2
Apply latest patches for Microsoft Outlook	Patch	Microsoft Outlook	27	2
Apply latest patches for Microsoft Word	Patch	Microsoft Word	10	2
Upgrade to version 3.8.0.139 or later of Skype	Update	Skype	2	2
The vendor is working on a solution	Solution In Progress	Microsoft Word	2	2
Upgrade to a newer supported version	Workaround	Unspecified	2	2
Disable Third Party Cookies	Workaround	Apple Safari	1	1
The vendor has not acknowledged this vulnerability	Contact Vendor	Microsoft Windows	1	1
Disable support for RC4	Workaround	Apple Safari	1	1
Contact Vendor for an Update	Contact Vendor	Apple Safari	1	1
Disable Third Party Cookies	Workaround	Apple Safari	1	1

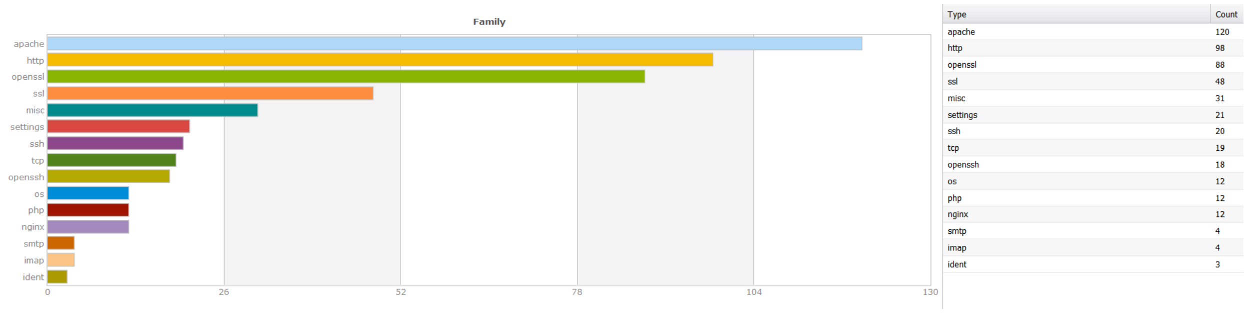
18 Rows

The solutions grid is configurable and includes the following columns:

- **Category** – Describes the type of the solution
- **High Risk** – Number of vulnerabilities identified as high risk
- **Medium Risk** – Number of vulnerabilities identified as medium risk
- **Low Risk** – Number of vulnerabilities identified as low risk
- **Open Issues** – Number of issues that can be resolved by applying the given solution
- **Product** – Displays the product to which the solution is applicable
- **Solution** – Indicates if there is an existing solution to the identified vulnerability
- **Targets** – Number of targets affected

2.7. Overview Tab

The Overview tab displays graphs using the vulnerability information from your report.



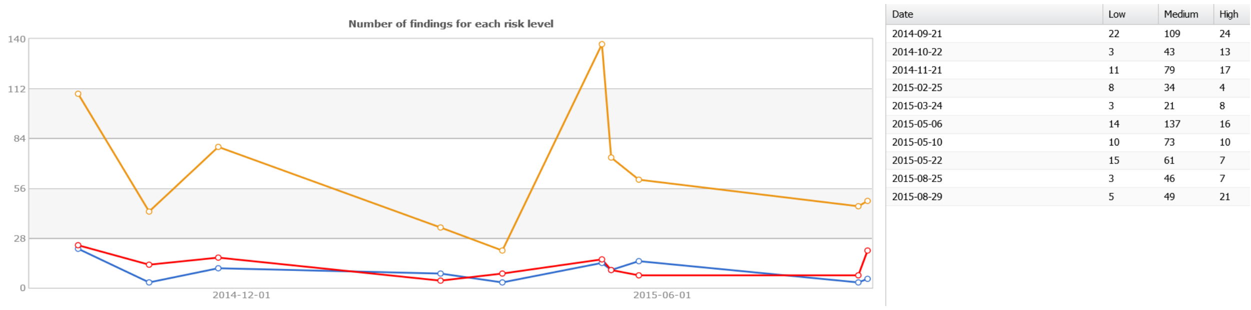
Type	Count
apache	120
http	98
openssl	88
ssl	48
misc	31
settings	21
ssh	20
tcp	19
openssh	18
os	12
php	12
nginx	12
smtp	4
imap	4
ident	3

The different graphs are:

- **Family vs. Count** – Number of findings in each script family
- **Port vs. Count** – Number of findings on each port
- **Risk vs. Count** – Number of findings at High, Medium and Low risk levels
- **Accepted Risk vs. Count** – Number of findings marked as accepted risks at High, Medium and Low risk levels

2.8. Trend Tab

The Trend tab displays the vulnerability evolution for a target over time. It is possible to select different time spans to be presented.



Date	Low	Medium	High
2014-09-21	22	109	24
2014-10-22	3	43	13
2014-11-21	11	79	17
2015-02-25	8	34	4
2015-03-24	3	21	8
2015-05-06	14	137	16
2015-05-10	10	73	10
2015-05-22	15	61	7
2015-08-25	3	46	7
2015-08-29	5	49	21

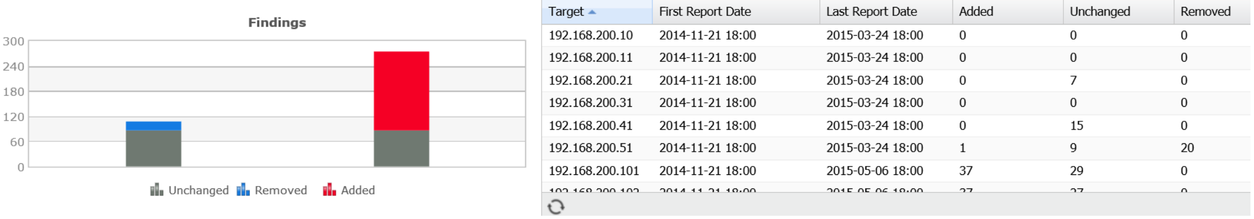
The graphs available are:

- **Number of findings for each risk level** – Displays a graph of the total number of findings at each risk level during the selected time span
- **Number of accepted risks for each risk level** – Displays a graph of the total number of accepted risks at each risk level during the selected time span
- **Delta findings for all targets** – Displays a graph of the total number of delta findings for all targets during the selected time span
- **Delta port trends for all targets** – Displays a graph of the total number of delta port trends for all targets during the selected time span

2.9. Delta Tab

The Delta tab contains two graphs:

- **Findings** – Displays the number of added and removed vulnerabilities for a target during a chosen period of time
- **Ports** – Displays delta information regarding opened, closed and unchanged ports



Target ▲	First Report Date	Last Report Date	Added	Unchanged	Removed
192.168.200.10	2014-11-21 18:00	2015-03-24 18:00	0	0	0
192.168.200.11	2014-11-21 18:00	2015-03-24 18:00	0	0	0
192.168.200.21	2014-11-21 18:00	2015-03-24 18:00	0	7	0
192.168.200.31	2014-11-21 18:00	2015-03-24 18:00	0	0	0
192.168.200.41	2014-11-21 18:00	2015-03-24 18:00	0	15	0
192.168.200.51	2014-11-21 18:00	2015-03-24 18:00	1	9	20
192.168.200.101	2014-11-21 18:00	2015-05-06 18:00	37	29	0
192.168.200.102	2014-11-21 18:00	2015-05-06 18:00	37	27	0

By clicking in the graph you can display the actual findings that the section correlates to. Once these are displayed you can perform the common functions of those findings.
It is possible to select different time spans to be presented.

2.10. Scheduling Tab

The Scheduling tab gives you the opportunity to schedule reports to be sent out based on either a target selection or by a report template.
Clicking *New* will open *Maintaining Report Schedule* which will present you with the following options:

- **Name** – Name of the scheduled report

- **Next Report** – What date and time this report will be sent to the recipient
- **Report Frequency** – How often the report if scheduled
- **Report Type** – Define the report type
- **Report Level** – Define how detailed the report should be
- **Include Information** – Define what kind of information that is to be included in the report
- **Send reports without vulnerabilities** – Checkbox used for selecting to send the report with or without vulnerabilities
- **Include report in PDF format –** Attach the report as PDF
- **Include report in XLS format –** Attach the report as XLS
- **Include report in XML format –** Attach the report as XML
- **Password** – Enter a password if you wish to export the report password protected
- **Recipient** – Choose what user is to receive the report. Custom is only available if you have super user privileges
- **E-mail PGP Public Key** – If desired, add a PGP Public Key to be used when emailing the report
- **Subject** – Custom subject for email
- **Add text:** - Customer text which will be included in the email
- **Report Template Grid** – Choose which Report Template you wish to use
- **Target Groups Grid** – Choose which Target Group you wish to include in the report
- **Scan Schedules** – Choose which Scan Schedules you want to include in the report
- **Target List** – Enter specific targets you wish to include in the report

Removing a scheduled report is done by selecting the scheduled report and click *Delete*. If you wish to send a report immediately, select the scheduled report and click *Send Now*.

2.11. Text Tab

The text tab allows you to customize the exported reports.
Clicking *New* will open *Maintaining Report Text* which will present you with the following options:

- **Report Section** – Choose if you wish to add pages at the beginning or the end
- **Report Type** – For what types of reports you want to apply this
- **Report Level** – For what type of report level you want to apply this
- **Report Template** – Name of template for which this custom text is applicable for
- **Sorting** – Define the order for this page
- **Headline** – Title of the page
- **Text** – Type the text that you wish to include in the report. You may use the following tags to format the text:
    - **[B:[Bold]]**
    - [U:[Underlined]]
    - *[I:[Italic]]*

The grid shows the custom texts that has been configured. There are several columns to choose:

- **Headline** – The title of the page added
- **Report Template** – If the report template is verified or not
- **Report Type** – Which report types that the custom text should be included in
- **Location** – Where in the report it should be placed, first or last
- **Sorting** – If several custom texts are to be placed at the same location, the sorting value will determine in what order they will appear

Delete will remove the selected entry.

2.12. Settings

Pressing the settings icon in the upper right corner on the window toolbar will give you access to the following report configurations:

- **Company Name** – Change the company name that is displayed in the report
- **Header** – Add additional text to the PDF report header
- **Footer** – Add additional text to the PDF report footer
- **Password** – Password protect exported PDF and Excel reports
- **Remediation risk age (days)** – Sets the remediation risk age. This will be displayed as a graph in Group Summary, Solution and Trend reports. This graph pictures vulnerabilities with remediation age older than the entered days
- **Treat port as vulnerability** – Checkbox for treating port as a vulnerability
- **Logo** – Change the logo displayed in the report, accepted formats are either GIF or PNG
- **FTP Settings** – HIAB only. Defining a server here will enable the option to send the report via FTP instead of e-mail in the Scheduling tab
- **SCP Settings** – HIAB only. Defining a server here will enable the option to send the report via SCP instead of e-mail in the Scheduling tab
- **CIFS Settings** – HIAB only. Defining a server here will enable the option to send the report via CIFS instead of e-mail in the Scheduling tab
- **NFS Settings** – HIAB only. Defining a server here will enable the option to send the report via NFS instead of e-mail in the Scheduling tab

3. Technical Support

Contact our 24/7 support team by e-mail or telephone:

E-mail support@outpost24.com

Tel (from the UK): +44 20 7193 8140
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