Host Integrity at Startup (HIS)

Web Portal Guide

Crossbow Release

March 8, 2011

Table of Contents

Introduction 3

- Goals 3
- Scope 3
- Terms and Acronyms 4

Web Portal Pages 5

- Alerts 5
- Alert Details 7
- Reports 9
- Machines 10
- PCR Values 11
- Statistics 12
- Help 13

Procedures 5

- Daily Check 9
- Email Notification 9
- Investigating Alerts
- Closing Alerts

References 6

Contact Information 8

Introduction

The Trusted Computing Group (TCG) has defined a series of specifications that defined how a commercial computing platform can support code measurement in a trusted manner. NSA's National Information Assurance Research Laboratory (NIARL) developed Host Integrity at Startup (HIS) to measure and report status for host PC platforms which contain a Trusted Platform Module (TPM). Included in the existing TCG TPM specifications are several protocols that support attesting these measurements to a third party for validation. However, these protocols are not well suited for web-based applications. The Host Integrity Protocol was developed by NIARL to support web-based attestation appraisals.

Goals

The gals for the HIS portal are:

1. To provide the system administrator information about HIS reports being collected on the system.
2. To provide information about alerts generated by the HIS appraiser and how to respond to them.
3. To provide utilities for analyzing the information collected by the HIS appraiser.

Scope

The HIS portal described by this paper provides the administrator access to the result of processing the integrity reports sent by machines that have been enrolled. Refer to "Host Integrity at Startup: A Web Service Example for TPM Provisioning and Attestation" [1] for further details on the integrity reporting process. This document also includes strategies for responding to HIS alerts and gaining value from machine statistics.

Terms and Acronyms

Alert – A notification that an integrity report sent from a machine displayed unapproved changes requiring investigation.

Host Integrity at Startup (HIS) – A research proof-of-concept system developed by NIARL to collect and report system integrity measurements while adhering to TCG standards.

HIS Appraiser – A server that analyzes and catalogs integrity reports.

National Information Assurance Research Laboratory (NIARL) – This is the organization that developed HIS and operates as a research group within NSA.

Privacy Certificate Authority (Privacy CA or PCA) – A special certificate authority designed to adhere to TCG standards for TPM identity management. The PCA enables the HIS Appraiser to validate signatures tied to each integrity report and certify the identity of enrolled machines.

Platform Configuration Register (PCR) – A hash representing a machine's hardware and software configuration during boot. The current TCG 1.2 specification allows for 24 total PCRs measuring everything from BIOS firmware and expansion devices to operating system kernels and checked files.

Trusted Computing Group (TCG) – An industry consortium that is defining a set of specifications to support trusted computing concepts. These include cryptographic chips on a machine's motherboard, self-encrypting hard drives, network connection protocols, and more.

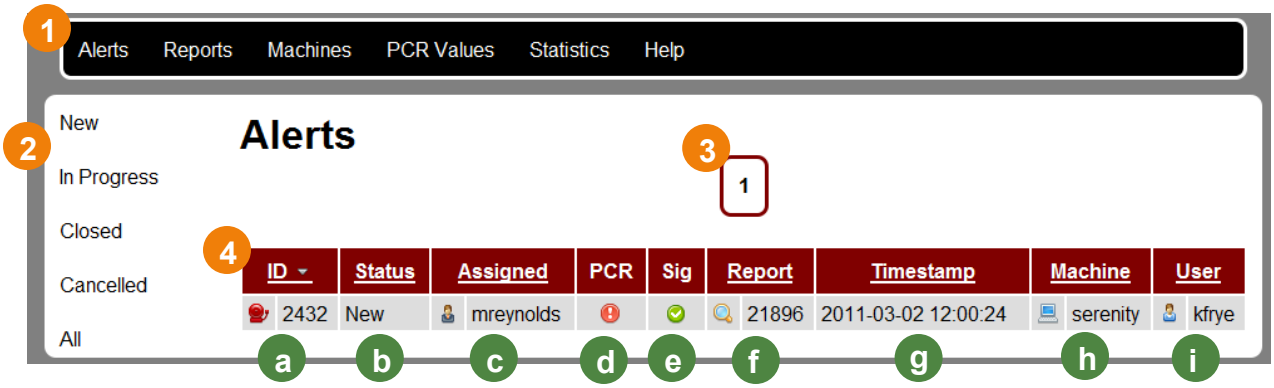
Trusted Platform Module (TPM) – A hardware security chip designed to specifications created by the TCG. The TPM can be used to collect system PCR measurements, protect secrets such as cryptographic keys, or store configuration information. The TPM can sign and attest data to a remote entity.

Web Portal Pages

The HIS Appraiser collects and processes integrity reports from machines enrolled with it. Results from the appraiser are presented through the HIS Web Portal. This section describes the various components of the web portal and their utility to network administrators.

Alerts

The portal defaults to the alerts page when first accessed. This page displays only new reports that triggered an alert. To view alerts in progress, closed, cancelled, or all alerts it is necessary to use the left-side filtering links.



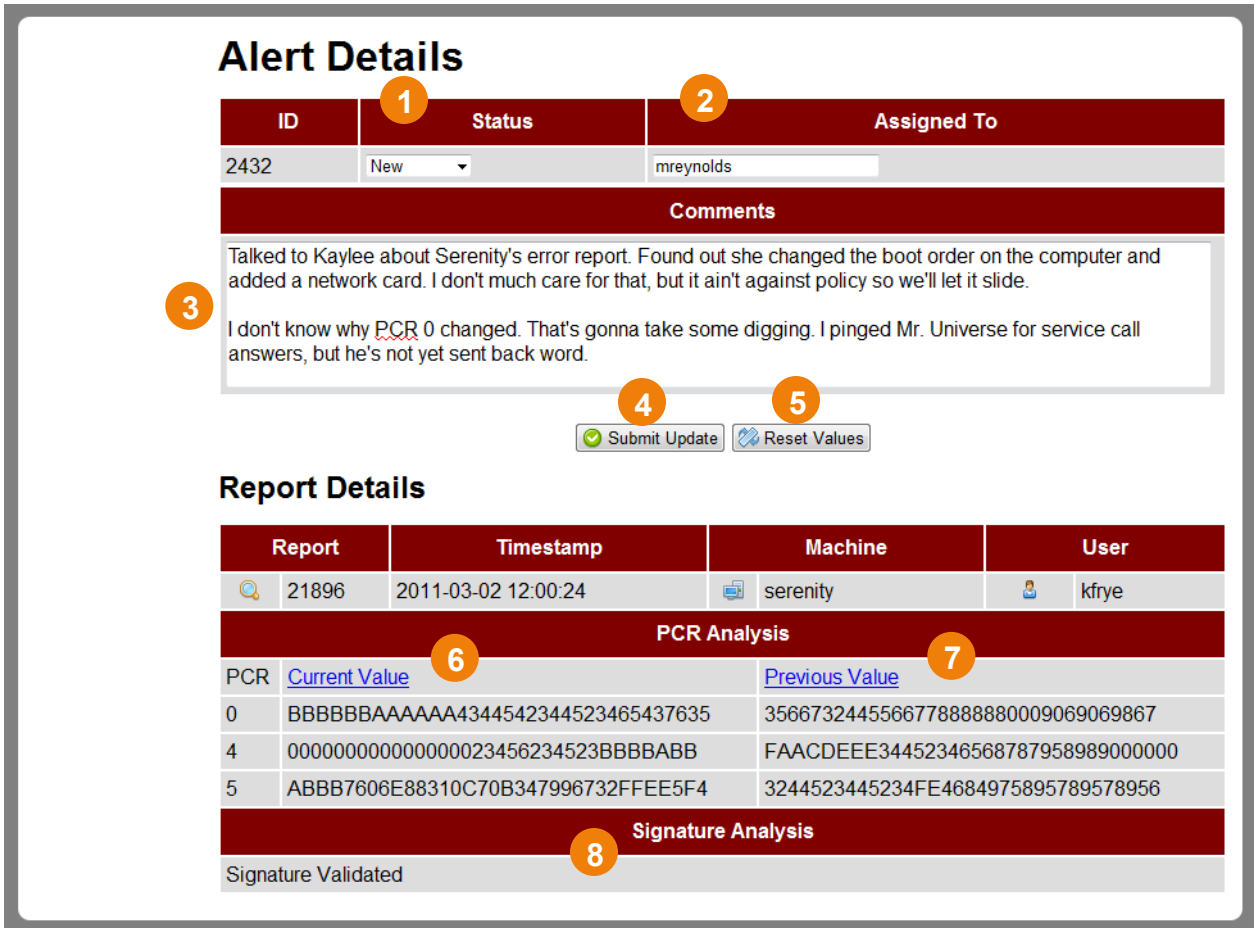
1. **Main Menu** – This menu allows access to the various data display pages that make up the HIS web portal. Each option in the main menu has a description in this section of the web portal guide. You are reading the alerts section.
2. **Filter Menu** – The filters on the alerts page are responsible for displaying alerts with a specific status. By default only new alerts are shown. Clicking the in progress, closed, and cancelled options will cause alerts with those specific statuses to appear in the table. Clicking on the all option will cause all alerts regardless of status to appear in the table.
3. **Page Selector** – The web portal generates a page for each 100 records returned from the database. In this example only 1 record was returned so there is need for only 1 page. When many pages are present one or more icons and page numbers will appear here. |< represents first page, < represents previous page, the current page and those around it are displayed by number, > represents next page, and >| represents last page. The page selector will remember filter and sorting settings.

4. **Alerts Table** – This table presents information about each alert and its corresponding integrity report. The underlined column headings can be used to sort the table. By default the table will be sorted counting down from the highest (most recent) alert ID number.
    a. **ID** – Each alert has an ID number that is unique. Click on the alarm bell icon to visit the alert details page.
    b. **Status** – Alerts are initially categorized as new. When an administrator is researching an explanation for an alert they can be moved to the In Progress status. When the explanation is determined, benign or malicious, the status for an alert can be set to Closed to show there has been a resolution. In the event of an alert was triggered by an error such as a network reconfiguration it may be necessary to use the Cancelled status to denote an alert that was not tied to a particular PCR change or signature failure.
    c. **Assigned** – Each alert can be assigned to an administrator for research and resolution. The name of the administrator is displayed here. To get a listing of all alerts assigned to a particular administrator click the administrator icon (user in black suit) to get a listing of all alerts assigned to that administrator. Note that filtering and sorting options will be remembered by the web portal.
    d. **PCR** – The PCR field indicates if PCR changes triggered a particular alert. A green checkmark indicates there were no PCR changes while a red exclamation point signifies PCR changes are present. Click the alert details to get more information about specific PCR changes. The PCR icon is not clickable.
    e. **Sig** – This is shorthand for signature. A green checkmark means that the report signature validated. A red exclamation point means that the signature did not validate and therefore the contents of the report cannot be trusted. Signatures are generated with a key created by a client's TPM with help from the Privacy CA.
    f. **Report ID** – Alerts are generated based on reports. The ID number for the report that triggered a specific alert is displayed as well as an icon to click on to see the full XML text of a report.
    g. **Timestamp** – Each report is tagged with a timestamp based on the time it is received. Since an alert is generated upon receipt of a report this timestamp also signifies when an alert was created.

h. **Machine** – The machine responsible for sending a report and triggering an alert is displayed. Click on the machine icon to see all reports from this specific machine.
i. **User** – The user operating a given machine when an alert-generating report was sent gets listed by their SID. Sometimes the machine triggers reports by itself. When that happens the user will appear as SYSTEM for Windows machines or ROOT for Linux machines. Click on the user icon (user in blue shirt) for a listing of all reports sent by this user.

Alert Details

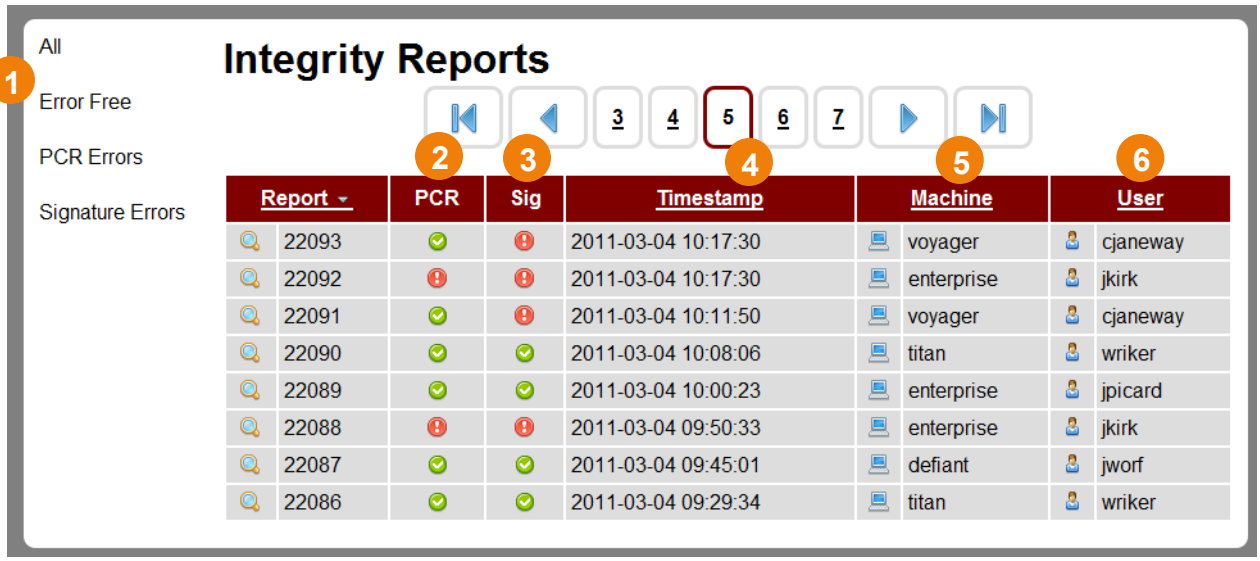
The alert details page gives detailed information about PCR changes, signature analysis, and comments from administrators working towards an alert resolution. This page can be updated by administrators to change status, assignments, and comments on a given alert and report pair.



1. **Status –** The status drop-down box allows administrators to set the alert status to New, In Progress, Closed, or Cancelled. By default all alerts are initially set to new. When an administrator has been assigned to research an alert it is appropriate to set the status to In Progress. When a resolution has been achieved it is appropriate to set the status to Closed. Only erroneous alerts should be given the Cancelled status. The drop-down box will default to the current status of an alert.
2. **Assigned To –** This text field is designed to list the SID of the administrator who is working on an alert. By default alerts are assigned to nobody.
3. **Comments –** Administrators should update the comments field with their findings. Causes for an alert, actions taken, and any information relevant to closing an alert is appropriate for this field.
4. **Submit Button –** This button triggers updates to post to the database. Updates cannot be undone. If the assigned to field is left blank the update will fail with an appropriate error message. The update confirmation page will automatically return administrators to the alerts page upon success.
5. **Reset Button –** This button will reset all fields in the form to the original values.
6. **PCR Current Value –** This section of the alert details breaks down individual PCR changes. Values from the current report are presented. The current value heading can be clicked to view the full text of the report. Each PCR is displayed beside its index number. Administrators can mouse over the PCR index number to see a tooltip that explains the meaning of each index. Detailed information about causes and resolutions for each PCR value can be found in the help section.
7. **PCR Previous Value –** Previous values are contrasted against the values presented in a machine's most recent report. The previous report can be viewed by clicking on the previous value heading.
8. **Signature Analysis –** The signature analysis simply informs administrators if the integrity report tied to this alert had a valid signature or not. In the event of an invalid signature a causes and resolutions informational blob will be presented.

Reports

The reports page is a catalog of all reports received by the HIS appraiser. The full XML text of each report, PCR analysis, signature validation, timestamp, machine, and user are all displayed here. Reports are displayed regardless of whether or not they triggered an alert requiring administrative action.

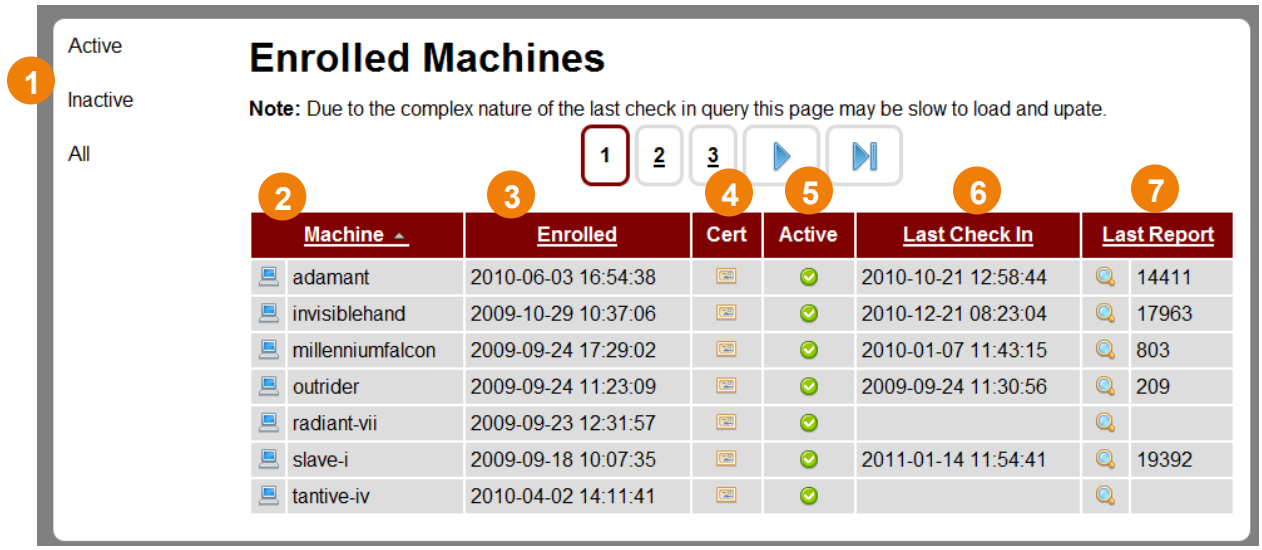


1. **Filter Menu** – By default all reports are shown. The filter menu allows administrators to see reports only with certain characteristics. Filter settings are remembered while paging through results or changing sort order.
2. **PCR Changes** – Any PCR change causes a red exclamation point to appear. A green checkmark appears when there are no changes present.
3. **Signature** – Valid signatures are displayed with a green checkmark. This verifies that the information contained in the report is valid and signed by the machine's TPM. In the event an invalid signature is encountered a red exclamation point will appear. This signals that the contents of the report cannot be validated nor can the identity of the machine be guaranteed.
4. **Timestamp** – Each report is tagged with the date and time it is received.
5. **Machine** – The machine in which is referenced in a report is indicated in this column. Click on the computer icon to get a list of integrity reports sent by that specific machine. This allows administrators to identify patterns of behaviors exhibited by machines as well as diagnose specific changes that may not have triggered and alert.

6. **User** – Each user responsible for using a machine when a report was sent is indicated here. Click on the user icon to get a full listing of integrity reports sent while this user was using an enrolled machine. Users are listed by their SID. However, ROOT and SYSTEM may appear if enrolled machines are set to report upon boot or when users are not logged in.

Machines

The machines page shows every machine enrolled for this HIS appraiser. By default active machines are shown when first visiting this page. The machines page can be sluggish to load due to the complex nature of the last check in query.

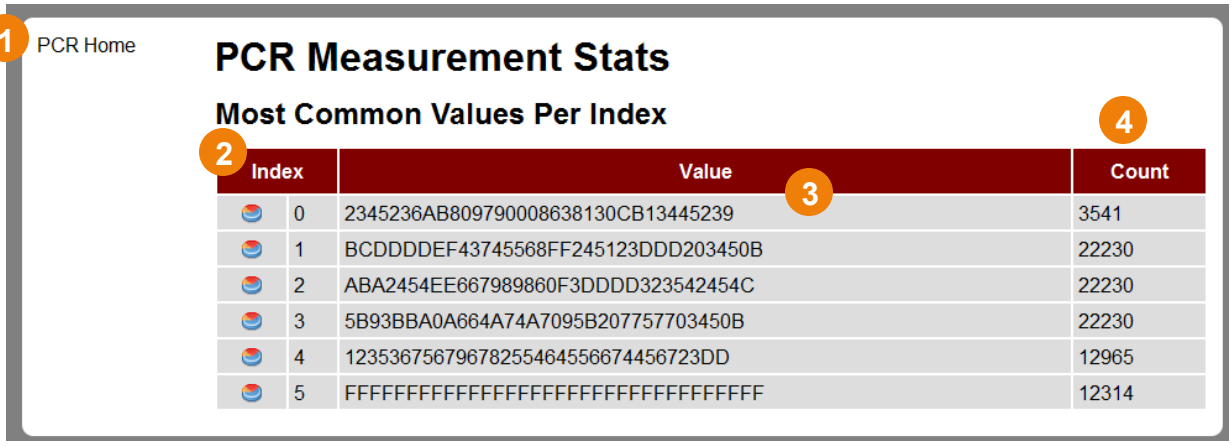


1. **Filter Menu** – By default only active machines are shown. To see inactive machines or all machines regardless of status click on the appropriate filter option. Filters are remembered regardless of sort or page selections.
2. **Machine** – Each machine is listed by name. Click on the machine icon to see a full listing of reports sent by a particular machine.
3. **Enrolled** – The enrollment date of each machine is listed here. This is generated when the machine is provisioned for use with this HIS appraiser. A re-enrollment causes the machine's current entry to become inactive and a new entry with a new enrollment date to appear. Administrators can tell each time a machine is enrolled or re-enrolled.

4. **Certificate** – This is the Attestation Identity Certificate (AIC). This certificate is generated during provisioning where the Privacy CA validates a machine's TPM Attestation Identity Key (AIK). The certificate is copied to the server for signature validation upon receipt of HIS reports.
5. **Active** – The active column indicates if a machine name and certificate pair is active or not. Only active machines may send integrity reports that can be fully trusted. By default all new enrollments and re-enrollments are active. Any previous instances of a machine's enrollment state are marked as inactive. Machines that have been removed from the HIS Appraiser may also appear as inactive.
6. **Last Check In** – This column displays the timestamp for the most recent integrity report received from this machine.
7. **Last Report** – The ID number and a link to the XML full-text of the last report this machine sent is presented here.

PCR Values

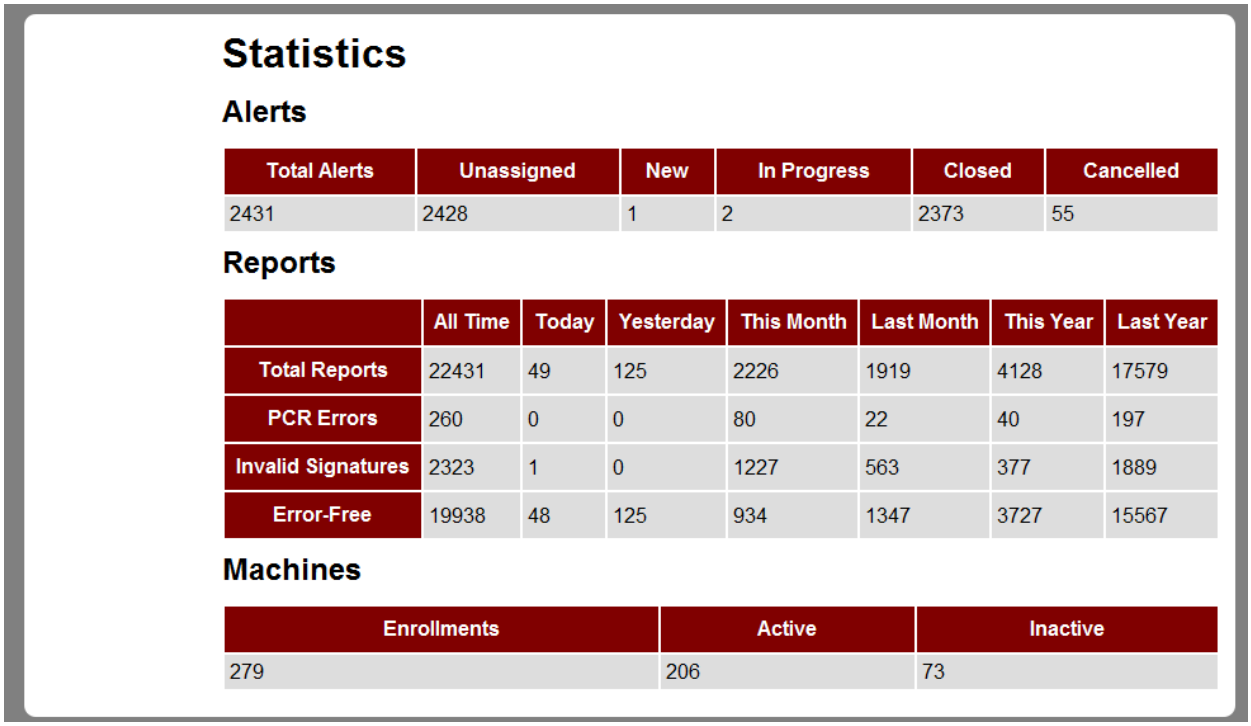
Blahblah



Blahblah

Statistics

Blahblah



Statistics

Alerts

Total Alerts	Unassigned	New	In Progress	Closed	Cancelled
2431	2428	1	2	2373	55

Reports

	All Time	Today	Yesterday	This Month	Last Month	This Year	Last Year
Total Reports	22431	49	125	2226	1919	4128	17579
PCR Errors	260	0	0	80	22	40	197
Invalid Signatures	2323	1	0	1227	563	377	1889
Error-Free	19938	48	125	934	1347	3727	15567

Machines

Enrollments	Active	Inactive
279	206	73

Blahblah

Help

Blahblah

Blahblah

Procedures

Blahblah

References

Blah