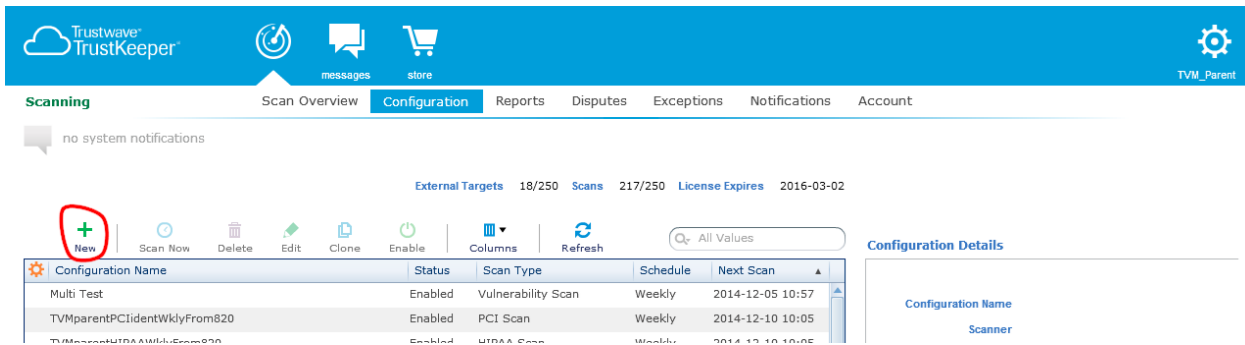


Vulnerability Management Scanning Quick Start Guide

Set Up Scans

1. From the Scanning menu, click **Configuration**.
2. Click **New** to create a new scan.

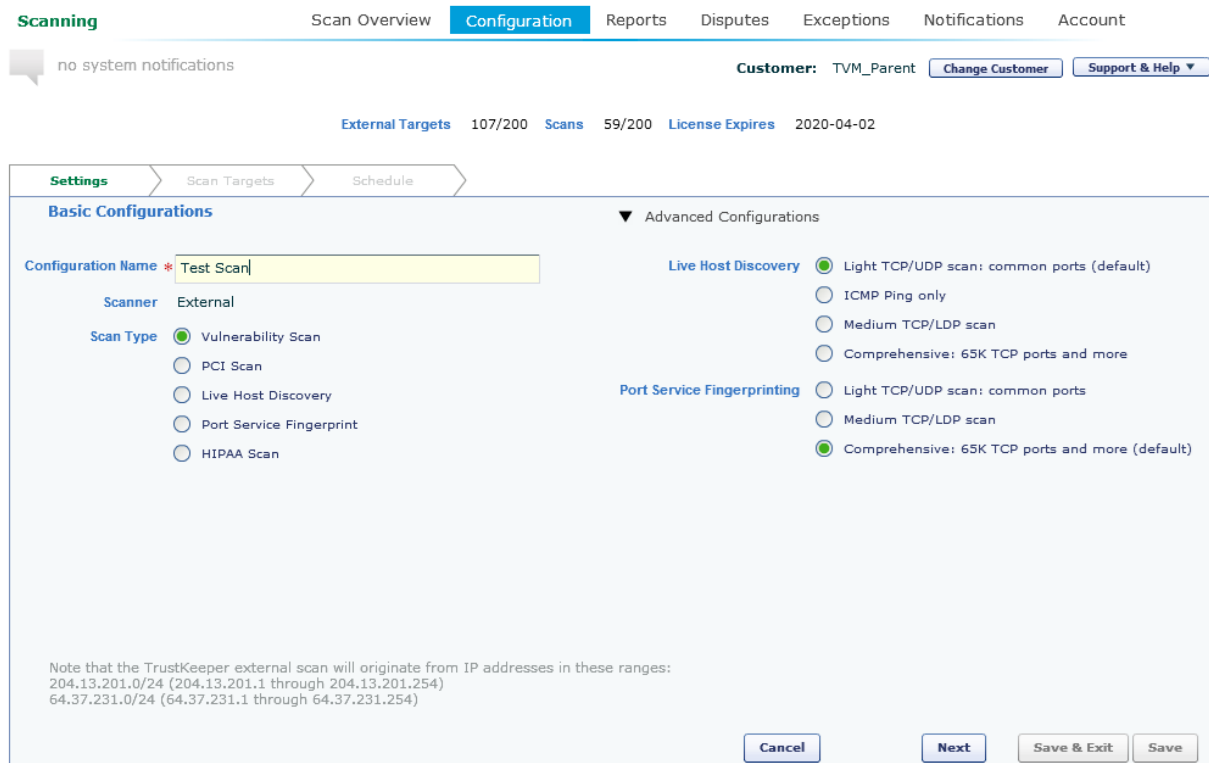


The screenshot shows the Trustwave TrustKeeper interface. At the top, there are navigation tabs: Scanning, Scan Overview, Configuration, Reports, Disputes, Exceptions, Notifications, and Account. The 'Configuration' tab is active. Below the navigation, there are statistics: External Targets 18/250, Scans 217/250, License Expires 2016-03-02. A toolbar contains buttons: New (circled in red), Scan Now, Delete, Edit, Clone, Enable, Columns, and Refresh. Below the toolbar is a table of existing configurations:

Configuration Name	Status	Scan Type	Schedule	Next Scan
Multi Test	Enabled	Vulnerability Scan	Weekly	2014-12-05 10:57
TVMparentPCIdentWklyFrom820	Enabled	PCI Scan	Weekly	2014-12-10 10:05
TVMparentHIPAAWklyFrom820	Enabled	HIPAA Scan	Weekly	2014-12-10 10:05

On the right side, there is a 'Configuration Details' panel with a 'Scanner' dropdown menu.

3. Next, name the scan and select a scan type. Advanced configuration is available, but default values are provided. Click **Next** to continue.



The screenshot shows the 'Basic Configurations' section of the scan configuration page. The 'Configuration Name' field contains 'Test Scan'. The 'Scanner' is set to 'External'. The 'Scan Type' is set to 'Vulnerability Scan'. The 'Advanced Configurations' section is expanded, showing 'Live Host Discovery' and 'Port Service Fingerprinting' options. The 'Live Host Discovery' section has 'Light TCP/UDP scan: common ports (default)' selected. The 'Port Service Fingerprinting' section has 'Comprehensive: 65K TCP ports and more (default)' selected. At the bottom, there are buttons for 'Cancel', 'Next', 'Save & Exit', and 'Save'.

Note that the TrustKeeper external scan will originate from IP addresses in these ranges:
204.13.201.0/24 (204.13.201.1 through 204.13.201.254)
64.37.231.0/24 (64.37.231.1 through 64.37.231.254)

Set Up Targets

Enter one or more IP addresses, ranges, domain names, URLs including protocol (http:// or https://) with or without subdirectories, or network blocks in CIDR format. Click **Next** to continue.

The screenshot shows the 'Configuration' tab of the TrustKeeper interface. At the top, there are navigation tabs: Scanning, Scan Overview, Configuration (active), Reports, Disputes, Exceptions, Notifications, and Account. Below these, there's a notification area with 'no system notifications' and a customer dropdown set to 'TVM_Parent'. A status bar shows 'External Targets 111/200', 'Scans 59/200', and 'License Expires 2020-04-02'. The main content area has three tabs: Settings, Scan Targets (active), and Schedule. The 'Scan Targets' tab is divided into 'Add Targets' and 'Included Targets'. The 'Add Targets' section is empty and includes examples for IP Address, IP Range, CIDR Block, Domain Name, and URL. The 'Included Targets' section contains one entry: '203.0.113.5/30 (Documentation Example)'. At the bottom, there are buttons for 'Cancel', 'Back', 'Next', 'Save & Exit', and 'Save'.



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

Configure Schedules

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. You can select the time zone to be used. The default time zone matches the configuration of your browser. Click **Save & Exit**.

Scanning | Scan Overview | **Configuration** | Reports | Disputes | Exceptions | Notifications | Account

no system notifications | Customer: TVM_Parent | Change Customer | Support & Help

External Targets | 111/200 | Scans | 59/200 | License Expires | 2020-04-02

Settings > Scan Targets > **Schedule**

Schedule

Occurs: Monthly
On: Day 5
Beginning: 2014-11-05 at 13:28
TimeZone: (GMT-06:00) Central Time (US & Canada)

Enable/Disable one instance of a series

▼ Blackouts

Scans will not run between the times 12 AM to 02 AM (2 hrs)
on **M T W Th F S Su**

on the following dates
11/05/2014 To 11/05/2014 Yearly

Included Blackouts

Recurring	Start	End
Every Monday	00:00:00	02:00:00
Yearly	12-05	12-06

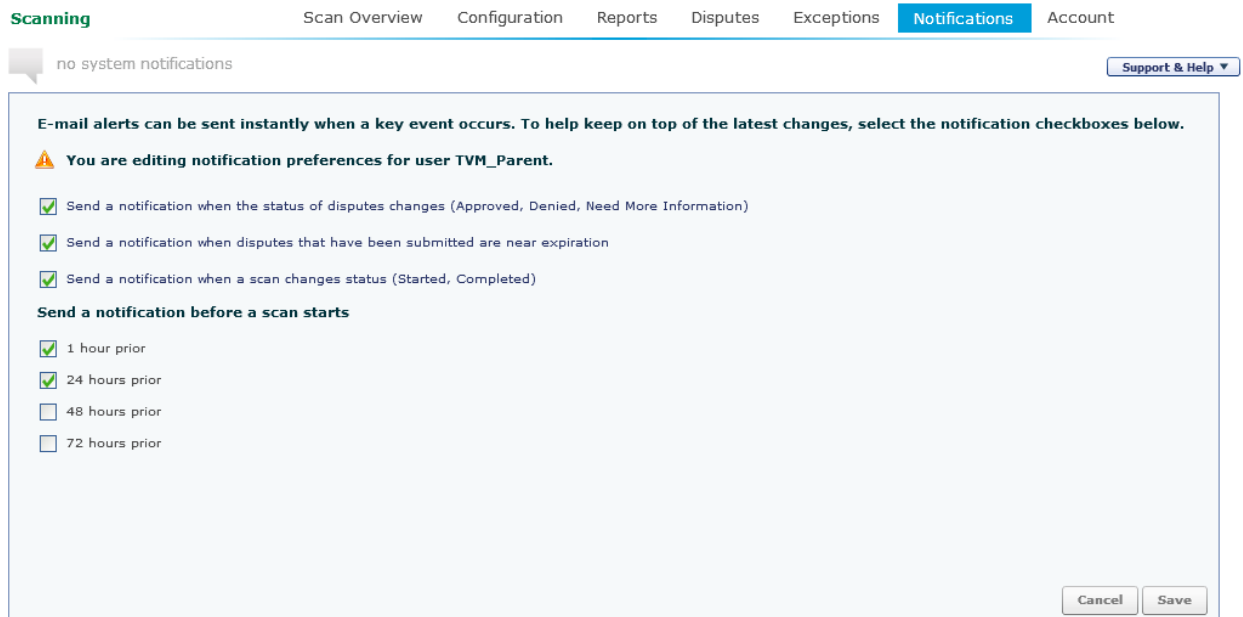
Displaying 1 to 2 of 2

Note that the TrustKeeper external scan will originate from IP addresses in these ranges:
204.13.201.0/24 (204.13.201.1 through 204.13.201.254)
64.37.231.0/24 (64.37.231.1 through 64.37.231.254)

Cancel | Back | Save & Exit | Save

Configure Notifications

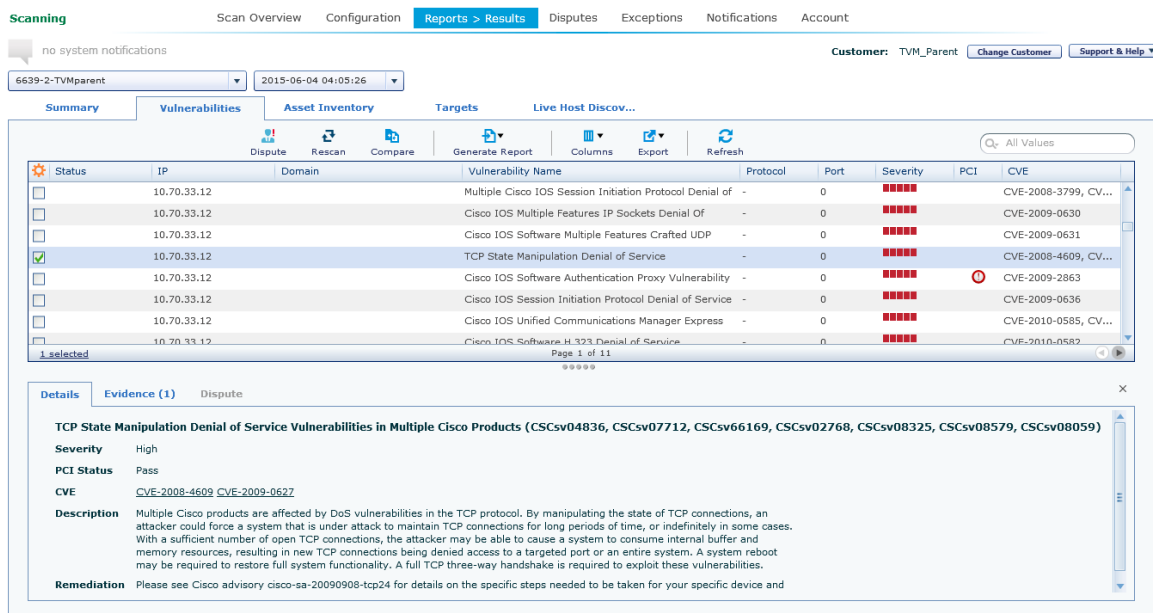
1. From the Scanning menu, click **Notifications**.



1. Select notification options for alerts.
2. Click **Save**.

View Results

1. To view results of scans, from the Scanning menu, click **Reports**.
2. Select an item and click **View Results** to get details.



PCI Disputes Management



Note: For non-PCI ASV scans, see **Exceptions Management**.

For External PCI scans, to dispute findings that you believe to be incorrect:

1. On the Vulnerabilities tab of the Report Results screen, select one or more findings using the checkboxes, and then click **Dispute**.

The screenshot shows the 'Scanning' interface with the 'Reports > Results' tab selected. The 'Vulnerabilities' tab is active, displaying a table of findings. The 'Dispute' button is circled in red. The table contains the following data:

Status	IP	Domain	Vulnerability Name	Protocol	Port	Severity	PCI	CVE
<input type="checkbox"/>	10.70.33.12		Multiple Cisco IOS Session Initiation Protocol Denial of	-	0	■■■■■		CVE-2008-3799, CV...
<input type="checkbox"/>	10.70.33.12		Cisco IOS Multiple Features IP Sockets Denial Of	-	0	■■■■■		CVE-2009-0630
<input type="checkbox"/>	10.70.33.12		Cisco IOS Software Multiple Features Crafted UDP	-	0	■■■■■		CVE-2009-0631
<input checked="" type="checkbox"/>	10.70.33.12		TCP State Manipulation Denial of Service	-	0	■■■■■		CVE-2008-4609, CV...
<input type="checkbox"/>	10.70.33.12		Cisco IOS Software Authentication Proxy Vulnerability	-	0	■■■■■	⊘	CVE-2009-2863

2. On the popup window:
 - Select a reason for the dispute using the menu.
 - Enter a descriptive title
 - Enter an explanation that gives details of the reason for disputing this finding.

The 'Dispute Findings for Scan' popup window contains the following text and form elements:

If you are disputing a set of findings, please make sure that the set of findings you are disputing all have a common reason to be disputed.

I think this finding is an error (false positive) (dropdown menu)

Title Briefly explain the details of the dispute

Please describe in detail why this finding is believed to have been reported in error (such as Windows vulnerabilities being reported on a Linux system).

Comment provide sufficient details for the ASV Engineer to understand and validate the evidence provided for this dispute

Buttons: **Cancel** **Save**

3. To review the status of disputes, see the **Disputes** page.

Disputes

Status	Series Name	IP	Port	Domain	Vulnerability Name	Scan Date	Dispute Date	Dispute Expi...
Approved	Parent_PCI_ident_immed	10.70.244.4	22		OpenSSH < 4.4 Multiple Vulnerabilities	2013-05-22	2013-05-22	2013-08-20
Disputed	TVMparentPCIidentWklyFrom820	10.70.244.46	514	scantest-centos6-1.tw	Unix R-Services Accessibility	2014-05-14	2014-05-20	
Disputed	6639-2-TVMparent	10.70.244.4	22		OpenSSH < 4.4 Multiple Vulnerabilities	2014-08-28	2014-08-28	
Disputed	6639EntView-TVMparent-1	10.70.244.4	22		OpenSSH < 4.4 Multiple Vulnerabilities	2014-08-30	2014-08-30	
Disputed	6639-2-TVMparent	10.70.244.4	22		OpenSSH < 4.4 Multiple Vulnerabilities	2014-09-04	2014-09-04	
Disputed	6639-2-TVMparent	10.70.244.4	22		OpenSSH < 4.4 Multiple Vulnerabilities	2014-09-11	2014-09-11	
Disputed	6639-2-TVMparent	10.70.244.4	22		OpenSSH < 4.4 Multiple Vulnerabilities	2014-09-18	2014-09-18	
Disputed	6639-2-TVMparent	10.70.244.4	22		OpenSSH < 4.4 Multiple Vulnerabilities	2014-09-25	2014-09-25	

Details | Evidence (1) | Dispute (4)

OpenSSH < 4.4 Multiple Vulnerabilities

Severity High

PCI Status Fail

CVE [CVE-2006-5051](#) [CVE-2006-5052](#)

Description OpenSSH prior to version 4.4 is affected by multiple vulnerabilities that may allow for a remote attacker to execute arbitrary code on the affected device.

Remediation This issue was fixed in OpenSSH version 4.4. Upgrade to a recent/stable version

Exceptions Management

For non-PCI ASV scans, to apply exceptions for findings that you believe to be mitigated:

1. On the Vulnerabilities tab of the Report Results screen, select one or more findings using the checkboxes, and then click **Exception**.

Vulnerabilities

Status	IP	Domain	Vulnerability Name	Pro...	Port	Se...	CVE
<input type="checkbox"/> Excepted	10.70.24...		OpenSSH Duplicate Block Denial of Service Vulnerability	tcp	22	■■■■■	CVE-200...
<input type="checkbox"/> Excepted	10.70.24...		OpenSSH < 4.4 Multiple Vulnerabilities	tcp	22	■■■■■	CVE-200...
<input type="checkbox"/> Excepted	10.70.24...		OpenSSH Privilege Separation Monitor Weakness	tcp	22	■■■■■	CVE-200...
<input checked="" type="checkbox"/>	10.70.24...		OpenSSH X11 Cookie Local Authentication Bypass Vulnerability	tcp	22	■■■■■	CVE-200...
<input type="checkbox"/>	10.70.24...		AJP (Apache JServ Protocol) Service Detected	tcp	8009	■■■■■	
<input type="checkbox"/>	10.70.24...		OpenSSH X11 Session Hijacking Vulnerability	tcp	22	■■■■■	CVE-200...
<input type="checkbox"/>	10.70.24...		Apache Tomcat Denial of Service via Slow HTTP Requests	tcp	8080	■■■■■	CVE-201...

1 selected

- On the form that displays, enter descriptive information and choose how widely you want the exception to apply.

Vulnerability Exception ✕

Exception Name *

Description *

Duration Expiration Date

Forever

Apply to This one instance of this vulnerability for this one target (IP, Domain, URL)

All instances of this vulnerability in THIS scan configuration

All instances of this vulnerability in ALL subsequent scans(does not include currently running scans)

- To review and manage exceptions, see the **Exceptions** screen.

Scanning Scan Overview Configuration Reports Disputes **Exceptions** Notifications Account

notifications history available

Show Deleted Exceptions

Status	Exception Name	Vulnerability Name	Scan Name	IP	Port	Domain	Created ...	Expiration ...
<input type="checkbox"/> Enabled	Test-0309	Remote Access Service Detected	Any	10.70.244.46	Any		2015-03-10	2015-03-20
<input type="checkbox"/> Enabled	This Field Cannot Hold More than ...	Cisco SSH Denial of Service Vuln...	IVS-MixTargetTypeRegressionTest	Any	Any		2015-03-10	
<input type="checkbox"/> Enabled	All Instances of this vulnerability i...	Cisco IOS IPv4 Denial of Service ...	IVS-MixTargetTypeRegressionTest	Any	Any		2015-03-10	2015-06-10
<input type="checkbox"/> Enabled	All Instances of this vulnerability i...	Cisco IOS Secure Shell Server V...	Any	Any	Any		2015-03-10	2015-06-10
<input type="checkbox"/> Enabled	test-0310	Cisco SSH Denial of Service Vuln...	Any	10.70.33.12	Any		2015-03-11	2015-04-06
<input type="checkbox"/> Enabled	This is the test for Exception Nam...	Cisco SSH Denial of Service Vuln...	Any	10.70.33.12	Any		2015-03-11	2015-03-14
<input type="checkbox"/> Enabled	This is the test for Exception Nam...	CISCO IOS H.323 Protocol Imple...	Any	10.70.33.12	Any		2015-03-11	2015-03-14

Page 1 of 1

Details ✕

Summary 🔄

Scan Name	IP	Port	Domain	Scan Date
IVS-MixTargetTypeRegressionTest	10.70.33.12	0		2015-03-06
IVS-MixTargetTypeRegressionTest	10.70.33.12	0		2015-03-06
IVS-	10.70.33.12	0		2015-03-06

Displaying 1 to 3 of 3