Trustwave®
Smart security on demand

TRUSTWAVE VULNERABILITY MANAGEMENT USER GUIDE

Table of Contents

Introducing Trustwave Vulnerability Management

Trustwave Vulnerability Management (TVM) is a network vulnerability scanning product.

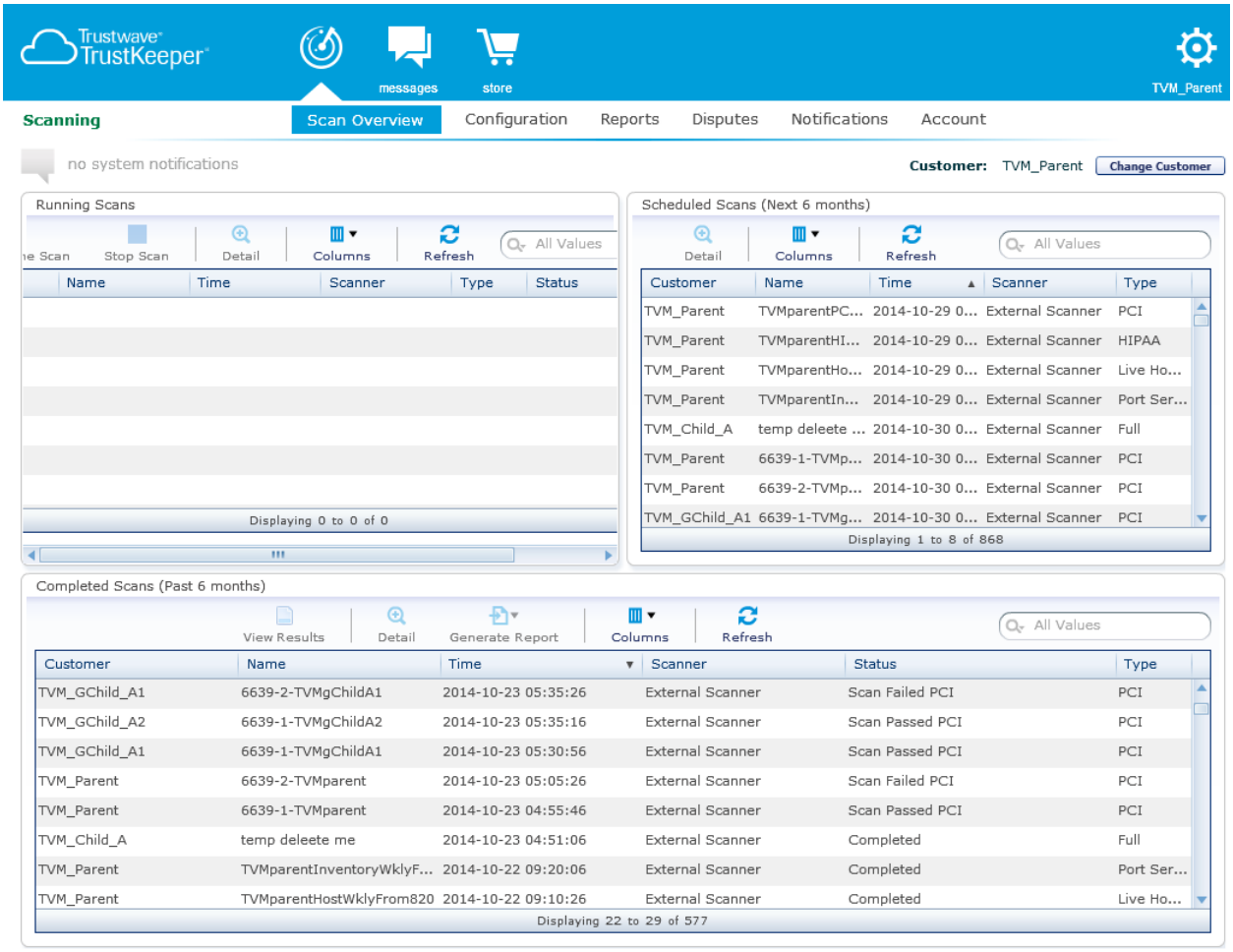
You can use TVM to

- Schedule a variety of network scans (including Live Host Discovery, Port Service Fingerprinting, PCI, or Full scans)
- Perform internal or external vulnerability scans
- Choose “blackout” dates and times when scanning will not be performed
- Review the scan results
- Dispute PCI scan findings
    - Renew disputes with every recurring scan
    - Extend dispute expiration dates
- Manage Scan and Dispute Notifications
- Maintain an asset list
- Compare scan results from month to month
- Create reports of scans and findings
- Manage scans and findings for an enterprise with parent and child companies (choose to manage items for the entire enterprise or a sub-group). *(This function is in Beta test and is not available unless enabled for a customer by Trustwave.)*

1 Logging In and Accessing Scans

To access the TVM interface, log in at https://login.trustwave.com

Select the scans icon to see the **Scan Overview** as shown below. This is the default view of TVM. The screen shows lists of running scans, scheduled scans (all instances within the next 6 months), and completed scans run within the past 6 months.



Tip: In the Running Scans pane, hover over the Status to see the progress of the scan. Refresh the pane to update the status.

For each list on this screen, you can:

- See additional items (if any) using the scrollbar at the right.
- Click a column heading to sort by that column.

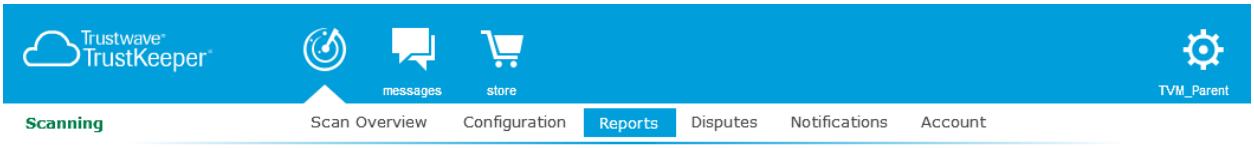
- Filter the list by text in any column, using the search box at the top of the pane. Click the icon to filter on text in a single column.
- Select a row in the list and use the buttons at the top of the list to take action:
    - View details of the scan
    - Stop or pause/resume a running scan
    - View detailed results of a completed scan
    - Generate a report of a completed scan (for scan types that support generation of reports)

Tip: You can expand any of the lists to a full screen view. To expand a list, hover over the pane that contains the list. A “Maximize” icon displays at the top right of the pane. Click this icon to expand the list pane. To return to the default view, click the “Restore” icon on the maximized pane.

1.1 Portal Navigation and Utility Functions

1.1.1 Navigation

To access the functions included in TVM, use the breadcrumb menu below the icons.



Tip: Click the arrow at the right of the list (if it is present) to access additional items.

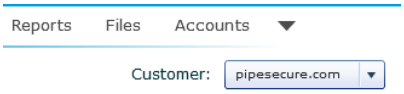
When you are viewing a specific item such as a report, the menu shows a sub-item with an arrow: 

1.1.2 Notifications

Messages from the Portal system display at the top left (immediately below the menu). To see a list of notifications, click .

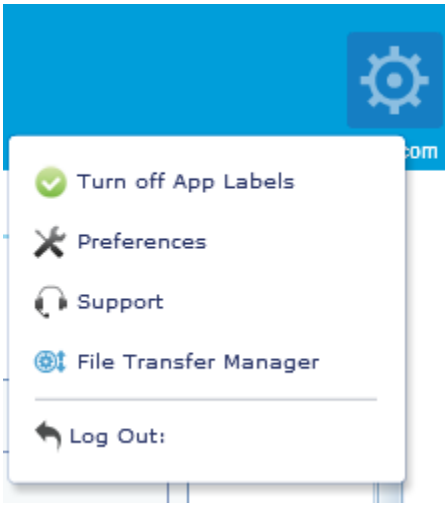
1.1.3 Company Selection

If your login is connected to more than one company, you can view information for each company by using the menu at the top right of each screen as shown below. This selection affects the Dashboard, support request, reports, and all other features of the Managed Security section.



1.1.4 Utility Functions

The gear icon at the top right of the page gives access to utility functions. Click this icon to log out, change your password or contact information, or get support information about your session.



1.1.4.1 Preferences

Use this option to:

- Add **contact information**. This information will be visible to other users if they have permission.
- Add or change **security information** (change your password and set security questions).

1.1.4.2 Support

Use this option to see support contact information, and to find customer and session details that can be useful for Portal support calls.

1.1.4.3 File Transfer Manager

Use this option to view the status of file downloads from the Portal (and uploads to the Portal Files section where supported). Transfers in progress are also indicated by an icon at the top right near the gear icon, and completed transfers are reported in the notifications.

Note: The Portal uses its own secure download feature, and does not use the download feature built in to web browsers.

1.1.4.4 Log Out

Use this option to end your Portal session. **Trustwave recommends** you *always log out* when you are finished with the Portal (do not just close your browser window or navigate away from the page).

1.1.5 Column and Export Options

Some screens include a “gear” menu. This menu may be available above the list  or at the left of the list header row  . You can use this menu to choose columns in a list, to copy data to the clipboard, or to export data in file formats.

Shortcuts to these functions may also be available as “action bar” icons above the list.

1.1.5.1 Column Chooser

Click the gear and then select **Choose Columns** (or see the Columns section of the context menu).

On the Choose Columns window:

- Check the columns you want to show.
- If a choice **Show All** is available, check it to display all available columns.
- If required, click **OK** to apply your selection.
- Alternatively, use the column chooser menu above a list  to select from available columns. Check or uncheck boxes to change the displayed columns.

1.1.5.2 Clipboard Tool

Click the gear and then select **Copy Page to Clipboard**. Or, use the clipboard menu  .

Choose CSV or HTML format (or select **Export > Copy as CSV** or **Export > Copy as HTML** from the context menu).

- **CSV** (Comma Separated Value) exports data in a format suitable for pasting to a spreadsheet or other table.
- **HTML** exports data in a format suitable for pasting to a word processing document or web page.

1.1.5.3 Data Export

Click the gear and then click **Export** (or see the Export section of the context menu).

On the Export Grid Data window:

- Choose a format. Available formats include:
    - Excel
    - CSV (For use with a spreadsheet or database).
    - PDF (Best for immediate presentation, but consumes more resources to generate).
    - HTML (For use with web pages or word processing).
    - XML (For import to other tools that understand this format).
- Choose the columns you want to export.
- Choose whether to include a header row that gives the column names (does not apply to XML output).

- Click **Export** to select a download location and begin generation.

1.1.6 Data refresh

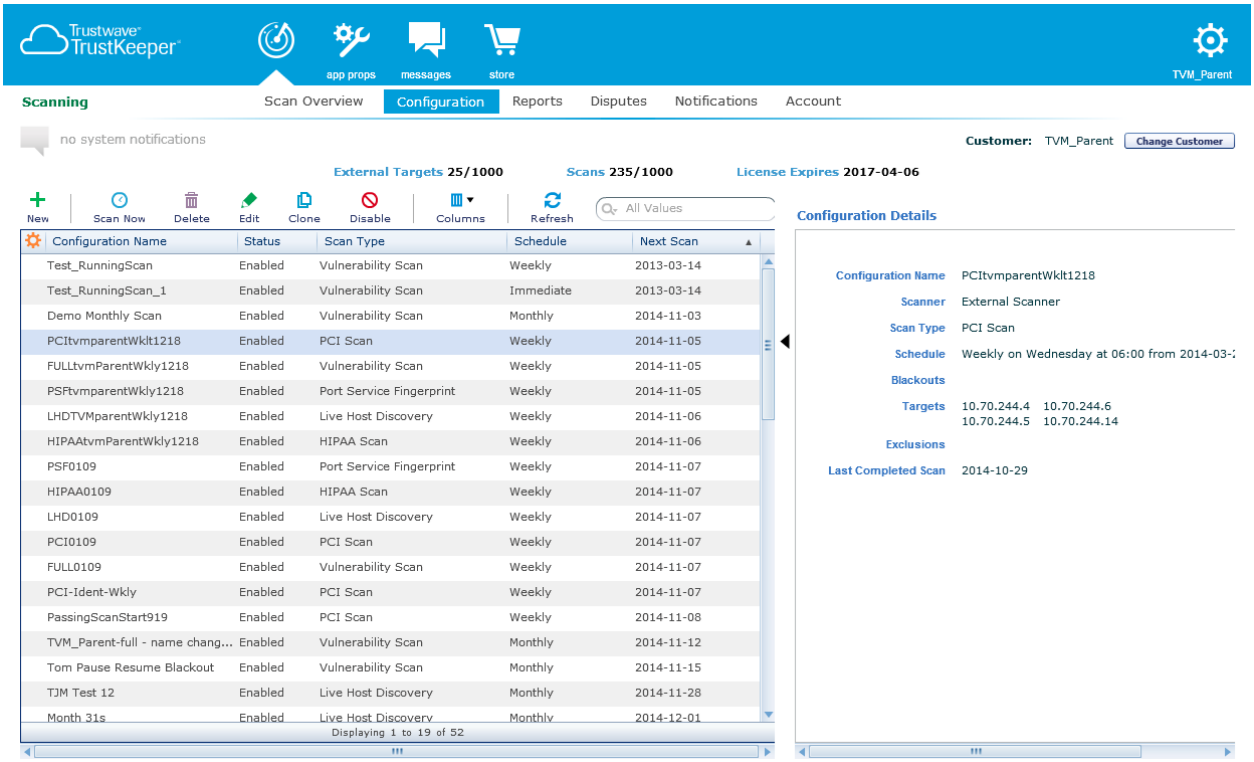
Use the refresh button  or  to check for new data on any screen or list.

1.1.7 Action Bar

From the  context menu of a list, you can choose to display links to list options above the list. By default the action bar shows icons (*Compact*). You can choose to hide it (*Hidden*), or to include text with the icons (*Visual*).

2 Scan Configuration

Click **Configuration** in the main navigation to see all the existing scan profiles as shown below.



This screen provides a list of configured scans. For each scan profile, the next scan time displays. The screen also shows licensing information at the top.

- Select a row in the list to see more information about the scan in the right pane.
- Use the icons above the list to take action on the selected scan:
    - **Scan Now** to start the scan immediately, even if it is disabled.
    - **Delete** the scan.
    - **Edit** the scan properties. See Section 3 for a description of available options.
    - **Clone** the scan (create a new scan with the same properties). The cloned scan will be created disabled. You can edit the clone, make any required changes, and enable it.
    - **Disable** or **Enable** the scan (depending on the scan status). A disabled scan remains in the list, but it will never be started automatically even if it is scheduled.
- Click **New** to create a new scan.

- You can scroll through the list, or use the filter control above the list, to find specific scans. You can sort the list on the values in any column by clicking the column header.

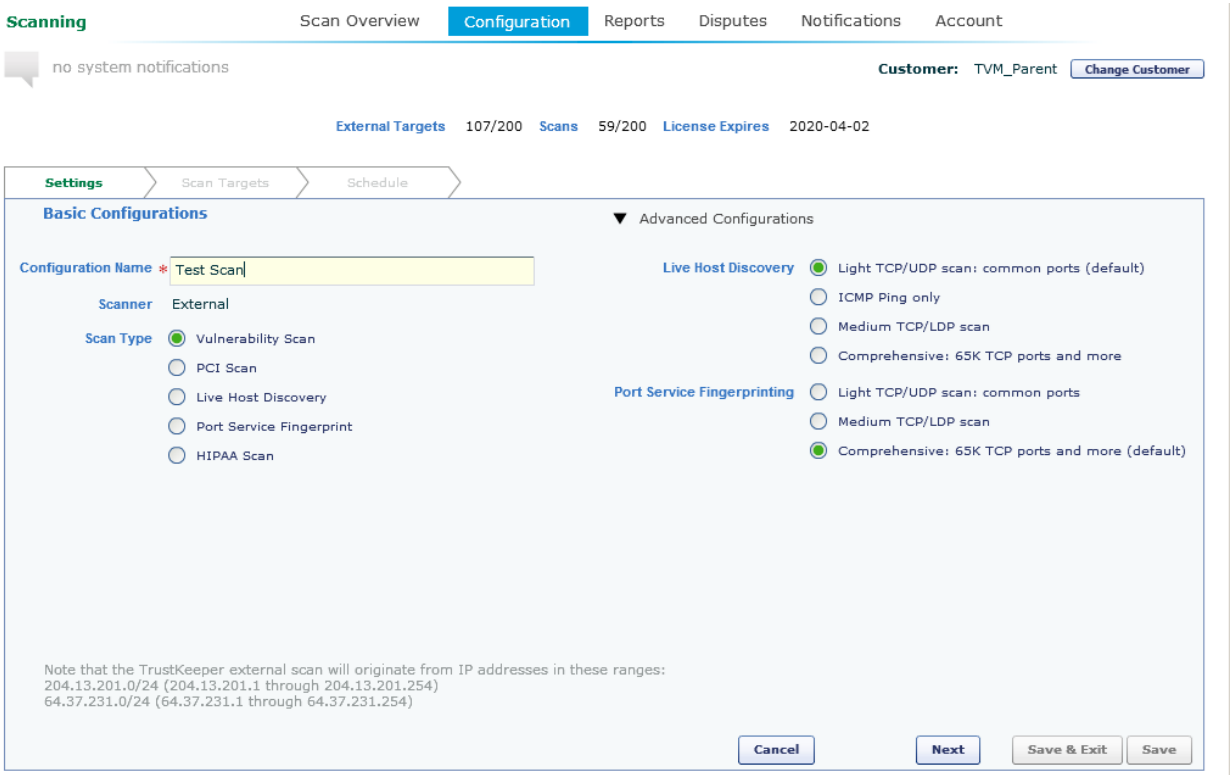
3 Creating and Editing Scans

To create a new scan (one-time or series), on the Configuration page, click **New** + at the top left. Review or complete information on the next three panes. The system provides default values where possible.

Tip: To return to the Configuration page, click **Cancel** at the bottom of the pane. You cannot exit the configuration editor by clicking items in the main site menu.

3.1 Scan Settings

On the **Settings** pane, complete the name, scanner, and scan type.



- If you have one or more internal scanners you can select them; otherwise you can only use the External Scanner option.

Choose from the following scan types:

- **Vulnerability Scan**: This scan executes all tools and tests against the target network. This type of scan cannot be used as the PCI Compliance Affecting scan. It could be used in to show fixed or updated findings within a PCI Report on Compliance (RoC).

    - *Optional:* Choose **Advanced Configurations** to change the default port scanning options (see Table 1 for details of the options). Select the arrow or text to expand this section.

- **PCI Scan**: This scan type is used to confirm PCI compliance. With this type of scan, you cannot change the settings for Live Host Discovery or Port Service Fingerprinting, as these are specified by the PCI SSC. If you also use Trustwave's PCI Manager, you can choose whether the scan is a PCI compliance affecting scan.
    - Specify whether you have a load balancer and whether all the servers behind the load balancer are identically configured or not.
- **Live Host Discovery**: A lightweight scan designed to identify live hosts on the network through a number of different enumeration techniques. This scan is useful to assist in understanding the number of hosts on a network before running a PCI or Full scan.
    - *Optional:* Choose **Advanced Configurations** to change the default port scanning options (see Table 1 for details of the options). Select the arrow or text to expand this section.
- **Port Service Fingerprint:** A proprietary advanced port fingerprinting scan to identify which protocols and services are running on live hosts. This scan examines the specified TCP and UDP ports for each host, and attempts to identify the services if any that are responding. It can be used to understand what services are present on the network (such as web servers, mail servers or database servers).
    - *Optional:* Choose **Advanced Configurations** to change the default port scanning options (see Table 1 for details of the options). Select the arrow or text to expand this section.
- **HIPAA Scan:** A full scan that generates a report suited to the requirements of HIPAA.

After selecting configurations, click **Next** to continue.

3.1.1 Advanced Configurations

Some scan types allow you to choose network scanning configurations. These configurations are defined as follows:

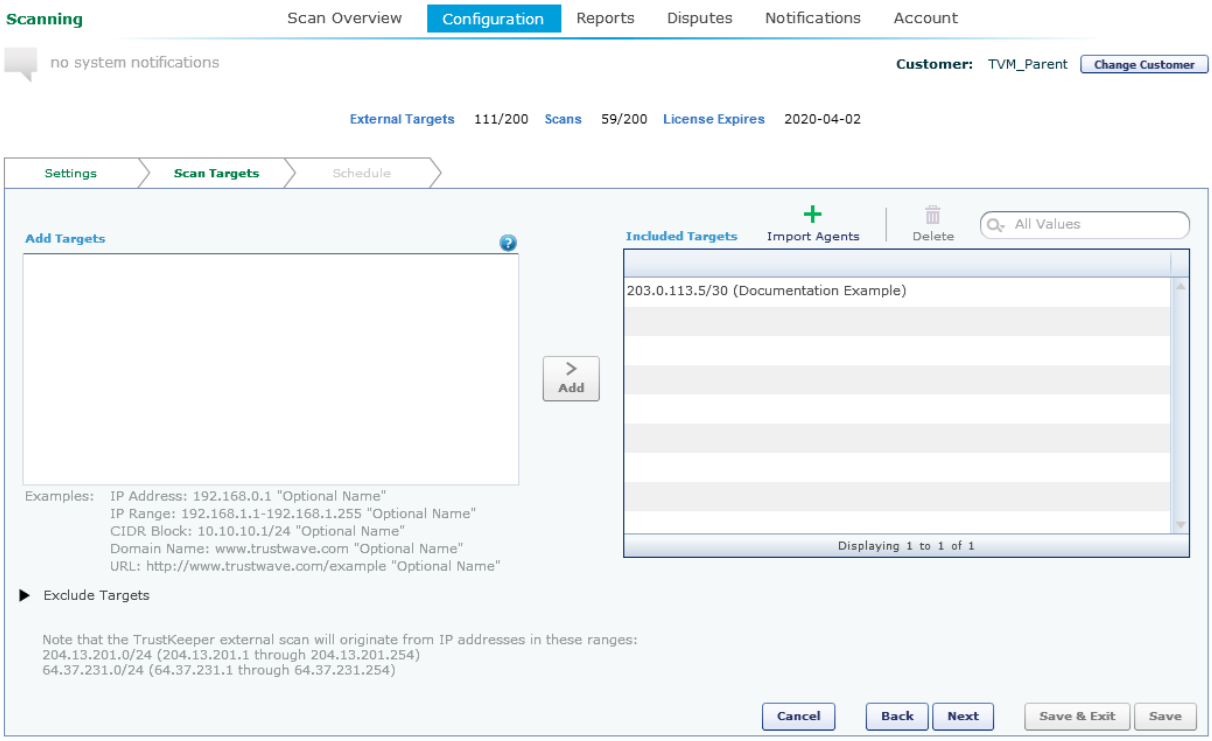
Table 1: Advanced Configuration Options

Configuration Type	Description
ICMP Ping	For host discovery, uses only a network ping to determine accessible host addresses
Light TCP/UDP scan: common ports	In addition to ICMP, scans on TCP commonly used ports (21, 22, 23, 25, 53, 80, 110, 111, 135, 139, 143, 389, 443, 445, 993, 995, 1433, 1521, 1723, 3306, 3389, 5432, 5631, 5900, 8080) and UDP commonly used ports (53, 67, 68, 69, 123, 137, 138, 161, 500). • This is the default configuration for live host discovery.
Medium TCP/LDP scan	In addition to ICMP, scans on TCP ports 0 – 1023, as well as TCP ports 1433, 1521, 1723, 3306, 3389, 5432, 5631, 5900, 8080 and commonly used UDP ports (53, 67, 68, 69, 123, 137, 138, 161, 500).

Configuration Type	Description
Comprehensive scan (65000 TCP ports and more)	In addition to ICMP, scans on all TCP ports and commonly used UDP ports (53, 67, 68, 69, 123, 137, 138, 161, 500). Also checks all other available methods. • This is the default configuration for port service fingerprinting.

3.2 Scan Targets

On the **Scan Targets** pane, click in the **Add Targets** box to add targets.



Targets can be entered as an IP address, range of IP addresses, CIDR network block, domain name, or URL. You can give each target a friendly name (entered in quotes after the target information).

Note the examples shown below the target field, and hover over for more suggestions.

Note: A URL must start http:// or https:// and can include subdirectories. A domain entry cannot include subdirectories.

- Once you have entered the text, click **Add** to populate the Included Targets list.
- You can also select Agents – to provide the IP address of internet facing devices to be scanned – by clicking **Import Agents** + (found above the Included Targets list).

Note: Agents can only be used with External Vulnerability Scans [EVS]. They cannot be used to configure Internal Vulnerability Scans [IVS] run from a Trustwave appliance.

- To delete a target, select it and then click **Delete** .
- Click **Next** to continue.

3.2.1 Exclusions

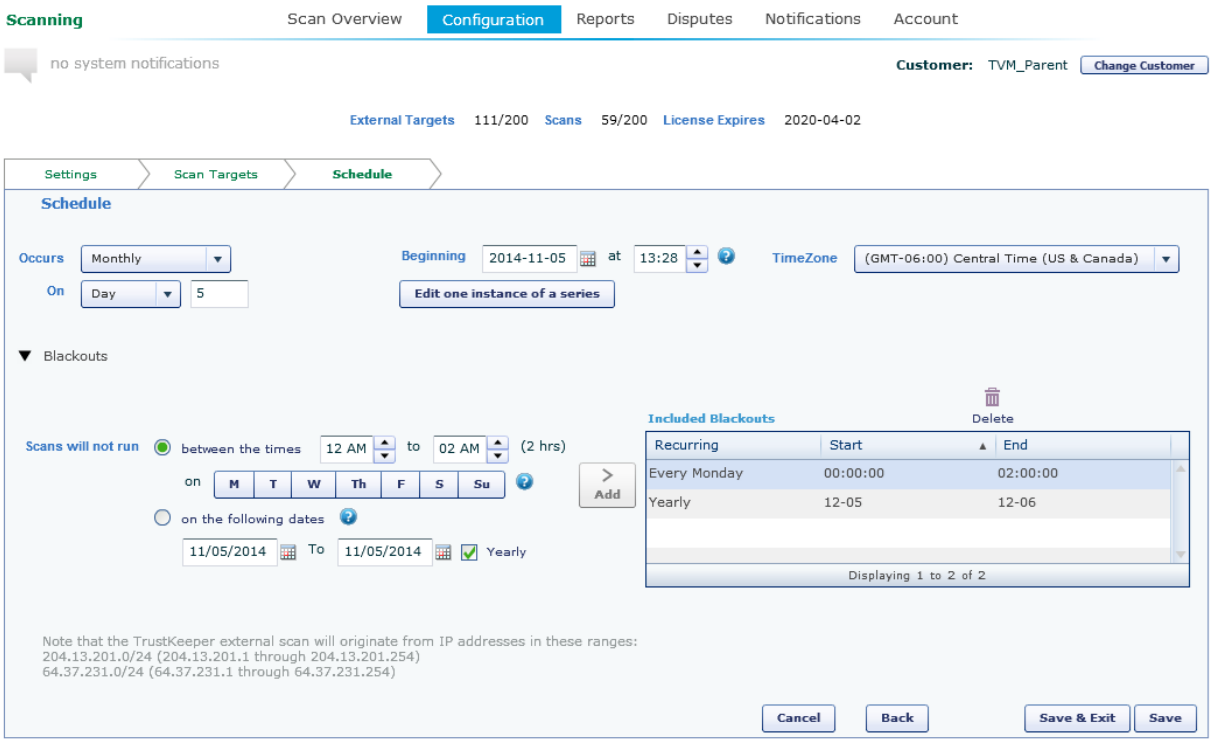
You may want to exclude some devices within the target ranges. To exclude devices, click the **Excluded Targets** arrow at bottom left to expand the exceptions/exclusions section. Click in the **Add Exceptions** box to enter targets that will not be scanned. Use the same techniques as for the Scan Targets pane.

After configuring targets, click **Next** to continue or **Back** to return to the Settings pane.

3.3 Schedule

On the Schedule pane, choose when the scan should run. You can choose an immediate one-time scan, or schedule a scan to run once, weekly, monthly, or quarterly. For monthly scans you can choose the date of the scan or the recurring day of the week each month.

Enter a date and time for the first scan. Select the timezone. The default timezone matches the timesone of your browser.



3.3.1 Blackouts

You may want to prevent scanning on particular dates or at certain times of day. To set up these options, click the **Blackouts** arrow to expand the blackouts section.

In the blackouts section, optionally enter dates or times when scanning should be suspended.

- You can choose to black out specific times on certain days of the week.
- You can choose to black out specific dates.
- You can add more than one set of blackout dates or times to build complex rules.

Be aware that blackouts can cause the scan to take a long time.

To add a blackout period:

- Select times and days, or select a starting and ending date and optionally select Yearly to repeat every year.
- Click **Add** to add the blackout period to Included Blackouts.
- To remove a blackout period, select it in the list and then click **Delete** .

Click **Save & Exit** to save and enable the scan or scan series. The scan or series is added to the list viewable from the schedule pane. The scan will run as scheduled, unless you disable it.

3.4 Editing a Scan Series and Disabling Individual Scans

After you save a scan or series, you can edit it. To edit, select the scan in the list on the Configuration page, and then click **Edit** . Alter scheduling or targets as required. Some settings such as the basic scan type are disabled and cannot be changed.

To disable an individual scan in a series:

- On the Schedule pane click **Edit one instance of a series**.
- The pop-up window shows all instances of the series for the next year. To disable an instance, clear the associated checkbox. To re-enable an instance, check the box.
- When you have made all selections, click **Close** to close the pop-up, and then click **Save & Exit** on the Schedule pane (or click **Cancel** to ignore any changes).

3.5 Deleting a Scan Series

To delete a scan series, select it from the list and then click **Delete** .

Note: If you want to cancel a single instance of a scan in a series, see Section 3.4.

4 Viewing Reports

Select the scans icon and click **Reports** in the main navigation to see the Reports Summary screen.

This screen includes two lists:

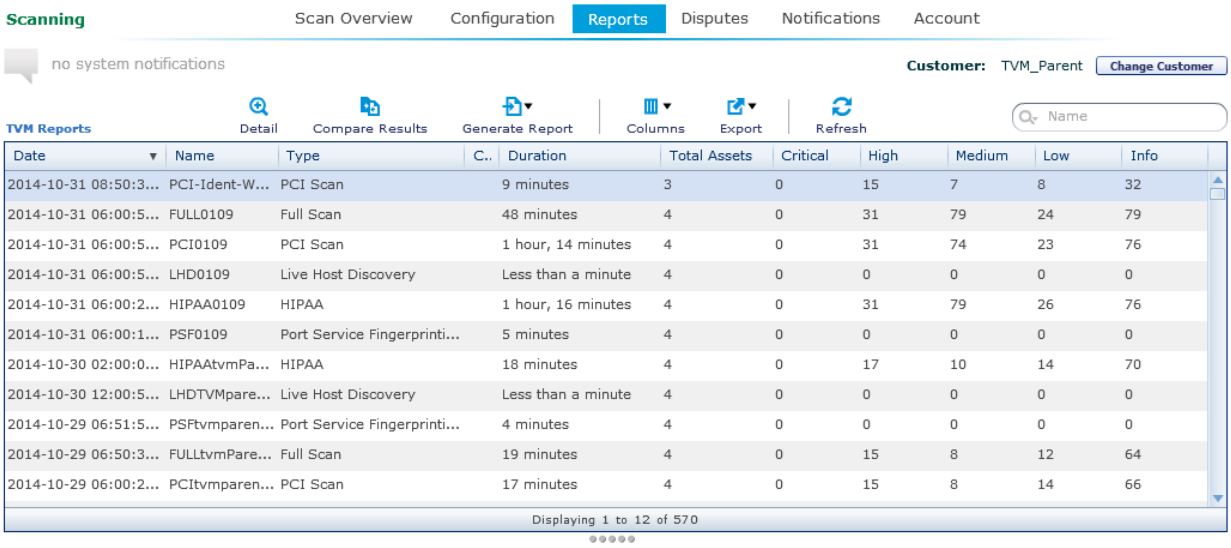
TVM Reports provides a summary of completed scans and identified vulnerabilities. You can export the summary data in several formats. You can view detailed results of each scan online. Depending on the type of scan you can generate Executive Summary, Full Vulnerability, Vulnerabilities by IP, Vulnerabilities by Severity, or PCI reports in PDF format. You can also generate reports from the Completed Scans pane on the Scan Overview tab, and from the Vulnerabilities tab when viewing scan results.

Report Files allows you to generate importable data files (in CSV format) that list detailed scan results, disputes, or targets for a range of dates. The list shows files that have been requested or completed.

Tip: You you can adjust the size of the lists by dragging the handle between the panes.

4.1 TVM Reports

The TVM Reports list shows all successfully completed scans along with scan summary information. This listing provides a quick view across all scans and can be used to track assets or aggregate finding counts by risk. You can sort and filter scan results, and export summary results into several formats.



Use the filter field at top right to limit the list results by name or scan type (click to select the limit).

If the list includes many results, use the scrollbar at right to move through the list.

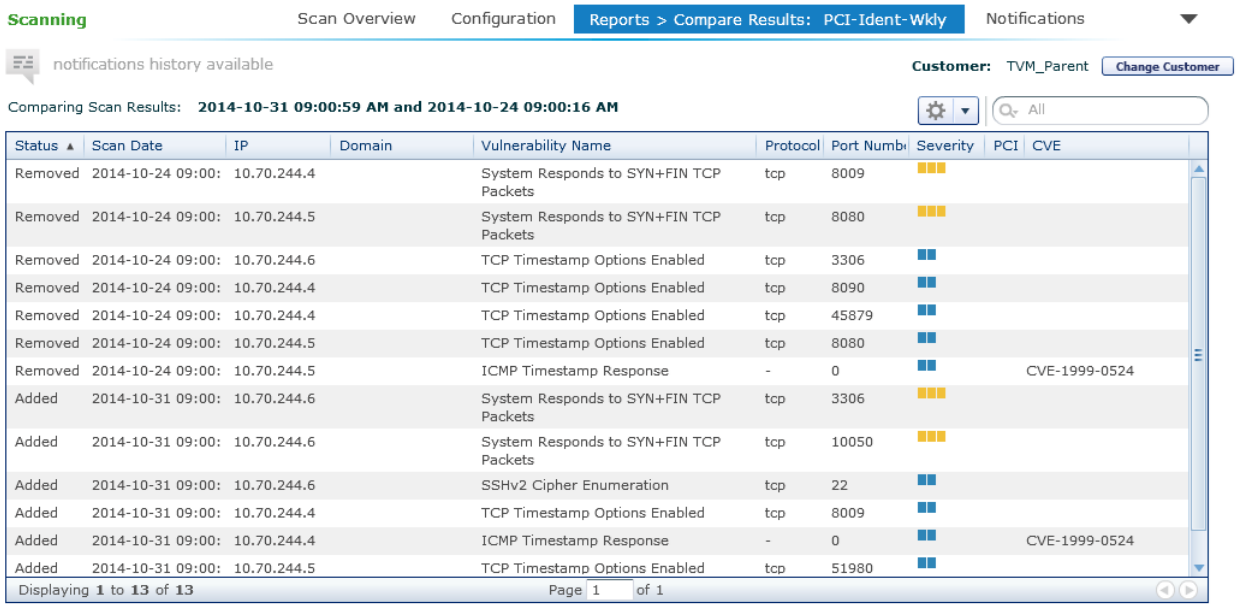
Use the icons above the list to choose specific columns, to copy data to the clipboard, or to export data in a variety of formats. For details of the available options, see Section 1.1.5 above.

To see detailed scan results and asset information, select a specific row in the list and click **Detail** , or double-click the row. For details of this information see Section 4.2.

To generate a report in PDF format, click **Generate Report** and then select the type of report. Reports are generated and downloaded using the browser functionality.

Note: Full vulnerability reports can be very large and take a long time to generate. In some cases your web browser might time out before the report is generated and returned. In these cases you can use the Report Files function to create a CSV listing of vulnerabilities. The CSV files are generated in the background and can be quickly downloaded when ready.

To compare results of two scans (in the same series), select a row and click **Compare Results** . On the pop-up list, choose two scans to compare, and then click **Compare**. The result shows changes in vulnerability status between the scans.



4.2 Reports Results

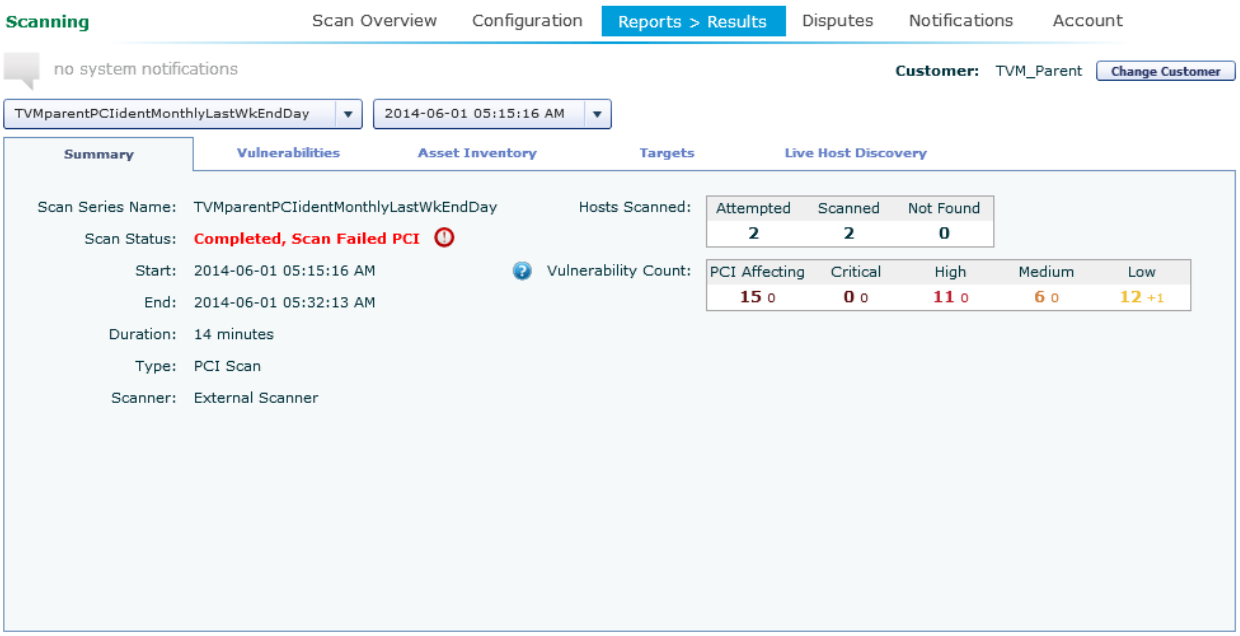
The Results screen shows details of vulnerability findings and asset inventory for a specific scan. The screen includes the following tabs: Summary, Vulnerabilities, Asset Inventory, Targets, and Live Host Discovery.

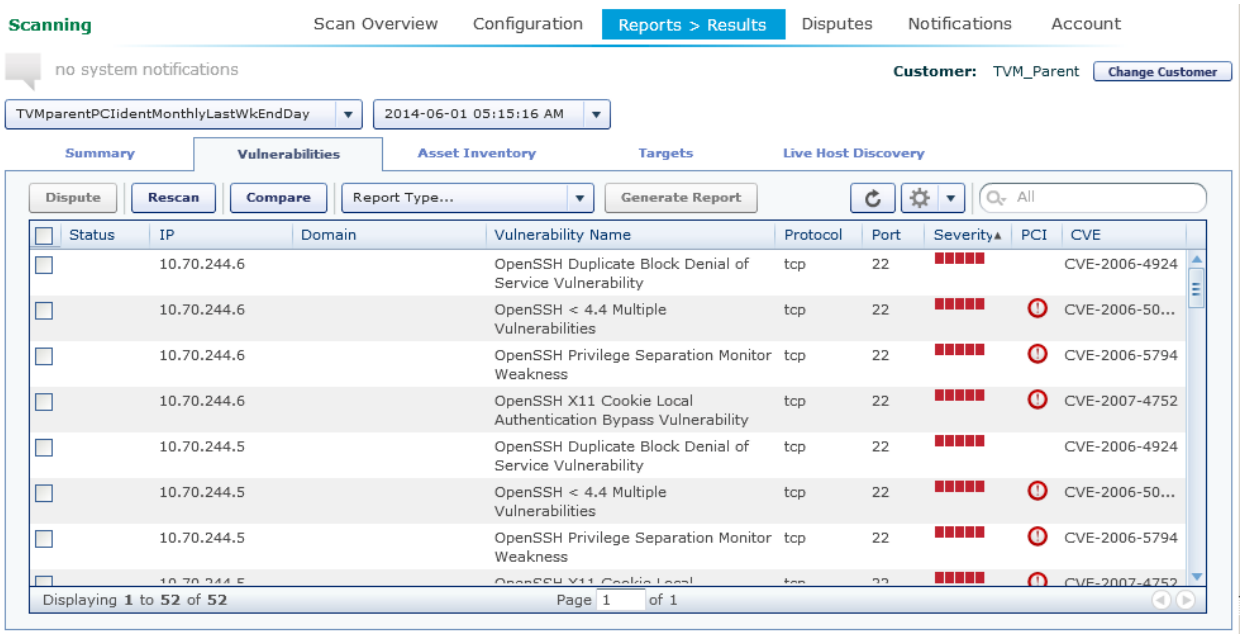
You can return to the Reports listing by clicking Reports in the main navigation.

From any tab, you can move between scan series and scans using the two menus at the top of the listing.

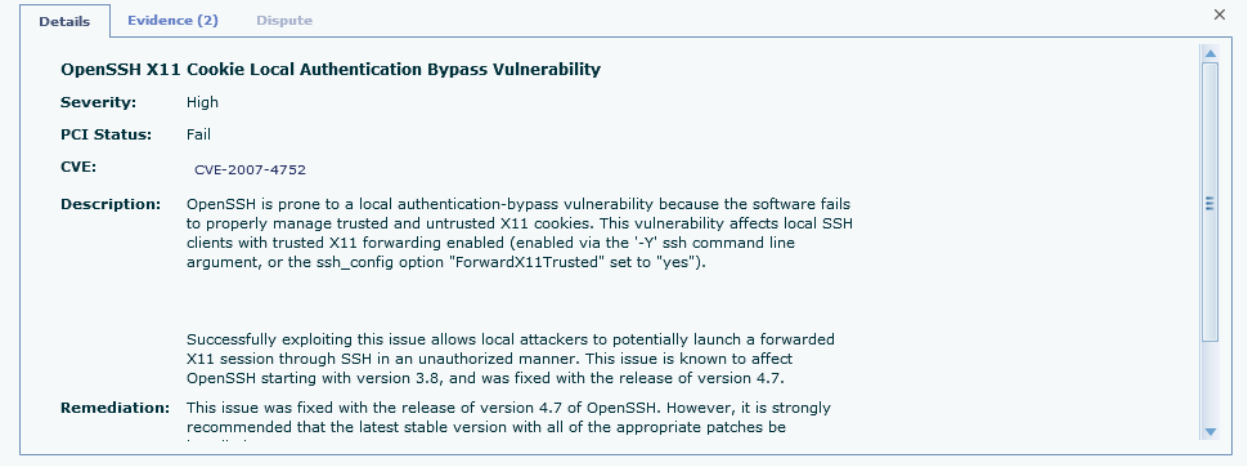
4.2.1 Vulnerabilities

This screen shows vulnerability findings for a specific scan.





Select a row to view more details in a pane below the list. On this pane, the Details tab includes a description of the issue, and remediation steps. The Evidence tab includes any available evidence of the vulnerability that was gathered during the scan. For vulnerabilities that have been disputed (as described in Sections 4.3 through 4.5), dispute history will be shown in the Disputes tab.



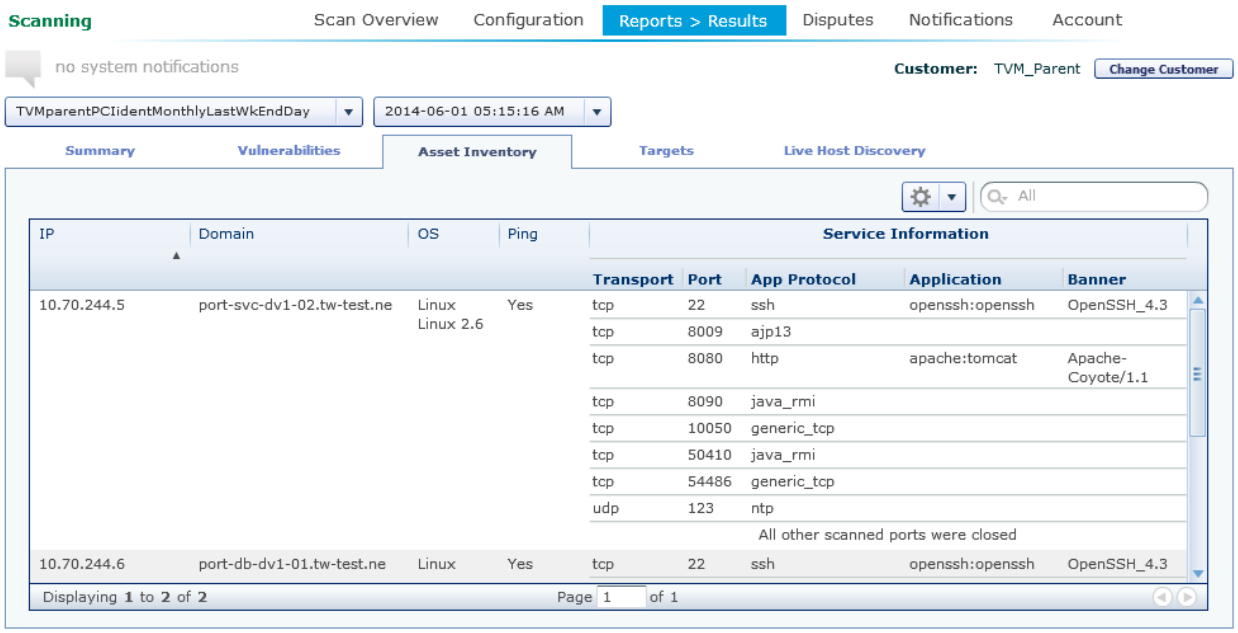
- **Rescan:** Click this button to re-run the last scan. A rescan does not count against your total scan count.

Note: This option re-runs an entire scan. It is not limited to items that are selected.

- **Compare:** Click this button to compare the results of two scans in a series.

4.2.2 Asset Inventory

The Asset Inventory tab contains a list of all discovered hosts with host information such as open ports and service banners. The list can be sorted or filtered on IP, Domain, OS, or Ping Status, and exported in a variety of formats.



4.2.3 Targets

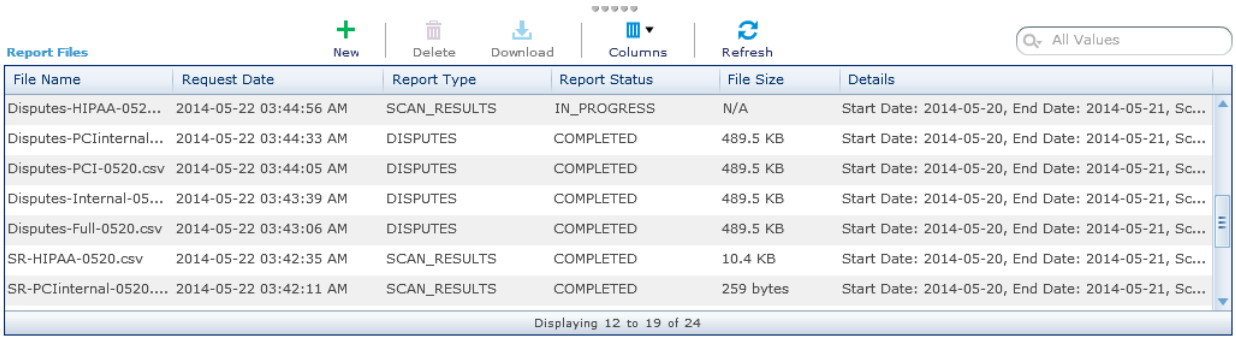
The Targets tab shows a list of the included and excluded targets for the scan.

4.2.4 Live Host Discovery

The Host Detection tab shows a list of targets that were detected, or not detected, during the scan.

4.3 Report Files

This section of the main reports screen allows you to generate CSV data files containing details of scan results, disputes, or scan targets. The list shows files that have been requested.



To create a report file, click **New** . On the pop-up window, enter a name. Select dates to report on and a report type. For reports on results or targets, enter a scan type. Click **Export** to start generation of the file. You can check the status of the report in the list.

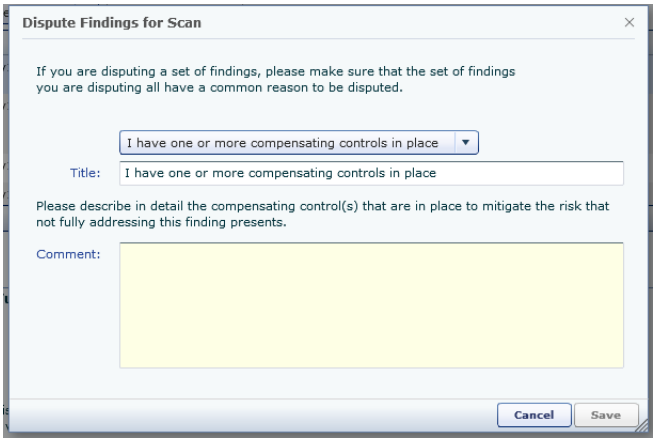
- The result file includes all disputes that match the dates selected, all targets of scans that match the dates and scan type selected, or all results of all scans that match the dates and scan type selected.

To download a file (if the status is COMPLETED), select the row and then click **Download** . The file downloads using File Transfer Manager as described in Section 1.1.4.

To remove a file from the list, select the row and then click **Delete** .

4.4 Disputes

Due to the nature of external vulnerability scanning and certain compliance requirements, there may be times when scan results report vulnerabilities that are incorrect or are not valid security risks because they are mitigated through technical or non-technical controls or processes. When these cases occur, you can dispute the finding using the **Dispute** button on the vulnerabilities list. Use the checkboxes to select one or more vulnerabilities to dispute, and then click the button. On the form that displays, enter a reason and comments. For non-PCI compliance affecting scans, these disputes will be automatically accepted. For PCI scans, a support representative will review the information provided and help resolve the issue.



4.5 Bulk Disputes

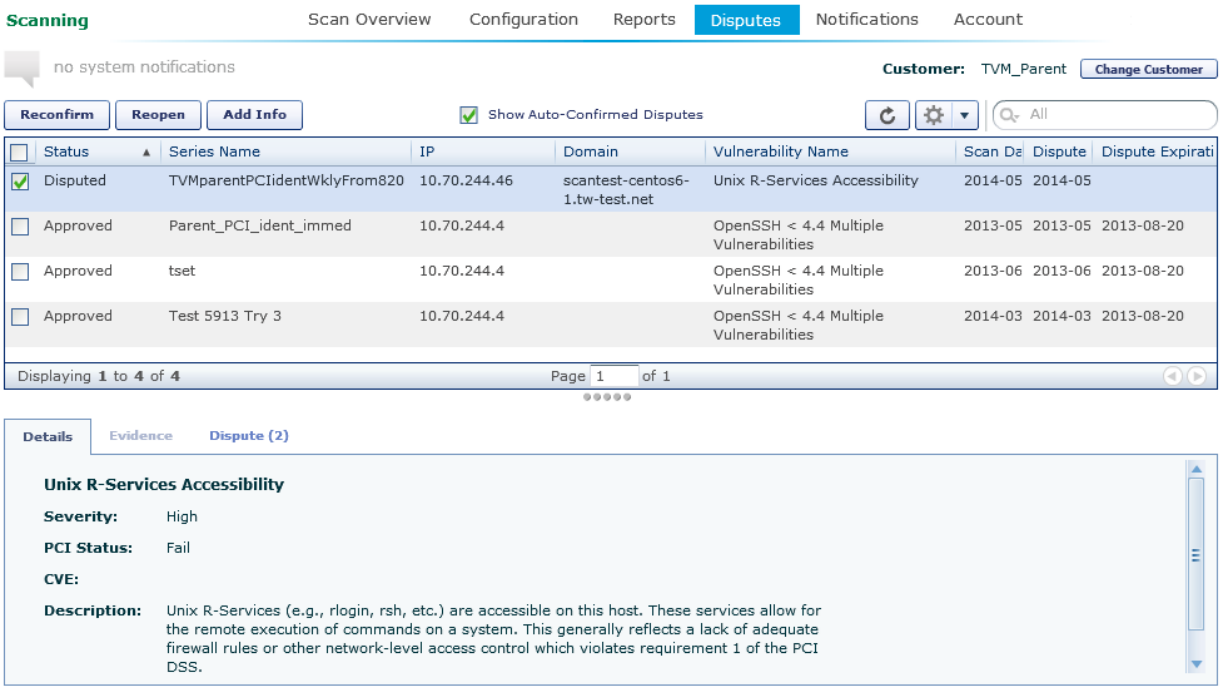
In addition to disputing a single finding, multiple vulnerability findings in a single scan can be selected and then disputed at the same time if they have the same dispute reason. For example, certain Linux operating systems patch software packages using a process called “backporting”. When software is “backported”, bugs, including security vulnerabilities, are fixed but the software banner version is not always updated. This frequently causes issues when detecting vulnerabilities remotely through vulnerability scanning. During scanning, if this occurs it generally results in a vulnerability finding being reported for all hosts that run that version of software when the test relies on the banner version. To ease the process of disputing these findings, multiple findings can be selected and disputed at once.

You can also apply a filter to the findings table to provide a list of specific vulnerabilities, such as “Apache 2.2 prior to 2.2.15 Multiple Vulnerabilities”, which can then be bulk disputed. To set a filter, enter the search terms in the filter box in the top right section of the vulnerability findings table.

4.6 Disputes Screen

The dispute management screen provides a view of all disputes and provides a way to reconfirm expiring disputes, reopen closed disputes, or add information for the Trustwave support team. For PCI scans, vulnerability disputes must be expired after 3 months. For non-PCI scans, disputes are automatically accepted.

Select a dispute to see details in a new section below the list.



The status of disputes can be one of the following:

- **Disputed:** The dispute requests has been submitted but not yet reviewed by Trustwave
- **Need Info:** The dispute has been reviewed and is currently denied. However, with additional information it will be reconsidered and is likely to be accepted.
- **Denied:** The dispute has been reviewed and rejected. The original vulnerability finding stands.
- **Approved:** The dispute has been reviewed and accepted.

Available actions on the Disputes screen include:

- **Reconfirm:** Request an extension of time for an approved dispute
- **Reopen:** Request reconsideration of a denied dispute
- **Add Info:** Provide additional information for a dispute that is currently in the Disputed or Need Info status.

4.7 PDF Reports

When a scan has completed, several different PDF reports can be generated from the Vulnerabilities tab.

Currently the following report types are supported, depending on the scan type:

- Executive Summary: A one-page summary of the scan, scan findings, trends, and top vulnerabilities.
- PCI Report: A report suitable for submitting for PCI compliance detailing all PCI violations.
- Vulnerabilities by IP: all vulnerabilities found for each IP address. A simple list with severity, CVSS, vulnerability name, CVEs, ports and services.

- Vulnerabilities by Severity: all vulnerabilities found, each listed once. A simple list with severity, CVSS, vulnerability name, IP addresses and port.
- Full Vulnerability Report: A complete vulnerability report containing an executive summary, scan inventory, Vulnerabilities & Policy Violations, Web Servers and Part 4 SSL Certificate Information, and any Disputed Vulnerabilities and Policy Violations.

Note: Full vulnerability reports can be very large and take a long time to generate. In some cases your web browser might time out before the report is generated and returned. In these cases you can use the Report Files function to create a CSV listing of vulnerabilities. The CSV files are generated in the background and can be quickly downloaded when ready.

To generate a report, select the appropriate report type from the dropdown on the top left area of the vulnerability findings table, then select “Generate Report”.

4.8 Notifications

E-mail alert notifications can be sent instantly when certain scan events occur by selecting the notification checkboxes. When these are selected, email alerts will be sent for all scans.

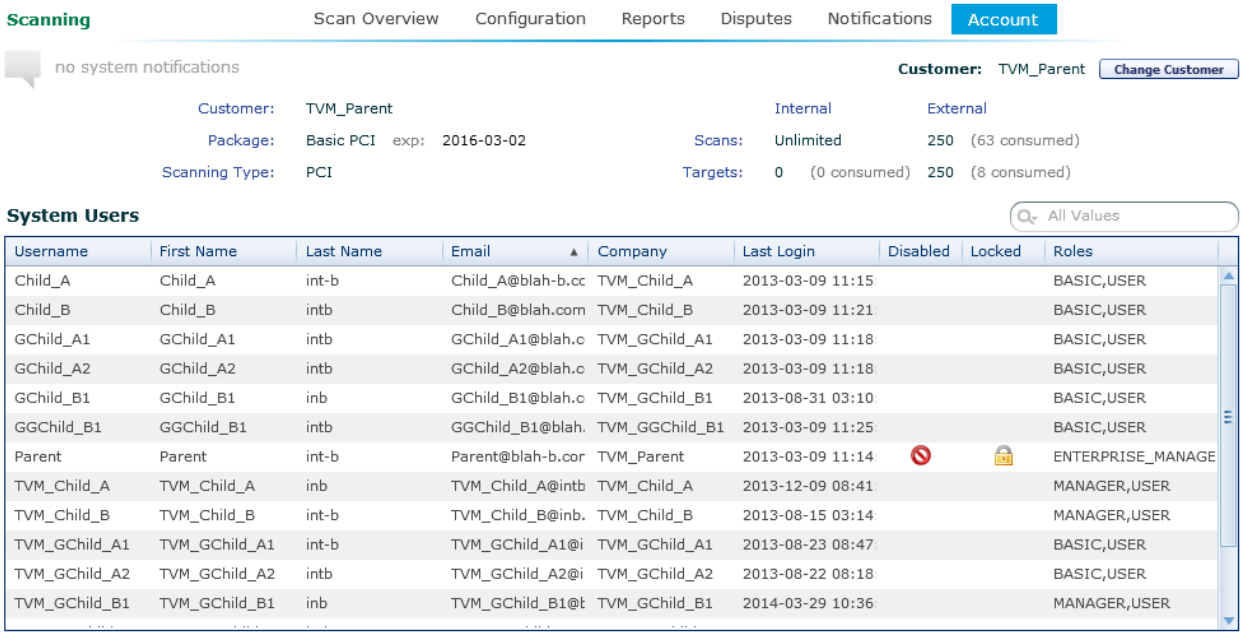
Email notifications can be sent for one or more of the following actions:

- Scan Scheduled and Completed
- Status change for Disputes (information needed, accepted, declined)
- Dispute Expiration
- Scan Notification 1 hour prior to scan starting
- Scan Notification 24 hour prior to scan starting
- Scan Notification 48 hour prior to scan starting
- Scan Notification 72 hour prior to scan starting

By default, scan notifications are enabled for scan changes, 1 and 24 hours before the scan starts.

5 Reviewing Account Information

Click **Account** in the sub-menu to see information about your account.



The box at the top of this screen shows the customer information, including details of the package and expiration, and the scans available and consumed.

The **System Users** box includes details of users in the enterprise hierarchy, and their roles. This feature allows users from the higher levels of the organization to have an overview of the users and roles for all entities set up under them. Users at lower levels do not see information about the entities above them. For more details of the enterprise features, see the next section.

6 Managing Scans for the Enterprise *(in Beta)*

A customer using TVM can request Trustwave to set up a hierarchy of views for child companies. This is a beta feature that requires the approval of Trustwave on a case by case basis. The hierarchy can have up to four levels.

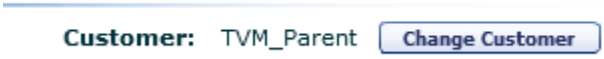
Logins can be created with any one of three roles, known as Enterprise Manager, Manager, and User. This feature allows users from the higher levels of the organization to have an overview of the scans for all entities set up under them, while allowing the other entities to set up and review only their own scans.

In addition to the three roles, TVM provides for each role to have either read only or read/write access.

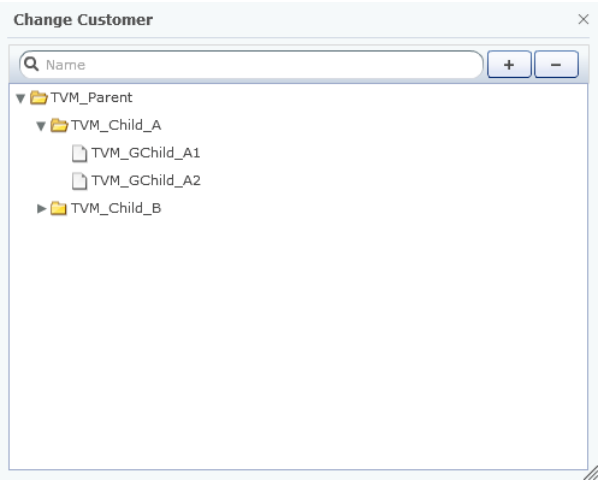
Hierarchy Rules

- A person can be assigned to only one company.
- A login with the Enterprise Manager role can see ALL companies in the hierarchy, regardless of what company their user account is in.
- A login with the Manager role can have access to more than one company, defined by the company hierarchy structure. Any company 'below' the one in which they are a user is accessible. For example, in the list shown below, a Manager in TVM_Child_A would also see scans created for TVM_GChild_A1 and TVM_GChild_A2.
- A login with the User role would *never* have access to a company other than the one in which they are a user. For example, in the list shown below, a User in TVM_Parent would have access only to scans created for TVM_Parent.
- For each role there are two access levels available: read/write [full] or read only.
- The company hierarchy can be up to 4 layers deep, after which it becomes too difficult to manage.

If your login is set up as an Enterprise Manager or Manager, at the top right of the screen you will see the name of the Customer currently shown, and a Change Customer button:



Click **Change Customer** to view the list of customer names available to you:



You can filter entries by name. You can expand or collapse the entire hierarchy using the + and – buttons. You can expand or collapse a branch using the arrow for that branch. To select a customer, click that name.

About Trustwave

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit https://www.trustwave.com.