

# **TrustKeeper Scanning FAQ's**

# 1. Why am I being required to scan my system?

The Payment Card Industry Data Security Standard (PCI DSS) states that any device involved in the processing, transmission, or storage of credit card holder data over the Internet, or any device which may be connected to such a system must have a passing vulnerability scan once every quarter.

Your service in TrustKeeper PCI Manager is set up to perform scans once a month. This schedule allows merchants to maintain compliance in case PCI failing vulnerabilities are detected.

For more information, please visit the PCI Security Standards website for the requirements mandated by the PCI Security Council at <u>www.pcisecuritystandards.org/</u>

## 2. How long will the scan take?

When you schedule a scan, it will be placed in the queue. When it reaches the top of the line, it will begin scanning. The duration of the scan itself depends on many factors, which makes predicting the exact duration of a scan difficult. However, if you are scanning a single IP, your scan should take just a few hours.

Some of the variables that can affect scan duration include:

- The IP address only. (If it's a firewall blocking everything, it may last just a couple of minutes. If it's a web server and is more responsive, it may take more time.)
- The response time of the system being scanned.
- The overall congestion in the network.

You do not need to be logged into TrustKeeper PCI Manager or even at your computer while the scan runs. Your computer needs to be on during the scan, but the scan will operate entirely in the background, and should not impact your day-to-day business at all. If you have any concerns or experience any problems while scanning, please contact Trustwave Support at 800-363-1621 or by email <u>support@trustwave.com</u> and we will gladly assist you further.

# 3. How do I find my external IP address for scanning? Does it change?

As you proceed through the Trustwave portal, the scan setup will walk you through finding the IP address and setting up a scanning profile. The external IP address is assigned to your router or server. There are two kinds of external IP addresses, dynamic and static. Most small businesses have a dynamic IP address. This means it will change from time to time, such as if your router was turned off and back on.

To verify the IP address has not changed and Trustwave is scanning the correct IP address, click on "Support" in the upper right of your Trustwave account, then click "User Information." Your IP address will be shown based on the internet connection you are currently using.

If the IP address has changed, please visit the Scan Setup section to remove the old IP address and create a new profile for the new IP address. Schedule a new scan to run by editing the scan schedule.

Copyright © 2014 Trustwave Holdings, Inc. All rights reserved.



## 4. Can I add multiple IP addresses or domain names to my scans?

Yes. PCI requirements mandate that any websites or IP addresses involved in the storage, processing, or transmission of cardholder data *under your control* must be scanned.

TrustKeeper PCI Manager will not allow you to enter IP addresses that are not externally accessible. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks:

10.0.0.0 --- 10.255.255.255 (10/8 prefix) 172.16.0.0 --- 172.31.255.255 (172.16/12 prefix) 192.168.0.0 --- 192.168.255.255 (192.168/16 prefix)

If you are attempting to add a domain ending with ".gov," you will be unable to do so. Please determine if the .gov website is actually in scope. If it is, please contact Trustwave Support at 1-800-363-1621 or by email at <a href="support@trustwave.com">support@trustwave.com</a> to have it added. If it's not in scope, there is no need to add the domain to your scan.

## 5. Will the scan have negative impacts on my infrastructure?

The TrustKeeper scan is meant to provide a non---intrusive, external vulnerability scan. You may experience some speed reduction on your Internet connection while this scan occurs (because the scan will use a portion of your available bandwidth while the scan is running), but it should not affect your infrastructure or cause any devices to stop responding. If you still have concerns we recommend scheduling your scan for a date when your infrastructure is not likely to be in heavy use.

#### 6. How can I reschedule a scan?

In order to reschedule a scan, please begin by logging into your TrustKeeper PCI Manager account. Once you are in your account click "Setup" located in the center of the screen next to the PCI Network Vulnerability Scan.

In the page that loads you should see a box labeled "Edit Schedule." Then choose the day you would like to run your scan and click "Save".

# 7. What should I do if I do not understand the scan report?

We suggest consulting an IT professional familiar with your system. If you happen to be a small business using a router, consider contacting your internet service provider.

If these methods do not provide a resolution, please contact our support center. While our analysts cannot provide guidance in any changes to your system, they may find alternative options for you to seek out.



## 8. Why did my scan receive a 'fail' result? What should I do?

To understand why your TrustKeeper vulnerability scan was non--compliant, consult your latest scan report. Simply click the "Scanning" link on the top of the screen once logged into TrustKeeper PCI Manager.

Click on the "PDF Report" to see the complete scan report. This details all of the vulnerabilities found within

your network environment. A detailed description is provided for each, along with a column to the right labeled "Remediation" with recommendations to help you take action to fix it. The description may contain additional reference links that may be helpful in troubleshooting the issue.

# Only vulnerabilities with a red box with the letters "PCI" in the score column affect your compliance status.

Once these issues are corrected, you may initiate a new scan using the "Scan Now" link on the Scan Setup page to clear the non--compliant findings from your report.

## 9. My scans were passing for a long time, but now they are failing? What happened?

First, confirm your external IP address has not changed. Many small businesses have a dynamic IP address that is consistently changing – due to this you may be scanning an old or outdated IP. You'll need to update your IP in the scan setup section of your dashboard.

If you have checked your IP address and it has not changed, then it is possible that Trustwave has discovered a new vulnerability – as we are continually adding new tests as new vulnerabilities arise. Take a look at your PDF scan report and review the vulnerabilities details. You may need to consult with an IT professional familiar with your system. Then, make the necessary changes and run a rescan.

#### 10. My scan failed because of Scan Interference, what do I do?

Please whitelist the Trustwave IP addresses (204.13.201.0/24 and 64.37.231.0/24) where the scan is originating, Whitelisting allows the scan to run normally on your network while maintaining your system security. Your IT professional or Internet Service Provider should be able to assist.

We recommend ensuring that any active defense measures likes IPS (Intrusion Prevention System), WAF (Web Application Firewalls), SYN Flood Protection, etc. devices are configured to allow our connections. IPS devices or modules should be set to allow our scanners' source IP addresses (204.13.201.0/24 and 64.37.231.0/24), but we do not recommend whitelisting these addresses on your firewall (only whitelist us on the IPS module on the firewall, if there is one). Many IPS devices will block the scanner's packets because they send so many requests in a short amount of time, and some of those may be detected as suspicious or malicious since they are probing for possible vulnerabilities.



# 11. What if the scan appears to identify vulnerabilities that are not actually present in my environment?

If the TrustKeeper scanner has falsely identified a vulnerability that you believe does not actually exist on your system, then you should file a dispute against the vulnerability.

In order to dispute vulnerabilities, please begin by logging into your TrustKeeper PCI Manager account. Once you are in your account, click the "Scanning" link from the menu at the top of the screen. When that page loads, you should find a list of all vulnerabilities found. Click on the vulnerability you'd like to dispute. Click on the "Dispute Findings" button towards the top-left of the page.

In the next window that loads, select the category of the dispute from the drop down box, place a short description of the dispute in the "Title" field, and in the "Comment" field provide a detailed justification for why you believe this vulnerability should be disputed. Click "Save" when you are done. An engineer will then review the dispute and deny or accept the request. Please allow five business days for a response to a dispute.

Trustwave engineers do need to investigate each client's disputes manually which occasionally may cause a longer than 5 day turnaround timeframe.

## 12. What do I need to write in my dispute to get my scan to pass?

To receive a passing scan by dispute requires written explanations for each PCI level failing vulnerability. The explanation will need to include why the vulnerability found on your system will not allow an unauthorized party to access credit card data as that data is processed, transmitted or stored. This explanation needs to very specific information, such as providing full versions of the software and operating systems in use, configuration information, etc.

Dispute comments such as, "I do not understand why I failed" or "I feel these findings are false positives" cannot be accepted by the scan engineers to approve your scan. A detailed explanation must be provided.

The scan engineers will run a manual investigation based on the information you file in your dispute.

#### 13. My dispute has been denied, what do I do next?

If your dispute has been denied, the engineer will provide further information under the "Dispute" tab towards the bottom of the screen within the scanning portion of your account. Click the "Denied" line and the information will be presented. The engineer may need more information or will provide further steps. You may resubmit a new dispute or simply provide additional information to be approved for a passing scan.

#### 14. Can I speak to someone in engineering regarding my dispute request?

Trustwave engineers are not available to accept phone calls to resolve scan vulnerabilities. However, for specific vulnerability questions, click the "Ask Support" button within the Scanning section of your TrustKeeper PCI Manager account to initiate email communication with Trustwave Vulnerability Scan support.