

SAINT®



ASV Portal

User Guide

Table of Contents

What is the SAINT ASV Portal?.....	4
Responding to PCI ASV Attestation Requirements.....	4
How Does the Portal Work?.....	4
Log in.....	4
User Options under the UserID.....	5
Profile.....	6
Two-factor Authentication.....	6
Change Password.....	6
Log Out.....	6
Help.....	6
Scan Tab.....	6
Step 1 - Targets.....	7
Selection Method.....	7
Step 2 – Compliance (Set ASV Options).....	8
Step 3 – Options (Additional Options).....	9
Step 4 – Schedule.....	10
Pre-scan Attestations.....	11
Scan Status.....	11
Delete a Scan.....	12
Email Notifications.....	12
Results Tab.....	12
Create Reports.....	13
ASV Attestations.....	14
Targets Running No Services.....	15
Scan Scope.....	15
Vulnerability Disputes.....	16
Customer Identity.....	18
Special Notes.....	19
Final Approval.....	20
Partner Portal and Customer Management Dashboard.....	21
Login.....	21
Manage Customers.....	22
New Customer.....	22
Edit Customer Profiles.....	24
Manage Customer Scans.....	24
Manage Scans.....	24
Manage Results.....	25

Logout	25
Need Further Help?.....	26
Technical Support	26
ASV Disputes and Attestation submissions	26
Security Services	26

What is the SAINT ASV Portal?

Cybersecurity is an overwhelming and complex subject for most small businesses. The highest risks to small business are often the internet-facing systems that host critical business systems such as company websites, shopping carts and the access points to internal networks. As a business, it is essential that you know where you are vulnerable and have information to take action to mitigate against risks to your business and your customer's sensitive information.

SAINT's ASV portal is designed as an easy-to-use cloud-hosted scanning service for businesses to quickly assess your Cardholder Data Environment (CDE) internet-facing systems for the types of vulnerabilities and risk exposures used by attackers to breach systems and steal your most valued information and identify issues that impact compliance with the Payment Card Industry's (PCI) Data Security Standards (DSS).

Responding to PCI ASV Attestation Requirements

In addition to running scans and viewing results in various report formats, the ASV portal also enables our customers to submit scan output to our SAINT ASV assessors for review and for Attestation of Scan Compliance (AoSC), to meet PCI requirement 11.3.2 and the ASV Program Guide. Users can also run scans proactively, on-demand, to assess Card Holder Data (CDE) environments in between quarterly attestation submissions to conduct continuous analysis and monitor the target environments for compliance throughout the license period.

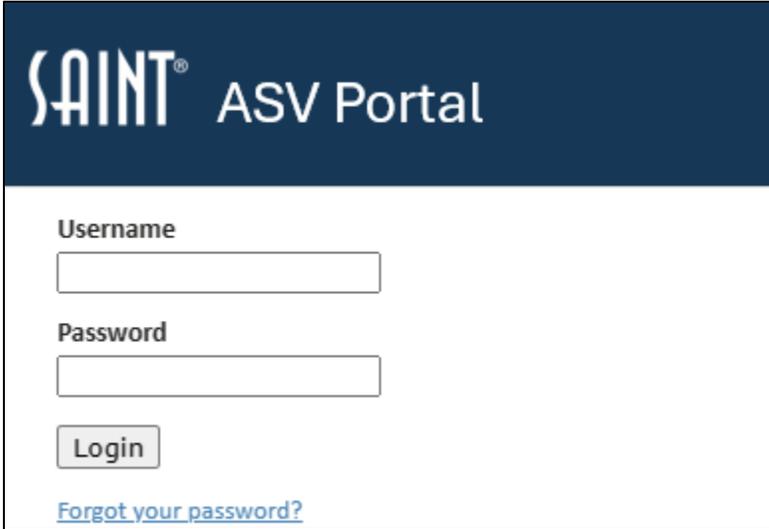
How Does the Portal Work?

This portal provides the same scanning power of our flagship product, SAINT Security Suite, but in a much more condensed set of scanning and reporting workflows. Behind the scenes, the engine conducts a scan of TCP, UDP, and RPC services on the target hosts. When the engine detects a service that has a history of possible security concerns (e.g., Web access to the password file), it performs a more detailed interrogation with vulnerability check probes that are updated on a daily basis. The results of the assessment are then made available through the reporting engine, using pre-designed report templates.

Log in

1. Open a browser window and navigate to <https://asv.saintcorporation.com>

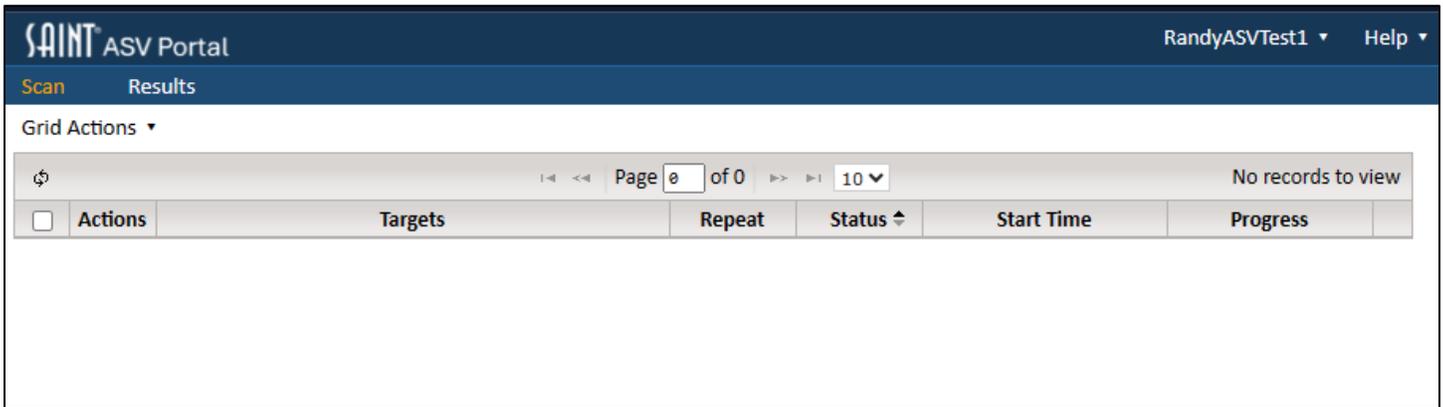
The first thing you will see is a login dialog box for the SAINT ASV portal.

The image shows a login dialog box for the SAINT ASV Portal. The header is dark blue with the SAINT logo and 'ASV Portal' text. Below the header, there are two input fields: 'Username' and 'Password'. A 'Login' button is positioned below the password field. At the bottom, there is a blue hyperlink that says 'Forgot your password?'.

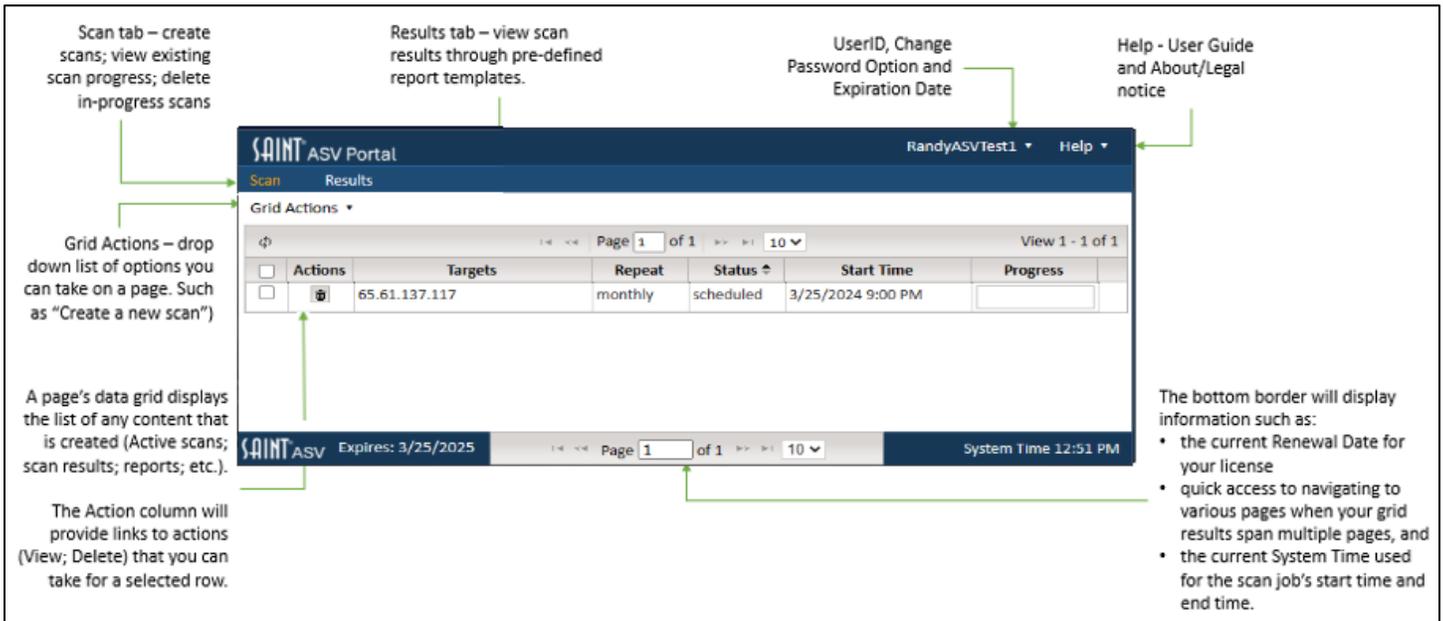
2. Enter your User ID and Password provided in your Welcome email when you purchased your license.
3. Click the *Login* button

Select the "Forgot your password?" hyperlink if you forgot or need to reset your password.

The system will authenticate your access, launch the portal and provide a web page to create Scan Jobs and manage scan progress, as shown below:



When you first log in, you will notice that the main section of the page is blank, with menu options to Scan and create and interact with Results. To ensure simplicity, the portal is designed to provide everything you need for quick scanning and management of scan results from these two pages.



The following provides an overview of each feature that was designed to support the PCI ASV scan, dispute, attestation and reporting processes.

User Options under the UserID

There are three (3) important options available to you under your UserID, displayed in the upper right corner of the portal:

The screenshot shows the SAINT ASV Portal interface. At the top, the user is logged in as 'RandyASVTest1' and has access to 'Profile' and 'Log Off' options. The main area displays the 'Results' tab with a 'Report Type' of 'PCI Executive' and a 'Format' of 'HTML'. Below this, there is a table with the following data:

Actions	Data Set	Targets
	Latest Scan	65.61.137.117
	Mon Mar 25 2024 9:28:44 PM	65.61.137.117
	Mon Mar 25 2024 11:45:34 AM	65.61.137.117

At the bottom of the page, the system time is 12:15 PM and the account expires on 3/25/2025.

Profile

This profile option, under the UserID, at the top right of the window, displays account and license information, to include your user account, the license expiration date, email address, and cell phone we have on file for your account. Note: If your account is expired, this option is disabled. You will be prompted to renew your account subscription.

Two-factor Authentication

To help secure your account, it is recommended that you turn on 2FA from the Profile option. Once it is turned on, you will be prompted to enter a six-digit verification code whenever you log into the portal, unless you previously checked “Don’t ask again on this device” when entering the verification code from the same device. You must provide a cell phone number before turning on 2FA in order to receive the verification codes.

Change Password

Select the “Change” hyperlink from the Profile option, to update/reset your account password.

Log Out

Select the “Log Off” hyperlink from the Profile option, to log you out of the SAINT ASV portal.

Help

Select the “Help” option from the top menu to access the complete User Guide, as well as a link to the “About” link that includes the product portal version, copyright notice, and a reference to the applicable US Government Commercial Computer Software License clause.

Scan Tab

Initiating a PCI ASV scan is done from the **Scan** tab. As shown below, creating a new scan is done by selecting the “Create Scan” option from the Scan page’s Grid Actions drop down menu.

SAINT ASV Portal RandyASVTest1 ▾ Help ▾

Scan Results

Grid Actions ▾
 Create Scan
 Delete Selected

Page 1 of 1 10 ▾ View 1 - 1 of 1

Actions	Targets	Repeat	Status	Start Time	Progress
<input type="checkbox"/>	65.61.137.117	monthly	scheduled	3/25/2024 9:00 PM	

SAINT ASV Expires: 3/25/2025 Page 1 of 1 10 ▾ System Time 1:03 PM

The screen will refresh to display the Scan creation wizard, as shown below. The wizard will display the current list of scan targets you have registered with your license, as well as Selection Methods for selecting from the Pick List (checkboxes) or free-form entry.

Create New Scan ✕

1 Targets
Select scan targets.

2 Compliance
Set ASV options.

3 Options
Additional Options.

4 Schedule
Select scan schedule and finish.

Step 1: Select Scan Targets

Selection Method: Target Pick List ▾

	Target
<input type="checkbox"/>	
<input type="checkbox"/>	65.61.137.117
<input type="checkbox"/>	New Target

Selected Target(s)

Page 1 of 1 10 ▾

Previous
Next
Finish

Step 1 - Targets

The list of available targets should be the same full list of targets you registered with your license or within the total number of scan targets that are licensed for the current ASV subscription period. The Target selection step provides the follow options:

Selection Method

- 1) Option 1: Target Pick List
 - a) Select from a "Target Pick List" of available targets
 - b) Click the checkbox for each host to be scanned. All selected targets will be added to the "Selected Target(s)" box.
 - c) Press the **Enter** key once all of your hosts have been entered.

- 2) Option 2: Free form target entry
 - a) Manually type the list of targets to be scanned.
 - b) Press the **Enter** key once all of your hosts have been entered.
- 3) Option 3: New Target
 - a) If this is the first time you have entered your target list or your target list includes any hosts other than the ones from your registered targets, you must certify that you have permissions to access and scan these new hosts.

The scan wizard will display the following *license and service agreement to attest that you have authorization to scan the new host(s)*.

Approve Added Targets ✕

I acknowledge and accept the condition that, if SAINT is used as the ASV, SAINT will share customer scan results with the PCI council, if requested, as specified in the ASV Compliance Test Agreement, Section 6.2: To the extent any data or other information obtained by Vendor relating to any Vendor Client in the course of providing Vendor Services [ie. PCI scanning and ASV services] is subject to any confidentiality restriction between Vendor and such Vendor Client, the applicable agreement containing such restriction (and in the absence of any such agreement, a separate written agreement between Vendor and such Vendor) must (i) permit Vendor to disclose such information to PCI SSC and/or its Members, as requested by the Vendor Client, (ii) to the extent any Member obtains such information in accordance with preceding clause 6.2(a)(i), permit each Member to disclose such information on an as needed basis to other Members and to such Members' respective member Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies and (iii) permit Vendor to disclose any such information as necessary to comply with its obligations and requirements pursuant to clause 3.6. Accordingly, notwithstanding anything to the contrary in clause 6.1(a), to the extent requested by a Vendor Client, PCI SSC may disclose Confidential Information relating to such Vendor Client and obtained by PCI SSC in connection with this Agreement to Members in accordance with this clause 6.2, and such Members may in turn disclose such information to their respective member Financial Institutions and other Members. Vendor hereby consents to such disclosure by PCI SSC and its Members. The confidentiality of any information provided to Members by Vendor or any Vendor Client is outside the scope of this Agreement and may be subject to such confidentiality arrangements as may be established from time to time between such Member, on the one hand, and Vendor or such Vendor Client (as applicable), on the other hand.

I certify that the address(es) 192.168.0.1, 192.168.0.2 belong to my organization or a related organization which has requested that they be scanned, and that I am authorized to request this security scan. I understand that any security scan could possibly cause instability in the host(s) that are scanned. I will hold SAINT Corporation blameless for any subsequent problems that may arise from this scan.

Your Name: Title: Organization:

Signature: [Click here to sign](#) Date: 3/26/2024 Account ID: RandyASVTest1

IMPORTANT: If you wish to INCREASE YOUR TARGET COUNT for this ASV service, contact your [Account Representative](#) or Service Provider, if your subscription was granted through a partner.

Click the **Next** button to move to the next step in setting up a scan

Step 2 – Compliance (Set ASV Options)

This Compliance (Set ASV options) step is specifically designed to support the Payment Card Industry (PCI) Approved Scanning Vendor (ASV) Attestation of Scan Compliance (AoSC) requirement. You have the option to run scans of your selected hosts, whenever you like, at whatever frequency you need to support your ongoing assessment of the vulnerabilities impacting your host environment. Additionally, this step configures the Scan to submit the scan results for Attestation of Scan Compliance (AoSC) by SAINT's ASV team.

IMPORTANT: Your SAINT ASV subscription includes support for one primary submission each quarter as well as a resubmission each quarter in the case where an initial scan resulted in a Failed result. This resubmission is provided to allow you time to remediate those issues, conduct a follow-up scan, and resubmit for AoSC during the same quarter.

Additional submissions, if required, may be purchased at an additional cost, by contacting your [Account Representative](#) or Service Provider, if your subscription was granted through a partner.

Create New Scan

1 Targets
Select scan targets.

2 Compliance
Set ASV options.

3 Options
Additional Options.

4 Schedule
Select scan schedule and finish.

Step 2: Set ASV options

Compliance Options

Request ASV Attestation of Scan Compliance

Previous Next Finish

By checking this box, your scan results will be assessed against the PCI ASV Program Guide’s metrics and standards; and adhere to vulnerability scanning requirements as defined by the latest PCI Data Security Standards (DSS), Requirement 11.3.2.

Click the **Next** button to move to the next step in setting up a scan

Step 3 – Options (Additional Options)

The SAINT scan process can be performed quickly just by selecting the target hosts and scheduling the scan. However, the following “Additional Options” are optional, and enable additional types of checks and/or use credentials to facilitate lower levels of access to system resources.

Create New Scan

1 Targets
Select scan targets.

2 Compliance
Set ASV options.

3 Options
Additional Options.

4 Schedule
Select scan schedule and finish.

Step 3: Additional Options

Scan Configuration Options

? Enable dangerous checks

? Windows domain admin Login

Password

? SNMP community string

Previous Next Finish

IMPORANT: These options will not be active for scans that are being submitted for ASV Attestation. All PCI-required scan configurations for submitted scans are controlled by the SAINT pre-configured ASV scan policy that adheres to the ASV Program Guide and PCI DSS Requirement 11.3.2.

The following describes each option and how to enable them during the scan setup process.

- **Enable dangerous checks** - SAINT's scan process includes an option to "Enable dangerous checks." If this option is enabled, SAINT will launch buffer overflow exploits which may yield more definitive results. This option may help SAINT eliminate false alarms by verifying the existence of certain vulnerabilities but can cause services on the target hosts to crash. If this option is not selected, SAINT will skip these dangerous tests.
- **Windows Domain Administrator** - To conduct the most thorough and accurate scan possible, SAINT gives you the option of authenticating to targets. Enter a valid Login and Password with administrative privileges on the domain. Authentication allows SAINT to access the registry and file attributes on the remote target. There are two benefits to authentication.
 - An authenticated scan can detect additional vulnerabilities, such as client vulnerabilities and missing hotfixes, which could not otherwise be detected by probing network services.
 - An authenticated scan is sometimes able to check for fixes whose presence could not otherwise be determined, thereby reducing false alarms.
- **SNMP Community** - The Simple Network Management Protocol (SNMP) runs on routers and switches, as well as some printers, servers, and workstations to communicate configuration and status information. SNMP access is controlled using *communities*. A *community string* identifies the community and can be thought of as the password for SNMP access.

Click the **Next** button to move to the next step in setting up a scan

Step 4 – Schedule

Scans can be performed immediately or scheduled to run at a defined date/time or scheduled intervals. For example, you may want to run a scan immediately to assess the current security posture of target hosts prior to submitting a scan for ASV Attestation. Then, once you've gone through that process and have determined your schedule for quarterly report, set up a recurring schedule to sync with your PCI reporting requirements.

The screenshot shows a web-based wizard titled "Create New Scan" with a close button in the top right corner. On the left side, there are four numbered steps in colored boxes: 1. Targets (green), 2. Compliance (green), 3. Options (green), and 4. Schedule (orange). The "Schedule" step is currently selected and highlighted. The main content area is titled "Step 4: Select Scan Schedule and Finish" and contains a "Scan Schedule" section. Under "Scan Schedule", there are radio buttons for "Immediately" (selected), "Once", "Weekly", "Monthly", and "Quarterly". Below these are input fields for "At" (with dropdowns for hour, minute, and AM/PM) and "On" (with a dropdown for day of the week). The text "(U.S. Eastern)" is displayed next to the AM/PM dropdown. At the bottom of the wizard, there are three buttons: "Previous" (disabled), "Next" (disabled), and "Finish" (active).

Click the **FINISH** button to start your scan now or scan on the selected Schedule

Pre-scan Attestations

Scans submitted for ASV attestation will enter our formal PCI ASV attestation process. As part of that process, the PCI ASV Program Guide requires scan customers to attest to specific questions regarding the scan environment, and permission granted to SAINT, as your ASV, to conduct the assessment.

If you checked the *Request ASV Attestation of Scan Compliance* box in Step 2 in the Scan wizard, then the Pre-scan Attestation form will appear after you click on the *Finish* button in the scan wizard. An example of this Pre-scan Attestation form is shown here.

After Checking the box for each required attestation question, a *Continue* button will be displayed.

Click *Continue* to complete the Pre-scan Attestation step and schedule your scan.

After the scan is complete, the PCI Attestation report will provide instructions on how to proceed – including processes for disputing results, entering declarations for special notes, validating the scope, etc.

Pre-scan Attestation

Please read the statements below and check the corresponding boxes if you agree. Your scan will be scheduled after all required boxes have been checked.

* = required

- * I attest that this scan includes all components which should be in scope for PCI DSS; any component considered out-of-scope for this scan is properly segmented from my cardholder data environment; and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete.
- * I understand that, in addition to providing all external-facing IP addresses, I must also supply all fully qualified domain names and other unique entryways into applications for the entire in-scope infrastructure, including domains for all web servers, domains for mail servers, domains used in name-based virtual hosting, and web server URLs to "hidden" directories that cannot be reached by crawling the website from the home page.
- * I understand that proper scoping of this external scan is my responsibility.
- * I understand that the scan results only indicate whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.
- * I attest that any intrusion detection system or intrusion prevention system will be configured to monitor and log but not act against the originating IP address of scanning activities.
- I attest that any infrastructure behind load balancers is synchronized in terms of configuration.
- * I attest that there is a communications path to my environment from the originating IP address of the scanning activities which is not filtered by active protection mechanisms.
- * I agree that SAINT shall be granted all necessary rights, licenses and other permissions necessary for SAINT to comply with its obligations and requirements pursuant to the PCI ASV Compliance Test Agreement ([PCI DSS Validation Requirements for Approved Scanning Vendors, Appendix A](#)).
- * I agree that any confidentiality restriction between myself and SAINT permits (a) SAINT to disclose obtained data to PCICo and/or its Members, and (b) each Member to disclose such information on an as needed basis to its respective member Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies.
- * I agree to make available any appropriate reviews and reports to monitor SAINT's compliance with required data protection handling practices as PCICo or its Members may reasonably request from time to time.

Scan Status

Click on the "Scan" tab to view a list of scheduled scans. From this page, you can identify what is being scanned, the frequency of the scan, and the current progress and status of your active and scheduled scans. Use the grid options at the bottom of the page to control the number of records you want to see per page, and to scroll through pages if the total number of scans exceed the number you've set per page (example: 10 per page).

The following shows examples of scan status for 1) scans currently scheduled, 2) the scheduled job has been queued up for execution, and 3) scan is running (2% complete).

SAINT ASV Portal RandyASVTest1 Help

Scan Results

Grid Actions

Page 1 of 1 View 1 - 4 of 4

Actions	Targets	Repeat	Status	Start Time	Progress
<input type="checkbox"/>	https://demo.saintcorporation.com		queued	3/26/2024 11:33 AM	
<input type="checkbox"/>	65.61.137.117		running	3/26/2024 11:26 AM	
<input type="checkbox"/>	https://demo.saintcorporation.com 65.61.137.117	quarterly	scheduled	3/26/2024 9:00 PM	
<input type="checkbox"/>	65.61.137.117	monthly	scheduled	4/25/2024 9:00 PM	

SAINT ASV Expires: 3/25/2025 System Time 11:33 AM

Delete a Scan

You may delete a scan from this page. To delete the scan, click on the applicable row's check box, and select the "Delete Scan" (Trash can) button.

Email Notifications

Once a scan has been completed, SAINT transmits an email notification of the scan's status, with a link to login and view the findings from the scan.

SAINT ASV scan completed for RandyASVTest1

 <support@saintcorporation.com>
To  Laudermilk, Randall D.

 We removed extra line breaks from this message.

Your SAINT ASV scan has completed. To view the results, please visit <https://asv.saintcorporation.com>, log in, and choose "Results".

  Reply  Reply A

Results Tab

Select the "Results" tab to view scan results for completed scans. The following shows an example of a completed scan for the one previously scheduled.

SAINT ASV Portal RandyASVTest1 Help

Scan Results

Report Type PCI Attestation ?

Page 1 of 1 View 1 - 3 of 3

Actions	Data Set	Targets
	Latest Scan	65.61.137.117
	Mon Mar 25 2024 9:28:44 PM	65.61.137.117
	Mon Mar 25 2024 11:45:34 AM	65.61.137.117

SAINT ASV Expires: 3/25/2025 System Time 11:40 AM

Create Reports

SAINT's ASV reporting capabilities provides many of the same reporting templates as in other SAINT products, such as SAINT Security Suite and SAINTcloud, to include the report templates required by PCI for the ASV attestation requirement.

To create a report for a selected scan:

1. Select the Report Type that best suits your needs.
For Trend Analysis reports only – Choose 2 or more scans that you wish to include in the trend analysis. Hosts and vulnerabilities will be tracked chronologically across the chosen scans, producing historical charts and status classifications.
2. Select the Report Format from the drop-down list of available formats.
 - HTML is usually the best choice for quick screen analysis. This report format uses Portable Network Graphic (PNG) images to graphically display pie charts and bar graphs. It also uses HTML frames to provide a linked table of contents for report navigation.
 - Frameless HTML is like the HTML format except that it does not provide a linked table of contents.
 - Simple HTML displays pie charts and bar graphs in-line, not as PNG images. However, the pie charts are only viewable on Internet Explorer.
 - PDF is the most often used and most convenient format to download and share with others.
 - XML is useful if the scan data is to be ingested into a 3rd party XML-enabled application.
 - Text is a useful alternative if you intend to view or ingest the scan data, in its unformatted form, into a 3rd party application.
 - CSV is the most often used format for simple text-based content usage or viewing in Microsoft Excel.
 - Tab-separated and comma-separated reports are useful for importing into documents, spreadsheets or databases. These formats are often useful with the Technical Overview report.
3. Click on the "Create Report" option, under the Actions column, for a selected scan to create and view the report.
4. The report will be generated and displayed in a separate browser tab.
5. You can view, print and save scan output from the displayed report. In most browsers, this is done by choosing *Save As* under the **File** menu.

Adobe Acrobat also supports these actions from within the browser window, as shown in the following example:

Contents

- Part 1. Scan Information
- Part 2. Component Compliance Summary
- Part 3a. Vulnerabilities Noted for each Component
- Part 3b. Special Notes to Scan Customer by Component
- Part 3c. Special Notes - Full Text
- Part 4a. Scope Submitted by Scan Customer for Discovery
- Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)
- Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

SAINT®

ASV Scan Report Executive Summary

Report Generated: March 14, 2024

Part 1. Scan Information

Scan Customer Company: ASV Company: SAINT Corporation
 Scan Date: March 1, 2024 Scan Expires: March 1, 2025

Part 2. Component Compliance Summary

Host Name	PCI Compliant?
	FAIL

Part 3a. Vulnerabilities Noted for each Component

Component:Port	Vulnerability / Service	CVE	PCI Severity	CVSS Base Score	PCI Compliant?	Exceptions, False positives, or Compensating Controls Noted by the ASV for this Vulnerability
mail.saintcorporation.com:22	OpenSSH 3.1p1 is vulnerable	CVE-2003-0693	high	10.0	PASS	DoS vulnerabilities do not affect PCI compliance
mail.saintcorporation.com:22	OpenSSH 3.1p1 is vulnerable	CVE-2002-0640	high	10.0	PASS	DoS vulnerabilities do not affect PCI compliance
mail.saintcorporation.com:22	OpenSSH 3.1p1 is vulnerable	CVE-2002-0639	high	10.0	PASS	DoS vulnerabilities do not affect PCI compliance
mail.saintcorporation.com:21	possible vulnerability in wu-ftpd 2.6.2	CVE-2004-0185	high	10.0	FAIL	
mail.saintcorporation.com:21	possible vulnerability in wu-ftpd 2.6.2	CVE-2003-0466	high	10.0	FAIL	
mail.saintcorporation.com:443	Arhilla 0.1.6.1 is vulnerable	CVE-2002-0548	high	7.5	FAIL	
mail.saintcorporation.com:443	Arhilla 0.1.6.1 is vulnerable	CVE-2002-0549	high	7.5	FAIL	Cross-site scripting is an automatic failure
mail.saintcorporation.com:80	Nagios negative content length overflow	CVE-2006-2489	high	7.5	FAIL	
mail.saintcorporation.com:22	OpenSSH 3.1p1 is vulnerable	CVE-2002-0575	high	7.5	PASS	DoS vulnerabilities do not affect PCI compliance
mail.saintcorporation.com:22	OpenSSH 3.1p1 is vulnerable	CVE-2003-0682	high	7.5	PASS	DoS vulnerabilities do not affect PCI compliance
mail.saintcorporation.com:22	OpenSSH 3.1p1 is vulnerable	CVE-2003-0695	high	7.5	PASS	DoS vulnerabilities do not affect PCI compliance

ASV Attestations

If you requested an ASV Attestation of Scan Compliance (AoSC) in Step 2 of the wizard when you created your scan, there are several requirements you must satisfy before the attestation can be issued.

Complete the following steps after the scan completes to fulfill these requirements:

1. Navigate to the *Results* tab and choose the *PCI Attestation* report type from the drop-down menu.

SAINT® ASV Portal RandyASVTest1 ▾ Help ▾

Scan **Results**

Report Type **PCI Attestation** ▾ ?

Page 1 of 1 10 ▾ View 1 - 4 of 4

Actions	Data Set ▾	Targets
	Latest Scan	https://demo.saintcorporation.com
	Tue Mar 26 2024 11:54:28 AM	65.61.137.117
	Mon Mar 25 2024 9:28:44 PM	65.61.137.117
	Mon Mar 25 2024 11:45:34 AM	65.61.137.117

SAINT ASV Expires: 3/25/2025 Page 1 of 1 10 ▾ System Time 1:45 PM

2. Click on the *Create Report* button under the Actions column for the selected scan.
3. SAINT will evaluate the selected scan and determine if there are any further actions needed to obtain the completed attestation report. In most cases, there will be actions required before the reports can be generated, as shown below:

Post Scan ASV Attestation Dataset: current

🔗 ⚙️ Get Attestation 📄 Feedback Form

Actions	Status ▾	Requirement	Instructions
	X	Was pre-scan attestation submitted?	Run the scan again, and check <i>request ASV attestation of scan compliance</i> before running the scan.
	X	Did scan include all targets which belong in scope?	Run the scan again including www.saintcorporation.com , mx1-us1.ppe-hosted.com , mx2-us1.ppe-hosted.com , or attest that they are out of scope .
	X	Did all scan results pass?	Go back and view the PCI Detail report to find out which vulnerabilities caused failure. You may fix the vulnerabilities and re-scan, or dispute the results .
	X	Was identity information provided?	Provide the customer identity information .
	X	Were results approved by certified ASV staff?	After all of the above are green, submit results for approval.
	✓	Were all targets successfully scanned?	
	✓	Were declarations provided for special notes?	

🔗 ⚙️ Get Attestation 📄 Feedback Form

- For each row of the checklist which has a red X in the Status column, follow the instructions in the Instructions column. Click on the wrench icon in the Actions column or the appropriate hyperlink in the Instructions column to complete each required task.
- See the following sections for information about the most commonly listed requirements:

Targets Running No Services

If the scan detected one or more targets with no listening services, you must confirm that this is the correct result, and not indicative of a scan malfunction. If this is the correct result, click on the action button beside *All targets successfully scanned* or click on the *attest that the target runs no listening services* hyperlink, check the box, and submit the form.

Target Returned no Results ✕

192.0.2.12 returned no results.

I attest that, to the best of my knowledge, the targets specified above have no known listening services, and the lack of results from those targets does not indicate a scanner or network malfunction.

Scan Scope

The PCI DSS requires scanning of all externally accessible system components owned or utilized by the scan customer that are part of the cardholder data environment or may provide access to the cardholder data environment. Although proper scoping is the responsibility of the scan customer, the ASV is required to report any potential scoping discrepancies and confirm with the customer that they are out of scope. If potential scoping discrepancies are found, click on the action button beside *Scan included all targets which belong in scope* or on the *attest that they are out of scope* hyperlink. This displays a table containing information about each scoping discrepancy. If each of the listed components are truly out of scope, check the box and submit the form.

Related Hosts ✕

The scan discovered the following hosts which are related to scanned targets but which were not scanned.

Host	Referrer	Relationship
192.0.2.11	192.0.2.11	This host was included in a previous scan but omitted from this scan.
mail.example.com	www.example.com	This host is the mail exchanger for the primary target's domain.

I attest that the hosts specified above are not in scope for PCI DSS, and are properly segmented from my cardholder data environment.

Vulnerability Disputes

If vulnerabilities which cause PCI failure are detected, you may either remediate the vulnerabilities and run the scan again or dispute the failing vulnerability findings. A vulnerability may be disputed for the following reasons:

1. False positive – You may dispute the vulnerability if you believe the vulnerability does not actually exist on the system.
2. Compensating controls – You may dispute the vulnerability if there is an acceptable compensating control in place which eliminates the risk of the vulnerability.
3. Incorrect CVSS score – You may dispute the vulnerability if you believe the CVSS score is incorrect.

Follow these steps if you choose to dispute a finding:

1. From the “Post Scan ASV Attestation” table, click on the Actions button beside *All scan results pass* or the *Dispute the results* hyperlink.
2. Click on the New Dispute tab.

Disputes ✕

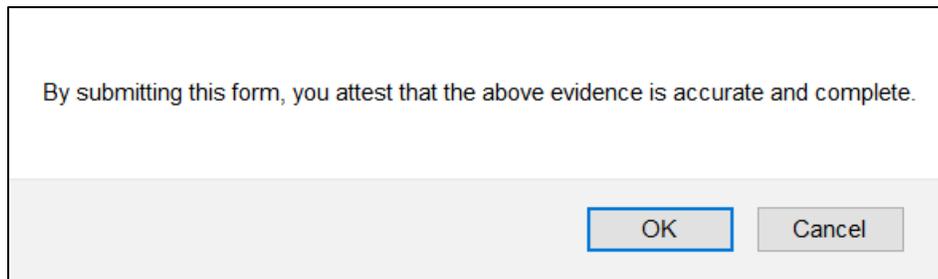
Existing Disputes
New Dispute

⚙ + Dispute Selected
Page 1 of 1
13
View 1 - 9 of 9

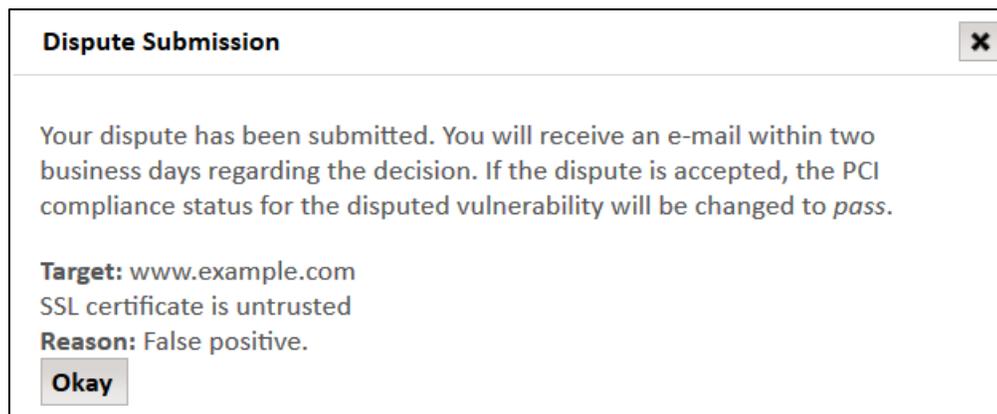
	Actions	Target ↕	Vulnerability
<input type="checkbox"/>			
<input type="checkbox"/>	+	www.example.com	SSL certificate is untrusted
<input type="checkbox"/>	+	www.example.com	vulnerable Apache version: 2.4.6
<input type="checkbox"/>	+	www.example.com	server is susceptible to BEAST attack
<input type="checkbox"/>	+	www.example.com	Web server allows cross-site tracing
<input type="checkbox"/>	+	www.example.com	web server autoindex enabled
<input type="checkbox"/>	+	www.example.com	Server supports TLS 1.0 protocol
<input type="checkbox"/>	+	www.example.com	SSL certificate subject does not match target
<input type="checkbox"/>	+	www.example.com	SSL/TLS server supports RC4 ciphers
<input type="checkbox"/>	+	www.example.com	vulnerability in OpenSSL 1.0.2k

⚙ + Dispute Selected
Page 1 of 1
13
View 1 - 9 of 9

3. Click on the Dispute button (plus icon) beside the vulnerability that you wish to dispute or check the rows corresponding to the vulnerabilities you wish to dispute and click on *Dispute Selected*. If the vulnerability you are looking for does not appear on the first page, use the pager buttons at the top and bottom of the grid to page through the vulnerabilities, or enter terms into the filter boxes at the top of the columns to search for the vulnerability.
4. Complete and submit the Create Dispute form. Include a detailed explanation and/or evidence that supports your claim that the vulnerability should not cause PCI failure. For example, if the vulnerability finding is a false positive resulting from backported fixes in Linux packages, you may want to include a screen shot which shows the installed package version.



5. Click the *OK* button to attest that the submitted evidence is accurate and complete.
6. SAINT will transmit a message informing you that the dispute has been submitted to the ASV staff.



7. When the ASV staff has made a decision regarding the dispute, you will receive an e-mail notification informing you of the result. The result will be one of the following:
 - **Approval** – The vulnerability status is changed to Pass, and the ASV’s reason for approving the dispute will appear in the Exceptions column of the ASV Executive report. This text cannot be modified by the customer.
 - **Denial** – The vulnerability status remains unchanged. The ASV’s reason for denying the dispute is provided in the e-mail notification. The dispute cannot be modified, however, a new dispute for the same vulnerability can be created. Appeals may be sent to support@saintcorporation.com. Appeals should *not* be sent to the PCI SSC.
 - **Request for more evidence** – The ASV requires further information or evidence in order to make a decision regarding the dispute. See the next paragraph for information on modifying your dispute.

The following steps describe how to check the status or modify a dispute you’ve already submitted:

1. From the “Post Scan ASV Attestation” table, click the Action button beside *All scan results pass* or the *dispute the results* hyperlink.
2. Click on the Existing Disputes tab. The status of each existing dispute will be one of the following:
 - **Open** – The dispute is being reviewed by ASV staff.
 - **Pending** – The ASV staff is waiting for the customer to provide additional evidence.
 - **Accepted** – The dispute has been accepted.
 - **Denied** – The dispute has been denied.

The screenshot shows a web interface titled "Disputes" with a close button (X) in the top right corner. Below the title are two tabs: "Existing Disputes" (active) and "New Dispute". The main area contains a table with a header row: "Actions", "Status", "Targets", and "Vulnerabilities". Above the table is a pagination bar showing "Page 1 of 1" and "View 1 - 3 of 3". Below the table is another identical pagination bar. The table has three rows of data:

Actions	Status	Targets	Vulnerabilities
	accepted	• www.example.com	• vulnerability in OpenSSL 1.0.2k
	open	• www.example.com	• SSL certificate is untrusted
	pending	• www.example.com	<ul style="list-style-type: none"> • vulnerable Apache version: 2.4.6 • server is susceptible to BEAST attack • Server supports TLS 1.0 protocol • SSL certificate subject does not match target • SSL/TLS server supports RC4 ciphers

3. Find the desired dispute on the grid. If it doesn't appear on the first page, use the pager bar at the top or bottom of the grid to page through the disputes, or use the filter boxes at the top of each column to search for the desired dispute.
4. To view the activity regarding a dispute, click on the *Log* button (notebook icon) under the *Actions* column for the desired dispute.
5. *For pending disputes only:* Click on the *Edit* button (pencil icon) to open a form allowing you to modify the dispute or upload additional evidence. This form is similar to the form you originally used to create the dispute. Submitting this form will change the dispute status back to *Open*.

Customer Identity

All ASV scans require information about the scan Customer in order to complete the Attestation of Scan Compliance reports. Click on the Action button for the Requirement that asks: “Was Identity information provided?” or click on the “*Provide the customer identity information*” hyperlink under the Instructions column.

Complete all information requested in the form, as shown below:

Customer Identity ✕

Please provide the following contact information for the scan customer.

Name: **Address:**

Title: **City:**

Company: **State:**

Phone: **Zip Code:**

E-mail: **Country:**

URL:

Special Notes

The ASV Program Guide specifies that certain findings be documented in the ASV Executive report as Special Notes. These are findings which don't always constitute a failure but still require a declaration from the Customer to assure the ASV that they do not expose the Cardholder Data Environment (CDE) to any unnecessary risk.

Perform the following steps to view the special notes and enter required declarations:

1. Click on the Action button for the *"Declarations provided for special notes"* or on the corresponding hyperlink.
2. SAINT will display the scan results, by target, that require input for the special notes, as shown below:

PCI Special Notes ✕

Page 1 of 1 10 View 1 - 3 of 3

Actions	Status	Target	Special Note
	X	192.0.2.9	Remote access ports: 443 (web admin)
	X	192.0.2.9	Web server allows index display
	X	192.0.2.9	Embedded links detected: www.google-analytics.com, fonts.googleapis.com, ajax.googleapis.com

Page 1 of 1 10 View 1 - 3 of 3

3. Click on the *Edit* button (pencil icon) for each special note that contains a red **X** in the Status column.
4. SAINT will display a dialog, providing further instructions and a form to enter the declaration.

Special Note Declaration ✕

IP Address
192.0.2.9

Noted Item
Remote access ports: 443 (web admin)

Due to increased risk to the cardholder data environment when remote access software is present, 1) justify the business need for this software to the ASV and confirm it is implemented securely, or 2) confirm it is disabled/removed. Consult your ASV if you have questions about this Special Note.

▾

Declaration that software is implemented securely (minimum 50 characters)

5. Choose the appropriate option from the drop-down menu and enter a declaration which satisfies the instructions.
6. Click on the **Submit** button to save your information.

Repeat the previous two steps until all rows in the special notes grid have a green X check mark.

PCI Special Notes ✕

Page 1 of 1 10 View 1 - 3 of 3

Actions	Status	Target	Special Note
	✓	192.0.2.9	Remote access ports: 443 (web admin)
	✓	192.0.2.9	Web server allows index display
	✓	192.0.2.9	Embedded links detected: www.google-analytics.com, fonts.googleapis.com, ajax.googleapis.com

Page 1 of 1 10 View 1 - 3 of 3

7. Click the *Close* button once all declarations have been completed and the status is green for all rows.

Final Approval

Once all rows in the “Post Scan ASV Attestation” table have green checkmarks, the last action is to “Submit results for approval” by selecting the hyperlink under the Instructions column for the Requirement: “Results approved by certified ASV staff”, as shown below:

Post Scan ASV Attestation			Dataset: current
Actions	Status	Requirement	Instructions
	X	Results approved by certified ASV staff.	Submit results for approval.
	✓	Pre-scan attestation submitted.	
	✓	All targets successfully scanned.	
	✓	Scan included all targets which belong in scope.	
	✓	All scan results pass.	
	✓	Identity information provided.	
	✓	Declarations provided for special notes.	

Once the ASV staff has reviewed your scan report, you will receive an e-mail notification of the decision. There are two possible outcomes:

- **Denied** – The ASV staff did not accept the scan report. The explanation for the denial can be found in the e-mail notification as well as in the “Post Scan ASV Attestation” table. If the explanation warrants it, you may go back to the “Post Scan ASV Attestation” table and make corrections, and then re-submit the report for approval.
- **Accepted** – The ASV staff accepted the scan report. Navigate to the “Post Scan ASV Attestation” table and click on the buttons at the bottom of the table to download all required reports by selecting the “Get Attestation” option and “ASV Feedback Form”, as shown in the following example:

Post Scan ASV Attestation			Dataset: current
Actions	Status	Requirement	Instructions
	✓	Pre-scan attestation submitted.	
	✓	All targets successfully scanned.	
	✓	Scan included all targets which belong in scope.	
	✓	All scan results pass.	
	✓	Identity information provided.	
	✓	Declarations provided for special notes.	
	✓	Results approved by certified ASV staff.	
Get Attestation Feedback Form			

Partner Portal and Customer Management Dashboard

For our partners that onboard Customers to SAINT’s ASV service, there is a separate Dashboard that provides a feature to submit New Customer requests to the SAINT Sales team, provides the capabilities to manage those customer’s access to their ASV portal account, and access those customers’ scan status, attestation dates/status, renewal dates and access their accounts to assist them, as needed, in the execution of the scan, attestation and reporting processes. The following describes this dashboard in more detail.

Login

Navigate to https://asv.saintcorporation.com/cgi-bin/secure/partner_portal.cgi from a new browser window, and Enter the UserID and Password provided to you by your SAINT Account Rep or Partner Manager.

SAINT ASV Partner Portal

Login

Password

The login process will authenticate your access and display the SAINT ASV Partner Portal Dashboard (Home), as illustrated below:

The screenshot shows the SAINT ASV Portal interface. At the top, there is a navigation bar with 'Home', 'New Customer', and 'Logout' links. Below this is a 'Demo Partner SAINT ASV Portal' header. A search bar with a 'Submit' button is present. The main content area features a table with the following columns: Actions, ID, Customer, Latest ASV Scan, Previous Scan, Previous Scan, Previous Scan, AoSC Expires, and Next Scan. A single row of data is visible for 'RandyASVTest1' under the 'Customer' column, with 'SAINT Test' in the adjacent cell. Below the table, it says 'Page 1 of 1'.

From the Home screen, partners can see all SAINT ASV customers that they manage or have been onboarded to SAINT through a channel partnership. If the list of customers is large, then individual customers may be found by using the Search box at the top of the page.

The partner table provides information about each customer, such as the customer’s unique ID and Customer name, and information about their PCI Attestation status. Additionally, the “AoSC Expires” column provides you with the expiration/renewal date for their customer, based on their annual subscription to the SAINT ASV service.

Manage Customers

New Customer

Partners can create new Customers directly from the SAINT ASV partner portal, by selecting the “New Customer” menu option. Once selected, the page redirects you to the “Create New Customer” form, as shown below:

Create New Customer

Login:

Password:

Confirm Password:

Company/Organization:

Email Address:
Comma-separated list of all e-mail addresses which should receive notifications for this account. May include yourself, the customer, or both.

Target Addresses:
Comma-separated list of IP addresses, ranges, or URLs, if known. Example: 192.0.2.1, 192.0.2.5-192.0.2.10, http://example.com

Target Limit:
Maximum number of targets that user can scan.

New account notification?

- Login – Enter the UserID to be used by the customer to log into their ASV portal account.
- Password – Enter a password for the customer account. The password should be at least 8 characters and include an upper and lower-case character, at least 1 special character, and at least 1 number. For convenience, you may also create a randomly generated password, by selecting the “Generate Random” button.
- Confirm Password – Enter the same password as entered in the Password field.
- Company/Organization – Enter the name that the customer wishes to use as their Company or Organization, as it applies to the PCI ASV process.
- Email address – This email address list is used to notify partners and customers of actions performed in the portal and when scans have been completed. When submitting a new customer/prospect for SAINT Sales, the default email address for this submission is you, as the partner. Once a quote has been generated and approved by the prospective customer, partners may use the “[Edit](#)” option, for the new customer, from the partner portal, to update the email addresses for the customer.
- Target Addresses – This list is the comma-separated list of targets to be applied to the customer account, to support scanning, dispute workflows, SAINT Attestation of Scan Compliance (AoSC) and PCI ASV reporting. This list does not include other non-ASV-related scan targets that a customer may wish to include in their local scanning requirements. In those cases, SAINT can support those requirements with other scan products and services. Contact your SAINT account representatives for more information.
- Target Limit – In cases where the customer may not know the specific scan targets, by IP, URL, etc., or cases where the specific addresses may change, you can enter the total number of targets to be supported by SAINT, for the ASV service.
- New account notification – Click this option if you wish to have an email notification, once you have submitted the “New Customer” request.

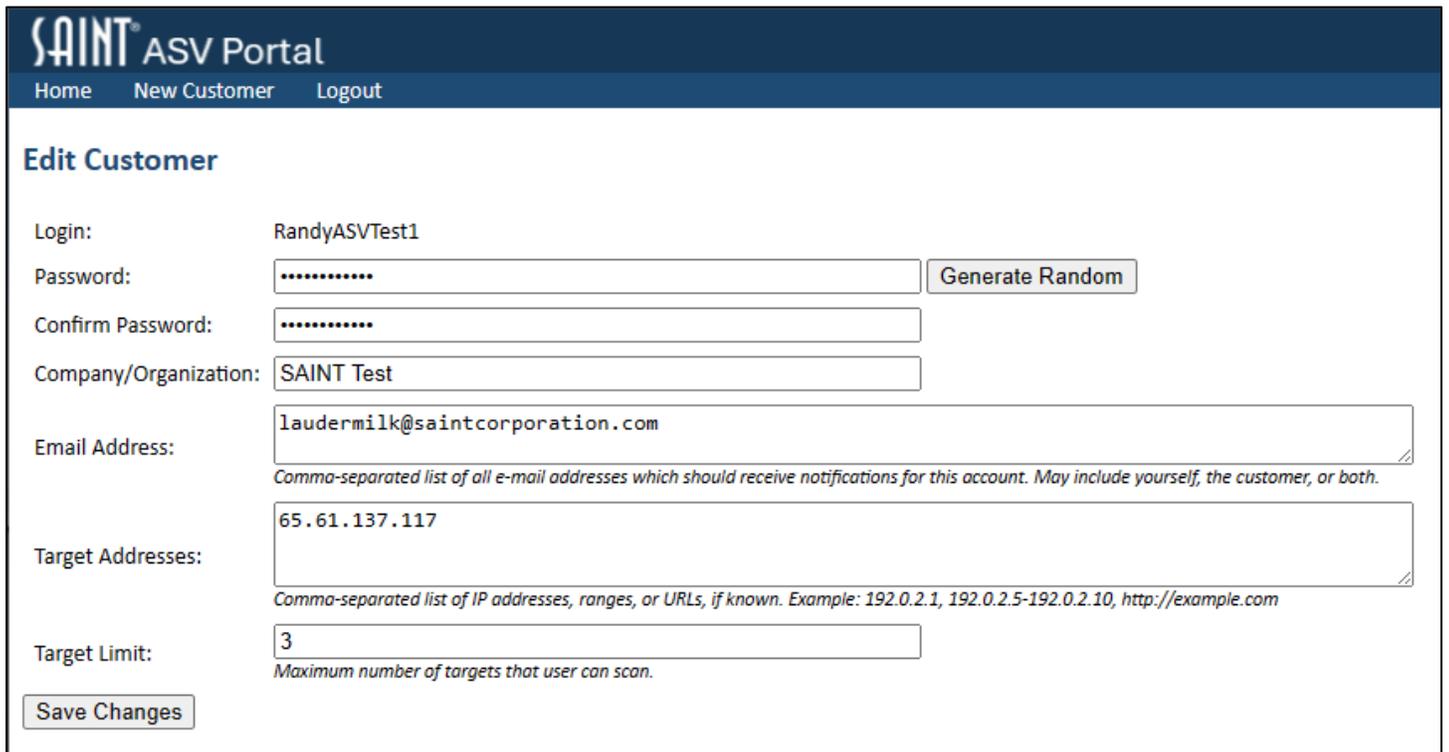
Click the “Create Customer” button to complete this process and submit the request to SAINT Sales.

The screen will provide a confirmation message that the customer submission has been completed.

Select the “Create Another Customer” hyperlink to create another customer or select the “Return to Customer List” hyperlink to return to the partner Home page.

Edit Customer Profiles

Select the “Edit” option for a selected Customer to take actions such as password changes, Company/Organization updates, email contact updates and scan Target information. Note that passwords may be changed manually or using a password generator, using the “Generate Random” button.



The screenshot shows the SAINT ASV Portal interface. At the top, there is a navigation bar with links for Home, New Customer, and Logout. Below this is the 'Edit Customer' section. The form contains the following fields and controls:

- Login:** RandyASVTest1
- Password:** A text box with masked characters (dots) and a 'Generate Random' button.
- Confirm Password:** A text box with masked characters (dots).
- Company/Organization:** SAINT Test
- Email Address:** laudermilk@saintcorporation.com. Below the text box is a note: "Comma-separated list of all e-mail addresses which should receive notifications for this account. May include yourself, the customer, or both."
- Target Addresses:** 65.61.137.117. Below the text box is a note: "Comma-separated list of IP addresses, ranges, or URLs, if known. Example: 192.0.2.1, 192.0.2.5-192.0.2.10, http://example.com"
- Target Limit:** 3. Below the text box is a note: "Maximum number of targets that user can scan."

A 'Save Changes' button is located at the bottom left of the form.

Once changes are made, select the “Save Changes” button. The screen will provide a confirmation message that the customer information has successfully been modified.

Select the “Return to Customer List” hyperlink to return to the partner Home page.

Manage Customer Scans

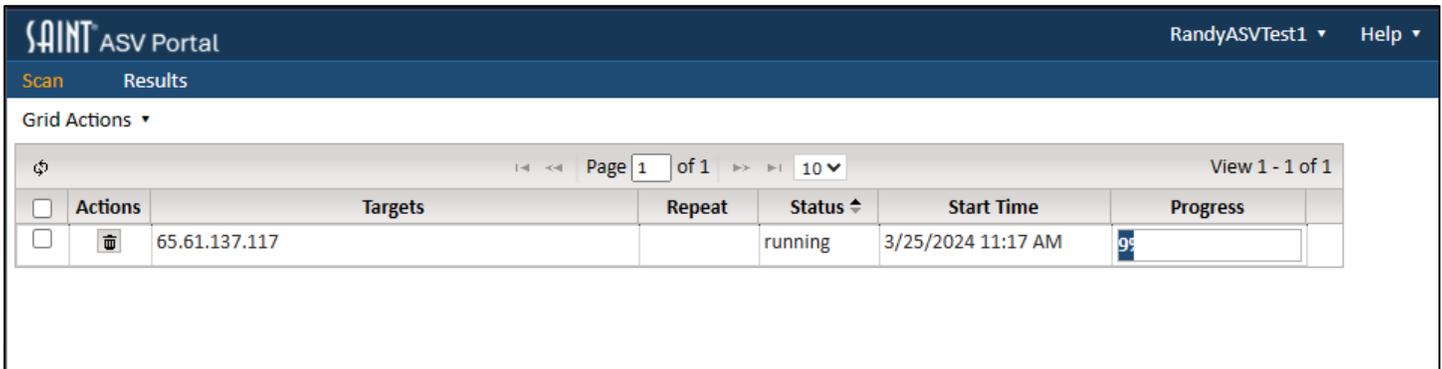
Partners may also take actions, on behalf of the customer, by selecting options from the “Actions” column. Each of these options are described below.

IMPORTANT: By selecting the Scans or Results option for a Customer, a new browser window will be opened, to enable you to manage both your partner actions and the actions of a selected customer. You must Logout of the selected customer’s portal page once actions have been completed.

Manage Scans

One of the greatest advantages of the partner customer portal is in taking actions on behalf of the customer. By selecting the “Scans” option, the user focus is changed to the selected customer, and the SAINT ASV portal displays the selected customer’s current Scan page.

The example, shown below, displays a new customer’s first scan, to include the Targets, any scheduled scans for those targets (Repeat), current Status of displayed scans, when the scans were started, and current Progress. In the example, the scan was set up as a single scan, and is approximately 9% complete.

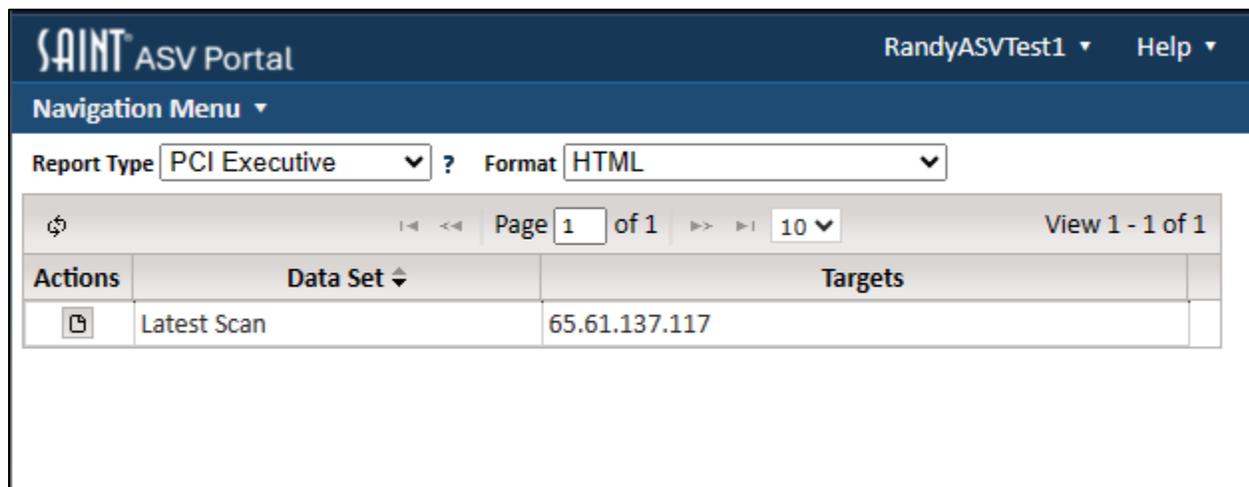


From this page, partners can take actions such as deleting a selected scan (delete option under the “Actions” column) or create new scans, by selecting the “Create Scan” option under the “Grid Actions” drop down menu.

Refer to the detailed instructions in the [Scan Tab](#) section of this help document for creating and managing scans.

Manage Results

From the Results page, a partner can take actions, on the customer’s behalf, to view the current outcome of a Scan (create Report option under the “Actions” column), as well as perform actions, such as disputes and customer attestations when choosing the “PCI Attestation” option under the Report Type drop down menu.



To view the result of a scan, select the “Report Type” and “Format” from the drop-down menus, and then select the “Create Report” button from the required scan.

Note that SAINT provides a number of report templates that are unrelated to the PCI ASV report submission requirement. These report templates are provided for your convenience and to support processes such as prioritization and remediation of failed scan results, and security services that our partners may provide to the customer.

If there are actions to be taken, when selecting the “PCI Attestation” report template, refer to the applicable sections in this help guide for detailed instructions. These actions may include working through failed scan results, obtaining attestations (Get Attestation), and completing the Feedback Form. Each of these actions are described in the [ASV Attestations](#) section.

Logout

As noted earlier, SAINT’s partner portal launches a new browser tab whenever you choose to perform actions on behalf of a selected customer. Once all actions have been completed, select the “Log Off” option under the customer’s UserID at the top right side of the page.

Need Further Help?

As your trusted advisor, we understand that finding vulnerabilities and other types of risk exposure is only the first step in maintaining a secure environment. As a SAINT ASV partner or customer, we provide three levels of support:

Technical Support

Our [Technical Support team](#) is available to assist you in using the SAINT ASV portal. At no additional cost, our support teams can help you with things like logging in and setting up scans; managing target lists and scheduling scans; creating reports; problems with access and licenses; and connecting you to other team members to learn more about other products and services.

ASV Disputes and Attestation submissions

As part of the PCI ASV process, customers may have questions or issues with scan findings, or request assistance as it relates to how to complete the scanning, disputes, attestation submission and report collection processes. As such, the SAINT ASV team is available to assist with these issues. These processes are described in the [ASV Attestation](#) section of this guide.

Any other issues or questions may be submitted through the [Technical Support team](#), as described in the previous section.

Security Services

Our security experts are availability to assist you in understanding your scan data and performing the security services needed to remediate existing issues and provide guidance on actions you can take to mitigate against future threats. Contact our [Services Team](#) for more information about our services and how you can extend the value from SAINT.