



# Intellitactics SAFE LP

PCI Report List



[www.intellitactics.com](http://www.intellitactics.com)

## **Copyright Information**

© 1998-2008 Intellitactics Inc. All rights reserved.

No part of this document may be reproduced in any form by any photographic, electronic, mechanical or other means, or used in any information storage and retrieval system, without prior written permission from Intellitactics Inc.

All other product and brand names in this document are trademarks or registered trademarks of their respective owners.

# PCI Reports

## 1. Install and Maintain a Firewall Configuration

Reports supporting compliance with section 1 of the PCI Data Security Standard.

### Cisco ASA/PIX

Reports and Event Views supporting Cisco ASA/PIX.

#### **Administration Activity**

This report shows all administration events within a specified time period.

Change is one of the greatest sources of risk in a system; changes can be made improperly, have unintended side effects or be made towards malicious goals. Change must be carefully managed and controlled. This report, in providing a record of administrative events, can be used to verify change control process in support of Requirement 1.1.1 of the PCI DSS.

#### **Administrative Users List**

This report shows all administrative event activity, grouped by administrator, within a specified time period.

Administrators often have access that circumvents all other security controls in place. This is why the PCI DSS, through Requirement 1.1.4, requires a written description of groups, roles, and responsibilities for the logical management of the network. This report allows for verification that only appropriate users are performing administrative activities and that each administrator is performing actions that are in accordance with their documented role and responsibilities.

## Connections to Selected Addresses from VPN

This report lists access to selected hosts through VPN connections within a specified time period. It is essential to enter a host or select a list of hosts for the report to return data.

The PCI DSS requires strict control over communication between untrusted networks and the cardholder data environment. VPN access often allows a host (e.g. a mobile user) on an untrusted network to have direct access to sensitive internal resources, even including the cardholder data environment. This report allows for access to any such defined resources to be reviewed, supporting verification of PCI DSS Requirements 1.2 and 1.3.

## Summary of Errors and Availability Events

This report shows all events related to error and availability activities, determined by highest count, within a specified time period.

Many of the PCI DSS statements in Requirement 1 focus on the initial implementation of a secure network (build). However, once the network is built, its security controls and configurations must be maintained. Firewalls should be reviewed on a frequent basis (no less than quarterly) to ensure that performance is acceptable and settings are being maintained. This report summarizes all events related to errors and availability. This allows the system or security administrator to identify suspicious events for further review or to troubleshoot problems with firewall availability.

## Communication Control

### Port Traffic Control

This report shows events (by target port) to indicate which ports are blocking or allowing events, within a specified time period. This provides an overview of the types of applications that are allowed by the firewall, and which ones are denied.

In summarizing the ports on which traffic is allowed and denied, this report facilitates verification of documentation required by PCI DSS Requirement 1.1.5. This report can also be used to support the review of firewall rules as specified by PCI DSS Requirement 1.1.8. Finally, this report can be used to review and verify traffic controls as specified by PCI DSS Requirements 1.2 and 1.3.

## Proxy Use by Selected Hosts

This report shows selected hosts or users of the proxy within a specified time period. It is essential to enter a host or user value or select a list of hosts or list of users for the report to return data.

PCI DSS Requirement 1.3 specifies that network configuration should prohibit direct access between the Internet and the cardholder environment in both directions. Proxy servers may prevent direct access but can still represent a significant degree of connectivity and risk. This report can be used to ensure that any web access by selected addresses - in particular, those in the cardholder data environment - is controlled by a proxy. Further, as hosts in the cardholder data environment should have limited need for access, this report can be used to verify that all access is necessary and legitimate as specified by PCI DSS Requirement 1.2.1.

## Top Targeted Services

This report shows the top services reported in the selected events within a specified time period.

PCI DSS requires that only services necessary to accomplish the business should be available. Organizations should define what services are allowed and necessary for business within their written policy. Examples of service are HTTP/HTTPS, SMTP, and FTP. The firewall settings are used to enforce this policy. Network or system administrators should use this report to ensure the organization policies are being enforced. This report assists in complying with Requirements 1.2 and 1.3 of the PCI DSS.

## Traffic Control Summary

This report shows granted and denied connections for firewall devices within a specified time period.

In presenting a high level summary of traffic control activity for each firewall, this report can reveal abnormal or unexpected traffic patterns. For instance, a significant increase in traffic blockage may represent a misconfiguration or significant change in the behavior of hosts on the network. Review of such macro-level firewall activity helps support ongoing compliance with PCI DSS Requirements 1.2 and 1.3.

## VPN Gateways

This report shows hosts reporting VPN logins within a specified time period. This report shows the detector; detector zone; number of users; number of

sources from which logins were made; and the number of successful and unsuccessful logins.

A VPN provides for the protection of the data in transit but also often represents a direct path into trusted segments of the network. These gateways into the network must be carefully controlled and protected. This report identifies all hosts accepting VPN connection requests and can be used to verify network documentation as specified by PCI DSS Requirements 1.1.2 and 1.1.5.

## 2. Secure Configuration

Reports supporting compliance with section 2 of the PCI Data Security Standard.

### Default Account Use

#### Changes to Selected Accounts

This report shows all changes to selected accounts within a specified time period. It is essential to enter an account or select a list of accounts for the report to return data

Commercial network and system components are usually delivered in an insecure state and must be configured for security. The PCI DSS requires that these settings be examined for their necessity and defaults changed prior to deployment into the operational environment. This configuration can involve changes to default credentials and account settings. This report can be used to verify the requisite changes have been made to default accounts, assisting in compliance with Requirement 2.1 and 2.2 of the PCI DSS.

#### User Activity

This report shows user activity, grouped by device or host, that occurred within a specified time period. The report shows the first and last time the activity occurred; the event ID; and the event count.

Commercial network and system components are usually delivered in an insecure state and must be configured for security. The PCI DSS requires that these settings be examined for their necessity and defaults changed prior to deployment into the operational environment. This configuration can involve disabling and renaming accounts. This report can be used to identify any usage

of default and otherwise restricted accounts, assisting in compliance with Requirement 2.1 and 2.2 of the PCI DSS.

## 5. Use Anti-Virus Software

Reports supporting compliance with section 5 of the PCI Data Security Standard.

### Active Malware

This report shows all active malware detected within a specified time period.

Malware or malicious software is a threat to your systems and data. This type of threat can include viruses, spyware, adware and root-kits. The purpose of anti-virus and anti-malware software is to prevent these types of threats from getting on your hosts and in to your data. Check all systems regularly for active malware. This report assists in the notification of any active malware that has been detected on a host, and also assists in verifying compliance with Requirement 5 of the PCI DSS.

### Exposure of Selected Hosts to Malware

This report shows the exposure of selected hosts to malware within a specified time period. It is essential to enter a user value or select a list of users for the report to return data.

Malware includes viruses, adware, root-kits and any other malicious software and can pose a serious threat, in particular when they affect sensitive systems. This report identifies any exposure of selected hosts to malware. This report will assist in verifying and complying with Requirement 5.1 of the PCI-DSS.

### Hosts Exposed to Selected Malware

This report shows hosts exposed to selected malware within a specified time period. It is essential to enter a malware or select a list of malware for the report to return data.

A host exposed to malware can cause network issues, loss of data and other issues. Some infections are particularly dangerous. This report allows for the identification of hosts exposed to a specified type of malware. As a tool for investigating and managing malware infections, this report supports compliance with Requirement 5.1 of the PCI DSS.

## **Least Common Malware**

This report shows the least common malware detected within a specified time period.

Uncommon malware infections may reveal unique or uncommon attack vectors and may pose special risks. This report allows for identification of uncommon types of malware. As a tool for investigating and managing malware infections, this report supports compliance with Requirement 5.1 of the PCI DSS.

## **Most Infected Hosts**

This report list the most infected hosts within a specified time period.

Hosts most frequently infected by malware should be reviewed and secured. As a tool for investigating and managing malware infections, this report supports compliance with Requirement 5.1 of the PCI DSS.

## **Scans Disabled on Selected Hosts**

This report shows the scans disabled on selected hosts within a specified time period. It is essential to enter a host or select a list of hosts for the report to return data.

Anti-Virus software inspects files and objects on a schedule, on demand or on access. This scanning activity can put load on the system and, despite policy, may be disabled by end-users. This report will identify users who have disabled scans, helping to ensure compliance with Requirement 5.2 of the PCI DSS.

## **Top Malware**

This report shows the top malware within a specified time period.

This report identifies the most commonly observed malware types. As a tool for investigating and managing malware infections, this report supports compliance with Requirement 5.1 of the PCI DSS.

## **Users Most Frequently Disabling Protection**

This report shows users who have frequently disabled system protection within a specified time period.

Anti-Virus software inspects files and objects on a schedule, on demand or on access. This scanning activity can put load on the system and, despite policy, may be disabled by end-users. This report will identify users who have disabled scans, helping to ensure compliance with Requirement 5.2 of the PCI DSS.

## 6. Develop Secure Systems and Applications

Reports supporting compliance with section 6 of the PCI Data Security Standard.

### Administration and Change

#### Administration Activity

This report shows all administration events within a specified time period.

Change is one of the greatest sources of risk in a system; changes can be made improperly, have unintended side effects or be made towards malicious goals. Change must be carefully managed and controlled. This report, in providing a record of administrative events, can be used to verify change control process in support of Requirement 6.4 of the PCI DSS.

#### Administrative Users List

This report shows all administrative event activity, grouped by administrator, within a specified time period.

Change is one of the greatest sources of risk in a system; changes can be made improperly, have unintended side effects or be made towards malicious goals. Change must be carefully managed and controlled. This report, in providing an accounting of administrative users and their activities, can be used to verify change control process in support of Requirement 6.4 of the PCI DSS.

#### Database Schema Modifications

This report shows all schema modification events within a specified time period. Schema modifications are rare and warrant review. Results are grouped by data module and detector.

A database schema is the structure of the data and how it will be organized and stored on a computer. It is represented or implemented by a Data Base Management System. Once a database schema is defined and implemented, changes to it are infrequent. This is because one or more software applications may be using the data. Any change to the database has the potential to impact or cause errors in the software applications that access the database. This report assists in verifying compliance with Requirement 6.4 of the PCI DSS.

## Separation of Duties

### Logon to Selected DB Server by Selected Users

This report shows hosts accessed by users within a specified time period. Although users have the system level access to sensitive databases, they should not be accessing them. Entering host or user values is optional.

PCI DSS Requirement 6.3.3 requires a separation of duties between development, test and production environments. When applied to production databases and test/development user accounts, this report can identify non-compliance with Requirement 6.3.3.

### Selected Users Accessing Selected Files

This report shows any users who accessed the selected files, within a specified time period. The report can be used to identify access to business files by privileged system users (such as administrators). It is essential to enter a file name or select a list of files for the report to return data. The report results are grouped by user.

PCI DSS Requirement 6.3.3 requires separation of duties within the development, test, and production environments. When applied to production files and test/development user accounts, this report can identify non-compliance with Requirement 6.3.3.

## 7. Restrict Access to Cardholder Data

Reports supporting compliance with section 7 of the PCI Data Security Standard.

## DB Access

### All Denied DB Login Attempts

This report shows all failed login attempts to database services within a specified time period. Any failed login attempts should be considered suspicious. This report is sorted by data module, and the number of attempts is also shown.

Databases are most commonly parts of backend systems in the cardholder data environment and accessed by few accounts. Accidental failed access attempts are relatively rare and the probability of a purposeful attempt warrants review. This report supports PCI DSS Requirement 7.1 by revealing possible illegitimate attempts to access cardholder data.

### New Users Accessing Databases

This report shows users accessing a database server within a specified time period. Few users directly access databases, so any occurrences of this are worth reviewing.

Databases are most commonly parts of backend systems in the cardholder data environment and accessed by few accounts. Access by new accounts is rare and should be well justified. This report allows for review of new account access in support of PCI DSS Requirement 7.1.

### Users Connecting to DB from New Sources

This report shows users accessing a database server from a new client address within a specified time period.

Databases are most commonly parts of backend systems in the cardholder data environment and accessed by few accounts and usually from the same client hosts. Logins from new addresses may represent unauthorized account usage and should be reviewed. This report allows for review of access from new sources in support of PCI DSS Requirement 7.1.

## File Access

## Denied File Access Summary

This report shows a detailed summary of denied attempts, grouped by user, to access files within a specified time period. The objective is to find users who are attempting to misuse or exceed their rightful access.

Files containing sensitive cardholder data must not be accessed, except by those authorized to do so. This report provides a summary of those users attempting to access these files and have been denied access. The attempts should be reviewed to determine if the user is authorized access but having difficulty logging in, or to investigate why an unauthorized user is attempting to login. This report assists in verifying compliance with Requirement 7.1 and Requirement 7.2 of the PCI DSS.

## Denied Files List

This report shows files that users have unsuccessfully attempted to access, grouped by the originating IP address, within a specified time period. Files with very high numbers of attempts may be accessed by automated tools.

A high number of access attempts on sensitive files can be caused by automated tools or unauthorized users attempting to access them. Security or system administrators should review who is attempting to access these files in order to ensure that there are no malicious activities occurring. This report assists in verifying compliance with access control measures in accordance with Requirement 7.1 of the PCI DSS.

## New Users of Selected Files

This report shows users accessing selected files for the first time, within a specified time period. It is essential to enter a file name or select a list of files for the report to return data.

There should be a select list of users allowed to access sensitive cardholder data. Whenever a new user accesses these files, their access should be reviewed to verify that they have a business need to access these files and have been given proper authorization. This report lists the users that have accessed these selected files for the first time. Review of this report assists in ensuring that these users should have this access. This report assists in verifying compliance with Requirement 7.1 of the PCI DSS.

## Selected File Accessed by New Program

This report shows the access of selected files by new programs within a specified time period. Highly sensitive files are usually accessed in a limited number of

ways, and any access by a new program should be reviewed. It is essential to enter a file name or select a list of files for the report to return data.

Cardholder data should be accessed and modified in well understood, consistent and controlled ways. As such, files containing cardholder data are usually accessed using select applications. Access by new applications may represent an unauthorized use of such data and should be reviewed. This report identifies any new program accessing selected sensitive files and assists in verifying compliance with Requirement 7.1 of the PCI DSS.

### **Selected Users Accessing Selected Files**

This report shows any users who accessed the selected files, within a specified time period. The report can be used to identify access to business files by privileged system users (such as administrators). It is essential to enter a file name or select a list of files for the report to return data. The report results are grouped by user.

A select user base has access to cardholder data, while other groups have no legitimate need for access. For instance, administrators and IT consultants should rarely access cardholder data. This report allows any access by such users to be reviewed and justified in support of compliance with Requirement 7.1 of the PCI DSS.

### **Users Accessing Selected Files**

This report shows all users who have accessed the specified file(s) (which are usually sensitive resources) for the specified time period. It is essential to enter a file name or select a list of files for the report to return data. The results are grouped by file.

PCI DSS Requirement 7.1 specifies that only users with legitimate need should have access to cardholder data. This report, in listing users accessing files containing cardholder data, supports compliance with the requirement.

### **Users Accessing Selected Files (Detail)**

This report shows all users who have accessed the specified file(s) (which are usually sensitive resources) for the specified time period. It is essential to enter a file name or select a list of files for the report to return data. The results are grouped by file.

PCI DSS Requirement 7.1 specifies that only users with legitimate need should have access to cardholder data. This report, in listing users accessing files containing cardholder data, supports compliance with the requirement.

## 8. Identity and Authentication

Reports supporting compliance with section 8 of the PCI Data Security Standard.

### Account Management

#### Account Management by Selected Users

This report shows all management events performed against accounts or groups by the selected or excluded user within a specified time period. It is essential to enter a user value or select a list of users for the report to return data.

Some users may have privileges within a system to affect user accounts but may not be assigned to do so as part of their job function. When configured to exclude authorized user accounts, this report allows for all account management by non-authorized users to be reviewed in support of Requirement 8.5.1 of the PCI DSS.

#### Accounts Created

This report shows all accounts created within a specified time period.

PCI DSS Requirement 8.5.1 specifies that account creation, deletion and modification be controlled. This report allows for review of all account creation as part a change control process in support of the requirement.

#### Accounts Deleted

This report shows all accounts deleted within a specified time period.

This report allows for review of all account deletion as part a change control process in support of PCI DSS Requirement 8.5.1. Additionally, if policy is to delete accounts for inactive/terminated users, this report allows for verification that such accounts have in fact been deleted, thus supporting Requirements 8.5.4 and 8.5.5.

#### Accounts Disabled

This report shows all accounts disabled within a specified time period.

This report allows for review of all account disablement as part a change control process in support of PCI DSS Requirement 8.5.1. Additionally, if policy is to disable accounts for inactive/terminated users, this report allows for verification that such accounts have in fact been disabled, thus supporting Requirements 8.5.4 and 8.5.5.

### **Accounts Enabled**

This report shows all accounts enabled within a specified time period.

This report allows for review of all account enablement as part a change control process in support of PCI DSS Requirement 8.5.1. Additionally, this report allows for review of enablement of vendor/maintenance accounts in support of PCI DSS Requirement 8.5.6.

### **Accounts Locked Out**

This report shows all accounts locked out within a specified time period.

A lockout of an account occurs because a specific number of attempts to login have failed. A user not remembering his/her password could cause this lockout. Someone who is attempting to break in using another person's User ID could cause it also. The number of login attempts before a lockout occurs is specified by company policy, however PCI DSS requires lockout after six failed attempts. When a lockout occurs, the user is may need to wait for 30 or more minutes before trying again or be instructed to contact the system administrator for assistance. This report assists in verifying compliance with Requirements 8.5.1, 8.5.13 and 8.5.14 of the PCI DSS.

### **Accounts Modified**

This report shows all accounts modified within a specified time period.

PCI DSS Requirement 8.5.1 specifies that account creation, deletion and modification be controlled. This report allows for review of all administrative account modification as part a change control process in support of the requirement.

### **Accounts Modified by Owner**

This report shows all modification events performed by the selected account within a specified time period. It is essential to enter an account value or select a list of accounts for the report to return data.

PCI DSS Requirement 8.5.1 specifies that account creation, deletion and modification be controlled. This report allows for review of all account self-modification as part a change control process in support of the requirement.

### **Accounts Unlocked**

This report shows all accounts unlocked within a specified time period.

Accounts are locked primarily if there are several attempts to login to a company's computer resources using the wrong ID or password. The lockout time is specified in a company policy. To unlock an account, the user must call an administrator or wait a predetermined period of time for the account to automatically unlock. In organizations using a minimum lockout period, system administrators should review this report to review frequency of unlocks. Repeated unlocks could indicate suspicious activity. This report assists in verifying compliance with Requirement 8.5.1, 8.5.13 and 8.5.14 of the PCI DSS.

### **Changes to Selected Accounts**

This report shows all changes to selected accounts within a specified time period. It is essential to enter an account or select a list of accounts for the report to return data

This report allows for review of changes of selected user accounts. This allows for review of changes to sensitive account classes, such as those of administrators, contractors and those working with cardholder data in support of overall account change control as specified by PCI Requirements 8.5.1 and 8.5.6.

### **Changes to Selected Groups**

This report shows changes to selected groups within a specified time period. It is essential to enter a group or select a list of groups for the report to return data

This report allows for review of changes of selected group accounts. This allows for review of changes to sensitive groups, such as those of administrators, contractors and those working with cardholder data in support of overall account change control as specified by PCI Requirement 8.5.1.

### **Group Members Added**

This report shows all groups that had members added within a specified time period.

This report allows for review of the addition of members to selected group accounts. This allows for review of changes to sensitive groups, such as those of

administrators, contractors and those working with cardholder data in support of overall account change control as specified by PCI Requirement 8.5.1.

### **Group Members Removed**

This report shows all groups that had users removed within a specified time period.

This report allows for review of the removal of members from selected group accounts. This allows for review of changes to sensitive groups, such as those of administrators, contractors and those working with cardholder data in support of overall account change control as specified by PCI Requirements 8.5.1.

### **Groups Created**

This report shows all groups created within a specified time period.

PCI DSS Requirement 8.5.1 specifies that account creation, deletion and modification be controlled. This report allows for review of all group creation as part a change control process in support of the requirement.

### **Groups Deleted**

This report shows all groups deleted within a specified time period.

PCI DSS Requirement 8.5.1 specifies that account creation, deletion and modification be controlled. This report allows for review of all group deletion as part a change control process in support of the requirement.

### **Groups Modified**

This report shows all groups modified within a specified time period.

PCI DSS Requirement 8.5.1 specifies that account creation, deletion and modification be controlled. This report allows for review of all group attribute modification as part a change control process in support of the requirement.

## **Authentication**

### **All Denied DB Login Attempts**

This report shows all failed login attempts to database services within a specified time period. Any failed login attempts should be considered suspicious. This report is sorted by data module, and the number of attempts is also shown.

Databases are most commonly parts of backend systems in the cardholder data environment and accessed by few accounts. Accidental failed access attempts are relatively rare and the probability of a purposeful attempt warrants review. This report supports PCI DSS Requirement 8.5.16 by revealing possible illegitimate attempts to access cardholder data.

### **Authentication Failure for Selected Users**

This report shows files that users have unsuccessfully attempted to access within a specified time period. Files with very high numbers of attempts may be accessed by automated tools. It is essential to enter a user value, or select a list of users, for the report to return data.

This report supports PCI DSS Requirement 8.5 by facilitating the review of authentication activity.

### **Local Login to Selected Hosts**

This report shows local login attempts to selected hosts, such as critical servers, within a specified time period. It is essential to enter a host value or select a list of hosts for the report to return data.

This report supports PCI DSS Requirement 8.5 by facilitating the review of authentication activity.

### **New Users Accessing Databases**

This report shows users accessing a database server within a specified time period. Few users directly access databases, so any occurrences of this are worth reviewing.

This report supports PCI DSS Requirement 8.5 by facilitating the review of authentication activity.

### **Top Accounts Authenticating**

This report shows users with the highest successful login rates for the specified time period.

This report supports PCI DSS Requirement 8.5 by facilitating the review of authentication activity.

### **Top Accounts Failing to Authenticate**

This report shows the users with the highest rate of failed logins within a specified time period.

This report supports PCI DSS Requirement 8.5 by facilitating the review of authentication activity.

### **Users Authenticating from Multiple Sources**

This report shows the users who successfully and unsuccessfully attempt to authenticate from many sources during a specified time period.

Login to a single account from multiple hosts can indicate a lack of control over the usage of the account. For instance, the account may be used to run services, automated tasks, or may be used by multiple people. This report facilitates verification of compliance with PCI DSS Requirement 8.5.8 which prohibits sharing of accounts.

### **Users Connecting to DB from New Sources**

This report shows users accessing a database server from a new client address within a specified time period.

Login to a single account from multiple hosts can indicate a lack of control over the usage of the account. Different functions should access the databases using different accounts to facilitate assignment of least privilege and accountability. This report supports verification of compliance with PCI DSS Requirement 8.5.8 which prohibits sharing of accounts.

## **9. Restrict Physical Access to Cardholder Data**

Reports supporting compliance with section 9 of the PCI Data Security Standard.

## Local Login to Selected Hosts

This report shows local login attempts to selected hosts, such as critical servers, within a specified time period. It is essential to enter a host value or select a list of hosts for the report to return data.

PCI DSS requires restriction of physical access to cardholder data. Review of local console logins to hosts in the cardholder data environment can help identify those who have physical access to the environment and allows for review of any such access. This report assists in verifying compliance with Requirement 9.1 of the PCI DSS.

## 10. Audit and Monitor

Reports supporting compliance with section 10 of the PCI Data Security Standard.

### Audit Trail

#### Audit Subsystem Events

This report shows the summarized events related to auditing information received from data sources within a specified time period.

PCI DSS Requirements 10.2.3, 10.2.6, and 10.5 specify that control over audit trails be maintained. This report, in listing events relating to the audit trail, supports verification of compliance with those requirements.

#### New Users of Selected Files

This report shows users accessing selected files for the first time, within a specified time period. It is essential to enter a file name or select a list of files for the report to return data.

PCI DSS Requirements 10.2.3, 10.2.6, and 10.5 specify that control over audit trails be maintained. This report, when applied to audit trail files, supports verification of compliance with those requirements.

## **Report Use**

This report shows report usage, grouped by user, that occurred within a specified time period.

PCI DSS Requirements 10.2.3, 10.2.6, and 10.5 specify that control over audit trails be maintained and that all access to audit trails be logged. Reports themselves offer a means to access audit trail data. This report, in listing all usage of reports, supports verification of compliance with those requirements.

## **Selected File Accessed by New Program**

This report shows the access of selected files by new programs within a specified time period. Highly sensitive files are usually accessed in a limited number of ways, and any access by a new program should be reviewed. It is essential to enter a file name or select a list of files for the report to return data.

PCI DSS Requirements 10.2.3, 10.2.6, and 10.5 specify that control over audit trails be maintained. This report, when applied to audit trail files, lists new types of access to audit trail data, supporting verification of compliance with those requirements.

## **Selected Users Accessing Selected Files**

This report shows any users who accessed the selected files, within a specified time period. The report can be used to identify access to business files by privileged system users (such as administrators). It is essential to enter a file name or select a list of files for the report to return data. The report results are grouped by user.

PCI DSS Requirements 10.2.3, 10.2.6, and 10.5 specify that control over audit trails be maintained. This report, in listing events relating to the audit trail, supports verification of compliance with those requirements.

## **Users Accessing Selected Files**

This report shows all users who have accessed the specified file(s) (which are usually sensitive resources) for the specified time period. It is essential to enter a file name or select a list of files for the report to return data. The results are grouped by file.

PCI DSS Requirements 10.2.3, 10.2.6, and 10.5 specify that control over audit trails be maintained. This report, in listing events relating to the audit trail, supports verification of compliance with those requirements.

### **Users Accessing Selected Files (Detail)**

This report shows all users who have accessed the specified file(s) (which are usually sensitive resources) for the specified time period. It is essential to enter a file name or select a list of files for the report to return data. The results are grouped by file.

PCI DSS Requirements 10.2.3, 10.2.6, and 10.5 specify that control over audit trails be maintained. This report, in listing events relating to the audit trail, supports verification of compliance with those requirements.

## **Automated Notification**

### **Notification Summary**

This report shows the defined notification types and how many notifications have been sent within the specified time period.

PCI DSS Requirement 10.6 specifies that audit logs be reviewed. SAFE notification rules allow for automated review and alerting. This report supports verification of compliance with requirement 10.6 by summarizing notifications generated by SAFE.

### **Notifications by Policy**

This report summarizes notifications according to policy tag within the specified time period.

PCI DSS Requirement 10.6 specifies that audit logs be reviewed. SAFE notification rules allow for automated review and alerting. This report supports verification of compliance with requirement 10.6 by summarizing notifications generated by SAFE.

### **Notifications by Process**

This report summarizes notifications by process tag within the specified time period.

PCI DSS Requirement 10.6 specifies that audit logs be reviewed. SAFE notification rules allow for automated review and alerting. This report supports verification of compliance with requirement 10.6 by summarizing notifications generated by SAFE.

## Log Management

### Data Sources

This report shows details of the status and operation of SAFE and of the data sources providing logs to SAFE within a specified time period. This report may also reveal spikes in event rates. The parameters within the report can also list the detectors associated with various types of events.

PCI DSS Requirement 10.6 requires review of logs and recommends use of Log harvesting, parsing, and alerting tools, such as SAFE, for achieving compliance with the requirement. This report provides an overview of the logs processed by SAFE in support of requirement 10.6.

### Summary of Errors and Availability Events

This report shows all events related to error and availability activities, determined by highest count, within a specified time period.

Events relating to host errors and availability should be recorded and reviewed. This information can be used to track such activities as failed logins, system downtime, etc. This report examines the top events related to errors and availability and reports on the number of times these events occurred. This report assists in verifying compliance with Requirement 10, 10.2, and 10.3 of the PCI DSS.

### Top Acting Users

This report shows the most active users, grouped by event type, within a specified time period.

This report provides an overview of the users whose activities are monitored through the logs processed by SAFE. The information from this report assists in verification of compliance with Requirement 10, 10.1, 10.2, 10.3 and 10.6 of the PCI DSS.

### Top Detectors

This report shows the top detectors, determined by the highest event count within a specified time period.

This report provides an overview of the hosts whose logs are processed by SAFE. The information from this report assists in verification of compliance with Requirement 10, 10.1, 10.2, 10.3 and 10.6 of the PCI DSS.

### **Top Event Types**

This report shows the top event types within a specified time period.

This report provides an overview of the types of events monitored through the logs processed by SAFE. The information from this report assists in verification of compliance with Requirement 10, 10.1, 10.2, 10.3 and 10.6 of the PCI DSS.

## **11. Regularly Test Security**

Reports supporting compliance with section 11 of the PCI Data Security Standard.

### **Asset Vulnerabilities**

This report shows the asset vulnerabilities within a specified time period.

By allowing for review of vulnerability scan results, this report supports PCI DSS Requirement 11.2.

### **Asset Vulnerability History**

This report shows the asset vulnerability history within the specified time period.

By allowing for review of vulnerability scan results, this report supports PCI DSS Requirement 11.2.

### **Assets with Selected Vulnerability**

This report shows assets and their related vulnerability ID within a specified time period.

By allowing for review of vulnerability scan results, this report supports PCI DSS Requirement 11.2.

### **Most Common Vulnerabilities**

This report shows the most common vulnerabilities with a specified time period.

By allowing for review of vulnerability scan results, this report supports PCI DSS Requirement 11.2.

### **Most Severe Vulnerabilities**

This report shows the most severe vulnerabilities within a specified time period.

By allowing for review of vulnerability scan results, this report supports PCI DSS Requirement 11.2.

### **Most Vulnerable Assets**

This report shows the most vulnerable assets within the specified time period.

By allowing for review of vulnerability scan results, this report supports PCI DSS Requirement 11.2.

### **Most Vulnerable Zones**

This report shows the most vulnerable zones within a specified time period.

By allowing for review of vulnerability scan results, this report supports PCI DSS Requirement 11.2.

## **12. Maintain a Security Policy**

Reports supporting compliance with section 12 of the PCI Data Security Standard.

### **Notifications by Policy**

This report summarizes notifications according to policy tag within the specified time period.

PCI DSS Requirement 10.6 specifies that audit logs be reviewed. SAFE notification rules allow for automated review and alerting. This report supports veri-

fication of compliance with requirement 10.6 by summarizing notifications generated by SAFE.

## **Notifications by Process**

This report summarizes notifications by process tag within the specified time period.

PCI DSS Requirement 10.6 specifies that audit logs be reviewed. SAFE notification rules allow for automated review and alerting. This report supports verification of compliance with requirement 10.6 by summarizing notifications generated by SAFE.