Confidential Information

The information contained in this document is confidential to Coalfire Systems and is submitted to the above Organization for the sole purpose of evaluating Coalfire Systems as a business partner and service provider. Use of this document for any other purpose is expressly prohibited. Do not copy or re-distribute without permission from Coalfire.
Getting Started

You will receive an automated email from our Coalfire team with the username and activation link. Sample below:

From: do_not_reply@coalfiresystems.com
Sent: Monday, September 13, 2014 10:50 AM
To: Customer Name
Subject: Your Navis Account

Dear Customer -

A new account has been established for you in the Coalfire Navis™ platform.

Your username is: Coalfire Systems

In order to begin using the Navis platform, you need to verify your email account. Please click on the following link to continue your new account setup.

Customer Site: http://10.29.100.96?id=323f807e-4678-4be9-9196-12e9e0c96a13&idval=kFg8dHA3m11FH6TR38tMZR2RDO841f9W8R6eALTJE4%3d&md=activate

Please note that this link will expire within 72 hours. At the end of 72 hours, you will need to request a new activation code in order to finish the process.

You have been added as a site administrator, so you can add as many additional users from your organization as you like. To add another user from your organization, simply click on "Administration" in the upper right hand corner of the top banner. Then click on "Add new user" on the new screen.

Please don’t hesitate to contact us with any questions, comments, or issues. You may contact us directly at servicedesk@coalfiresystems.com.
After you have clicked on the link above, pick and answer the five security questions.

Passwords must be from 8 - 40 characters long and must include 3 of the 4 types of following characters: Upper case letters, lower case letters, numbers, and symbols.
Once you complete the registration process, you will see the Navis dashboard.

*Depending on your purchased services you will see one of the two Navis dashboard

*Navis RapidScan Dash Board 1:

*Navis RapidScan Dash Board 2:
Scan Scheduling

To schedule a scan, go to the schedules tab and click on Create New Scan Schedule.

Scheduling an External Scan

Enter the scan name, choose to run on demand or for later date/time.
Pick the date/time and how often you would like to scan.
Scan Results View:

Once the scan is complete, the Navis RapidScan will display the scan results:

There are a few options on how to view the scan results. Results By IP Address, Results By Vulnerability and Specials Hosts.

Results By IP Address will show you which IP, what the vulnerability is and the compliance status of that IP (pass or fail).
**Disputes View:**

*SEE APPENDIX A FOR DETAILED DISPUTE PROCESS*

Disputes can also be filed by leveraging “Results by Vulnerability”. This is useful when you need to file disputes for multiple targets that have same vulnerabilities.

Details will show you the vulnerability, the severity level and the specifics of that vulnerability (shown on the right).

PLEASE NOTE:
Disputes are tied to reports, which are tied to scans, which are tied to scan schedules, which contain the scan targets. If you delete/remove/deactivate one of these items, you effectively remove the connection/relation to all of these items, as they are tied together at the root level.
Scan Report Review:

To view the scan report, click the tab “Reports”.

In this section, you will see the scans that have runned. The schedule name, compliance status (fail or pass) and the date of the reports.

You can run the reports and download with three different views:
- Summary Report – PCI Executive Summary
- Detail Report – PCI Vulnerability Report
- Remediation Tracking Report – PCI Vulnerabilities

Summary Report – PCI Executive Summary

The PCI Executive Summary Report is a high level scan report that contains three sections:

Scan information (Customer name, scan completion date, ASV company and scan expiration date).

Component Compliance Summary which lists the IP Address(s) and if it passed or failed.

Vulnerabilities Noted for each IP Address
The PCI Vulnerability Details Report is a detailed report that explains each vulnerability in detail. The report includes the severity level of the vulnerability, the description, which IP address is affected, port number, compliance status, evidence and Disputes, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability.

The report also provides the solution to the vulnerability.
The remediation tracking report will provide you with a “Recommended Remediation” plan for all vulnerabilities.

The Remediation Tracking Report includes the priority level, description, recommended remediation; affected hosts and the status of the IP (pass or fail).

In this section you will also be able to download the Attestation of Scan Compliance (AOSC). The AOSC provides the overall Pass/Fail of the scan as well as the scan scope, customer contact, and ASV contact information. This document is used by the scan customer to convey compliance to their acquirer, processor and/or QSA to demonstrate that they are fulfilling their PCI DSS 11.2.1 requirements for ASV external and/or internal scanning.
APPENDIX A:
The Dispute Process and Acquiring an Attestation of Scan Compliance

Inevitably a vulnerability will need to be disputed, either as a False Positive or for remediation. Of the vulnerabilities, those flagged as "Fail" (in the Compliance column) require action, in the form of remediation then rescanning, which will act as proof of remediation once assuming the scan is clean & flagged as a "Pass". **In the event that remediation is not possible or not applicable, a dispute still needs to be flagged in accordance to the context of the finding.**

When filing a dispute, begin with the Dispute Category radio buttons and select the Category that best matches the situation.

**Acceptable Risk** means the risk is considered low, or the probability of exploitation is low. *Low is in reference to CVSS scoring, which falls between 0-3.9.*

**Compensating Controls** may be considered when remediation cannot occur as stated in the associated reporting, due to legitimate technical or documented business constraints. A Compensating Control has to be proven to sufficiently mitigate the risk associated with the vulnerability through the implementation of other controls (ex: a firewall is in place with an applicable ACL in addition an IDS is in place with applicable signatures).

Compensating controls must:

1. Meet the intent and rigor of the original stated PCI DSS requirement;
2. Provide a similar level of defense as the original PCI DSS requirement;
3. Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.
A False Positive is applicable only when proven that the vulnerability could not, or does not, exist on the associated target. For example, an IIS vulnerability identified on an Apache server, or where software is flagged as hosting a vulnerable version of Apache when in reality the Apache instance is patched. These will require evidence (screenshots, articles) and are both truly False Positives.

Once the Dispute Category has been selected, an appropriate Explanation as to why this is being disputed is required in the Comment field. This field has a 4,000 character limit, and what is typed here will be included in the scan reports once the dispute is accepted. An adequate Explanation would include all factors that make this dispute acceptable, and provide a summary of detailed information which supports the Dispute Category selected, leaving no question in the mind of the reviewer to doubt if the comment is true. Providing a reference link to a vendor-written article (& stating what data to look for), command-line output or other text-type evidence can also be submitted here.

Finally, and arguably most importantly, Evidence in support of the Explanation is required for all disputes submitted for consideration of acceptance. Per the PCI-SSC: ALL Evidence should include a chain of custody: when, where, and how it was gathered. Evidence can be composed of a screenshot (demonstrating the IP address is the OS/version flagged), vendor statements, articles, command line output, etc.

**Additional items to consider when submitting disputes:**

Once you have acquired an acceptance for a dispute, the acceptance will be applicable for every scan run against the same target that identifies the same finding, within the same 90-day quarter. After the 90-day quarter has passed, new disputes will have to be submitted for each finding. The ScanDesk team is here to help with interpreting reporting, advising on remediation, and testing the validity of certain vulnerabilities. Please reach out when needed for assistance or if you have any questions in regards to your scanning subscription, or need additional information on other Coalfire products and services.
Uploading Evidence:

First navigate to the Scans tab, then click on the results tab.

Locate the vulnerability you would like to dispute and click on Create Dispute.

Optionally: Create the dispute by vulnerability; for scenarios where the same dispute is to be applied to the vulnerability found among more than one scan target.

Either of the above steps will lead to this screen, where you will find the red hyperlink: "Click here to add or modify evidence."
The next steps are to upload the evidence from your computer to Navis by starting with the "Upload File(s) to Library" button which will put the files into the right column (Evidence Library). The user must click the left facing arrow to move the file(s) to the left column (Associated Evidence) which attaches the evidence to the dispute opened. Once the evidence is ready to be associated, click the "Update Associated Evidence" button. After the window closes, do not forget to click "Save" before exiting the dispute.