TIBCO LogLogic® Compliance Suite - PCI Edition
Guide

Software Release 3.9.0
November 2017
Document Updated: April 2018

Two-Second Advantage®

TIBCO®

Important Information

This document contains excerpted portions of the Payment Card Industry ("PCI") standards (collectively, the "Regulatory Language"). The Regulatory Language is provided by TIBCO solely for your convenience and to provide context for certain functionality of the TIBCO LogLogic® products. The inclusion or omission by TIBCO of any Regulatory Language is in no way intended as legal advice regarding the PCI standards and does not constitute any representation or warranty that any TIBCO products comply with the terms contained in such Regulatory Language. If you have additional questions about the PCI standards, you should consult with an attorney for further legal guidance.

Contents

Figures 7
TIBCO Documentation and Support Services 8
Establishment of IT Controls for PCI Compliance 9
The TIBCO LogLogic® Compliance Suite - PCI Edition Overview 10
Compliance Reports and Alerts Overview 10
The TIBCO LogLogic Compliance Suite Setup 12
Installing the Compliance Suite 12
The Compliance Suite Usage 14
The Compliance Suite Reports 14
Viewing Compliance Suite Reports and Output Data 14
Customizing Compliance Suite Reports 16
The Compliance Suite Alerts 17
Accessing Available Compliance Suite Alerts 17
Enabling Compliance Suite Alerts 17
Viewing Compliance Suite Alert Results 19
Payment Card Industry Data Security Standard (PCI DSS) Requirements 21
Requirement 1: Install and maintain a firewall configuration to protect cardholder data 21
Sub-Requirements 1.1.1, 1.1.8 and 1.1.9 22
Sub-Requirements 1.1.5, 1.1.6, 1.2, 1.3.2 and 1.3.5 (Update: v3.0 11/2013) 22
Sub-Requirement 1.1.7 23
Sub-Requirement 1.3.1 23
Sub-Requirement 1.5 (Update: v3.0 11/2013) 24
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters 24
Sub-Requirement 2.2.2and 2.2.3 (Update: v3.0 11/2013) 25
Sub-Requirement 2.3 25
Sub-Requirement 2.5 (Update: v3.0 11/2013) 26
Requirement 3: Protect stored cardholder data 26
Sub-Requirement 3.7 (Update: v3.0 11/2013) 26
Requirement 4: Encrypt transmission of cardholder data across open public networks 27
Sub-Requirement 4.3 (Update: v3.0 11/2013) 27
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs 27
Sub-Requirement 5.4 (Update: v3.0 11/2013) 28
Requirement 6: Develop and maintain secure systems and applications 28
Sub-Requirement 6.1 29
Sub-Requirement 6.2 (Update:v3.0 11/2013) 29
Sub-Requirement 6.3.3 30

Sub-Requirement 6.4 30
Sub-Requirement 6.7 (Update: v3.0 11/2013) 31
Requirement 7: Restrict access to cardholder data by business need-to-know 31
Sub-Requirement 7.1 and 7.2 31
Sub-Requirement 7.3 Update: v3.0 11/2013) 32
Requirement 8: Assign a unique ID to each person with computer access 32
Sub-Requirement 8.1 and 8.5.8 33
Sub-Requirement 8.1.5 (Update v3.0 11/2013) 34
Sub-Requirement 8.5.1 (Update: v3.0 11/2013) 34
Sub-Requirement 8.5.4 35
Sub-Requirement 8.5.6 35
Sub-Requirement 8.5.9 35
Sub-Requirement 8.5.13 36
Sub-Requirement 8.5.16 36
Sub-Requirement 8.6 36
Sub-Requirement 8.8 (Update: v3.0 11/2013) 36
Requirement 9: Restrict physical access to cardholder data 37
Sub-Requirement 9.10 (Update: v3.0 11/2013) 37
Requirement 10: Track and monitor all access to network resources and cardholder data 37
Sub-Requirement 10.1 39
Sub-Requirement 10.2.1, 10.2.2 and 10.2.4 40
Sub-Requirements 10.2.3, 10.2.6, 10.5 and 10.6 40
Sub-Requirement 10.2.5 41
Sub-Requirement 10.2.7 41
Sub-Requirement 10.3 42
Sub-Requirement 10.7 42
Sub-Requirement 10.8 (Update: v3.0 11/2013) 43
Requirement 11: Regularly test security systems and processes 43
Sub-Requirement 11.4 44
Sub-Requirement 11.5 44
Sub-Requirement 11.6 (Update v3.0 11/2013) 44
Requirement 12: Maintain a policy that addresses information security for employees and contractors 45
Sub-Requirement 12.2 45
Sub-Requirement 12.9.5 45
TIBCO LogLogic Reports and Alerts for PCI 46
TIBCO LogLogic Reports for PCI 46
TIBCO LogLogic Alerts for PCI 70
TIBCO LogLogic Reports and Alerts Quick Reference 78
PCI and COBIT 4.0 Control Objectives Mapping 150

Introduction to COBIT 150
PCI Requirements and COBIT 4.0 Control Objectives Mapping 150

Figures

Loading a Compliance Suite File 12
Selected Entities to be Imported 13
Compliance Suite Reports 14
Failed Logins Report Details 15
Failed Logins Report Results 15
Advanced Options and Update Saved Custom Report Views 16
Compliance Suite Alerts 17
Login Failed Alert Filters 18
Available and Selected Devices 19
Aggregated Alert Log 20

TIBCO Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

Product-Specific Documentation

The following documents for this product can be found on the TIBCO Documentation site:

- *TIBCO LogLogic® Compliance Suite - PCI Guide*
- *TIBCO LogLogic® Compliance Suite - PCI Readme*
- *TIBCO LogLogic® Compliance Suite - PCI Release Notes*

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit http://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, you can request one by clicking Register on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to https://community.tibco.com.

Establishment of IT Controls for PCI Compliance

In recent years, cardholder security breaches have seriously harmed company reputations and damaged consumer trust and confidence. To address these issues, American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International have established the Payment Card Industry (PCI) Security Standards Council to develop and administer the PCI Data Security Standard (DSS) and its supporting programs. The overriding goal of the PCI DSS is to ensure the security and integrity of cardholder data and uphold consumer confidence in card payments. The PCI Security Standards Council released version 1.1 of the PCI DSS in September, 2006. This version of the TIBCO LogLogic® Compliance Suite - PCI Edition supports version 2.0 of the PCI DSS.

The intent of the standard is to provide compliance requirements that dictate how cardholder data should be protected in environments that store, process, or transmit this data. Merchants and service providers that do not comply with the standard face the prospect of substantial fines or of being permanently barred from the card acceptance programs, should a security breach occur which involves their systems or processes. PCI compliance applies to any organization that stores, processes or transmits cardholder data and consequently affects brick and mortar and online merchants as well as many banks, processors and service providers.

Note that these PCI DSS Requirements apply to all Members, merchants, and service providers that store, process or transmit cardholder data. Additionally, these security requirements apply to all “system components”, defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components include, but are not limited to, firewalls, switches, routers, wireless access points, VPNs, and other security Appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP. Applications include all purchased and custom applications, including internally-used and external-facing applications.

Critical infrastructure data in the form of log files from corporate firewalls, VPN concentrators, web proxies, IDS systems, email servers, operating systems, enterprise applications and backup systems provide valuable insight into risks, IT performance, and the use of corporate assets. However, these logs are often not readily available or accessible when corporations need them most – during compliance audits, security incident response, or when responding to information requests from legal, human resources and other business units. Achieving compliance requires you to be able, in real-time, to access, search through and organize such data quickly and cost-effectively.

Today, tens of thousands of log data messages are produced by enterprise systems, applications and network devices every day. In many Fortune 1000 enterprises, these messages add up to multiple terabytes of data per month. At these rates, it is not humanly possible to extract necessary information from logs using homegrown scripts or manual processes. For example, to satisfy PCI compliance, you must not only ensure that appropriate IT controls are in place, you must also provide independent auditors with evidence of functioning controls and the documented results of testing procedures. This could take days using scripts and manual process - a luxury and expense that you cannot afford.

The TIBCO LogLogic® Compliance Suite - PCI Edition Overview

The TIBCO LogLogic® Compliance Suite - PCI Edition is the first solution of its kind. It delivers automated process validation and includes reporting and alerts that can be used to evidence and enforce business and IT policies related to compliance. By automating compliance reporting and alerting based on critical data collected and stored by TIBCO LogLogic's Appliances, the TIBCO LogLogic® Compliance Suite - PCI Edition removes the complexity and resource requirements typically needed to implement control frameworks to successfully meet PCI and other compliance requirements.

TIBCO LogLogic® Compliance Suite - PCI Edition:

- Automates compliance activities and dramatically improves audit accuracy.
- Reduces the time to mitigate the risk factor.
- Allows organizations to use infrastructure data to provide evidence of and enforce IT controls.
- Provides industry-leading reporting depth and breadth, including real-time reporting and alerting for PCI compliance. Fifty (50) PCI DSS requirements were identified that can be evidenced or validated by TIBCO LogLogic reports and alerts.
- Delivers approximately 387 out-of-the-box Compliance Reports and 140 out-of-the-box Alerts.
- Enables customization of any Compliance Report to map specifically to your organization's unique policies and requirements.

Compliance Reports and Alerts Overview

Log data allows organizations to manage the challenge of achieving and maintaining PCI compliance. TIBCO LogLogic's compliance reports and alerts generally fall into the following categories:

- Security and Threat Management
- Change and Configuration Management
- Identity and Access Management
- Monitoring and Reporting

Security and Threat Management

The TIBCO LogLogic® Compliance Suite - PCI Edition includes reports and alerts to show that all network security devices, including firewalls which control traffic into a company's network, as well as intrusion detection systems which monitor the traffic, have been configured appropriately to allow only the requested and approved traffic in and out of the network.

Non-compliance in this area may result in unauthorized access from the Internet. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network and are featured prominently in the PCI DSS.

Change and Configuration Management

The TIBCO LogLogic® Compliance Suite - PCI Edition includes reports and alerts to show that all system changes are appropriately requested, approved, tested, and validated by authorized personnel prior to implementation in the production environment.

Non-compliance in this area may result in unauthorized changes and/or improper roll-out of new source code to key systems. This may negatively impact the confidentiality, integrity, and availability of cardholder information.

Identity and Access Management

The TIBCO LogLogic® Compliance Suite - PCI Edition includes reports and alerts to show that all PCI-related systems (i.e., networks, applications, and databases) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data, and that the division of roles and responsibilities has been implemented to reduce the possibility for a single individual to subvert a critical process. Management needs to ensure that personnel are performing only authorized duties relevant to their respective jobs and positions.

Non-compliance may result in unauthorized or inappropriate access to key systems, which may negatively impact the confidentiality, integrity, and availability of cardholder information.

Monitoring and Reporting

The TIBCO LogLogic® Compliance Suite - PCI Edition includes reports and alerts to allow customers to continuously monitor the IT infrastructure for security violations and other anomalies. Reports are provided in a format meaningful to stakeholders. The monitoring statistics should be analyzed and acted upon to identify trends for individual systems and the overall PCI environment.

Non-compliance in this area could significantly impact service availability as well as security of the IT infrastructure.

The TIBCO LogLogic Compliance Suite Setup

Setting up the TIBCO LogLogic® Compliance Suite - PCI Edition comprises checking that all prerequisites are met before starting the installation process, installing the Compliance Suite file, and enabling the alerts.

Installing the Compliance Suite

Prerequisites

Before installing the TIBCO LogLogic® Compliance Suite - PCI Edition, ensure that you have:

- TIBCO LogLogic LX or MX or ST Appliance running TIBCO LogLogic Release 5.7.x or higher
- TIBCO LogLogic® Log Source Packages (LSP) 32.1 or 33 installed

The Compliance Suite includes one XML file containing PCI search filters, custom reports, and alerts:

- `PCI.xml` – PCI Search Filters, Custom Reports, and Alerts

If you have previously imported any earlier versions of the Compliance Suite files, importing this version of the Compliance Suite will not overwrite the original files or any changes that have been made, unless you have saved the changes to the object using the default name.

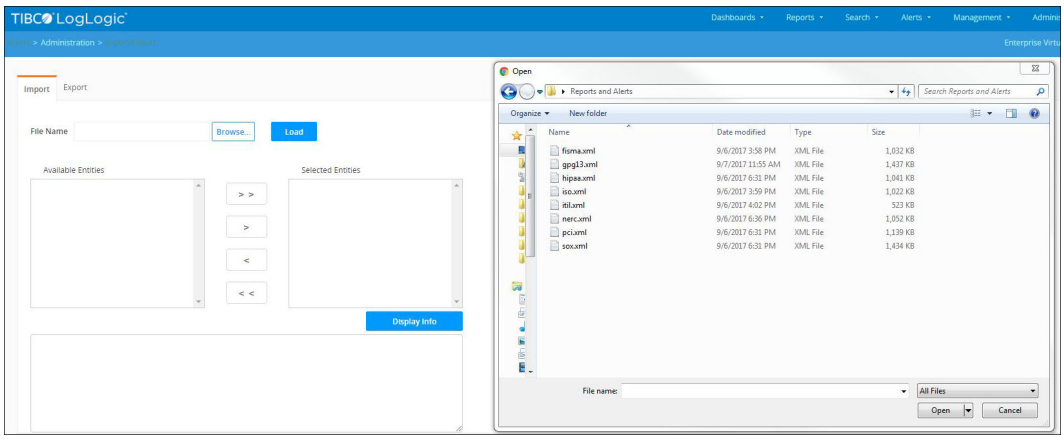
If you have made any changes to base Compliance Suite alerts, search filters, or custom reports, TIBCO recommends saving these items with non-default names. This will help ensure that the latest Compliance Suite updates can be installed without any compatibility issues or naming conflicts.

Procedure

1. Log in to your TIBCO LogLogic LX or MX or ST Appliance as admin.
2. From the navigation menu, select **Administration** > **Import or Export** .
3. The **Import** and **Export** tabs appear.
4. Load the Compliance Suite file by completing the following steps:
   a) In the **Import** tab, click **Browse**.
   b) In the **File Upload** window, select the appropriate XML file and then click **Open**.

   The following figure shows the **File Upload** window that appears after clicking **Browse** on the **Import** tab.

   Loading a Compliance Suite File



c) Click **Load**.

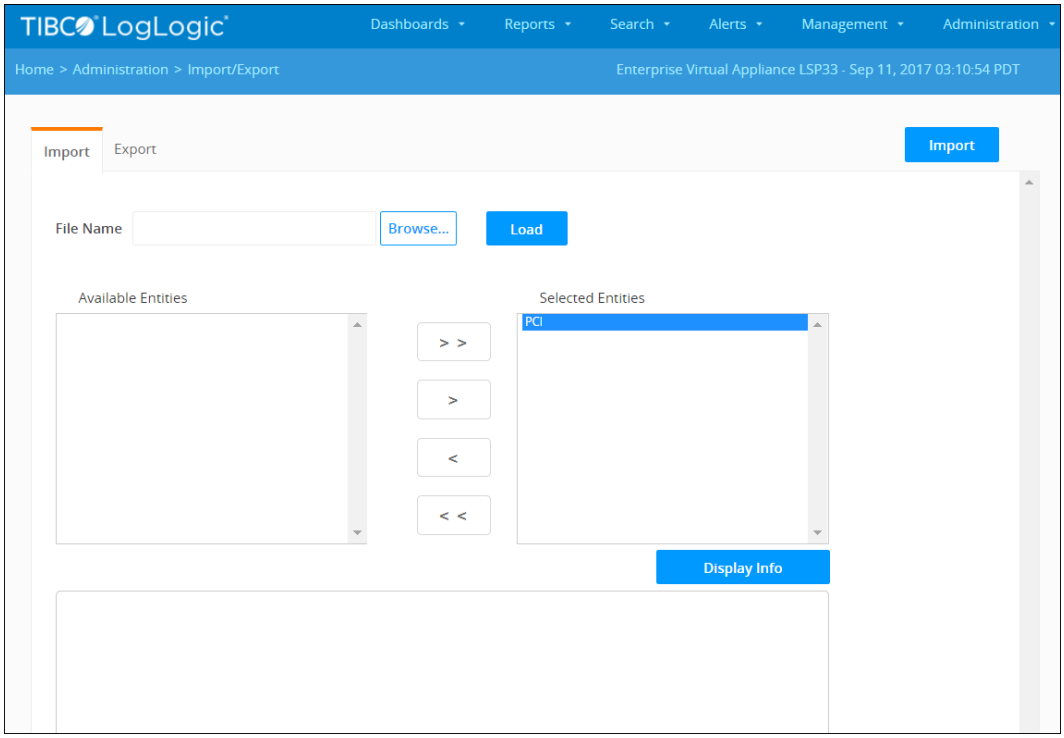
This loads the **Available Entities** from the XML file.

d) Click **Add All Entities**.

You can also select the specific PCI entity from the **Available Entities** text block, and then click **Add Selected Entities**.

The following figure shows all entities of the PCI XML file that were selected by clicking **Add All Entities**.

Selected Entities to be Imported



5. Click **Import**.

An import successfully completed message appears above the **File Name** text field.

Installation is complete after the XML file is imported successfully.

The Compliance Suite Usage

Once you have successfully installed the TIBCO LogLogic® Compliance Suite - PCI Edition, you can begin using the custom reports and alerts. The following sections help you view, test, and modify, the packaged custom reports and alerts. The custom reports and alerts were designed to run out-of-the box; however, TIBCO LogLogic enables you to perform further customization if necessary.

The Compliance Suite Reports

All TIBCO LogLogic® Compliance Suite - PCI Edition reports are designed to run out-of-the box as well as to be flexible if you need to make modifications based on your business needs.

For a description of all custom reports in this Compliance Suite, see TIBCO LogLogic Reports for PCI.

Viewing Compliance Suite Reports and Output Data

Procedure

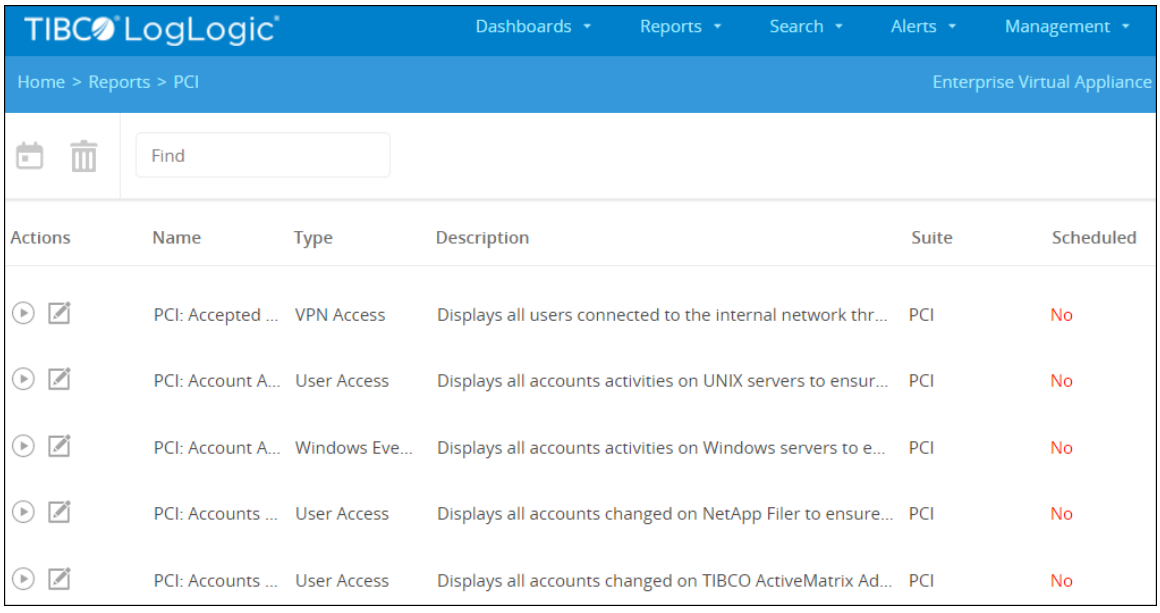
1. Log in to your TIBCO LogLogic LX/MX/ST Appliance as admin.
2. From the navigation menu, select **Reports** > **PCI** .

   You can also access all of your custom reports on the Appliance including the Compliance Suite reports you installed, by selecting **Reports** > **All Saved Reports** .
3. On the **Reports** page, you can see all of the custom reports you loaded during the installation process.

   You can navigate through all of the custom reports using the page navigation buttons at the top and bottom of the **Reports** page.

   The following figure shows a cropped list of the Compliance Suite reports loaded from the PCI XML file.

   Compliance Suite Reports

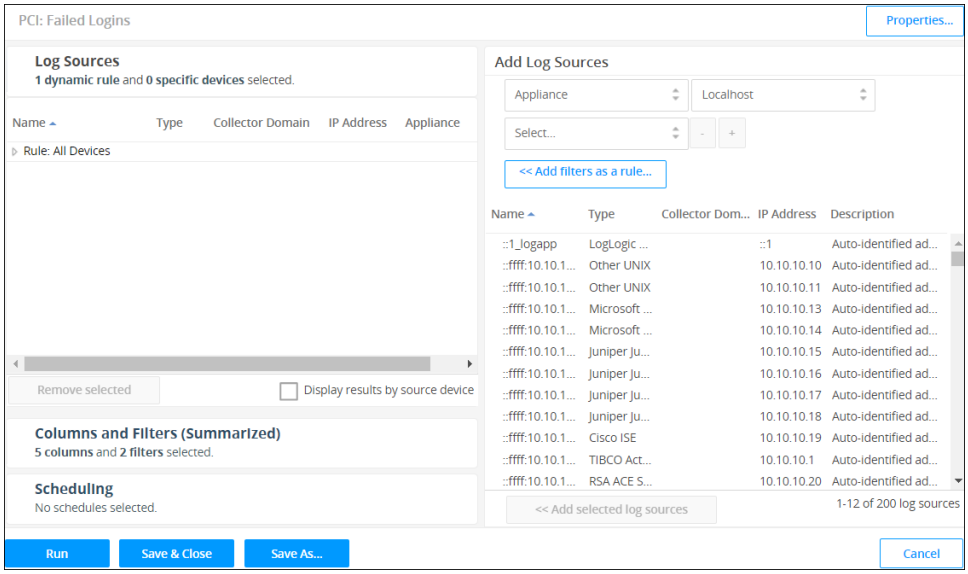


4. Click the **Edit** button of a report to see details such as, the Appliance where the report runs, the associated device type, and when the report runs.
   a) To view the filter parameters, click **Columns and Filters**.

b) To view details about a report such as the report name and description, click **Properties**.

The following figure shows the details of the **PCI: Failed Logins** report.

Failed Logins Report Details



5. Run the report to view the report output data by completing the following steps:

a) Click **Run**.

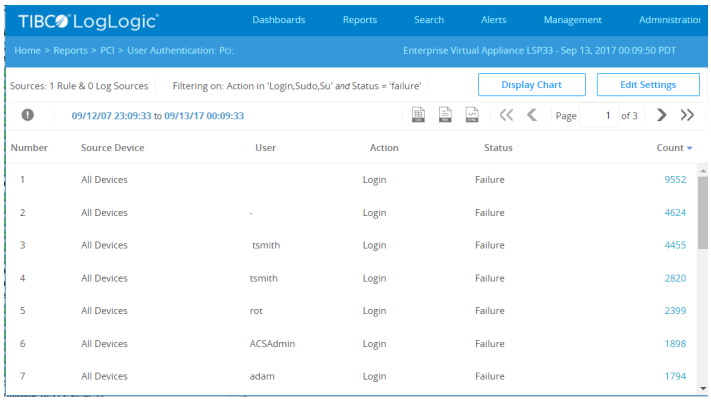
The report runs and returns data based on the set parameters.

b) To view detailed drill-down information, click the Count column link.

You can use the **Back to summarized results** button to return to the main data output view.

The following figure shows sample results from the **PCI: Failed Logins** report.

Failed Logins Report Results



If you want to modify the main data output view, you can modify the report parameters and then run the report again.

Customizing Compliance Suite Reports

The TIBCO LogLogic® Compliance Suite - PCI Edition reports are designed to run out-of-the-box to meet specific compliance requirements. However, you may want to modify the reports to include additional information or devices depending on your business needs.

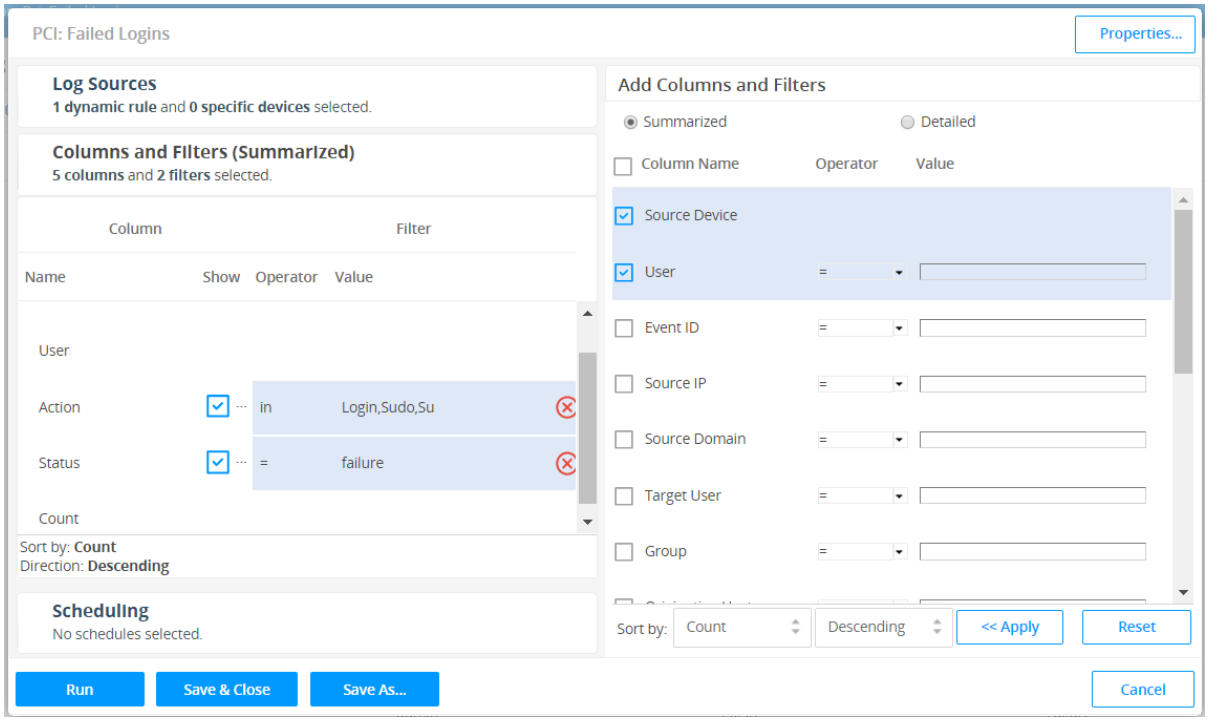
Procedure

1. Make sure that you are on the **Reports** page and click the **Edit** button of a report you want to modify.
2. Modify the report details (i.e., name, description, etc.), filters, and parameters.

   TIBCO LogLogic enables you to customize everything pertaining to the summarization and presentation of the reports. You can modify the device(s) on which the report runs, schedule when the report runs, and set specific report search filters.

   The following figure shows the report filters available under **Columns and Filters**.

   Advanced Options and Update Saved Custom Report Views



It is a good practice to test your modifications to ensure that the report meets your business needs.

3. To test the report, click **Run**.

   The report runs and returns data based on the set parameters. Verify that the returned data is what you want. Continue modifying and testing the report as needed.

4. Save the report by completing the following steps:
   a) Click **Save As**.

      Make any necessary modifications to the report details (i.e., **Report Name**, **Report Description**, etc.).
   b) Click **Save & Close**.

      A report saved message appears. Your report is now modified. Consider testing the output of the report again to ensure you are returning all of the data you need from this report.

The Compliance Suite Alerts

The TIBCO LogLogic® Compliance Suite - PCI Edition alerts enable you to manage activities helping you to maintain PCI compliance. Activities can include detecting unusual traffic on your network or detecting Appliance system anomalies. By default, the Compliance Suite alerts are disabled so that you can configure your environment with only those alerts that are necessary.

For a description of all alerts in this Compliance Suite, see TIBCO LogLogic Alerts for PCI.

Accessing Available Compliance Suite Alerts

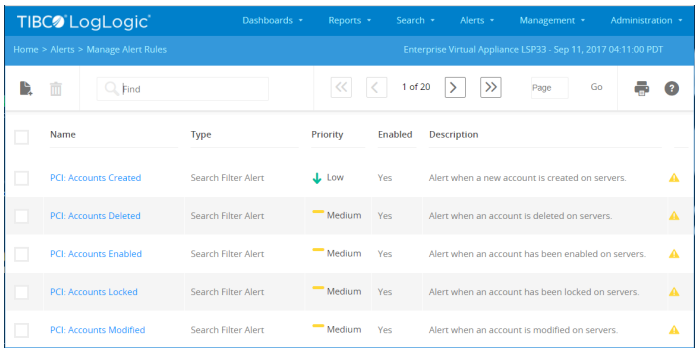
The Compliance Suite package contains a number of alerts that can be easily enabled and modified for your business needs.

Procedure

1. From the navigation menu, click **Alerts** > **Manage Alert Rules** .

   The following figure shows a cropped list of the Compliance Suite alerts loaded from the PCI XML file.

   Compliance Suite Alerts



2. To view details of a specific alert, click the **Name** of the alert.

   The **General** tab is selected by default, but each tab on the page contains information required to enable an alert.

3. Click on each of the tabs to view the default entries.

   Make sure that you identify the default entries and areas that might need to be modified.

Enabling Compliance Suite Alerts

By default, the compliance suite alerts have pre-configured information to help you get started. In some instances, you can simply enable the alert, since the default settings are aimed at capturing a broad range of alerts.

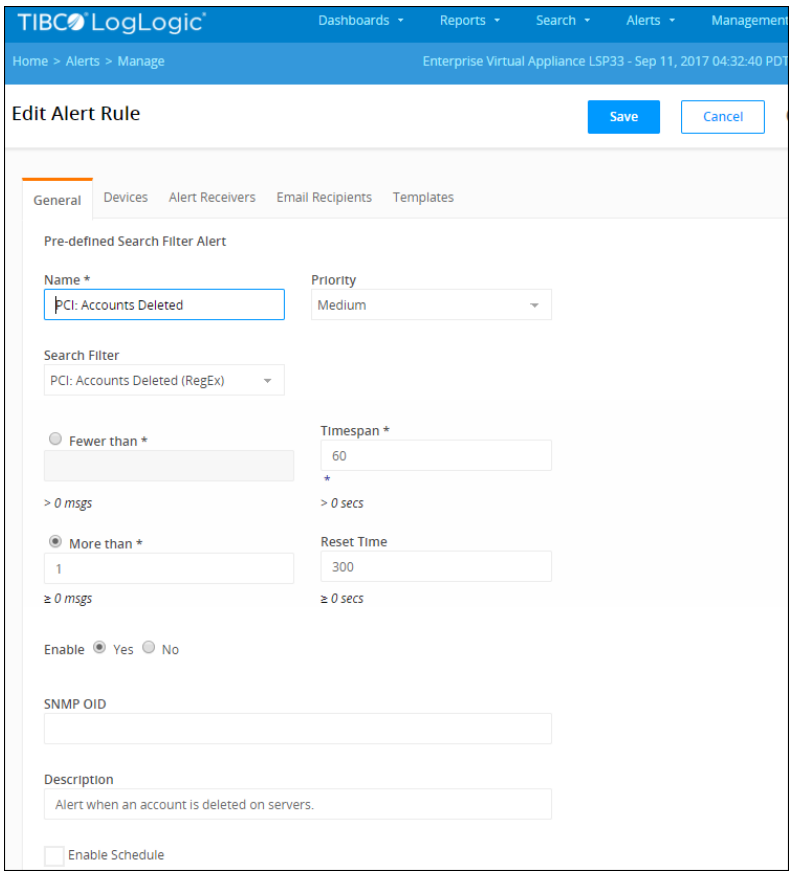
To enable alerts, you must set at least the device(s) to monitor, the SNMP trap receivers, as well as who receives an alert notification and how they receive it.

Procedure

1. From the navigation menu, select **Alerts** > **Manage Alerts** .
2. Click the **Name** of the alert.
3. On the **General** tab, for **Enable** select the **Yes** radio button.

   The following figure shows the **General** tab for the **PCI: Accounts Deleted** alert.

Login Failed Alert Filters



4. Select the device(s) to be alerted on by completing the following steps:

   You can define alerts for all devices, a selection of devices, or a single device.

   a) Select the **Devices** tab.

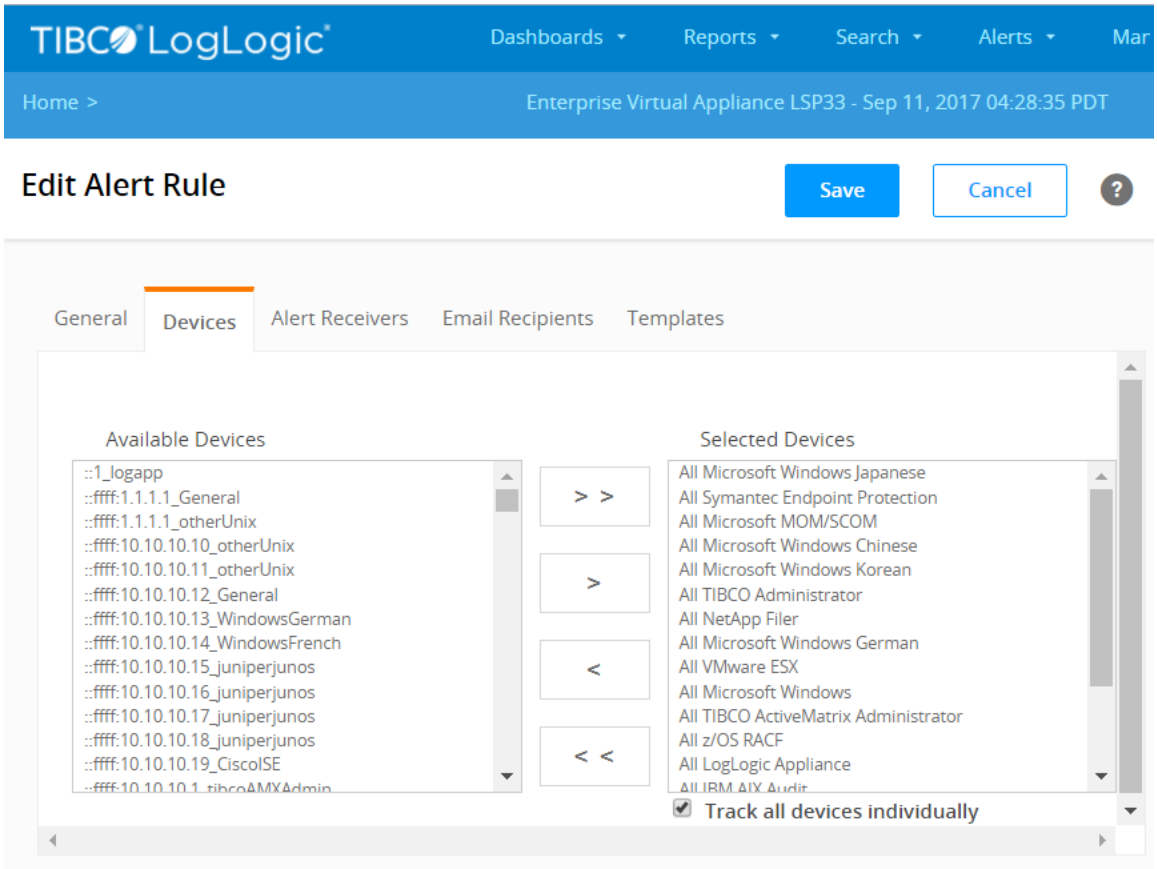
   b) In the **Available Devices** text block, select the appropriate log sources (i.e., devices) you want to monitor and be alerted on when an alert rule is triggered.

   > If the **Show Only Device Groups** setting is enabled on the Appliance, then the **Available Devices** text block lists only device groups. To enable or disable this feature, go to **Administration** > **System Settings** > **General** tab, scroll down to the **System Performance Settings** section and modify the **Optimize Device Selection List** option.

   c) Click **Add All** or **Add Selected Device(s)**.

   The following figure shows the **Devices** tab for the selected alert.

Available and Selected Devices



5. The Appliance has the ability to generate an SNMP trap that is sent to an SNMP trap receiver when an alert rule is triggered. Select the alert receivers available to your device(s) by completing the following steps:
   a) Select the **Alert Receivers** tab.
   b) In the **Available Alert Receivers** text block, select the appropriate alert receivers available for your device(s).
   c) Click **Add All** or **Add Selected Receiver(s)**.
6. Select the email recipients to be alerted with a notification email when an alert rule is triggered by completing the following steps:
   a) Select the **Email Recipients** tab.
   b) In the **Available Users** text block, select the appropriate email recipients.
   c) The **Available Users** text block lists all of the user accounts on the Appliance.
   d) Click **Add All** or **Add Selected User(s)**.
7. Click **Update**.

Viewing Compliance Suite Alert Results

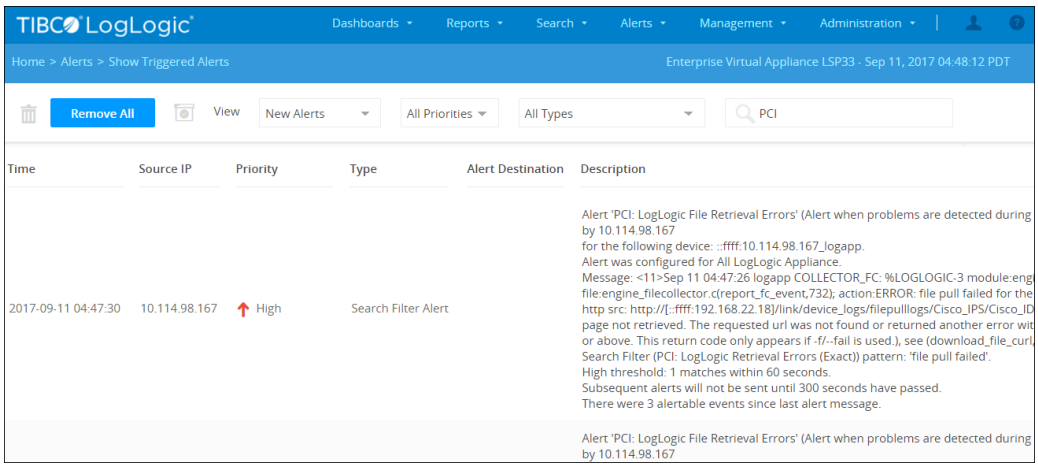
After you have enabled at least one alert, and that alert is triggered, you can view the results.

Procedure

1. In the navigation menu, select **Alerts** > **Show Triggered Alerts** .

   The following figure shows a cropped version of the **Show Triggered Alerts** page.

Aggregated Alert Log



2. From the **Show** drop-down menus, select the desired alert and priority filters to show only those alerts you want to display. The defaults are **New Alerts** and **All Priorities**.
3. (Management Station Appliances Only) From the **From Appliance** drop-down menu, select the appliance from which you want to view the alerts.
4. View the results of your query. You can navigate through all of the data by using the page navigation buttons or page text field.
5. You can either acknowledge or remove an alert. Click the checkbox next to the alert name, then click either **Acknowledge**, **Remove**, or **Remove All**.

Each alert was triggered based on your set alert parameters, so care must be taken when acknowledging or removing the alert.

Payment Card Industry Data Security Standard (PCI DSS) Requirements

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open public networks
- Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure systems and applications
- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes
- Requirement 12: Maintain a policy that addresses information security for employees and contractors

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether via e-commerce, employee Internet access, email traffic, or other pathways. Often, seemingly insignificant paths to and from the Internet can provide unprotected access into key systems. Firewalls are a key protection mechanism for any computer network.

The following table lists the specific sub-requirements in Requirement 1 that are addressed by TIBCO LogLogic® Compliance Suite - PCI Edition.

Requirement 1	Install and maintain a firewall configuration to protect Cardholder data
1.1.1	A formal process for approving and testing all external network connections and changes to the firewall configuration
1.1.5	Documented list of services and ports necessary for business
1.1.6	Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN (Update: v3.0 November 2013)
1.1.7	Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented
1.1.8	Quarterly review of firewall and router rule sets

Requirement 1	Install and maintain a firewall configuration to protect Cardholder data
1.1.9	Configuration standards for routers
1.2	Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment
1.3.1	Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters)
1.3.2	Not allowing internal addresses to pass from the Internet into the DMZ
1.3.5	Restricting inbound and outbound traffic to that which is necessary for the cardholder data
1.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Update: v3.0 August 2013)

Sub-Requirements 1.1.1, 1.1.8 and 1.1.9

- 1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration
- 1.1.8 Quarterly review of firewall and router rule sets
- 1.1.9 Configuration standards for routers

Illustrative Controls and the TIBCO LogLogic Solution

Administrators must identify all changes to firewall and router configurations and ensure that a formal process is in place for all changes, including management approval and testing for all changes to external network connections and the firewall configuration. Administrators must also ensure all changes are authorized and that rule sets are periodically reviewed. The most efficient way to identify configuration changes is at the time of the modification. Administrators should setup alerts so that any changes to the configuration, authorized or otherwise, are detected.

Administrators must also periodically review all firewall rules to ensure accurate access control lists. In addition, administrators must review network traffic correlated with the firewall policy to ensure appropriate access control rules are used to protect the environment.

Reports and Alerts

Refer TIBCO LogLogic Reports and Alerts Quick Reference to see the 1.1.1, 1.1.8, 1.1.9 reports and alerts.

Sub-Requirements 1.1.5, 1.1.6, 1.2, 1.3.2 and 1.3.5 (Update: v3.0 11/2013)

- 1.1.5 Documented list of services and ports necessary for business
- 1.1.6 Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN. (Maps to prior Requirement. 1.1.5)
- 1.2 Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment

- 1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ
- 1.3.5 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment

Illustrative Controls and the TIBCO LogLogic Solution

Administrators must document all services and ports necessary for business and identify all ports and protocols passed through the firewall besides HTTP (generally port 80/tcp), SSL (generally port 443/tcp), SSH (generally port 22/tcp), and VPN (Virtual Private Network, generally IP protocols 50 and 51 and port 500/udp – though other ports and protocols may be used). Once identified, administrators must review the exception list and document any justification related to the allowance of these protocols.

If necessary, administrators should identify the timeframe in which these protocols should be allowed, and promptly remove them from the configuration after this period has expired. Administrators should setup network policy alerts to detect any unauthorized traffic passing through the firewalls.

Reports and Alerts

Use the following links/references to see the 1.1.5, 1.1.6, 1.2, 1.3.2, 1.3.5 reports and alerts:

- 1.1.5 reports and alerts on page 79.
- 1.1.6 reports and alerts on page 81.
- 1.2, 1.3.2, 1.3.5 reports and alerts on page 90.

Sub-Requirement 1.1.7

1.1.7 Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented.

Illustrative Controls and the TIBCO LogLogic Solution

Administrators must identify and document all risky protocols and services that are allowed to pass through the firewall. Documentation should include reasons for use of protocol and security features implemented. These risky services include, but are not limited to, FTP (21/tcp), Telnet (23/tcp), Rlogin (513/tcp), Rsh (514/tcp), Netbios (137-139/tcp,udp), and others. Administrators can utilize the following custom reports to help identify risky services and protocols.

To add additional services that are considered risky to the organization, administrators can modify the advanced options in these custom reports. Administrators should also configure network policy alerts to get immediate notification of any allowed risky services.

Reports and Alerts

Use the following link/reference to see the 1.1.7 reports and alerts: 1.1.7 on page 83.

Sub-Requirement 1.3.1

1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters)

Illustrative Controls and the TIBCO LogLogic Solution

A De-Militarized Zone (DMZ) is a network segment where servers are placed if they have to process inbound traffic from the Internet. These servers in the DMZ are responsible for brokering communication between the Internet and other internal servers. This adds an extra layer of protection for the internal network.

No Internet traffic should be able to access internal servers directly. All inbound traffic should be directed to IP addresses within the DMZ. Administrators must configure their firewall policy to specifically deny any Internet traffic to the internal network.

Administrators should review firewall logs to ensure no traffic is initiated from the Internet to the internal network. Administrators should also setup real-time alerts to ensure any such traffic is reviewed. Any firewall policy allowing inbound traffic directly to the internal network should be heavily scrutinized.

Reports and Alerts

Use the following link/reference to see the 1.3.1 reports and alerts: 1.3.1 on page 92.

Sub-Requirement 1.5 (Update: v3.0 11/2013)

1.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior requirement 12.2)

- Examine documentation interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:
  - Documented
  - In use
  - Known to all affected parties

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis.

Reports and Alerts

- Use the link/reference to see the 1.5 reports and alerts: 1.5 on page 93.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Attackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. The following table lists the specific sub-requirements in Requirement 2 that are addressed by TIBCO LogLogic® Compliance Suite - PCI Edition.

Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure-for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. Update: v3.0 November 2013
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access

Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. Update: v3.0 November 2013

Sub-Requirement 2.2.2and 2.2.3 (Update: v3.0 11/2013)

- 2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)
- 2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure-for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. (Maps to prior Requirement 12.2)

Illustrative Controls and the TIBCO LogLogic Solution

Unnecessary services may include risky services such as FTP (21/tcp), Telnet (23/tcp), Rlogin (513/tcp), Rsh (514/tcp), Netbios (137-139/tcp,udp), and others. If these types of risky services are detected at the firewall, it may be a signal that hosts and devices have not been adequately secured according to the standards mandated in PCI requirement 2.2.

Administrators can utilize the following custom reports to help identify risky services and protocols. To add additional services that are considered risky to the organization, administrators can modify the advanced options in these custom reports.

Administrators should also configure network policy alerts to receive notification when any of these risky services are permitted. To add additional unnecessary services to the network policy alerts, administrators can edit the network policy configured for the following alerts. Administrators can also configure a network policy for ONLY allowed services, and be alerted on any services that are not in the allowed list.

Reports and Alerts

Use the following link/reference to see the 2.2.2 and 2.2.3 reports and alerts: 2.2.2 and 2.2.3 on page 94.

Sub-Requirement 2.3

2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (Transport Layer Security) for web-based management and other non-console administrative access

Illustrative Controls and the TIBCO LogLogic Solution

All remote connections by administrative users must be encrypted to limit the possibility of credentials (e.g., usernames and passwords) being intercepted and captured while traversing the network. Technologies such as SSH (generally port 22/tcp), SSL (generally port 443/tcp) and VPN (SSL or IPsec) are typically used to implement this encryption. Administrators should setup network policy alerts to detect any unauthorized traffic passing through the firewalls.

Reports and Alerts

Use the following link/reference to see the 2.3 reports and alerts: 2.3 on page 96.

Sub-Requirement 2.5 (Update: v3.0 11/2013)

2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

- Examine documentation interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:
  - Documented
  - In use
  - Known to all affected parties

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis

Reports and Alerts

Use the link/reference to see the 2.5 reports and alerts: 2.5 on page 98.

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Requirement 3	Protect stored cardholder data
3.7	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. Update: v3.0 November 2013

Sub-Requirement 3.7 (Update: v3.0 11/2013)

3.7 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

Illustrative Controls and the TIBCO LogLogic Solution

The encryption solution should not allow for or accept substitution of keys coming from unauthorized sources or unexpected processes.

Reports and Alerts

Use the link/reference to see the 3.7 reports and alerts: 3.7 on page 98.

Requirement 4: Encrypt transmission of cardholder data across open public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Mis-configured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

Requirement 4	Encrypt transmission of cardholder data across open public networks
4.3	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. Update: v3.0 November 2013

Sub-Requirement 4.3 (Update: v3.0 11/2013)

4.3 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis.

Reports and Alerts

Use the link/reference to see the 4.3 reports and alerts: 4.3 on page 98.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"-including viruses, worms, and Trojans-enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

Requirement 5	Protect all systems against malware and regularly update anti-virus software or programs
5.4	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. Update: v3.0 November 2013

Sub-Requirement 5.4 (Update: v3.0 11/2013)

5.4 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.

Reports and Alerts

Use the link/reference to see the 5.4 reports and alerts: 5.4 on page 98.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

The following table lists the specific sub-requirements in Requirement 6 that are addressed by TIBCO LogLogic's Compliance Suite - PCI Edition.

Requirement 6	Develop and maintain secure systems and applications
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release. Install relevant security patches within one month of release.
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. Update: v3.0 November 2013.
6.3.3	Separation of duties between development, test, and production environments
6.4.1	Follow change control procedures for all system and software configuration changes. The procedures must include the following: Documentation of impact
6.4.2	Follow change control procedures for all system and software configuration changes. The procedures must include the following: Management sign-off by appropriate parties
6.4.3	Follow change control procedures for all system and software configuration changes. The procedures must include the following: Testing of operational functionality

Requirement 6	Develop and maintain secure systems and applications
6.4.4	Follow change control procedures for all system and software configuration changes. The procedures must include the following: Back-out procedures
6.7	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.

Sub-Requirement 6.1

6.1 Ensure that all system components and software have the latest vendor-supplied security patches:

Install relevant security patches within one month of release.

Illustrative Controls and the TIBCO LogLogic Solution

Security patch management includes deploying security updates and related softwarereleases into the production environment. The goal of security patches is to help the organization maintain system and data integrity and prevent exploitation of known vulnerabilities.

This process helps organizations maintain operational efficiency and effectiveness, overcome security vulnerabilities, and sustain the stability of the production environment. A number of security vulnerabilities can exist in the IT environment that can be exploited and lead to downtime and loss of revenue and/or intellectual property.

Organizations must determine and maintain a known level of trust within the IT environment and ensure that vendor-supplied security patches have been properly tested and installed within a reasonable period of time.

To satisfy this requirement, administrators must continually ensure that all security patches have been installed on in-scope systems.

Reports and Alerts

Use the following link/reference to see the 6.1 reports and alerts: 6.1 on page 99.

Sub-Requirement 6.2 (Update:v3.0 11/2013)

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. (Maps to prior Requirment 6.1)

Illustrative Controls and the TIBCO LogLogic Solution

Security patch management includes deploying security updates and related software releases into the production environment. The goal of security patches is to help the organization maintain system and data integrity and prevent exploitation of known vulnerabilities.

This process helps organizations maintain operational efficiency and effectiveness, overcome security vulnerabilities, and sustain the stability of the production environment. A number of security vulnerabilities can exist in the IT environment that can be exploited and lead to downtime and loss of revenue and/or intellectual property.

Organizations must determine and maintain a known level of trust within the IT environment and ensure that vendor-supplied security patches have been properly tested and installed within a reasonable period of time.

To satisfy this requirement, administrators must continually ensure that all security patches have been installed on in-scope systems.

Reports and Alerts

Use the link/reference to see the 6.2 reports and alerts: 6.2 on page 99.

Sub-Requirement 6.3.3

6.3.3 Separation of duties between development, test, and production environments.

Illustrative Controls and the TIBCO LogLogic Solution

Organizations must confirm that there is appropriate segregation of duties between the staff responsible for production deployment of systems and applications and the staff responsible for the development of these systems and applications. In addition, organizations must consider whether or not changes are performed in a segregated and controlled environment.

To satisfy this requirement, administrators must ensure that logins to servers as well as permissions assigned to these users are appropriate for the tasks they are allowed to perform. Users with overlapping permission sets could indicate a compromise in the segregation of duties control consideration. Administrators should also review the process used to request and grant access to systems and data and confirm that the same person does not perform these functions.

Reports and Alerts

Use the following link/reference to see the 6.3.3 reports and alerts: 6.3.3 on page 100.

Sub-Requirement 6.4

6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:

- 6.4.1 Documentation of impact
- 6.4.2 Management sign-off by appropriate parties
- 6.4.3 Testing of operational functionality
- 6.4.4 Back-out procedures

Illustrative Controls and TIBCO LogLogic Solution

Effective change management procedures address how an organization introduces change into the in-scope environment in an authorized, tested, and controlled fashion. Deficiencies in this area may significantly impact the confidentiality, integrity, and availability of cardholder data. Businesses must ensure that requests for program changes, system changes, and maintenance (including changes to system software) are standardized, documented, and subject to formal change management procedures.

To satisfy this requirement, administrators must review all changes to the production environment and compare the changes to documented approvals to ensure the approval process is followed. From the archived audit log data, obtain a sample of regular and emergency changes made to applications/systems to determine whether they were adequately tested and approved before being placed into a production environment. Trace the sample of changes back to the change request log and supporting documentation.

Reports and Alerts

Use the following link/reference to see the 6.4.1, 6.4.2, 6.4.3, 6.4.4 reports and alerts:6.4.1, 6.4.2, 6.4.3, and 6.4.4 on page 103.

Sub-Requirement 6.7 (Update: v3.0 11/2013)

6.7 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

- Examine documentation interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:
  - Documented
  - In use
  - Known to all affected parties

Illustrative Controls and the TIBCO LogLogic Solution

- Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis

Reports and Alerts

Use the link/reference to see the 6.7 reports and alerts: 6.7 on page 107.

Requirement 7: Restrict access to cardholder data by business need-to-know

This requirement ensures that sensitive data is accessed in an authorized manner. The following table lists the specific sub-requirements in Requirement 7 that are addressed by TIBCO LogLogic® Compliance Suite - PCI Edition.

Requirement 7	Restrict aces to cardholder data by business ned-to-know
7.1	Limit access to computing resources and cardholder information only to those individuals whose job requires such access
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed
7.3	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. Update: v3.0 November 2013.

Sub-Requirement 7.1 and 7.2

- 7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access
- 7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed

Illustrative Controls and the TIBCO LogLogic Solution

User access rights to systems and data should be in line with defined and documented business needs and job requirements. Accurately managing user access rights addresses the issues of unintended or malicious modifications of sensitive data (including cardholder information). Administrators must determine that the following requirements are met:

- Access rights for privileged User IDs are restricted to the least privileges necessary to perform the job.
- Assignment of privileges to individuals is based on job classification and function.
- Authorization forms signed by management and specifying required privileges are maintained for each access control modification.
- An automated access control system is being used.
- The system is configured to “deny all” by default (meaning that a default user would have no access).

To help validate these requirements, administrators must periodically review user access to files and programs to ensure the users have not accessed items outside of their role.

Reports and Alerts

Use the following link/reference to see the 7.1 and 7.2 reports and alerts:

- 7.1 on page 108
- 7.2 on page 114.

Sub-Requirement 7.3 Update: v3.0 11/2013)

7.3 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

Examine documentation interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:

- Documented
- In use
- Known to all affected parties

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis

Reports and Alerts

Use the link/reference to see the 7.3 reports and alerts: 7.3 on page 118.

Requirement 8: Assign a unique ID to each person with computer access

This requirement ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. The following table lists the specific sub-requirements in Requirement 8 that are addressed by TIBCO LogLogic® Compliance Suite - PCI Edition.

Requirement 8	Assign a unique ID to each person with computer aces
8.1	Identify all users with a unique username before allowing them to access system components or cardholder data

Requirement 8	Assign a unique ID to each person with computer aces
8.1.5	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows (Type - Clarification): Enabled only during the time period needed and disabled when not in use Monitored when in use Update: v3.0 November 2013
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. Update: v3.0 November 2013
8.5.4	Immediately revoke access for any terminated users
8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed
8.5.8	Do not use group, shared, or generic accounts and passwords
8.5.9	Change user passwords at least every 90 days
8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts
8.5.16	Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows (Type - Evolving Requirement): Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
8.8	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. Update: v3.0 November 2013.

Sub-Requirement 8.1 and 8.5.8

- 8.1 Identify all users with a unique username before allowing them to access system components or cardholder data
- 8.5.8 Do not use group, shared, or generic accounts and passwords

Illustrative Controls and the TIBCO LogLogic Solution

All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. Ensuring all users have uniquely identifiable IDs enables the maintenance of accurate and complete audit trails. Deficiencies in this area can significantly impact accountability.

To satisfy this requirement, administrators must ensure all logins are unique and not shared. Administrators must review user lists to identify IDs that may be generic or shared and develop plans to eliminate this shared access. Administrators should report on logins using known default administrative-level accounts as well (including "Administrator" on Windows systems and 'root' on Unix systems). These accounts are by definition shared, and direct access with these accounts should be disallowed.

Reports and Alerts

Use the following link/reference to see the 8.1 and 8.5.8 reports and alerts:

8.1 and 8.5.8 on page 120.

Sub-Requirement 8.1.5 (Update v3.0 11/2013)

8.1.5 Enable accounts used by vendors for remote maintenance only during the time period needed. (Maps to prior Requirement 8.5.6)

Illustrative Controls and the TIBCO LogLogic Solution

Accounts must often be created for vendors to perform remote troubleshooting and maintenance of IT systems and applications. Care must be taken to ensure that these vendors only have access during maintenance hours and when personnel are available to monitor the process. Administrators must identify all access to ensure vendors are only logging in during approved maintenance periods.

Reports and Alerts

Use the link/reference to see the 8.1.5 reports and alerts: 8.1.5 on page 118.

Sub-Requirement 8.5.1 (Update: v3.0 11/2013)

8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects Illustrative Controls and the TIBCO LogLogic Solution Administrators must monitor any account management activities such as user or group addition/deletion/modification to ensure all user access privileges are appropriate and approved. Set up real-time alerts to detect any unauthorized or unapproved changes to users or groups.

Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by a unified user account management policy and process. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for both normal and emergency cases.

Administrators must perform regular management review of all accounts and related privileges. Demonstrate that procedures exist for the registration, change, and deletion of users from in-scope systems and applications on a timely basis and confirm that the procedures are followed. Procedures must exist and be followed to ensure timely action relating to requesting, establishing, issuing, suspending, and closing user accounts.

To satisfy this requirement, administrators must ensure that permissions have been granted to the appropriate users. Permissions incorrectly assigned to users can indicate failure to meet this requirement. Also, administrators must ensure that all network and application access requests are adequately documented and approved by appropriate management personnel. As proof, administrators can select a sample of terminated employees to ensure the accounts for these employees have been disabled or deleted in a timely manner.

Reports and Alerts

Use the following link/reference to see the 8.5.1 reports and alerts: 8.5.1 on page 123.

Sub-Requirement 8.5.4

8.5.4 Immediately revoke access for any terminated users.

Illustrative Controls and the TIBCO LogLogic Solution

Administrators must demonstrate that user access privileges are revoked in a timely manner upon job change or termination. Review reports and alerts on account activities, accounts created/deleted, group members added/deleted, and successful logins to VPN devices and critical servers.

Take expedient actions regarding job changes, especially job terminations. Knowledge transfer needs to be arranged, responsibilities reassigned and access rights removed such that risks are minimized and continuity of the function is guaranteed. When a person changes jobs or is terminated from a company, user access privileges must be modified according to the company's business guidelines.

To satisfy this requirement, administrators must periodically ensure that only current and authorized employees have access to in-scope systems and applications. Administrators must ensure that all terminated users have been disabled. In addition, administrators must ensure that logins to servers as well as permissions assigned to users who changed jobs are appropriate for the new role they are in.

To ensure the requirements listed above are met, administrators must review reports of all user deletions and group member modifications. This ensures terminated users are removed and users who have changed jobs have had their rights appropriately adjusted.

Reports and Alerts

Use the following link/reference to see the 8.5.4 reports and alerts: 8.5.4 on page 126.

Sub-Requirement 8.5.6

8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.

Illustrative Controls and the TIBCO LogLogic Solution

Accounts must often be created for vendors to perform remote troubleshooting and maintenance of IT systems and applications. Care must be taken to ensure that these vendors only have access during maintenance hours and when personnel are available to monitor the process. Administrators must identify all access to ensure vendors are only logging in during approved maintenance periods.

Reports and Alerts

Use the following link/reference to see the 8.5.6 reports and alerts: 8.5.6 on page 129.

Sub-Requirement 8.5.9

8.5.9 Change user passwords at least every 90 days.

Illustrative Controls and the TIBCO LogLogic Solution

Requiring frequent password changes is a good general security practice that limits an attacker's ability to acquire and use compromised user accounts and passwords. It is generally recommended that passwords be changed every 30 to 90 days.

In addition to setting explicit system policies, administrators should identify and review password change events to ensure users are changing passwords at least every 90 days. For example, Windows platforms generate events with the ID of 4723 and 4724 for password change attempts.

Reports and Alerts

Use the following link/reference to see the 8.5.9 reports and alerts: 8.5.9 on page 130.

Sub-Requirement 8.5.13

8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.

Illustrative Controls and the TIBCO LogLogic Solution

Account lockouts help ensure that brute force password attacks have limited success in the PCI environment. All in-scope systems and authentication mechanisms must be configured to lock out users after no more than six consecutive failed login attempts.

Reports and Alerts

Use the following link/reference to see the 8.5.13 reports and alerts: 8.5.13 on page 130.

Sub-Requirement 8.5.16

8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

Illustrative Controls and the TIBCO LogLogic Solution

As the majority of cardholder data is stored in databases, it is essential to protect these systems. Requiring authentication for all database connections helps ensure the security of cardholder data. Administrators should regularly review login reports for all databases containing cardholder data.

Reports and Alerts

Use the following link/reference to see the 8.5.16 reports and alerts: 8.5.16 on page 131.

Sub-Requirement 8.6

8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows (Type - Evolving Requirement):

- Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
- Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
- New Requirement: v3.0 November 2013

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.

Reports and Alerts

Use the link/reference to see the 8.6 reports and alerts: 8.6 on page 133.

Sub-Requirement 8.8 (Update: v3.0 11/2013)

8.8 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

- Examine documentation interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:
  - Documented

- In use
- Known to all affected parties

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis

Reports and Alerts

Use the link/reference to see the 8.8 reports and alerts: 8.8 on page 133.

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hard copies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

Requirement 9	Restrict physical access to cardholder data
9..10	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. Update: v3.0 November 2013.

Sub-Requirement 9.10 (Update: v3.0 11/2013)

9.10 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.

Reports and Alerts

Use the link/reference to see the 9.10 reports and alerts: 9.10 on page 133.

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical. Effective logging and auditing mechanisms across all in-scope systems and applications helps ensure thorough tracking and analysis when troubleshooting or forensic investigation is required. Determining the root cause of a system or data compromise is difficult or impossible without appropriate system activity logs.

The following table lists the specific sub-requirements in Requirement 10 that are addressed by TIBCO LogLogic® Compliance Suite - PCI Edition.

Requirement 10	Track and monitor al aces to network resources and cardholder data
10.1	Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to each individual user
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data
10.2.2	Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges
10.2.3	Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails
10.2.4	Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts
10.2.5	Implement automated audit trails for all system components to reconstruct the following events: Use of identification and authentication mechanisms
10.2.6	Implement automated audit trails for all system components to reconstruct the following events: Initialization of the audit logs
10.2.7	Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system-level objects
10.3.1	Record at least the following audit trail entries for all system components for each event: User identification
10.3.2	Record at least the following audit trail entries for all system components for each event: Type of event
10.3.3	Record at least the following audit trail entries for all system components for each event: Date and time

Requirement 10	Track and monitor al aces to network resources and cardholder data
10.3.4	Record at least the following audit trail entries for all system components for each event: Success or failure indication
10.3.5	Record at least the following audit trail entries for all system components for each event: Origination of event
10.3.6	Record at least the following audit trail entries for all system components for each event: Identity or name of affected data, system component, or resource
10.5.1	Limit viewing of audit trails to those with a job-related need
10.5.2	Protect audit trail files from unauthorized modifications
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter
10.5	Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)
10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). (Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6)
10.7	Retain audit trail history for at least one year, with a minimum of three months available online
10.8	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. Update:v3.0 November 2013.

Sub-Requirement 10.1

10.1 Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to each individual user

Illustrative Controls and the TIBCO LogLogic Solution

All users (internal, external and temporary) and their activity on in-scope systems (business applications, operating systems, network devices) must be uniquely identifiable. Administrators and root users should never directly access system components, as these accounts are generally shared and can be difficult to track back to a specific individual. Instead, these users should be accessing these components using commands such as sudo or su; or in the Windows environment, be assigned to a administrative group. This setup allows the actions of specific individuals to be tracked.

To satisfy this requirement, administrators should regularly review user lists on in-scope systems to identify IDs that may be generic or shared.

Reports and Alerts

Use the following link/reference to see the 10.1 reports and alerts: 10.1 on page 134.

Sub-Requirement 10.2.1, 10.2.2 and 10.2.4

10.2 Implement automated audit trails for all system components to reconstruct the following events:

- 10.2.1 All individual user accesses to cardholder data
- 10.2.2 All actions taken by any individual with root or administrative privileges
- 10.2.4 Invalid logical access attempts

Illustrative Controls and the TIBCO LogLogic Solution

To satisfy this requirement, administrators must assess the authentication mechanisms used to validate user credentials (new and existing) to support the validity of transactions. Server and application activities must be monitored for failed access attempts, as they can represent malicious activities. Administrators must monitor and verify all user access to programs and data, and all access to cardholder data (that includes the full PAN – Primary Account Number) must be logged.

Reports and Alerts

- Use the following link/reference to see the 10.2.1 and 10.2.2 reports and alerts: 10.2.1 and 10.2.2 on page 135.
- Use the following link/reference to see the 10.2.4 and alerts: 10.2.4 on page 137.

Sub-Requirements 10.2.3, 10.2.6, 10.5 and 10.6

10.2 Implement automated audit trails for all system components to reconstruct the following events:

- 10.2.3 Access to all audit trails
- 10.2.6 Initialization of the audit logs

10.5 Secure audit trails so they cannot be altered, including the following:

- 10.5.1 Limit viewing of audit trails to those with a job-related need
- 10.5.2 Protect audit trail files from unauthorized modifications
- 10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter
- 10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

Log collection, parsing, and alerting tools may be used to meet compliance with Requirement 10.6

Illustrative Controls and the TIBCO LogLogic Solution

A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed. To realize this benefit, administrators must ensure that security tools and applications are tested and monitored proactively. These controls should be reaccredited periodically to ensure the approved security level is maintained.

Access to the logging information must be in line with business requirements in terms of access rights and retention requirements, and security administrators must monitor and log security activity, and identify security violations to report to senior management. To satisfy this requirement, administrators must review the user access logs on a daily basis for any access violations or unusual activity. In addition, administrators must ensure that all relevant log sources are logging properly to a centralized log management system.

TIBCO LogLogic's solution is developed from the ground up to be a regulatory compliance solution. All log messages, once received by the Appliances, will be transferred via TCP to ensure reliability. All log files stored on the ST, LX and MX Appliances have a separate MD5 signature, stored separately from the file, to ensure no files are tampered so that they can be detected.

Reports and Alerts

- Use the following link/reference to see the 10.2.3 reports and alerts: 10.2.3 on page 136.
- Use the following link/reference to see the 10.2.6 reports and alerts: 10.2.6 on page 137.
- Use the following link/reference to see the 10.5 reports and alerts: 10.5 on page 142.
- Use the following link/reference to see the 10.6 reports and alerts: 10.6 on page 142.

Sub-Requirement 10.2.5

10.2.5 Implement automated audit trails for all system components to reconstruct the following events:

- Use of identification and authentication mechanisms

Illustrative Controls and TIBCO LogLogic Solution

To satisfy this requirement, administrators must ensure that login attempts to in-scope systems (including hosts, applications, databases, and network devices) are logged. This includes both successful and failed attempts, and also includes other operations involving authentication mechanisms (e.g., switching user context).

Reports and Alerts

Use the following link/reference to see the 10.2.5 reports and alerts: 10.2.5 on page 138.

Sub-Requirement 10.2.7

10.2.7 Implement automated audit trails for all system components to reconstruct the following events:

- Creation and deletion of system-level objects

Illustrative Controls and the TIBCO LogLogic Solution

Audit trails related to user creation and deletion of system-level objects, for example, files, folders, registry keys, and others, are critical in the troubleshooting and forensic analysis processes.

To satisfy this requirement, administrators should specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object. Administrators should also regularly review audit trails related to object creation and deletion to ensure appropriate access.

Reports and Alerts

Use the following link/reference to see the 10.2.7 reports and alerts: 10.2.7 on page 140.

Sub-Requirement 10.3

10.3 Record at least the following audit trail entries for all system components for each event:

- 10.3.1 User identification
- 10.3.2 Type of event
- 10.3.3 Date and time
- 10.3.4 Success or failure indication
- 10.3.5 Origination of event
- 10.3.6 Identity or name of affected data, system component, or resource

Illustrative Controls and the TIBCO LogLogic Solution

Incident detection and response functions address how an organization identifies, documents and responds to events that fall outside of normal operations. Organizations must maintain a complete and accurate audit trail for network devices, servers and applications to enable this type of investigation.

By alerting on any failures that occur, administrators can respond rapidly to potential problems and incidents that might affect availability, security, or performance. Real-time data monitoring and reporting capabilities reduce time to repair after incidents, reducing costs, and improving application availability.

The TIBCO LogLogic® Log Management Intelligence (LMI) solution will automatically record the event date and time, event status (success or failure), event origin (log source IP address) and event type (firewall connection, access or authentication, IDS, E-Mail, or web access) for every single event. In addition, TIBCO LogLogic's solution will identify all users, system components or resources within the events to help administrator correctly analyze the events.

The TIBCO LogLogic Dashboard for Log Source Status provides an up to date view of the log files that the TIBCO LogLogic Appliance is collecting.

Reports and Alerts

Use the following link/reference to see the 10.3 reports and alerts: 10.3.1 on page 141.

Sub-Requirement 10.7

10.7 Retain audit trail history for at least one year, with a minimum of three months available online.

Illustrative Controls and the TIBCO LogLogic Solution

Audit trails maintain a record of system activity both by system and application processes and by users of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. Audit trail retention provides auditors and administrators a means to help accomplish several security-related objectives, including establishing individual accountability, event reconstruction, intrusion detection, and problem analysis.

To satisfy this requirement, LogLogic® LMI solution simplifies, automates, and reduces the cost of log data retention. TIBCO LogLogic's ST product comes with either 2.8 terabytes of usable onboard storage (up to 33.6 TB of compressed data) or interfaces to NAS devices and SAN for the 202x-SAN appliances.

ST Appliances archive up to ten years of log data while eliminating the need for servers, tape libraries, and archive administrators. When used with TIBCO LogLogic's LX/MX Appliances, the ST Appliance also guarantees complete and accurate transmission of network equipment logs from anywhere on the enterprise WAN.

To maximize storage, TIBCO LogLogic's ST solution stores all raw log data in compressed text format with a compression ratio of 12:1. Logs can be extracted from the ST's easy-to-use UI without any impact to the collection and processing of raw log data.

Reports and Alerts

Use the following link/reference to see the 10.7 reports and alerts: 10.7 on page 143.

Sub-Requirement 10.8 (Update: v3.0 11/2013)

10.8 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

- Examine documentation interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:
  - Documented
  - In use
  - Known to all affected parties

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis

Reports and Alerts

Use the link/reference to see the 10.8 reports and alerts: 10.8 on page 143.

Requirement 11: Regularly test security systems and processes

Vulnerabilities are continually being discovered by hackers and researchers and more such flaws are also introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and through changes. The following table lists the specific sub-requirements in Requirement 11 that are addressed by TIBCO LogLogic® Compliance Suite - PCI Edition.

Requirement 11	Regularly test security systems and processes
11.4	Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.
11.5	Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.
11.6	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. Update: v3.0 November 2013.

Sub-Requirement 11.4

11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.

Illustrative Controls and the TIBCO LogLogic Solution

To satisfy this requirement, administrators must regularly review IDS logs to ensure the IDS tools are properly updated and appropriately deployed. Review all remote access to the IT infrastructure via VPN or through firewalls. Detect any anomalies such as excessive IDS attacks or firewall traffic using behavioral-based alerts.

Reports and Alerts

Use the following link/reference to see the 11.4 reports and alerts: 11.4 on page 144.

Sub-Requirement 11.5

11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.

Illustrative Controls and the TIBCO LogLogic Solution

To satisfy this requirement, administrators must deploy file integrity monitoring software on in-scope systems and ensure that file comparisons are performed at least weekly. Additionally, administrators should ensure that alerts and messages from file integrity monitoring software are appropriately incorporated into incident detection, investigation, and response procedures.

Reports and Alerts

Refer TIBCO LogLogic Reports and Alerts Quick Reference to see the 11.5 reports and alerts.

Each Tripwire configuration will include critical files, data, and directories that are unique to each installation, thus no pre-configured alerts are included for Tripwire. The included Tripwire report can be used to help baseline the environment and determine which alerts are required.

Sub-Requirement 11.6 (Update v3.0 11/2013)

11.6 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (Maps to prior Requirement 12.2)

- Examine documentation interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:
  - Documented
  - In use
  - Known to all affected parties

Illustrative Controls and the TIBCO LogLogic Solution

Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis

Reports and Alerts

Refer TIBCO LogLogic Reports and Alerts Quick Reference to see the 11.5 reports and alerts.

Requirement 12: Maintain a policy that addresses information security for employees and contractors

While audits to validate PCI compliance may occur only once a year, maintaining compliance requires regular daily activities to validate compliance controls and ensure the security of cardholder data. The following table lists the specific sub-requirements in Requirement 12 that are addressed by TIBCO LogLogic® Compliance Suite - PCI Edition.

Requirement 12	Regularly test security systems and processes
12.2	Maintain a Policy that addresses information security for employees and contractors
12.9.5	Implement an incident response plan. Be prepared to respond immediately to a system breach: Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.

Sub-Requirement 12.2

12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).

Illustrative Controls and the TIBCO LogLogic Solution

LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - PCI Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.

Reports and Alerts

All PCI reports and alerts.

Sub-Requirement 12.9.5

12.9.5 Implement an incident response plan. Be prepared to respond immediately to a system breach:

- Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.

Illustrative Controls and the TIBCO LogLogic Solution

To satisfy this requirement, administrators must regularly review IDS logs and alerts. Events with the potential to adversely affect cardholder data or systems in the payment card environment must be investigated according to the procedures outlined in the incident response plan.

Reports and Alerts

Use the following link/reference to see the 12.9.5 reports and alerts: 12.9.5 on page 146.

Each Tripwire configuration will include critical files, data, and directories that are unique to each installation, thus no pre-configured alerts are included for Tripwire. The included Tripwire report can be used to help baseline the environment and determine which alerts are required.

TIBCO LogLogic Reports and Alerts for PCI

- TIBCO LogLogicReports for PCI
- TIBCO LogLogic Alerts for PCI
- TIBCO LogLogic Reports and Alerts Quick Reference

TIBCO LogLogic Reports for PCI

The following table lists the Custom Reports included in the TIBCO LogLogic® Compliance Suite - PCI Edition.

Serial Number	TIBCO LogLogic Report	Description
1	PCI: Accepted VPN Connections - RADIUS	Displays all users connected to the internal network through the RADIUS VPN.
2	PCI: Account Activities on UNIX Servers	Displays all accounts activities on UNIX servers to ensure authorized and appropriate access.
3	PCI: Account Activities on Windows Servers	Displays all accounts activities on Windows servers to ensure authorized and appropriate access.
4	PCI: Accounts Changed on NetApp Filer	Displays all accounts changed on NetApp Filer to ensure authorized and appropriate access.
5	PCI: Accounts Changed on UNIX Servers	Displays all accounts changed on UNIX servers to ensure authorized and appropriate access.
6	PCI: Accounts Changed on Windows Servers	Displays all accounts changed on Windows servers to ensure authorized and appropriate access.
7	PCI: Accounts Changed on TIBCO ActiveMatrix Administrator	Displays all accounts changed on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
8	PCI: Accounts Changed on TIBCO Administrator	Displays all accounts changed on TIBCO Administrator to ensure authorized and appropriate access.
9	PCI: Accounts Created on NetApp Filer	Displays all accounts created on NetApp Filer to ensure authorized and appropriate access.
10	PCI: Accounts Created on NetApp Filer Audit	Displays all accounts created on NetApp Filer Audit to ensure authorized and appropriate access.
11	PCI: Accounts Created on Symantec Endpoint Protection	Displays all accounts created on Symantec Endpoint Protection to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
12	PCI: Accounts Created on TIBCO ActiveMatrix Administrator	Displays all accounts created on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
13	PCI: Accounts Created on TIBCO Administrator	Displays all accounts created on TIBCO Administrator to ensure authorized and appropriate access.
14	PCI: Accounts Created on Sidewinder	Displays all accounts created on Sidewinder to ensure authorized and appropriate access.
15	PCI: Accounts Created on UNIX Servers	Displays all accounts created on UNIX servers to ensure authorized and appropriate access.
16	PCI: Accounts Created on Windows Servers	Displays all accounts created on Windows servers to ensure authorized and appropriate access.
17	PCI: Accounts Deleted on NetApp Filer	Displays all accounts deleted on NetApp Filer to ensure authorized and appropriate access.
18	PCI: Accounts Deleted on NetApp Filer Audit	Displays all accounts deleted on NetApp Filer Audit to ensure authorized and appropriate access.
19	PCI: Accounts Deleted on Sidewinder	Displays all accounts deleted on Sidewinder to ensure authorized and appropriate access.
20	PCI: Accounts Deleted on Symantec Endpoint Protection	Displays all accounts deleted on Symantec Endpoint Protection to ensure authorized and appropriate access.
21	PCI: Accounts Deleted on TIBCO ActiveMatrix Administrator	Displays all accounts deleted on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
22	PCI: Accounts Deleted on TIBCO Administrator	Displays all accounts deleted on TIBCO Administrator to ensure authorized and appropriate access.
23	PCI: Accounts Deleted on UNIX Servers	Displays all accounts deleted on UNIX servers to ensure authorized and appropriate access.
24	PCI: Accounts Deleted on Windows Servers	Displays all accounts deleted on Windows servers to ensure authorized and appropriate access.
25	PCI: Active Directory System C hanges	Displays changes made within Active Directory.
26	PCI: Administrator Logins on Windows Servers	Displays all logins with the administrator account on Windows servers.

Serial Number	TIBCO LogLogic Report	Description
27	PCI: Administrators Activities o n Servers	Displays the latest activities performed by administrators and root users to ensure appropriate access.
28	PCI: Applications Through Firewalls	Displays the most active applications used through the firewalls.
29	PCI: Applications Under Attack	Displays all applications under attack as well as the attack signatures.
30	PCI: Applications Under Attack - Cisco IOS	Displays all applications under attack as well as the attack signatures by Cisco IOS.
31	PCI: Applications Under Attack - FireEye MPS	Displays all applications under attack as well as the attack signatures by FireEye MPS.
32	PCI: Applications Under Attack - ISS SiteProtector	Displays all applications under attack as well as the attack signatures by ISS SiteProtector.
33	PCI: Applications Under Attack - SiteProtector	Displays all applications under attack as well as the attack signatures by SiteProtector.
34	PCI: Applications Under Attack - Sourcefire Defense Center	Displays all applications under attack as well as the attack signatures by Sourcefire Defense Center.
35	PCI: Attack Origins	Displays the sources that have initiated the most attacks.
36	PCI: Attack Origins - Cisco IOS	Displays the sources that have initiated the most attacks by Cisco IOS.
37	PCI: Attack Origins - HIPS	Displays the sources that have initiated the most attacks.
38	PCI: Attack Origins - ISS SiteProtector	Displays the sources that have initiated the most attacks by ISS SiteProtector.
39	PCI: Attack Origins - SiteProtector	Displays the sources that have initiated the most attacks by SiteProtector.
40	PCI: Attack Origins - Sourcefire Defense Center	Displays the sources that have initiated the most attacks by Sourcefire Defense Center.
41	PCI: Attacks Detected	Displays all IDS attacks detected against servers and applications.
42	PCI: Attacks Detected - Cisco IOS	Displays all IDS attacks detected against servers and applications by Cisco IOS.
43	PCI: Attacks Detected - HIPS	Displays all IPS attacks detected against servers and applications.

Serial Number	TIBCO LogLogic Report	Description
44	PCI: Attacks Detected - ISS SiteProtector	Displays all IDS attacks detected against servers and applications by ISS SiteProtector.
45	PCI: Attacks Detected - SiteProtector	Displays all IDS attacks detected against servers and applications by SiteProtector.
46	PCI: Attacks Detected - Sourcefire Defense Center	Displays all IDS attacks detected against servers and applications by Sourcefire Defense Center.
47	PCI: Check Point Configuration Changes	Displays all Check Point audit events related to configuration changes.
48	PCI: Check Point Management Station Login	Displays all login events to the Check Point management station.
49	PCI: Check Point Objects Created	Displays all Check Point audit events related to object creation in policies.
50	PCI: Check Point Objects Deleted	Displays all Check Point audit events related to policy objects deleted.
51	PCI: Check Point Objects Modified	Displays all Check Point audit events related to policy objects modified.
52	PCI: Check Point SIC Revoked	Displays all Check Point audit events related to the security certificate being revoked.
53	PCI: Cisco ESA: Attacks by Event ID	Displays Cisco ESA attacks by Event ID.
54	PCI: Cisco ESA: Attacks Detected	Displays attacks detected by Cisco ESA.
55	PCI: Cisco ESA: Attacks by Threat Name	Displays Cisco ESA Attacks by threat name.
56	PCI: Cisco ESA: Scans	Displays scans using Cisco ESA.
57	PCI: Cisco ESA: Updated	Displays updates to Cisco ESA.
58	PCI: Cisco FWSM HA State Changed	Displays all Cisco FWSM firewall fail-over state change events.
59	PCI: Cisco ISE, ACS Accounts Created	Displays all accounts created on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
60	PCI: Cisco ISE, ACS Accounts Removed	Displays all accounts removed on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
61	PCI: Cisco ISE, ACS Configuration Changes	Displays Cisco ISE and Cisco SecureACS configuration changes.
62	PCI: Cisco ISE, ACS Password Changes	Displays all password change activities on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
63	PCI: Cisco Peer Reset/Reload	Displays all Cisco Peer reset and reload events.
64	PCI: Cisco Peer Supervisor Status Changes	Displays all Cisco Peer Supervisor status changes.
65	PCI: Cisco PIX, ASA, FWSM Failover Disabled	Displays all logs related to disabling Cisco PIX, ASA, and FWSM failover capability.
66	PCI: Cisco PIX, ASA, FWSM Failover Performed	Displays all logs related to performing a Cisco PIX, ASA, and FWSM failover.
67	PCI: Cisco PIX, ASA, FWSM Policy Changed	Displays all configuration changes made to the Cisco PIX, ASA, and FWSM devices.
68	PCI: Cisco PIX, ASA, FWSM Re started	Displays all Cisco PIX, ASA, or FWSM restart activities to detect unusual activities.
69	PCI: Cisco PIX, ASA, FWSM Routing Failure	Displays all Cisco PIX, ASA, and FWSM routing error messages.
70	PCI: Cisco Redundancy Version Check Failed	Displays all Cisco redundancy version check failures.
71	PCI: Cisco Routers and Switches Restart	Displays all Cisco routers and switches restart activities to detect unusual activities.
72	PCI: Cisco Switch Policy Changes	Displays all configuration changes to the Cisco router and switch policies.
73	PCI: Creation and Deletion of System Level Objects: AIX Audit	Displays AIX audit events related to creation and deletion of system-level objects.
74	PCI: Creation and Deletion of System Level Objects: DB2 Database	Displays DB2 database events related to creation and deletion of system-level objects.
75	PCI: Creation and Deletion of System Level Objects: HP-UX Audit	Displays HP-UX audit events related to creation and deletion of system-level objects.
76	PCI: Creation and Deletion of System Level Objects: Oracle	Displays Oracle database events related to creation and deletion of system-level objects.

Serial Number	TIBCO LogLogic Report	Description
77	PCI: Creation and Deletion of System Level Objects: Solaris BSM	Displays Solaris BSM events related to creation and deletion of system-level objects.
78	PCI: Creation and Deletion of System Level Objects: SQL Server	Displays Microsoft SQL Server events related to creation and deletion of system-level objects.
79	PCI: Creation and Deletion of System Level Objects: Windows	Displays all Windows events related to creation and deletion of system-level objects.
80	PCI: DB2 Database Configuration Changes	Displays DB2 database configuration changes.
81	PCI: DB2 Database Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
82	PCI: DB2 Database Successful Logins	Displays successful DB2 database logins.
83	PCI: DB2 Database User Additions and Deletions	Displays IBM DB2 Database events related to creation and deletion of database users.
84	PCI: Denied VPN Connections - RADIUS	Displays all users denied access to the internal network by the RADIUS VPN.
85	PCI: DHCP Activities on Microsoft DHCP	Displays all DHCP activities on Microsoft DHCP Server.
86	PCI: DHCP Activities on VMware vShield	Displays all DHCP activities on VMware vShield Edge.
87	PCI: DNS Server Error	Displays all events when DNS Server has errors.
88	PCI: Escalated Privilege Activities on Servers	Displays all privilege escalation activities performed on servers to ensure appropriate access.
89	PCI: ESX Accounts Activities	Displays all accounts activities on VMware ESX servers to ensure authorized and appropriate access.
90	PCI: ESX Accounts Created	Displays all accounts created on VMware ESX servers to ensure authorized and appropriate access.
91	PCI: ESX Accounts Deleted	Displays all accounts deleted on VMware ESX servers to ensure authorized and appropriate access.
92	PCI: ESX Failed Logins	Failed VMware ESX logins for known user.
93	PCI: ESX Group Activities	Displays all group activities on VMware ESX servers to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
94	PCI: ESX Kernel log daemon terminating	Displays all VMware ESX Kernel log daemon terminating.
95	PCI: ESX Kernel logging Stop	Displays all VMware ESX Kernel logging stops.
96	PCI: ESX Logins Failed Unknown User	Failed VMware ESX logins for unknown user
97	PCI: ESX Logins Succeeded	Displays successful logins to VMware ESX to ensure only authorized personnel have access.
98	PCI: F5 BIG-IP TMOS Login Failed	Displays all F5 BIG-IP TMOS login events which have failed.
99	PCI: F5 BIG-IP TMOS Login Successful	Displays all F5 BIG-IP TMOS login events which have succeeded.
100	PCI: F5 BIG-IP TMOS Password Changes	Displays all password change activities on F5 BIG-IP TMOS to ensure authorized and appropriate access.
101	PCI: F5 BIG-IP TMOS Restarted	Displays all events when the F5 BIG-IP TMOS has been restarted.
102	PCI: ESX Syslogd Restart	Displays all VMware ESX syslogd restarts.
103	PCI: Files Accessed on NetApp Filer Audit	Displays all files accessed on NetApp Filer Audit to ensure appropriate access.
104	PCI: Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
105	PCI: Files Accessed on Servers	Displays all files accessed on servers to ensure appropriate access.
106	PCI: Files Accessed through Juniper SSL VPN (Secure Access)	Displays all files accessed through Juniper SSL VPN (Secure Access).
107	PCI: Files Accessed through PANOS	Displays all files accessed through Palo Alto Networks.
108	PCI: FireEye MPS: Attacks by Event ID	Displays FireEye MPS attacks by Event ID.
109	PCI: FireEye MPS: Attacks by Threat Name	Displays FireEye MPS attacks by threat name.
110	PCI: FireEye MPS: Attacks Detected	Displays attacks detected by FireEye MPS.

Serial Number	TIBCO LogLogic Report	Description
111	PCI: Firewall Connections Accepted - Check Point	Displays all traffic passing through the Check Point firewall.
112	PCI: Firewall Connections Accepted - Cisco IOS	Displays all traffic passing through the Cisco IOS firewall.
113	PCI: Firewall Connections Accepted - Cisco Netflow	Displays all traffic passing through the Cisco Netflow.
114	PCI: Firewall Connections Accepted - Cisco NXOS	Displays all traffic passing through the Cisco NXOS device.
115	PCI: Firewall Connections Accepted - Cisco PIX	Displays all traffic passing through the Cisco PIX firewall.
116	PCI: Firewall Connections Accepted - F5 BIG-IP TMOS	Displays all traffic passing through the F5 BIG-IP TMOS device.
117	PCI: Firewall Connections Accepted - Juniper JunOS	Displays all traffic passing through the Juniper JunOS firewall.
118	PCI: Firewall Connections Accepted - PANOS	Displays all traffic passing through the Palo Alto Networks firewall.
119	PCI: Firewall Connections Accepted - Sidewinder	Displays all traffic passing through the Sidewinder firewall.
120	PCI: Firewall Connections Accepted - VMware vShield	Displays all traffic passing through the VMware vShield device.
121	PCI: Firewall Connections Denied - Check Point	Displays the applications that have been denied access the most by the Check Point devices.
122	PCI: Firewall Connections Denied - F5 BIG-IP TMOS	Displays the applications that have been denied access the most by the F5 BIG-IP TMOS.
123	PCI: Firewall Connections Denied - Cisco ASA	Displays the applications that have been denied access the most by the Cisco ASA devices.
124	PCI: Firewall Connections Denied - Cisco FWSM	Displays the applications that have been denied access the most by the Cisco FWSM devices.
125	PCI: Firewall Connections Denied - Cisco IOS	Displays the applications that have been denied access the most by the Cisco IOS.
126	PCI: Firewall Connections Denied - Cisco NXOS	Displays the applications that have been denied access the most by the Cisco NXOS devices.
127	PCI: Firewall Connections Denied - Cisco PIX	Displays the applications that have been denied access the most by the Cisco PIX devices.

Serial Number	TIBCO LogLogic Report	Description
128	PCI: Firewall Connections Denied - Cisco Router	Displays the applications that have been denied access the most by the Cisco Router.
129	PCI: Firewall Connections Denied - Fortinet	Displays the applications that have been denied access the most by the Fortinet devices.
130	PCI: Firewall Connections Denied - Juniper Firewall	Displays the applications that have been denied access the most by the Juniper Firewall.
131	PCI: Firewall Connections Denied - Juniper JunOS	Displays the applications that have been denied access the most by the Juniper JunOS.
132	PCI: Firewall Connections Denied - Juniper RT Flow	Displays the applications that have been denied access the most by the Juniper RT Flow.
133	PCI: Firewall Connections Denied - Nortel	Displays the applications that have been denied access the most by the Nortel devices.
134	PCI: Firewall Connections Denied - PANOS	Displays the applications that have been denied access the most by the Palo Alto Networks devices.
135	PCI: Firewall Connections Denied - Sidewinder	Displays the applications that have been denied access the most by the Sidewinder
136	PCI: Firewall Connections Denied - VMware vShield	Displays the applications that have been denied access the most by the VMware vShield.
137	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Check Point	Displays all traffic passing through the Check Point that is not HTTP, SSL and SSH.
138	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco ASA	Displays all traffic passing through the Cisco ASA that is not HTTP, SSL and SSH.
139	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco FWSM	Displays all traffic passing through the Cisco FWSM that is not HTTP, SSL and SSH.
140	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco IOS	Displays all traffic passing through the Cisco IOS that is not HTTP, SSL and SSH.
141	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco Netflow	Displays all traffic passing through the Cisco Netflow that is not HTTP, SSL and SSH.
142	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco PIX	Displays all traffic passing through the Cisco PIX that is not HTTP, SSL and SSH.

Serial Number	TIBCO LogLogic Report	Description
143	PCI: Firewall Traffic Besides HTTP, SSL and SSH - F5 BIG-IP TMOS	Displays all traffic passing through the F5 BIG-IP TMOS that is not HTTP, SSL and SSH.
144	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Fortinet	Displays all traffic passing through the Fortinet that is not HTTP, SSL and SSH.
145	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper Firewall	Displays all traffic passing through the Juniper Firewall that is not HTTP, SSL and SSH.
146	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper JunOS	Displays all traffic passing through the Juniper JunOS that is not HTTP, SSL and SSH.
147	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper RTFlow	Displays all traffic passing through the Juniper RT Flow that is not HTTP, SSL and SSH.
148	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Nortel	Displays all traffic passing through the Nortel that is not HTTP, SSL and SSH.
149	PCI: Firewall Traffic Besides HTTP, SSL and SSH - PANOS	Displays all traffic passing through the Palo Alto Networks that is not HTTP, SSL and SSH.
150	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Sidewinder	Displays all traffic passing through the Sidewinder that is not HTTP, SSL and SSH.
151	PCI: Firewall Traffic Besides HTTP, SSL and SSH - VMware vShield	Displays all traffic passing through the VMware vShield that is not HTTP, SSL and SSH.
152	PCI: Firewall Traffic Besides SSL and SSH - Check Point	Displays all traffic passing through the Check Point that is not SSL and SSH.
153	PCI: Firewall Traffic Besides SSL and SSH - Cisco ASA	Displays all traffic passing through the Cisco ASA that is not SSL and SSH.
154	PCI: Firewall Traffic Besides SSL and SSH - Cisco FWSM	Displays all traffic passing through the Cisco FWSM that is not SSL and SSH.
155	PCI: Firewall Traffic Besides SSL and SSH - Cisco IOS	Displays all traffic passing through the Cisco IOS that is not SSL and SSH.
156	PCI: Firewall Traffic Besides SSL and SSH - Cisco Netflow	Displays all traffic passing through the Cisco Netflow that is not SSL and SSH.
157	PCI: Firewall Traffic Besides SSL and SSH - F5 BIG-IP TMOS	Displays all traffic passing through the F5 BIG-IP TMOS that is not SSL and SSH.

Serial Number	TIBCO LogLogic Report	Description
158	PCI: Firewall Traffic Besides SSL and SSH - Cisco PIX	Displays all traffic passing through the Cisco PIX that is not SSL and SSH.
159	PCI: Firewall Traffic Besides SSL and SSH - Fortinet	Displays all traffic passing through the Fortinet that is not SSL and SSH.
160	PCI: Firewall Traffic Besides SSL and SSH - Juniper Firewall	Displays all traffic passing through the Juniper firewall that is not SSL and SSH.
161	PCI: Firewall Traffic Besides SSL and SSH - Juniper JunOS	Displays all traffic passing through the Juniper JunOS that is not SSL and SSH.
162	PCI: Firewall Traffic Besides SSL and SSH - Juniper RT Flow	Displays all traffic passing through the Juniper RT Flow that is not SSL and SSH.
163	PCI: Firewall Traffic Besides SSL and SSH - Nortel	Displays all traffic passing through the Nortel that is not SSL and SSH.
164	PCI: Firewall Traffic Besides SSL and SSH - PANOS	Displays all traffic passing through the Palo Alto Networks that is not SSL and SSH.
165	PCI: Firewall Traffic Besides SSL and SSH - Sidewinder	Displays all traffic passing through the Sidewinder that is not SSL and SSH.
166	PCI: Firewall Traffic Besides SSL and SSH - VMware vShield	Displays all traffic passing through the VMware vShield that is not SSL and SSH.
167	PCI: Firewall Traffic Considered Risky - Check Point	Displays Check Point allowed firewall traffic that is considered risky.
168	PCI: Firewall Traffic Considered Risky - Cisco ASA	Displays Cisco ASA allowed firewall traffic that is considered risky.
169	PCI: Firewall Traffic Considered Risky - Cisco FWSM	Displays Cisco FWSM allowed firewall traffic that is considered risky.
170	PCI: Firewall Traffic Considered Risky - Cisco IOS	Displays Cisco IOS allowed firewall traffic that is considered risky.
171	PCI: Firewall Traffic Considered Risky - Cisco Netflow	Displays Cisco Netflow allowed firewall traffic that is considered risky.
172	PCI: Firewall Traffic Considered Risky - Cisco PIX	Displays Cisco PIX allowed firewall traffic that is considered risky.
173	PCI: Firewall Traffic Considered Risky - F5 BIG-IP TMOS	Displays F5 BIG-IP TMOS allowed firewall traffic that is considered risky.
174	PCI: Firewall Traffic Considered Risky - Fortinet	Displays Fortinet allowed firewall traffic that is considered risky.

Serial Number	TIBCO LogLogic Report	Description
175	PCI: Firewall Traffic Considered Risky - Juniper Firewall	Displays Juniper Firewall allowed firewall traffic that is considered risky.
176	PCI: Firewall Traffic Considered Risky - Juniper JunOS	Displays Juniper JunOS allowed firewall traffic that is considered risky.
177	PCI: Firewall Traffic Considered Risky - Juniper RT Flow	Displays Juniper RT Flow allowed firewall traffic that is considered risky.
178	PCI: Firewall Traffic Considered Risky - Nortel	Displays Nortel allowed firewall traffic that is considered risky.
179	PCI: Firewall Traffic Considered Risky - PANOS	Displays Palo Alto Networks allowed firewall traffic that is considered risky.
180	PCI: Firewall Traffic Considered Risky - Sidewinder	Displays Sidewinder allowed firewall traffic that is considered risky.
181	PCI: Firewall Traffic Considered Risky - VMware vShield	Displays VMware vShield Edge allowed firewall traffic that is considered risky.
182	PCI: FortiOS: Attacks by Event ID	Displays FortiOS attacks by Event ID.
183	PCI: FortiOS: Attacks by Threat Name	Displays FortiOS attacks by threat Name.
184	PCI: FortiOS: Attacks Detected	Displays attacks detected by FortiOS.
185	PCI: FortiOS DLP Attacks Detected	Displays all DLP attacks detected by FortiOS.
186	PCI: Group Activities on TIBCO ActiveMatrix Administrator	Displays all group activities on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
187	PCI: Group Activities on UNIX Servers	Displays all group activities on UNIX servers to ensure authorized and appropriate access.
188	PCI: Group Activities on Windows Servers	Displays all group activities on Windows servers to ensure authorized and appropriate access.
189	PCI: Guardium SQL Guard Audit Configuration Changes	Displays all configuration changes on the Guardium SQL Guard Audit database.
190	PCI: Guardium SQL Guard Audit Data Access	Displays all select statements made on Guardium SQL Audit Server.
191	PCI: Guardium SQL Guard Audit Logins	Displays all login attempts to the Guardium SQL Server Audit database.

Serial Number	TIBCO LogLogic Report	Description
192	PCI: Guardium SQL Guard Configuration Changes	Displays all configuration changes on the Guardium SQL Guard database.
193	PCI: Guardium SQL Guard Data Access	Displays all select statements made on Guardium SQL Server.
194	PCI: Group Activities on NetApp Filer Audit	Displays all group activities on NetApp Filer Audit to ensure authorized and appropriate access.
195	PCI: Group Activities on Symantec Endpoint Protection	Displays all group activities on Symantec Endpoint Protection to ensure authorized and appropriate access.
196	PCI: Guardium SQL Guard Logins	Displays all login attempts to the Guardium SQL Server database.
197	PCI: Files Accessed through Pulse Connect Secure	Displays all files accessed through Pulse Connect Secure.
198	PCI: HP NonStop Audit Configuration Changes	Displays all audit configuration changes on HP NonStop.
199	PCI: HP NonStop Audit Login Failed	Displays all HP NonStop Audit login events which have failed.
200	PCI: HP NonStop Audit Login Successful	Displays all HP NonStop Audit login events which have succeeded.
201	PCI: HP NonStop Audit Object Changes	Displays HP NonStop Audit events related to object changes.
202	PCI: HP NonStop Audit Permissions Changed	Displays all permission modification activities on HP NonStop Audit to ensure authorized access.
203	PCI: i5/OS DST Password Reset	Displays i5/OS events related to the reset of the DST (Dedicated Service Tools) password.
204	PCI: i5/OS Files Accessed	Lists all events when a user gains access an i5/OS file.
205	PCI: i5/OS Network User Login Failed	Lists all events when a network user was denied access into the i5/OS.
206	PCI: i5/OS Network User Login Successful	Lists all events when a network user successfully logs into the i5/OS.
207	PCI: i5/OS Network User Profile Creation	Displays i5/OS events when a network user profile has been created.
208	PCI: i5/OS Network User Profile Deletion	Displays i5/OS events when a network user profile has been deleted.

Serial Number	TIBCO LogLogic Report	Description
209	PCI: i5/OS Network User Profile Modified	Displays i5/OS events when a network user profile has been modified.
210	PCI: i5/OS Object Permissions Modified	Displays all permission modification activities on i5/OS to ensure authorized access.
211	PCI: i5/OS Restarted	Lists all events when the i5/OS has been restarted.
212	PCI: i5/OS Service Started	Lists all events when a user starts a service on the i5/OS.
213	PCI: i5/OS User Login Failed	Lists all events when a user was denied access into the i5/OS.
214	PCI: i5/OS User Login Successful	Lists all events when a user successfully logs into the i5/OS.
215	PCI: i5/OS User Profile Creation	Displays i5/OS events when a user profile has been created.
216	PCI: i5/OS User Profile Modifications	Displays i5/OS events when a user profile has been modified.
217	PCI: Juniper Firewall HA State Changed	Displays all Juniper Firewall fail-over state change events.
218	PCI: Juniper Firewall Policy Changed	Displays all configuration changes to the Juniper Firewall policies.
219	PCI: Juniper Firewall Policy Out of Sync	Displays events that indicate the Juniper Firewall's HA policies are out of sync.
220	PCI: Juniper Firewall Reset Accepted	Displays events that indicate the Juniper Firewall has been reset to its factory default state.
221	PCI: Juniper Firewall Reset Imminent	Displays events that indicate the Juniper Firewall will be reset to its factory default state.
222	PCI: Juniper Firewall Restarted	Displays all Juniper Firewall restart events.
223	PCI: Juniper SSL VPN (Secure Access) Failed Logins by User	Displays all failed Juniper SSL VPN (Secure Access) logins based on user.
224	PCI: Juniper SSL VPN (Secure Access) Successful Logins by User	Displays all successful Juniper SSL VPN (Secure Access) logins based on user.
225	PCI: Juniper SSL VPN Failed Logins by User	Displays all failed logins per user at the Juniper SSL VPN.

Serial Number	TIBCO LogLogic Report	Description
226	PCI: Juniper SSL VPN Successful Logins by User	Displays all successful Juniper SSL VPN logins based on user.
227	PCI: Logins by Authentication Type	Displays all logins categorized by the authentication type.
228	PCI: LogLogic Disk Full	Displays events that indicate the LogLogic appliance's disk is near full.
229	PCI: LogLogic DSM Configuration Changes	Displays all configuration changes on the LogLogic DSM database.
230	PCI: LogLogic DSM Data Access	Displays all select statements made on LogLogic DSM database.
231	PCI: LogLogic DSM Logins	Displays all login attempts to the LogLogic DSM database.
232	PCI: LogLogic File Retrieval Errors	Displays all errors while retrieving log files from devices, servers and applications.
233	PCI: LogLogic HA State Change d	Displays all LogLogic appliance failover state change events.
234	PCI: LogLogic Management Center Account Activities	Displays all accounts activities on LogLogic management center to ensure authorized and appropriate access.
235	PCI: LogLogic Management Center Login	Displays all login events to the LogLogic management center.
236	PCI: LogLogic Management Center Password Changes	Displays all password change activities on LogLogic management center to ensure authorized and appropriate access.
237	PCI: LogLogic Management Center Upgrade Success	Displays all successful events related to the system's upgrade.
238	PCI: LogLogic Message Routing Errors	Displays all log forwarding errors on the LogLogic appliance to ensure all logs are archived properly.
239	PCI: LogLogic Universal Collector Configuration Changes	Displays LogLogic universal collector configuration changes.
240	PCI: McAfee AntiVirus: Attacks by Event ID	Displays McAfee AntiVirus attacks by Event ID.
241	PCI: McAfee AntiVirus: Attacks by Threat Name	Displays McAfee AntiVirus attacks by threat name.

Serial Number	TIBCO LogLogic Report	Description
242	PCI: McAfee AntiVirus: Attacks Detected	Displays attacks detected by McAfee AntiVirus.
243	PCI: Microsoft Operations Manager - Windows Accounts Activities	Displays all accounts activities on Windows servers to ensure authorized and appropriate access.
244	PCI: Microsoft Operations Manager - Windows Accounts Created	Displays all accounts created on Windows servers to ensure authorized and appropriate access.
245	PCI: Microsoft Operations Manager - Windows Accounts Enabled	Displays all accounts enabled on Windows servers to ensure authorized and appropriate access.
246	PCI: Microsoft Operations Manager - Windows Password Changes	Displays all password change activities on Windows servers to ensure authorized and appropriate access.
247	PCI: Microsoft Operations Manager - Windows Permissions Modified	Displays all permission modification activities on Windows servers to ensure authorized access.
248	PCI: Microsoft Operations Manager - Windows Policies Modified	Displays all policy modification activities on Windows servers to ensure authorized and appropriate access.
249	PCI: Microsoft Operations Manager - Windows Servers Restarted	Displays all Windows server restart activities to detect unusual activities.
250	PCI: Microsoft Sharepoint Content Deleted	Displays all events when content has been deleted from Microsoft Sharepoint.
251	PCI: Microsoft Sharepoint Content Updates	Displays all events when content is updated within Microsoft Sharepoint.
252	PCI: Microsoft Sharepoint Permissions Changed	Displays all user/group permission events to Microsoft Sharepoint.
253	PCI: Microsoft Sharepoint Policy Add, Remove, or Modify	Displays all events when a Microsoft Sharepoint policy is added, removed, or modified.
254	PCI: Microsoft SQL Server Configuration Changes	Displays Microsoft SQL database configuration changes.
255	PCI: Microsoft SQL Server Data Access	Displays data access events on Microsoft SQL Server databases.
256	PCI: Microsoft SQL Server Database Failed Logins	Displays failed Microsoft SQL Server database logins.

Serial Number	TIBCO LogLogic Report	Description
257	PCI: Microsoft SQL Server Database Successful Logins	Displays successful Microsoft SQL Server database logins.
258	PCI: Microsoft SQL Server Database Permission Events	Displays events related to Microsoft SQL Server database permission modifications.
259	PCI: Microsoft SQL Server Database User Additions and Deletions	Displays Microsoft SQL Server events related to creation and deletion of database users.
260	PCI: Microsoft SQL Server Password Changes	Displays password changes for Microsoft SQL Server database accounts.
261	PCI: NetApp Filer Accounts Locked	Displays all accounts locked out of NetApp Filer to detect access violations or unusual activities.
262	PCI: NetApp Filer Audit Accounts Enabled	Displays all accounts enabled on NetApp Filer Audit to ensure authorized and appropriate access.
263	PCI: NetApp Filer Audit Login Failed	Displays all NetApp Filer Audit Login events which have failed.
264	PCI: NetApp Filer Audit Login Successful	Displays all NetApp Filer Audit Login events which have succeeded.
265	PCI: NetApp Filer Audit Logs Cleared	Displays all audit logs clearing activities on NetApp Filer Audit to detect access violations or unusual activity.
266	PCI: NetApp Filer Audit Policies Modified	Displays all policy modification activities on NetApp Filer Audit to ensure authorized and appropriate access.
267	PCI: NetApp Filer Disk Failure	Displays all disk failure events on the NetApp Filer servers.
268	PCI: NetApp Filer File Activity	Displays all file activities on NetApp Filer.
269	PCI: NetApp Filer File System Full	Displays events that indicate the NetApp Filer's disk is near full.
270	PCI: NetApp Filer Login Failed	Displays all NetApp Filer Login events which have failed.
271	PCI: NetApp Filer Login Successful	Displays all NetApp Filer Login events which have succeeded.
272	PCI: NetApp Filer Password Changes	Displays all password change activities on NetApp Filer to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
273	PCI: NetApp Filer Disk Missing	Displays events that indicate disk missing on the NetApp Filer servers.
274	PCI: NetApp Filer Snapshot Error	Displays events that indicate backup on the NetApp Filer has failed.
275	PCI: Oracle Database Configuration Changes	Displays Oracle database configuration changes.
276	PCI: Oracle Database Data Access	Displays data access events on Oracle databases.
277	PCI: Oracle Database Failed Logins	Displays all failed login attempts to the Oracle database.
278	PCI: Oracle Database Successful Logins	Displays successful Oracle database logins.
279	PCI: Oracle Database Permission Events	Displays events related to Oracle Server database role and privilege management.
280	PCI: Oracle Database User Additions and Deletions	Displays Oracle database events related to creation and deletion of database users.
281	PCI: PANOS: Attacks by Event ID	Displays Palo Alto Networks attacks by Event ID.
282	PCI: PANOS: Attacks by Threat Name	Displays Palo Alto Networks attacks by threat name.
283	PCI: PANOS: Attacks Detected	Displays attacks detected by Palo Alto Networks.
284	PCI: Password Changes on Win dows Servers	Displays all password change activities on Windows servers to ensure authorized and appropriate access.
285	PCI: Periodic Review of Log Reports	Displays all review activities performed by administrators to ensure review for any access violations.
286	PCI: Periodic Review of User Access Logs	Displays all review activities performed by administrators to ensure review for any access violations.
287	PCI: Permissions Modified on Windows Servers	Displays all permission modification activities on Windows Servers to ensure authorized access.
288	PCI: Policies Modified on Windows Servers	Displays all policy modification activities on Windows servers to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
289	PCI: Pulse Connect Secure Failed Logins by User	Displays all failed Pulse Connect Secure logins based on user.
290	PCI: Pulse Connect Secure Policy Changed	Displays all configuration changes to the Pulse Connect Secure policies.
291	PCI: Pulse Connect Secure Successful Logins by User	Displays all successful Pulse Connect Secure logins based on user.
292	PCI: RACF Accounts Created	Displays all accounts created on RACF servers to ensure authorized and appropriate access.
293	PCI: RACF Accounts Deleted	Displays all accounts deleted on RACF servers to ensure authorized and appropriate access.
294	PCI: RACF Accounts Modified	Displays all events when a network user profile has been modified.
295	PCI: RACF Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
296	PCI: RACF Files Accessed	Displays all files accessed on RACF servers to ensure appropriate access.
297	PCI: RACF Password Changed	Displays all password change activities on RACF servers to ensure authorized and appropriate access.
298	PCI: RACF Permissions Changed	Displays all permission modification activities on RACF to ensure authorized access.
299	PCI: RACF Process Started	Displays all processes started on the RACF servers.
300	PCI: RACF Successful Logins	Displays successful logins to ensure only authorized personnel have access.
301	PCI: Root Logins	Displays root logins.
302	PCI: Sidewinder Configuration Changes	Displays Sidewinder configuration changes.
303	PCI: Software Update Successes on i5/OS	Displays all i5/OS successful events related to the system's software or patch update.
304	PCI: Successful Logins	Displays successful logins to ensure only authorized personnel have access.
305	PCI: Sybase ASE Database Configuration Changes	Displays configuration changes to the Sybase database.
306	PCI: Sybase ASE Database Data Access	Displays Sybase ASE events involving the SELECT statement.

Serial Number	TIBCO LogLogic Report	Description
307	PCI: Sybase ASE Database User Additions and Deletions	Displays Sybase database events related to creation and deletion of database users.
308	PCI: Sybase ASE Failed Logins	Displays failed Sybase ASE database logins.
309	PCI: Sybase ASE Successful Logins	Displays successful Sybase ASE database logins.
310	PCI: Symantec AntiVirus: Attacks by Threat Name	Displays Symantec AntiVirus attacks by threat name.
311	PCI: Symantec AntiVirus: Attacks Detected	Displays attacks detected by Symantec AntiVirus.
312	PCI: Symantec AntiVirus: Scans	Displays scans using Symantec AntiVirus.
313	PCI: Symantec AntiVirus: Updated	Displays updates to Symantec AntiVirus.
314	PCI: Symantec Endpoint Protection: Attacks by Threat Name	Displays Symantec Endpoint Protection attacks by threat name.
315	PCI: Symantec Endpoint Protection: Attacks Detected	Displays attacks detected by Symantec Endpoint Protection.
316	PCI: Symantec Endpoint Protection Configuration Changes	Displays Symantec Endpoint Protection configuration changes.
317	PCI: Symantec Endpoint Protection Password Changes	Displays all password change activities on Symantec Endpoint Protection to ensure authorized and appropriate access.
318	PCI: Symantec Endpoint Protection Policy Add, Remove, or Modify	Displays all events when a Symantec Endpoint Protection policy is added, removed, or modified.
319	PCI: Symantec Endpoint Protection: Updated	Displays updates to Symantec Endpoint Protection.
320	PCI: Symantec Endpoint Protection: Scans	Displays scans using Symantec Endpoint Protection.
321	PCI: TIBCO ActiveMatrix Administrator Failed Logins	Displays all TIBCO ActiveMatrix Administrator login events which have failed.
322	PCI: TIBCO ActiveMatrix Administrator Permission Changes	Displays events related to TIBCO ActiveMatrix Administrator permission modifications.

Serial Number	TIBCO LogLogic Report	Description
323	PCI: TIBCO ActiveMatrix Administrator Successful Logins	Displays successful logins to TIBCO ActiveMatrix Administrator to ensure only authorized personnel have access.
324	PCI: TIBCO Administrator Password Changes	Displays all password change activities on TIBCO Administrator to ensure authorized and appropriate access.
325	PCI: TIBCO Administrator Permission Changes	Displays events related to TIBCO Administrator permission modifications.
326	PCI: System Restarted	Displays all logs related to system restarts.
327	PCI: TrendMicro Control Manager: Attacks Detected	Displays attacks detected by TrendMicro Control Manager.
328	PCI: TrendMicro Control Manager: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro Control Manager by threat name.
329	PCI: TrendMicro OfficeScan: Attacks Detected	Displays attacks detected by TrendMicro OfficeScan.
330	PCI: TrendMicro OfficeScan: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro OfficeScan by threat name.
331	PCI: Tripwire Modifications, Additions, and Deletions	Displays system modifications, additions, and deletions detected by Tripwire.
332	PCI: Unauthorized Logins	Displays all logins from unauthorized users to ensure appropriate access to data.
333	PCI: Unencrypted Network Services - Check Point	Displays Check Point firewall traffic containing unencrypted network services.
334	PCI: Unencrypted Network Services - Cisco ASA	Displays Cisco ASA firewall traffic containing unencrypted network services.
335	PCI: Unencrypted Network Services - Cisco FWSM	Displays Cisco FWSM firewall traffic containing unencrypted network services.
336	PCI: Unencrypted Network Services - Cisco IOS	Displays Cisco IOS firewall traffic containing unencrypted network services.
337	PCI: Unencrypted Network Services - Cisco Netflow	Displays Cisco Netflow traffic containing unencrypted network services.
338	PCI: Unencrypted Network Services - Cisco PIX	Displays Cisco PIX firewall traffic containing unencrypted network services.

Serial Number	TIBCO LogLogic Report	Description
339	PCI: Unencrypted Network Services - Fortinet	Displays Fortinet firewall traffic containing unencrypted network services.
340	PCI: Unencrypted Network Services - Juniper Firewall	Displays Juniper Firewall traffic containing unencrypted network services.
341	PCI: Unencrypted Network Services - Juniper JunOS	Displays Juniper JunOS firewall traffic containing unencrypted network services.
342	PCI: Unencrypted Network Services - Juniper RT Flow	Displays Juniper RT Flow firewall traffic containing unencrypted network services.
343	PCI: Unencrypted Network Services - Nortel	Displays Nortel firewall traffic containing unencrypted network services.
344	PCI: Unencrypted Network Services - PANOS	Displays Palo Alto Networks firewall traffic containing unencrypted network services.
345	PCI: Unencrypted Network Services - Sidewinder	Displays Sidewinder firewall traffic containing unencrypted network services.
346	PCI: Unencrypted Network Services - VMware vShield	Displays VMware vShield firewall traffic containing unencrypted network services.
347	PCI: UNIX Failed Logins	Displays failed UNIX logins for known and unknown users.
348	PCI: vCenter Change Attributes	Modification of VMware vCenter and VMware ESX properties.
349	PCI: vCenter Data Move	Entity has been moved within the VMware vCenter infrastructure.
350	PCI: vCenter Datastore Events	Displays create, modify, and delete datastore events on VMware vCenter.
351	PCI: vCenter Failed Logins	Failed logins to the VMware vCenter console.
352	PCI: vCenter Orchestrator Change Attributes	Modification of VMware vCenter Orchestrator properties.
353	PCI: vCenter Orchestrator Datastore Events	Displays create, modify, and delete datastore events on VMware vCenter Orchestrator.
354	PCI: vCenter Orchestrator Data Move	Entity has been moved within the VMware vCenter Orchestrator infrastructure.
355	PCI: vCenter Orchestrator Failed Logins	Displays all failed logins for VMware vCenter Orchestrator.

Serial Number	TIBCO LogLogic Report	Description
356	PCI: vCenter Orchestrator Virtual Machine Created	Virtual machine has been created from VMware vCenter Orchestrator.
357	PCI: vCenter Orchestrator Virtual Machine Deleted	Virtual machine has been deleted from VMware vCenter Orchestrator.
358	PCI: vCenter Orchestrator Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter Orchestrator console.
359	PCI: vCenter Orchestrator Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter Orchestrator console.
360	PCI: vCenter Orchestrator vSwitch Added, Changed or Removed	vSwitch has been added, modified or removed from VMware vCenter Orchestrator console.
361	PCI: vCenter Modify Firewall Policy	Displays changes to the VMware ESX allowed services firewall policy.
362	PCI: vCenter Resource Usage Change	Resources have changed on VMware vCenter.
363	PCI: vCenter Restart ESX Services	VMware vCenter restarted services running on VMware ESX Server.
364	PCI: vCenter Shutdown or Restart of ESX Server	VMware ESX Server is shutdown or restarted from VMware vCenter console.
365	PCI: vCenter Successful Logins	Successful logins to the VMware vCenter console.
366	PCI: vCenter User Permission Change	A permission role has been added, changed, removed, or applied to a user on VMware vCenter server.
367	PCI: vCenter Virtual Machine Created	Virtual machine has been created from VMware vCenter console.
368	PCI: vCenter Virtual Machine Deleted	Virtual machine has been deleted or removed from VMware vCenter console.
369	PCI: vCenter Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter console.
370	PCI: vCenter Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter console.
371	PCI: vCenter vSwitch Added, Changed or Removed	vSwitch on VMware ESX server has been added, modified or removed from the VMware vCenter console.
372	PCI: vCloud Failed Logins	Failed logins to the VMware vCloud Director console.

Serial Number	TIBCO LogLogic Report	Description
373	PCI: vCloud Organization Created	VMware vCloud Director organization created events.
374	PCI: vCloud Organization Deleted	VMware vCloud Director organization deleted events.
375	PCI: vCloud Organization Modified	VMware vCloud Director organization modified events.
376	PCI: vCloud Successful Logins	Successful logins to the VMware vCloud Director console.
377	PCI: vCloud User Created	VMware vCloud Director user created events.
378	PCI: vCloud User Deleted or Removed	VMware vCloud Director users have been deleted or removed from the system.
379	PCI: vCloud vApp Created, Modified, or Deleted	VMware vCloud Director vApp created, deleted, and modified events.
380	PCI: vCloud vDC Created, Modified, or Deleted	VMware vCloud Director virtual datacenter created, modified, or deleted events.
381	PCI: VPN Users Accessing Corporate Network	Displays all users logging into the corporate network via Virtual Private Network to ensure appropriate access.
382	PCI: vShield Edge Configuration Changes	Displays changes to VMware vShield Edge policies.
383	PCI: Web Access to Applications - Fortinet	Displays all web-based access to applications to ensure appropriate and authorized access on Fortinet.
384	PCI: Web Access to Applications - F5 BIG-IP TMOS	Displays all web-based access to applications to ensure appropriate and authorized access on F5 BIG-IP TMOS.
385	PCI: Web Access to Application s - Microsoft IIS	Displays all web-based access to applications to ensure appropriate and authorized access on Microsoft IIS.
386	PCI: Web Access to Applications - PANOS	Displays all web-based access to applications to ensure appropriate and authorized access on Palo Alto Networks.
387	PCI: Web Access to Applications	Displays all web-based access to applications to ensure appropriate and authorized access.
388	PCI: Windows Accounts Enabled	Displays all accounts enabled on Windows servers to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
389	PCI: Windows Accounts Locked	Displays all accounts locked out of Windows servers to detect access violations or unusual activities.
390	PCI: Windows Audit Logs Cleared	Displays all audit logs clearing activities on Windows servers to detect access violations or unusual activity.
391	PCI: Windows New Services Installed	Displays a list of new services installed on Windows servers to ensure authorized access.
392	PCI: Windows Servers Restarted	Displays all Windows server restart activities to detect unusual activities.
393	PCI: Windows Software Update Activities	Displays all events related to the system's software or patch update.
394	PCI: Windows Software Update Failures	Displays all failed events related to the system's software or patch update.
395	PCI: Windows Software Update Successes	Displays all successful events related to the system's software or patch update.

TIBCO LogLogic Alerts for PCI

The following table lists the alerts included in the TIBCO LogLogic® Compliance Suite - PCI Edition.

Serial Number	TIBCO LogLogic Alert	Description
1	PCI: Accounts Created	Alerts when a new account is created on servers.
2	PCI: Accounts Deleted	Alerts when an account is deleted on servers.
3	PCI: Accounts Enabled	Alerts when an account has been enabled on servers.
4	PCI: Accounts Locked	Alerts when an account has been locked on servers.
5	PCI: Accounts Modified	Alerts when an account is modified on servers.
6	PCI: Active Directory Changes	Alerts when changes are made within Active Directory.
7	PCI: Anomalous Firewall Traffic	Alerts when firewall traffic patterns are out of the norm.
8	PCI: Anomalous IDS Alerts	Alerts when IDS anomalies are above or below defined thresholds.
9	PCI: Check Point Policy Changed	Alerts when a Check Point firewall's policy has been modified.

Serial Number	TIBCO LogLogic Alert	Description
10	PCI: Cisco ISE, ACS Configuration Changed	Alerts when configuration changes are made to the Cisco ISE or Cisco SecureACS.
11	PCI: Cisco ISE, ACS Passwords Changed	Alerts when a user changes their password via Cisco ISE or Cisco SecureACS.
12	PCI: Cisco PIX, ASA, FWSM HA State Change	Alerts when Cisco PIX, ASA, or FWSM has changed its failover state.
13	PCI: Cisco PIX, ASA, FWSM Commands Executed	Alerts when a Cisco PIX, ASA, or FWSM commands are executed.
14	PCI: Cisco PIX, ASA, FWSM Failover Disabled	Alerts when a Cisco PIX, ASA, or FWSM HA configuration is disabled.
15	PCI: Cisco PIX, ASA, FWSM Failover Performed	Alerts when a failover has occurred on the Cisco PIX, ASA, or FWSM devices.
16	PCI: Cisco PIX, ASA, FWSM Policy Changed	Alerts when a Cisco PIX, ASA, or FWSM firewall policy has been modified.
17	PCI: Cisco PIX, ASA, FWSM Routing Failure	Alerts when routing failure occurred in the Cisco PIX, ASA, or FWSM devices.
18	PCI: Cisco Switch Policy Changed	Alerts when Cisco router or switch configuration has been modified.
19	PCI: DB2 Database Configuration Change	Alerts when a configuration is changed on a DB2 database.
20	PCI: DB2 Database User Added or Dropped	Alerts when a user is added or dropped from a DB2 database.
21	PCI: DNS Server Shutdown	Alerts when DNS Server has been shutdown.
22	PCI: DNS Server Started	Alerts when DNS Server has been started.
23	PCI: Escalated Privileges	Alerts when a user or program has escalated the privileges.
24	PCI: F5 BIG-IP TMOS Risky Traffic	F5 BIG-IP TMOS traffic considered risky.
25	PCI: F5 BIG-IP TMOS Traffic Besides HTTP, SSH and SSL	F5 BIG-IP TMOS traffic besides HTTP, SSH and SSL.
26	PCI: F5 BIG-IP TMOS Traffic Besides SSH and SSL	F5 BIG-IP TMOS traffic besides SSH and SSL.

Serial Number	TIBCO LogLogic Alert	Description
27	PCI: Firewall Traffic Besides HTTP, SSL and SSH	Alerts on traffic besides HTTP, SSL & SSH passing the firewall.
28	PCI: Firewall Traffic Considered Risky	Alerts on non HTTP, SSL, or SSH traffic passing through the firewall.
29	PCI: Group Members Added	Alerts when new members are added to user groups.
30	PCI: Group Members Deleted	Alerts when members are removed from user groups.
31	PCI: Groups Created	Alerts when new user groups are created.
32	PCI: Groups Deleted	Alerts when a user group is deleted.
33	PCI: Groups Modified	Alerts when a user group has been modified.
34	PCI: Guardium SQL Guard Config Changes	Alerts when a configuration is changed on Guardium SQL Database.
35	PCI: Guardium SQL Guard Data Access	Alerts when a select statement is made on Guardium SQL Database.
36	PCI: Guardium SQL Guard Logins	Alerts when a user logs into the Guardium SQL Database.
37	PCI: HP NonStop Audit Configuration Changed	Alerts when configuration changes are made to the HP NonStop Audit.
38	PCI: HP NonStop Audit Permission Changed	Alerts on HP NonStop Audit permission changed events.
39	PCI: i5/OS Network Profile Changes	Alerts when any changes are made to an i5/OS network profile.
40	PCI: i5/OS Permission or Policy Change	Alerts when policies or permissions are changed on the i5/OS.
41	PCI: i5/OS Server or Service Status Change	Alerts when the i5/OS is restarted or a service stops or starts.
42	PCI: i5/OS Software Updates	Alerts when events related to the i5/OS software updates.
43	PCI: i5/OS User Profile Changes	Alerts when a user profile is changed on the i5/OS.
44	PCI: IBM AIX Password Changed	Alerts when an account password is changed on IBM AIX servers.
45	PCI: Juniper Firewall HA State Change	Alerts when Juniper Firewall has changed its failover state.

Serial Number	TIBCO LogLogic Alert	Description
46	PCI: Juniper Firewall Peer Missing	Alerts when a Juniper Firewall HA peer is missing.
47	PCI: Juniper Firewall Policy Changes	Alerts when Juniper Firewall configuration is changed.
48	PCI: Juniper Firewall Policy Out of Sync	Alerts when the Juniper Firewall's policy is out of sync.
49	PCI: Logins Failed	Alerts when login failures are over the defined threshold.
50	PCI: Logins Succeeded	Alerts when successful logins are over the defined threshold.
51	PCI: LogLogic Disk Full	Alerts when the LogLogic appliance's disk is near full.
52	PCI: LogLogic DSM Configuration Changes	Alerts when a configuration is changed on LogLogic DSM database.
53	PCI: LogLogic DSM Data Access	Alerts when a select statement is made on LogLogic DSM database.
54	PCI: LogLogic DSM Logins	Alerts when a user logs into the LogLogic DSM database.
55	PCI: LogLogic Management Center Passwords Changed	Alerts when users have changed their passwords.
56	PCI: LogLogic Management Center Upgrade Succeeded	Alerts for successful events related to the system's upgrade.
57	PCI: LogLogic Message Routing Errors	Alerts when problems are detected during message forwarding.
58	PCI: LogLogic Universal Collector Configuration Changed	Alerts when configuration changes are made to the LogLogic universal collector.
59	PCI: Microsoft Operations Manager - Permissions Changed	Alert when user or group permissions have been changed.
60	PCI: Microsoft Operations Manager - Windows Passwords Changed	Alerts when users have changed their passwords.
61	PCI: Microsoft Operations Manager - Windows Policies Changed	Alerts when Windows policies changed.

Serial Number	TIBCO LogLogic Alert	Description
62	PCI: LogLogic File Retrieval Errors	Alerts when problems are detected during log file retrieval.
63	PCI: Microsoft Sharepoint Content Deleted	Alerts on Microsoft Sharepoint content deleted events.
64	PCI: Microsoft Sharepoint Content Updated	Alerts on Microsoft Sharepoint content updated events.
65	PCI: Microsoft Sharepoint Permission Changed	Alerts on Microsoft Sharepoint permission changed events.
66	PCI: Microsoft Sharepoint Policies Added, Removed, Modified	Alerts on Microsoft Sharepoint policy additions, deletions, and modifications.
67	PCI: Microsoft Operations Manager Server Restarted	Alerts when a Windows server is restarted.
68	PCI: NetApp Authentication Failure	Alerts when NetApp authentication failure events occur.
69	PCI: NetApp Bad File Handle	Alerts when a bad file handle is detected on a NetApp device.
70	PCI: NetApp Bootblock Update	Alerts when the bootblock has been updated on a NetApp Filer.
71	PCI: NetApp Filer Audit Policies Changed	Alerts when NetApp Filer Audit policies changed.
72	PCI: NetApp Filer Disk Failure	Alerts when a disk fails on a NetApp Filer.
73	PCI: NetApp Filer Disk Inserted	Alerts when a disk is inserted into the NetApp Filer device.
74	PCI: NetApp Filer Disk Missing	Alerts when a disk is missing on the NetApp Filer device.
75	PCI: NetApp Filer Disk Pulled	Alerts when a RAID disk has been pulled from the Filer device.
76	PCI: NetApp Filer Disk Scrub Suspended	Alerts when the disk scrubbing process has been suspended.
77	PCI: NetApp Filer File System Full	Alerts when the file system is full on the NetApp Filer device.
78	PCI: NetApp Filer NIS Group Update	Alerts when the NIS group has been updated on the Filer device.

Serial Number	TIBCO LogLogic Alert	Description
79	PCI: NetApp Filer Snapshot Error	Alerts when an error has been detected during a NetApp Filer snapshot.
80	PCI: NetApp Filer Unauthorized Mounting	Alerts when an unauthorized mount event occurs.
81	PCI: Oracle Database Configuration Change	Alerts when a ALTER or UPDATE command is executed on Oracle DB's.
82	PCI: Oracle Database Data Access	Alerts when Oracle tables are accessed.
83	PCI: Oracle Database Permissions Changed	Alerts when permissions are changed on Oracle databases.
84	PCI: Oracle Database User Added or Deleted	Alerts when a user is added or deleted from an Oracle database.
85	PCI: RACF Files Accessed	Alerts when files are accessed on the RACF servers.
86	PCI: RACF Passwords Changed	Alerts when users have changed their passwords.
87	PCI: RACF Permissions Changed	Alerts when user or group permissions have been changed.
88	PCI: RACF Process Started	Alerts whenever a process is run on a RACF server.
89	PCI: Sidewinder Configuration Changed	Alerts when configuration changes are made to the Sidewinder.
90	PCI: Sybase ASE Database Config Changes	Alerts on Sybase ASE Database configuration change events.
91	PCI: Sybase ASE Database Data Access	Alerts on Sybase ASE Database data access events.
92	PCI: Symantec Endpoint Protection Configuration Changed	Alerts when configuration changes are made to the Symantec Endpoint Protection.
93	PCI: Symantec Endpoint Protection Policy Add, Delete, Modify	Alerts on Symantec Endpoint Protection additions, deletions, and modifications.
94	PCI: System Restarted	Alerts when systems such as routers and switches have restarted.
95	PCI: TIBCO ActiveMatrix Administrator Permission Changed	Alertss on TIBCO ActiveMatrix Administrator permission changed events.

Serial Number	TIBCO LogLogic Alert	Description
96	PCI: vCenter Create Virtual Machine	Alerts when virtual machine has been created from VMware vCenter console.
97	PCI: vCenter Data Move	Alerts when entity has been moved within the VMware vCenter infrastructure.
98	PCI: vCenter Datastore Event	Alerts on create, modify, and delete datastore events on VMware vCenter.
99	PCI: vCenter Delete Virtual Machine	Alerts when a virtual machine has been deleted or removed from VMware vCenter console.
100	PCI: vCenter Firewall Policy Change	Alerts when changes to the VMware ESX allowed services firewall policy.
101	PCI: vCenter Orchestrator Create Virtual Machine	Virtual machine has been created from VMware vCenter Orchestrator console.
102	PCI: vCenter Orchestrator Data Move	Entity has been moved within the VMware vCenter Orchestrator infrastructure.
103	PCI: vCenter Orchestrator Datastore Events	Alerts on create, modify, and delete datastore events on VMware vCenter Orchestrator.
104	PCI: vCenter Orchestrator Delete Virtual Machine	Alerts when a virtual machine has been deleted or removed from VMware vCenter Orchestrator console.
105	PCI: vCenter Orchestrator Login Failed	Failed logins to the VMware vCenter Orchestrator console.
106	PCI: vCenter Orchestrator Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter Orchestrator console.
107	PCI: vCenter Orchestrator Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter Orchestrator console.
108	PCI: vCenter Orchestrator vSwitch Add, Modify or Delete	vSwitch on VMware ESX server has been added, modified or removed from vCenter Orchestrator.
109	PCI: vCenter Permission Change	Alerts when a permission role has been added, changed, removed, or applied on VMware vCenter.
110	PCI: vCenter Restart ESX Services	Alerts when VMware vCenter restarted services running on VMware ESX Server.
111	PCI: vCenter Shutdown or Restart ESX	Alerts when VMware ESX Server is shutdown from vCenter console.
112	PCI: vCenter User Login Failed	Alerts on failed logins to the VMware vCenter console.

Serial Number	TIBCO LogLogic Alert	Description
113	PCI: vCenter User Login Successful	Alerts on successful logins to the VMware vCenter console.
114	PCI: vCenter Virtual Machine Shutdown	Alerts when virtual machine has been shutdown or paused from VMware vCenter console.
115	PCI: vCenter Virtual Machine Started	Alerts when virtual machine has been started or resumed from VMware vCenter console.
116	PCI: vCenter vSwitch Add, Modify or Delete	Alerts when vSwitch on VMware ESX server has been added, modified or removed from vCenter.
117	PCI: vCloud Director Login Failed	Alerts on failed logins to the VMware vCloud Director console.
118	PCI: vCloud Director Login Success	Alerts on successful logins to the VMware vCloud Director console.
119	PCI: vCloud Organization Created	Alerts when organization successfully created on VMware vCloud Director.
120	PCI: vCloud Organization Deleted	Alerts when organization successfully deleted on VMware vCloud Director.
121	PCI: vCloud Organization Modified	Alerts when organization successfully modified on VMware vCloud Director.
122	PCI: vCloud User Created	Alerts when a user successfully created on VMware vCloud Director.
123	PCI: vCloud User, Group, or Role Modified	Alerts when VMware vCloud Director user, group, or role has been modified.
124	PCI: vCloud vApp Created, Deleted, or Modified	Alerts when VMware vCloud Director vApp has been created, deleted, or modified.
125	PCI: vCloud vDC Created, Modified, or Deleted	Alerts when VMware vCloud Director Virtual Datacenters have been created, deleted, or modified.
126	PCI: vShield Edge Configuration Change	Alerts when configuration changes to VMware vShield Edge policies.
127	PCI: vShield Firewall Traffic Besides HTTP, SSH and SSL	VMware vShield Edge traffic besides HTTP, SSH and SSL.
128	PCI: vShield Firewall Traffic Besides SSH and SSL	Alerts on traffic besides SSH, and SSL passing through vShield Firewall.
129	PCI: vShield Risky Traffic	Alerts when VMware vShield Edge Traffic considered risky.

Serial Number	TIBCO LogLogic Alert	Description
130	PCI: Windows Audit Log Cleared	Alerts when audit logs on Windows servers have been cleared.
131	PCI: Windows Files Accessed	Show files accessed on the Windows servers.
132	PCI: Windows Objects Create/ Delete	Alerts when system-level objects have been created or deleted.
133	PCI: Windows Passwords Changed	Alerts when users have changed their passwords.
134	PCI: Windows Permissions Changed	Alerts when user or group permissions have been changed.
135	PCI: Windows Policies Changed	Alerts when Windows policies changed.
136	PCI: Windows Process Started	Alerts when a process has been started on a Windows server.
137	PCI: Windows Programs Accessed	Alertss when a program is accessed on a Windows server.
138	PCI: Windows Software Updates	Alerts when events related to the Windows' software updates.
139	PCI: Windows Software Updates Failed	Alerts when failed events related to the software updates.
140	PCI: Windows Software Updates Succeeded	Alerts for successful events related to the software updates.

TIBCO LogLogic Reports and Alerts Quick Reference

The following table lists the reports and alerts included in the TIBCO LogLogic® Compliance Suite - PCI Edition.

Requirement	Description	Compliance Suite Reports and Alerts
Requirement 1 - Install and maintain a firewall configuration to protect cardholder data		

Requirement	Description	Compliance Suite Reports and Alerts
1.1.1	A formal process for approving and testing all external network connections and changes to the firewall configuration	**Compliance Suite Reports** PCI: Check Point Configuration Changes PCI: Cisco ISE, ACS Configuration Changes PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: Sidewinder Configuration Changes PCI: Symantec Endpoint Protection Configuration Changes PCI: vCenter vSwitch Added, Changed or Removed PCI: vCenter Orchestrator vSwitch Added, Changed or Removed PCI: vShield Edge Configuration Changes **Compliance Suite Alerts** PCI: Cisco ISE, ACS Configuration Changed PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: Sidewinder Configuration Changed PCI: Symantec Endpoint Protection Configuration Changed PCI: vCenter Orchestrator vSwitch Add, Modify or Delete PCI: vCenter vSwitch Add, Modify or Delete PCI: vShield Edge Configuration Change

Requirement	Description	Compliance Suite Reports and Alerts
1.1.5	Documented list of services and ports necessary for business	**Compliance Suite Reports** PCI: Applications Through Firewalls PCI: Firewall Connections Accepted - Cisco PIX PCI: Firewall Connections Accepted - Check Point PCI: Firewall Connections Accepted - Cisco IOS PCI: Firewall Connections Accepted - Cisco Netflow PCI: Firewall Connections Accepted - Cisco NXOS PCI: Firewall Connections Accepted - F5 BIG-IP TMOS PCI: Firewall Connections Accepted - Juniper JunOS PCI: Firewall Connections Accepted - PANOS PCI: Firewall Connections Accepted - Sidewinder PCI: Firewall Connections Accepted - VMware vShield PCI: Firewall Traffic Besides HTTP, SSL and SSH - Check Point PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco ASA PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco FWSM PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco IOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco Netflow PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco PIX PCI: Firewall Traffic Besides HTTP, SSL and SSH - F5 BIG-IP TMOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Fortinet PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper Firewall PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper JunOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper RTFlow PCI: Firewall Traffic Besides HTTP, SSL and SSH - Nortel

Requirement	Description	Compliance Suite Reports and Alerts
1.1.5	Documented list of services and ports necessary for business	**Compliance Suite Reports** (Cont.) PCI: Firewall Traffic Besides HTTP, SSL and SSH - PANOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Sidewinder PCI: Firewall Traffic Besides HTTP, SSL and SSH - VMware vShield PCI: Sidewinder Configuration Changes PCI: Web Access to Applications PCI: Web Access to Applications - F5 BIG-IP TMOS PCI: Web Access to Applications - Microsoft IIS **Compliance Suite Alerts** PCI: Anomalous Firewall Traffic PCI: F5 BIG-IP TMOS Traffic Besides HTTP, SSH and SSL PCI: Firewall Traffic Besides HTTP, SSL and SSH PCI: Sidewinder Configuration Changed PCI: vShield Firewall Traffic Besides HTTP, SSL and SSH

Requirement	Description	Compliance Suite Reports and Alerts
1.1.6	Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN	**Compliance Suite Reports** PCI: Applications Through Firewalls PCI: Check Point Configuration Changes PCI: Cisco ISE, ACS Configuration Changes PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: Firewall Connections Accepted - Cisco PIX PCI: Firewall Connections Accepted - Check Point PCI: Firewall Connections Accepted - Cisco IOS PCI: Firewall Connections Accepted - Cisco Netflow PCI: Firewall Connections Accepted - Cisco NXOS PCI: Firewall Connections Accepted - F5 BIG-IP TMOS PCI: Firewall Connections Accepted - Juniper JunOS PCI: Firewall Connections Accepted - PANOS PCI: Firewall Connections Accepted - Sidewinder PCI: Firewall Connections Accepted - VMware vShield PCI: Firewall Traffic Besides HTTP, SSL and SSH - Check Point PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco ASA PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco FWSM PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco IOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco Netflow PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco PIX PCI: Firewall Traffic Besides HTTP, SSL and SSH - F5 BIG-IP TMOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Fortinet PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper Firewall PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper JunOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper RTFlow

Requirement	Description	Compliance Suite Reports and Alerts
1.1.6	Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN	**Compliance Suite Reports** (Cont.) PCI: Firewall Traffic Besides HTTP, SSL and SSH - Nortel PCI: Firewall Traffic Besides HTTP, SSL and SSH - PANOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Sidewinder PCI: Firewall Traffic Besides HTTP, SSL and SSH - VMware vShield PCI: Sidewinder Configuration Changes PCI: Symantec Endpoint Protection Configuration Changes PCI: vCenter vSwitch Added, Changed or Removed PCI: vCenter Orchestrator vSwitch Added, Changed or Removed PCI: vShield Edge Configuration Changes PCI: Web Access to Applications PCI: Web Access to Applications - Fortinet PCI: Web Access to Applications - F5 BIG-IP TMOS PCI: Web Access to Applications - Microsoft IIS PCI: Web Access to Applications - PANOS **Compliance Suite Alerts** PCI: Anomalous Firewall Traffic PCI: Cisco ISE, ACS Configuration Changed PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: F5 BIG-IP TMOS Traffic Besides HTTP, SSH and SSL PCI: Firewall Traffic Besides HTTP, SSL and SSH PCI: Sidewinder Configuration Changed PCI: vShield Firewall Traffic Besides HTTP, SSL and SSH PCI: Symantec Endpoint Protection Configuration Changed PCI: vCenter vSwitch Add, Modify or Delete PCI: vCenter Orchestrator vSwitch Add, Modify or Delete PCI: vShield Edge Configuration Change

Requirement	Description	Compliance Suite Reports and Alerts
1.1.7	Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented	**Compliance Suite Reports** PCI: Applications Through Firewalls PCI: Check Point Configuration Changes PCI: Cisco ISE, ACS Configuration Changes PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: Firewall Connections Accepted - Cisco PIX PCI: Firewall Connections Accepted - Check Point PCI: Firewall Connections Accepted - Cisco IOS PCI: Firewall Connections Accepted - Cisco Netflow PCI: Firewall Connections Accepted - Cisco NXOS PCI: Firewall Connections Accepted - F5 BIG-IP TMOS PCI: Firewall Connections Accepted - Juniper JunOS PCI: Firewall Connections Accepted - PANOS PCI: Firewall Connections Accepted - Sidewinder PCI: Firewall Connections Accepted - VMware vShield PCI: Firewall Traffic Besides HTTP, SSL and SSH - Check Point PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco ASA PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco FWSM PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco IOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco Netflow PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco PIX PCI: Firewall Traffic Besides HTTP, SSL and SSH - F5 BIG-IP TMOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Fortinet PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper Firewall PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper JunOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper RTFlow

Requirement	Description	Compliance Suite Reports and Alerts
1.1.7	Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented	**Compliance Suite Reports** (Cont.) PCI: Firewall Traffic Besides HTTP, SSL and SSH - Nortel PCI: Firewall Traffic Besides HTTP, SSL and SSH - PANOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Sidewinder PCI: Firewall Traffic Besides HTTP, SSL and SSH - VMware vShield PCI: Firewall Traffic Considered Risky - Check Point PCI: Firewall Traffic Considered Risky - Cisco ASA PCI: Firewall Traffic Considered Risky - Cisco FWSM PCI: Firewall Traffic Considered Risky - Cisco IOS PCI: Firewall Traffic Considered Risky - Cisco Netflow PCI: Firewall Traffic Considered Risky - Cisco PIX PCI: Firewall Traffic Considered Risky - F5 BIG-IP TMOS PCI: Firewall Traffic Considered Risky - Fortinet PCI: Firewall Traffic Considered Risky - Juniper Firewall PCI: Firewall Traffic Considered Risky - Juniper JunOS PCI: Firewall Traffic Considered Risky - Juniper RT Flow PCI: Firewall Traffic Considered Risky - Nortel PCI: Firewall Traffic Considered Risky - PANOS PCI: Firewall Traffic Considered Risky - Sidewinder PCI: Firewall Traffic Considered Risky - VMware vShield PCI: Sidewinder Configuration Changes PCI: Symantec Endpoint Protection Configuration Changes PCI: Unencrypted Network Services - Check Point PCI: Unencrypted Network Services - Cisco ASA PCI: Unencrypted Network Services - Cisco FWSM PCI: Unencrypted Network Services - Cisco IOS PCI: Unencrypted Network Services - Cisco Netflow PCI: Unencrypted Network Services - Cisco PIX PCI: Unencrypted Network Services - Fortinet PCI: Unencrypted Network Services - Juniper Firewall

Requirement	Description	Compliance Suite Reports and Alerts
		PCI: Unencrypted Network Services - Juniper JunOS
1.1.7	Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented	Compliance Suite Reports (Cont.) PCI: Unencrypted Network Services - Juniper RT Flow PCI: Unencrypted Network Services - Nortel PCI: Unencrypted Network Services - PANOS PCI: Unencrypted Network Services - Sidewinder PCI: Unencrypted Network Services - VMware vShield PCI: vCenter vSwitch Added, Changed or Removed PCI: vCenter Orchestrator vSwitch Added, Changed or Removed PCI: vShield Edge Configuration Changes PCI: Web Access to Applications PCI: Web Access to Applications - Fortinet PCI: Web Access to Applications - F5 BIG-IP TMOS PCI: Web Access to Applications - Microsoft IIS PCI: Web Access to Applications - PANOS **Compliance Suite Alerts** PCI: Anomalous Firewall Traffic PCI: Cisco ISE, ACS Configuration Changed PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: F5 BIG-IP TMOS Risky Traffic PCI: Firewall Traffic Besides HTTP, SSL and SSH PCI: Firewall Traffic Considered Risky PCI: Sidewinder Configuration Changed PCI: Symantec Endpoint Protection Configuration Changed PCI: vCenter vSwitch Add, Modify or Delete PCI: vCenter Orchestrator vSwitch Add, Modify or Delete PCI: vShield Edge Configuration Change PCI: vShield Firewall Traffic Besides HTTP, SSH and SSL PCI: vShield Risky Traffic

Requirement	Description	Compliance Suite Reports and Alerts
1.1.8	Quarterly review of firewall and router rule sets	**Compliance Suite Reports** PCI: Check Point Configuration Changes PCI: Cisco ISE, ACS Configuration Changes PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: Cisco Switch Policy Changes PCI: Juniper Firewall Policy Changed PCI: Juniper Firewall Policy Out of Sync PCI: LogLogic Universal Collector Configuration Changes PCI: Symantec Endpoint Protection Configuration Changes PCI: vCenter Modify Firewall Policy PCI: vCenter vSwitch Added, Changed or Removed PCI: vCenter Orchestrator vSwitch Added, Changed or Removed PCI: vShield Edge Configuration Changes **Compliance Suite Alerts** PCI: Check Point Policy Changed PCI: Cisco ISE, ACS Configuration Changed PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: Cisco Switch Policy Changed PCI: Juniper Firewall Policy Changes PCI: Juniper Firewall Policy Out of Sync PCI: LogLogic Universal Collector Configuration Changed PCI: Sidewinder Configuration Changed PCI: Symantec Endpoint Protection Configuration Changed PCI: vCenter Firewall Policy Change PCI: vCenter Orchestrator vSwitch Add, Modify or Delete PCI: vCenter vSwitch Add, Modify or Delete PCI: vShield Edge Configuration Change

Requirement	Description	Compliance Suite Reports and Alerts
1.1.8	Quarterly review of firewall and router rule sets	**Compliance Suite Alerts** (Cont.) PCI: Juniper Firewall Policy Changes PCI: Juniper Firewall Policy Out of Sync PCI: LogLogic Universal Collector Configuration Changed PCI: Symantec Endpoint Protection Configuration Changed PCI: vCenter Firewall Policy Change PCI: vCenter vSwitch Add, Modify or Delete PCI: vCenter Orchestrator vSwitch Add, Modify or Delete

Requirement	Description	Compliance Suite Reports and Alerts
1.1.9	Configuration standards for routers	**Compliance Suite Reports** PCI: Check Point Configuration Changes PCI: Cisco ISE, ACS Configuration Changes PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: Cisco Switch Policy Changes PCI: Juniper Firewall Policy Changed PCI: Juniper Firewall Policy Out of Sync PCI: LogLogic Universal Collector Configuration Changes PCI: Symantec Endpoint Protection Configuration Changes PCI: vCenter Modify Firewall Policy PCI: vCenter vSwitch Added, Changed or Removed PCI: vCenter Orchestrator vSwitch Added, Changed or Removed PCI: vShield Edge Configuration Changes **Compliance Suite Alerts** PCI: Check Point Policy Changed PCI: Cisco ISE, ACS Configuration Changed PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco PIX, ASA, FWSM Routing Failure PCI: Cisco Switch Policy Changed PCI: Juniper Firewall Policy Changes PCI: Juniper Firewall Policy Out of Sync PCI: LogLogic Universal Collector Configuration Changed PCI: Sidewinder Configuration Changed PCI: Symantec Endpoint Protection Configuration Changed PCI: vCenter Firewall Policy Change PCI: vCenter Orchestrator vSwitch Add, Modify or Delete PCI: vCenter vSwitch Add, Modify or Delete PCI: vShield Edge Configuration Change PCI: Juniper Firewall Policy Changes

Requirement	Description	Compliance Suite Reports and Alerts
1.1.9	Configuration standards for routers	**Compliance Suite Alerts** (Cont.) PCI: Juniper Firewall Policy Out of Sync PCI: LogLogic Universal Collector Configuration Changed PCI: Symantec Endpoint Protection Configuration Changed PCI: vCenter Firewall Policy Change PCI: vCenter vSwitch Add, Modify or Delete PCI: vCenter Orchestrator vSwitch Add, Modify or Delete
1.2	Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment	**Compliance Suite Reports** PCI: Applications Through Firewalls PCI: Firewall Connections Accepted - Cisco PIX PCI: Firewall Connections Accepted - Check Point PCI: Firewall Connections Accepted - Cisco IOS PCI: Firewall Connections Accepted - Cisco Netflow PCI: Firewall Connections Accepted - Cisco NXOS PCI: Firewall Connections Accepted - F5 BIG-IP TMOS PCI: Firewall Connections Accepted - Juniper JunOS PCI: Firewall Connections Accepted - PANOS PCI: Firewall Connections Accepted - Sidewinder PCI: Firewall Connections Accepted - VMware vShield PCI: Firewall Traffic Besides HTTP, SSL and SSH - Check Point PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco ASA PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco FWSM PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco IOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco Netflow PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco PIX PCI: Firewall Traffic Besides HTTP, SSL and SSH - F5 BIG-IP TMOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Fortinet PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper Firewall
1.3.2	Not allowing internal addresses to pass from the Internet into the DMZ	

Requirement	Description	Compliance Suite Reports and Alerts
1.3.5	Restricting inbound and outbound traffic to that which is necessary for the cardholder data	PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper JunOS
1.2	Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment	**Compliance Suite Reports** (Cont.) PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper RTFlow PCI: Firewall Traffic Besides HTTP, SSL and SSH - Nortel PCI: Firewall Traffic Besides HTTP, SSL and SSH - PANOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Sidewinder PCI: Firewall Traffic Besides HTTP, SSL and SSH - VMware vShield PCI: Web Access to Applications PCI: Web Access to Applications - Fortinet PCI: Web Access to Applications - F5 BIG-IP TMOS PCI: Web Access to Applications - Microsoft IIS PCI: Web Access to Applications - PANOS **Compliance Suite Alerts** PCI: Anomalous Firewall Traffic PCI: F5 BIG-IP TMOS Traffic Besides HTTP, SSH and SSL PCI: Firewall Traffic Besides HTTP, SSL and SSH PCI: vShield Firewall Traffic Besides HTTP, SSL and SSH
1.3.2	Not allowing internal addresses to pass from the Internet into the DMZ	
1.3.5	Restricting inbound and outbound traffic to that which is necessary for the cardholder data	

Requirement	Description	Compliance Suite Reports and Alerts
1.3.1		**Compliance Suite Reports**
		PCI: Firewall Connections Accepted - Check Point
		PCI: Firewall Connections Accepted - Cisco PIX
		PCI: Firewall Connections Accepted - Check Point
		PCI: Firewall Connections Accepted - Cisco IOS
		PCI: Firewall Connections Accepted - Cisco Netflow
		PCI: Firewall Connections Accepted - Cisco NXOS
		PCI: Firewall Connections Accepted - F5 BIG-IP TMOS
		PCI: Firewall Connections Accepted - Juniper JunOS
		PCI: Firewall Connections Accepted - PANOS
		PCI: Firewall Connections Accepted - Sidewinder
		PCI: Firewall Connections Accepted - VMware vShield
		PCI: Firewall Connections Denied - Check Point
		PCI: Firewall Connections Denied - Cisco ASA
		PCI: Firewall Connections Denied - Cisco FWSM
		PCI: Firewall Connections Denied - Cisco IOS
		PCI: Firewall Connections Denied - Cisco NXOS
		PCI: Firewall Connections Denied - Cisco PIX
		PCI: Firewall Connections Denied - Cisco Router
		PCI: Firewall Connections Denied - F5 BIG-IP TMOS
		PCI: Firewall Connections Denied - Fortinet
		PCI: Firewall Connections Denied - Juniper Firewall
		PCI: Firewall Connections Denied - Juniper JunOS
		PCI: Firewall Connections Denied - Juniper RT Flow
		PCI: Firewall Connections Denied - Nortel
		PCI: Firewall Connections Denied - PANOS
		PCI: Firewall Connections Denied - Sidewinder
		PCI: Firewall Connections Denied - VMware vShield
		Compliance Suite Alerts
		Not Applicable

Requirement	Description	Compliance Suite Reports and Alerts
1.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters		
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	**Compliance Suite Reports** PCI: DHCP Activities on Microsoft DHCP PCI: DHCP Activities on VMware vShield PCI: Firewall Connections Accepted - Cisco PIX PCI: Firewall Connections Accepted - Check Point PCI: Firewall Connections Accepted - Cisco IOS PCI: Firewall Connections Accepted - Cisco Netflow PCI: Firewall Connections Accepted - Cisco NXOS PCI: Firewall Connections Accepted - F5 BIG-IP TMOS PCI: Firewall Connections Accepted - Juniper JunOS PCI: Firewall Connections Accepted - PANOS PCI: Firewall Connections Accepted - Sidewinder PCI: Firewall Connections Accepted - VMware vShield PCI: Firewall Traffic Considered Risky - Check Point PCI: Firewall Traffic Considered Risky - Cisco ASA PCI: Firewall Traffic Considered Risky - Cisco FWSM PCI: Firewall Traffic Considered Risky - Cisco IOS PCI: Firewall Traffic Considered Risky - Cisco Netflow PCI: Firewall Traffic Considered Risky - Cisco PIX PCI: Firewall Traffic Considered Risky - F5 BIG-IP TMOS PCI: Firewall Traffic Considered Risky - Fortinet PCI: Firewall Traffic Considered Risky - Juniper Firewall PCI: Firewall Traffic Considered Risky - Juniper JunOS PCI: Firewall Traffic Considered Risky - Juniper RT Flow PCI: Firewall Traffic Considered Risky - Nortel PCI: Firewall Traffic Considered Risky - PANOS

Requirement	Description	Compliance Suite Reports and Alerts
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure-for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	PCI: Firewall Traffic Considered Risky - Sidewinder PCI: Firewall Traffic Considered Risky - VMware vShield PCI: Unencrypted Network Services - Check Point PCI: Unencrypted Network Services - Cisco ASA PCI: Unencrypted Network Services - Cisco FWSM PCI: Unencrypted Network Services - Cisco IOS PCI: Unencrypted Network Services - Cisco Netflow
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	**Compliance Suite Reports** (Cont.) PCI: Unencrypted Network Services - Cisco PIX PCI: Unencrypted Network Services - Fortinet PCI: Unencrypted Network Services - Juniper Firewall PCI: Unencrypted Network Services - Juniper JunOS PCI: Unencrypted Network Services - Juniper RT Flow PCI: Unencrypted Network Services - Nortel PCI: Unencrypted Network Services - PANOS PCI: Unencrypted Network Services - Sidewinder PCI: Unencrypted Network Services - VMware vShield **Compliance Suite Alerts** PCI: F5 BIG-IP TMOS Risky Traffic PCI: Firewall Traffic Considered Risky PCI: vShield Risky Traffic
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure-for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	

Requirement	Description	Compliance Suite Reports and Alerts
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**Compliance Suite Reports** PCI: Firewall Traffic Besides HTTP, SSL and SSH - Check Point PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco ASA PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco FWSM PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco IOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco Netflow PCI: Firewall Traffic Besides HTTP, SSL and SSH - Cisco PIX PCI: Firewall Traffic Besides HTTP, SSL and SSH - F5 BIG-IP TMOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Fortinet PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper Firewall PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper JunOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Juniper RTFlow PCI: Firewall Traffic Besides HTTP, SSL and SSH - Nortel PCI: Firewall Traffic Besides HTTP, SSL and SSH - PANOS PCI: Firewall Traffic Besides HTTP, SSL and SSH - Sidewinder PCI: Firewall Traffic Besides HTTP, SSL and SSH - VMware vShield PCI: Firewall Traffic Besides SSL and SSH - Check Point PCI: Firewall Traffic Besides SSL and SSH - Cisco ASA PCI: Firewall Traffic Besides SSL and SSH - Cisco FWSM PCI: Firewall Traffic Besides SSL and SSH - Cisco IOS PCI: Firewall Traffic Besides SSL and SSH - Cisco Netflow PCI: Firewall Traffic Besides SSL and SSH - Cisco PIX

Requirement	Description	Compliance Suite Reports and Alerts
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**Compliance Suite Reports** (Cont.) PCI: Firewall Traffic Besides SSL and SSH - F5 BIG-IP TMOS PCI: Firewall Traffic Besides SSL and SSH - Fortinet PCI: Firewall Traffic Besides SSL and SSH - Juniper Firewall PCI: Firewall Traffic Besides SSL and SSH - Juniper JunOS PCI: Firewall Traffic Besides SSL and SSH - Juniper RT Flow PCI: Firewall Traffic Besides SSL and SSH - Nortel PCI: Firewall Traffic Besides SSL and SSH - PANOS PCI: Firewall Traffic Besides SSL and SSH - Sidewinder PCI: Firewall Traffic Besides SSL and SSH - VMware vShield PCI: Unencrypted Network Services - Check Point PCI: Unencrypted Network Services - Cisco ASA PCI: Unencrypted Network Services - Cisco FWSM PCI: Unencrypted Network Services - Cisco IOS PCI: Unencrypted Network Services - Cisco Netflow PCI: Unencrypted Network Services - Cisco PIX PCI: Unencrypted Network Services - Fortinet PCI: Unencrypted Network Services - Juniper Firewall PCI: Unencrypted Network Services - Juniper JunOS PCI: Unencrypted Network Services - Juniper RT Flow PCI: Unencrypted Network Services - Nortel PCI: Unencrypted Network Services - PANOS PCI: Unencrypted Network Services - Sidewinder PCI: Unencrypted Network Services - VMware vShield **Compliance Suite Alerts** PCI: Anomalous Firewall Traffic PCI: F5 BIG-IP TMOS Traffic Besides HTTP, SSH and SSL PCI: F5 BIG-IP TMOS Traffic Besides SSH and SSL PCI: Firewall Traffic Besides HTTP, SSL and SSH PCI: vShield Firewall Traffic Besides HTTP, SSH and SSL PCI: vShield Firewall Traffic Besides SSH and SSL

Requirement	Description	Compliance Suite Reports and Alerts
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 3 Protect stored cardholder data		
3.7	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 4 Encrypt transmission of cardholder data across open, public networks		
4.3	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 5 Protect all systems against malware and regularly update anti-virus software or programs		
5.4	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 6 - Develop and maintain secure systems and applications		

Requirement	Description	Compliance Suite Reports and Alerts
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release	**Compliance Suite Reports** PCI: Cisco ESA: Updated PCI: LogLogic Management Center Upgrade Success PCI: Software Update Successes on i5/OS PCI: Symantec AntiVirus: Updated PCI: Symantec Endpoint Protection: Updated PCI: Windows Software Update Activities PCI: Windows Software Update Failures PCI: Windows Software Update Successes **Compliance Suite Alerts** PCI: i5/OS Software Updates PCI: LogLogic Management Center Upgrade Succeeded PCI: Windows Software Updates PCI: Windows Software Updates Failed PCI: Windows Software Updates Succeeded
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	**Compliance Suite Reports** PCI: Cisco ESA: Updated PCI: LogLogic Management Center Upgrade Success PCI: Software Update Successes on i5/OS PCI: Symantec AntiVirus: Updated PCI: Symantec Endpoint Protection: Updated PCI: Windows Software Update Activities PCI: Windows Software Update Failures PCI: Windows Software Update Successes **Compliance Suite Alerts** PCI: i5/OS Software Updates PCI: LogLogic Management Center Upgrade Succeeded PCI: Windows Software Updates PCI: Windows Software Updates Failed PCI: Windows Software Updates Succeeded

Requirement	Description	Compliance Suite Reports and Alerts
6.3.3	Separation of duties between development/ test and production environments	**Compliance Suite Reports** PCI: Account Activities on UNIX Servers PCI: Account Activities on Windows Servers PCI: Check Point Management Station Login PCI: Check Point Objects Created PCI: Check Point Objects Deleted PCI: Check Point Objects Modified PCI: DB2 Database Successful Logins PCI: ESX Accounts Activities PCI: ESX Group Activities PCI: ESX Logins Succeeded PCI: F5 BIG-IP TMOS Login Successful PCI: Group Activities on NetApp Filer Audit PCI: Group Activities on Symantec Endpoint Protection PCI: Group Activities on TIBCO ActiveMatrix Administrator PCI: Group Activities on UNIX Servers PCI: Group Activities on Windows Servers PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Successful PCI: HP NonStop Audit Object Changes PCI: i5/OS Network User Login Successful PCI: i5/OS Network User Profile Modified PCI: i5/OS Object Permissions Modified PCI: i5/OS User Login Successful PCI: i5/OS User Profile Modifications PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication Type PCI: LogLogic DSM Logins PCI: LogLogic Management Center Account Activities PCI: LogLogic Management Center Login PCI: Microsoft Operations Manager - Windows Accounts Activities

Requirement	Description	Compliance Suite Reports and Alerts
6.3.3	Separation of duties between development/ test and production environments	**Compliance Suite Reports** (Cont.) PCI: Microsoft SQL Server Database Successful Logins PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Oracle Database Successful Logins PCI: RACF Accounts Modified PCI: RACF Successful Logins PCI: Successful Logins PCI: Sybase ASE Successful Logins PCI: TIBCO ActiveMatrix Administrator Successful Logins PCI: Unauthorized Logins PCI: vCenter Change Attributes PCI: vCenter Resource Usage Change PCI: vCenter Successful Logins PCI: vCenter Virtual Machine Created PCI: vCenter Virtual Machine Deleted PCI: vCenter Orchestrator Change Attributes PCI: vCenter Orchestrator Virtual Machine Created PCI: vCenter Orchestrator Virtual Machine Deleted PCI: vCloud Organization Created PCI: vCloud Organization Deleted PCI: vCloud Organization Modified PCI: vCloud Successful Logins PCI: vCloud vApp Created, Modified, or Deleted PCI: vCloud vDC Created, Modified, or Deleted

Requirement	Description	Compliance Suite Reports and Alerts
6.3.3	Separation of duties between development/ test and production environments	**Compliance Suite Alerts** PCI: Group Members Added PCI: Groups Created PCI: Groups Deleted PCI: Groups Modified PCI: Guardium SQL Guard Logins PCI: i5/OS Network Profile Changes PCI: i5/OS User Profile Changes PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: vCenter Create Virtual Machine PCI: vCenter Delete Virtual Machine PCI: vCenter User Login Successful PCI: vCenter Orchestrator Create Virtual Machine PCI: vCenter Orchestrator Delete Virtual Machine PCI: vCloud Director Login Success PCI: vCloud Organization Created PCI: vCloud Organization Deleted PCI: vCloud Organization Modified PCI: vCloud vApp Created, Deleted, or Modified PCI: vCloud vDC Created, Modified, or Deleted
6.4.1	Follow change control procedures for all system and software configuration changes. The procedures should include: Documentation of impact	**Compliance Suite Reports** PCI: Active Directory System Changes PCI: Check Point Configuration Changes PCI: Cisco FWSM HA State Changed PCI: Cisco ESA: Updated PCI: Cisco ISE, ACS Configuration Changes PCI: Cisco Peer Reset/Reload PCI: Cisco Peer Supervisor Status Changes PCI: Cisco PIX, ASA, FWSM Failover Disabled PCI: Cisco PIX, ASA, FWSM Failover Performed PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco PIX, ASA, FWSM Restarted PCI: Cisco Redundancy Version Check Failed PCI: Cisco Routers and Switches Restart PCI: Cisco Switch Policy Changes
6.4.2	Follow change control procedures for all system and software configuration changes. The procedures should include: Management sign-off by appropriate parties	

Requirement	Description	Compliance Suite Reports and Alerts
6.4.3	Follow change control procedures for all system and software configuration changes. The procedures should include: Testing that verifies operational functionality	PCI: DB2 Database Configuration Changes PCI: F5 BIG-IP TMOS Restarted PCI: Guardium SQL Guard Audit Configuration Changes PCI: Guardium SQL Guard Audit Data Access PCI: Guardium SQL Guard Configuration Changes PCI: Guardium SQL Guard Data Access PCI: HP NonStop Audit Configuration Changes PCI: i5/OS Restarted PCI: Juniper Firewall HA State Changed PCI: Juniper Firewall Policy Changed PCI: Juniper Firewall Policy Out of Sync PCI: Juniper Firewall Reset Accepted PCI: Juniper Firewall Reset Imminent PCI: Juniper Firewall Restarted PCI: LogLogic DSM Configuration Changes PCI: LogLogic DSM Data Access PCI: LogLogic HA State Changed PCI: LogLogic Universal Collector Configuration Changes PCI: Microsoft Operations Manager - Windows Policies Modified
6.4.4	Follow change control procedures for all system and software configuration changes. The procedures should include: Back-out procedures	
6.4.1	Follow change control procedures for all system and software configuration changes. The procedures should include: Documentation of impact	**Compliance Suite Reports** (Cont.) PCI: Microsoft Operations Manager - Windows Servers Restarted PCI: Microsoft Sharepoint Policy Add, Remove, or Modify PCI: Microsoft SQL Server Configuration Changes PCI: Microsoft SQL Server Data Access PCI: Microsoft Operations Manager - Server Restarted PCI: NetApp Filer Audit Policies Modified PCI: NetApp Filer Disk Failure PCI: NetApp Filer Disk Missing PCI: Oracle Database Configuration Changes PCI: Oracle Database Data Access PCI: Policies Modified on Windows Servers PCI: Sidewinder Configuration Changes
6.4.2	Follow change control procedures for all system and software configuration changes. The procedures should include: Management sign-off by appropriate parties	

Requirement	Description	Compliance Suite Reports and Alerts
6.4.3	Follow change control procedures for all system and software configuration changes. The procedures should include: Testing that verifies operational functionality	PCI: Sybase ASE Database Configuration Changes PCI: Sybase ASE Database Data Access PCI: Symantec AntiVirus: Updated PCI: Symantec Endpoint Protection: Updated PCI: Symantec Endpoint Protection Configuration Changes PCI: Symantec Endpoint Protection Policy Add, Remove, or Modify PCI: System Restarted PCI: vCenter Change Attributes PCI: vCenter Modify Firewall Policy PCI: vCenter Resource Usage Change PCI: vCenter Shutdown or Restart of ESX Server PCI: vCenter Virtual Machine Created PCI: vCenter Virtual Machine Deleted PCI: vCenter Virtual Machine Shutdown PCI: vCenter Virtual Machine Started PCI: vCenter vSwitch Added, Changed or Removed PCI: vCenter Orchestrator Change Attributes PCI: vCenter Orchestrator Virtual Machine Created PCI: vCenter Orchestrator Virtual Machine Deleted PCI: vCenter Orchestrator Virtual Machine Shutdown PCI: vCenter Orchestrator Virtual Machine Started PCI: vCenter Orchestrator vSwitch Added, Changed or Removed
6.4.4	Follow change control procedures for all system and software configuration changes. The procedures should include: Back-out procedures	
6.4.1	Follow change control procedures for all system and software configuration changes. The procedures should include: Documentation of impact	**Compliance Suite Reports** (Cont.) PCI: vCenter Orchestrator vSwitch Added, Changed or Removed PCI: vCloud Organization Created PCI: vCloud Organization Deleted PCI: vCloud Organization Modified PCI: vCloud vApp Created, Modified, or Deleted PCI: vCloud vDC Created, Modified, or Deleted PCI: vShield Edge Configuration Changes PCI: Windows Servers Restarted **Compliance Suite Alerts** PCI: Active Directory Changes

Requirement	Description	Compliance Suite Reports and Alerts
6.4.2	Follow change control procedures for all system and software configuration changes. The procedures should include: Management sign-off by appropriate parties	PCI: Check Point Policy Changed PCI: Cisco ISE, ACS Configuration Changed PCI: Cisco PIX, ASA, FWSM HA State Change PCI: Cisco PIX, ASA, FWSM Failover Disabled PCI: Cisco PIX, ASA, FWSM Failover Performed PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco Switch Policy Changed PCI: DB2 Database Configuration Change PCI: DNS Server Shutdown PCI: DNS Server Started PCI: Guardium SQL Guard Config Changes PCI: Guardium SQL Guard Data Access PCI: HP NonStop Audit Configuration Changed PCI: i5/OS Server or Service Status Change PCI: Juniper Firewall HA State Change PCI: Juniper Firewall Peer Missing PCI: Juniper Firewall Policy Changes PCI: Juniper Firewall Policy Out of Sync PCI: LogLogic DSM Configuration Changes PCI: LogLogic DSM Data Access PCI: LogLogic Universal Collector Configuration Changed PCI: Microsoft Operations Manager - Windows Policies Changed
6.4.3	Follow change control procedures for all system and software configuration changes. The procedures should include: Testing that verifies operational functionality	
6.4.4	Follow change control procedures for all system and software configuration changes. The procedures should include: Back-out procedures	
6.4.1	Follow change control procedures for all system and software configuration changes. The procedures should include: Documentation of impact	**Compliance Suite Alerts** (Cont.) PCI: Microsoft Operations Manager - Windows Server Restarted PCI: Microsoft Sharepoint Policies Added, Removed, Modified PCI: NetApp Filer Audit Policies Changed PCI: NetApp Filer Disk Failure PCI: NetApp Filer Disk Inserted PCI: NetApp Filer Disk Missing PCI: NetApp Filer Disk Pulled PCI: Oracle Database Configuration Change PCI: Oracle Database Data Access PCI: Sybase ASE Database Config Changes
6.4.2	Follow change control procedures for all system and software configuration changes. The procedures should include: Management sign-off by appropriate parties	

Requirement	Description	Compliance Suite Reports and Alerts
6.4.3	Follow change control procedures for all system and software configuration changes. The procedures should include: Testing that verifies operational functionality	PCI: Sybase ASE Database Data Access PCI: Symantec Endpoint Protection Configuration Changed PCI: Symantec Endpoint Protection Policy Add, Delete, Modify PCI: System Restarted PCI: vCenter Create Virtual Machine PCI: vCenter Delete Virtual Machine PCI: vCenter Firewall Policy Change PCI: vCenter Shutdown or Restart ESX PCI: vCenter Virtual Machine Shutdown PCI: vCenter Virtual Machine Started PCI: vCenter vSwitch Add, Modify or Delete PCI: vCenter Orchestrator Create Virtual Machine PCI: vCenter Orchestrator Delete Virtual Machine PCI: vCenter Orchestrator Virtual Machine Shutdown PCI: vCenter Orchestrator Virtual Machine Started PCI: vCenter Orchestrator vSwitch Add, Modify or Delete PCI: vCloud Organization Created PCI: vCloud Organization Deleted PCI: vCloud Organization Modified PCI: vCloud vApp Created, Deleted, or Modified PCI: vCloud vDC Created, Modified, or Deleted PCI: vShield Edge Configuration Change PCI: Windows Policies Changed
6.4.4	Follow change control procedures for all system and software configuration changes. The procedures should include: Back-out procedures	
6.7	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 7 - Restrict access to data by business need-to-know		

Requirement	Description	Compliance Suite Reports and Alerts
7.1	Limit access to computing resources and cardholder information to only those individuals whose job requires such access.	**Compliance Suite Reports** PCI: Accepted VPN Connections - RADIUS PCI: Account Activities on UNIX Servers PCI: Account Activities on Windows Servers PCI: Accounts Changed on NetApp Filer PCI: Accounts Changed on TIBCO ActiveMatrix Administrator PCI: Accounts Changed on TIBCO Administrator PCI: Accounts Changed on UNIX Servers PCI: Accounts Changed on Windows Servers PCI: Active Directory System Changes PCI: Check Point Management Station Login PCI: Cisco FWSM HA State Changed PCI: Cisco Peer Supervisor Status Changes PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco Switch Policy Changes PCI: DB2 Database Successful Logins PCI: ESX Accounts Activities PCI: ESX Group Activities PCI: ESX Kernel log daemon terminating PCI: ESX Kernel logging Stop PCI: ESX Logins Succeeded PCI: ESX Syslogd Restart PCI: F5 BIG-IP TMOS Login Successful PCI: Files Accessed on NetApp Filer Audit PCI: Files Accessed on Servers PCI: Files Accessed through Juniper SSL VPN (Secure Access) PCI: Files Accessed through PANOS

Requirement	Description	Compliance Suite Reports and Alerts
7.1	Limit access to computing resources and cardholder information to only those individuals whose job requires such access.	**Compliance Suite Reports** (Cont.) PCI: Group Activities on NetApp Filer Audit PCI: Group Activities on Symantec Endpoint Protection PCI: Group Activities on TIBCO ActiveMatrix Administrator PCI: Group Activities on UNIX Servers PCI: Group Activities on Windows Servers PCI: Guardium SQL Guard Audit Data Access PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Data Access PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Successful PCI: HP NonStop Audit Permissions Changed PCI: i5/OS Files Accessed PCI: i5/OS Network User Login Successful PCI: i5/OS Object Permissions Modified PCI: i5/OS Service Started PCI: i5/OS User Login Successful PCI: Juniper Firewall HA State Changed PCI: Juniper Firewall Policy Changed PCI: Juniper Firewall Policy Out of Sync PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication Type PCI: LogLogic DSM Data Access PCI: LogLogic HA State Changed PCI: LogLogic DSM Logins PCI: LogLogic Management Center Account Activities PCI: LogLogic Management Center Login PCI: Microsoft Operations Manager - Windows Accounts Activities PCI: Microsoft Operations Manager - Windows Permissions Modified PCI: Microsoft Operations Manager - Windows Policies Modified

Requirement	Description	Compliance Suite Reports and Alerts
7.1	Limit access to computing resources and cardholder information to only those individuals whose job requires such access.	**Compliance Suite Reports** (Cont.) PCI: Microsoft Sharepoint Permissions Changed PCI: Microsoft Sharepoint Policy Add, Remove, or Modify PCI: Microsoft SQL Server Data Access PCI: Microsoft SQL Server Database Successful Logins PCI: Microsoft SQL Server Database Permission Events PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer Audit Policies Modified PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Oracle Database Data Access PCI: Oracle Database Permission Events PCI: Oracle Database Successful Logins PCI: Permissions Modified on Windows Servers PCI: Policies Modified on Windows Servers PCI: Pulse Connect Secure Successful Logins by User PCI: RACF Files Accessed PCI: RACF Permissions Changed PCI: RACF Process Started PCI: RACF Successful Logins PCI: Successful Logins PCI: Sybase ASE Database Data Access PCI: Sybase ASE Successful Logins PCI: Symantec Endpoint Protection Policy Add, Remove, or Modify PCI: TIBCO ActiveMatrix Administrator Permission Changes PCI: TIBCO ActiveMatrix Administrator Successful Logins PCI: TIBCO Administrator Permission Changes

Requirement	Description	Compliance Suite Reports and Alerts
7.1	Limit access to computing resources and cardholder information to only those individuals whose job requires such access.	**Compliance Suite Reports** (Cont.) PCI: vCenter Change Attributes PCI: vCenter Datastore Events PCI: vCenter Data Move PCI: vCenter Modify Firewall Policy PCI: vCenter Restart ESX Services PCI: vCenter Resource Usage Change PCI: vCenter Successful Logins PCI: vCenter Orchestrator Change Attributes PCI: vCenter Orchestrator Datastore Events PCI: vCenter Orchestrator Data Move PCI: vCenter User Permission Change PCI: vCloud Successful Logins PCI: VPN Users Accessing Corporate Network PCI: Web Access to Applications PCI: Web Access to Applications - Fortinet PCI: Web Access to Applications - F5 BIG-IP TMOS PCI: Web Access to Applications - Microsoft IIS PCI: Web Access to Applications - PANOS PCI: Windows New Services Installed

Requirement	Description	Compliance Suite Reports and Alerts
7.1	Limit access to computing resources and cardholder information to only those individuals whose job requires such access.	**Compliance Suite Alerts** PCI: Accounts Modified PCI: Active Directory Changes PCI: Check Point Policy Changed PCI: Cisco PIX, ASA, FWSM Commands Executed PCI: Cisco PIX, ASA, FWSM HA State Change PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco Switch Policy Changed PCI: Groups Modified PCI: Guardium SQL Guard Data Access PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Permission Changed PCI: i5/OS Permission or Policy Change PCI: i5/OS Server or Service Status Change PCI: Juniper Firewall HA State Change PCI: Juniper Firewall Peer Missing PCI: Juniper Firewall Policy Changes PCI: Juniper Firewall Policy Out of Sync PCI: Logins Succeeded PCI: LogLogic DSM Data Access PCI: LogLogic DSM Logins PCI: Microsoft Operations Manager - Permissions Changed PCI: Microsoft Operations Manager - Windows Policies Changed PCI: Microsoft Sharepoint Permission Changed PCI: Microsoft Sharepoint Policies Added, Removed, Modified PCI: NetApp Filer Audit Policies Changed PCI: NetApp Filer NIS Group Update PCI: NetApp Filer Unauthorized Mounting PCI: Oracle Database Data Access PCI: Oracle Database Permissions Changed

Requirement	Description	Compliance Suite Reports and Alerts
7.1	Limit access to computing resources and cardholder information to only those individuals whose job requires such access.	**Compliance Suite Alerts** (Cont.) PCI: RACF Files Accessed PCI: RACF Permissions Changed PCI: RACF Process Started PCI: Sybase ASE Database Data Access PCI: Symantec Endpoint Protection Policy Add, Delete, Modify PCI: TIBCO ActiveMatrix Administrator Permission Changed PCI: vCenter Datastore Event PCI: vCenter Data Move PCI: vCenter Firewall Policy Change PCI: vCenter Permission Change PCI: vCenter Restart ESX Services PCI: vCenter User Login Successful PCI: vCenter Orchestrator Data Move PCI: vCenter Orchestrator Datastore Events PCI: vCloud Director Login Success PCI: vCloud User, Group, or Role Modified PCI: Windows Files Accessed PCI: Windows Permissions Changed PCI: Windows Policies Changed PCI: Windows Process Started PCI: Windows Programs Accessed

Requirement	Description	Compliance Suite Reports and Alerts
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	**Compliance Suite Reports** PCI: Accepted VPN Connections - RADIUS PCI: Account Activities on UNIX Servers PCI: Account Activities on Windows Servers PCI: Active Directory System Changes PCI: Check Point Management Station Login PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco Switch Policy Changes PCI: DB2 Database Successful Logins PCI: ESX Accounts Activities PCI: ESX Group Activities PCI: ESX Kernel log daemon terminating PCI: ESX Kernel logging Stop PCI: ESX Logins Succeeded PCI: ESX Syslogd Restart PCI: F5 BIG-IP TMOS Login Successful PCI: Files Accessed on NetApp Filer Audit PCI: Files Accessed on Servers PCI: Files Accessed through Juniper SSL VPN (Secure Access) PCI: Files Accessed through PANOS PCI: Group Activities on NetApp Filer Audit PCI: Group Activities on Symantec Endpoint Protection PCI: Group Activities on TIBCO ActiveMatrix Administrator PCI: Group Activities on UNIX Servers PCI: Group Activities on Windows Servers PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Successful PCI: HP NonStop Audit Permissions Changed PCI: i5/OS Files Accessed PCI: i5/OS Network User Login Successful PCI: i5/OS Object Permissions Modified PCI: i5/OS Service Started PCI: i5/OS User Login Successful

Requirement	Description	Compliance Suite Reports and Alerts
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	**Compliance Suite Reports** (Cont.) PCI: Juniper Firewall Policy Changed PCI: Juniper Firewall Policy Out of Sync PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication Type PCI: LogLogic DSM Logins PCI: LogLogic Management Center Account Activities PCI: LogLogic Management Center Login PCI: Microsoft Operations Manager - Windows Accounts Activities PCI: Microsoft Operations Manager - Windows Permissions Modified PCI: Microsoft Operations Manager - Windows Policies Modified PCI: Microsoft Sharepoint Permissions Changed PCI: Microsoft Sharepoint Policy Add, Remove, or Modify PCI: Microsoft SQL Server Database Successful Logins PCI: Microsoft SQL Server Database Permission Events PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer Audit Policies Modified PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Oracle Database Successful Logins PCI: Oracle Database Permission Events PCI: Permissions Modified on Windows Servers PCI: Policies Modified on Windows Servers

Requirement	Description	Compliance Suite Reports and Alerts
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	**Compliance Suite Reports** (Cont.) PCI: RACF Files Accessed PCI: RACF Permissions Changed PCI: RACF Process Started PCI: RACF Successful Logins PCI: Successful Logins PCI: Sybase ASE Successful Logins PCI: Symantec Endpoint Protection Policy Add, Remove, or Modify PCI: TIBCO ActiveMatrix Administrator Permission Changes PCI: TIBCO ActiveMatrix Administrator Successful Logins PCI: TIBCO Administrator Permission Changes PCI: vCenter Datastore Events PCI: vCenter Data Move PCI: vCenter Modify Firewall Policy PCI: vCenter Restart ESX Services PCI: vCenter Successful Logins PCI: vCenter Orchestrator Datastore Events PCI: vCenter Orchestrator Data Move PCI: vCenter User Permission Change PCI: vCloud Successful Logins PCI: VPN Users Accessing Corporate Network PCI: Windows New Services Installed

Requirement	Description	Compliance Suite Reports and Alerts
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	**Compliance Suite Alerts** PCI: Active Directory Changes PCI: Check Point Policy Changed PCI: Cisco PIX, ASA, FWSM Policy Changed PCI: Cisco Switch Policy Changed PCI: Groups Modified PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Permission Changed PCI: i5/OS Permission or Policy Change PCI: i5/OS Server or Service Status Change PCI: Juniper Firewall Policy Changes PCI: Juniper Firewall Policy Out of Sync PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: Microsoft Operations Manager - Permissions Changed PCI: Microsoft Operations Manager - Windows Policies Changed PCI: Microsoft Sharepoint Permission Changed PCI: Microsoft Sharepoint Policies Added, Removed, Modified PCI: NetApp Filer Audit Policies Changed PCI: NetApp Filer NIS Group Update PCI: NetApp Filer Unauthorized Mounting PCI: Oracle Database Permissions Changed PCI: RACF Files Accessed PCI: RACF Permissions Changed PCI: RACF Process Started

Requirement	Description	Compliance Suite Reports and Alerts
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	**Compliance Suite Alerts** (Cont.) PCI: Symantec Endpoint Protection Policy Add, Delete, Modify PC: TIBCO ActiveMatrix Administrator Permission Changed PCI: vCenter Datastore Event PCI: vCenter Data Move PCI: vCenter Firewall Policy Change PCI: vCenter Permission Change PCI: vCenter Restart ESX Services PCI: vCenter User Login Successful PCI: vCenter Orchestrator Data Move PCI: vCenter Orchestrator Datastore Events PCI: vCloud Director Login Success PCI: vCloud User, Group, or Role Modified PCI: Windows Files Accessed PCI: Windows Permissions Changed PCI: Windows Policies Changed PCI: Windows Process Started PCI: Windows Programs Accessed
7.3	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 8 - Assign a unique ID to each person with computer access		
8.1.5	Mangage IDs used by vendors to access, support or maintain system components via remote access as follows: Enabled only during the time period needed and disabled when not in use. Monitored when in use.	**Compliance Suite Reports** PCI: Accepted VPN Connections - RADIUS PCI: Check Point Management Station Login PCI: ESX Logins Succeeded PCI: F5 BIG-IP TMOS Login Successful PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Successful

Requirement	Description	Compliance Suite Reports and Alerts
		PCI: i5/OS Network User Login Successful PCI: i5/OS User Login Successful PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication TypePCI: LogLogic DSM Logins PCI: LogLogic Management Center Login PCI: Microsoft SQL Server Database Successful Logins PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Oracle Database Successful Logins PCI: RACF Successful Logins PCI: Successful LoginsPCI: Sybase ASE Successful Logins PCI: TIBCO ActiveMatrix Administrator Successful Logins PCI: vCenter Successful Logins PCI: vCloud Successful Logins PCI: VPN Users Accessing Corporate Network **Compliance Suite Alerts** PCI: Guardium SQL Guard Logins PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: vCenter User Login Successful PCI: vCloud Director Login Success
8.1	Identify all users with a unique username before allowing them to access system components or cardholder data	**Compliance Suite Reports** PCI: Accepted VPN Connections - RADIUS PCI: Account Activities on UNIX Servers PCI: Account Activities on Windows Servers PCI: Accounts Changed on NetApp Filer PCI: Accounts Changed on TIBCO ActiveMatrix Administrator PCI: Accounts Changed on TIBCO Administrator PCI: Accounts Changed on UNIX Servers PCI: Accounts Changed on Windows Servers

Requirement	Description	Compliance Suite Reports and Alerts
8.5.8	Do not use group, shared, or generic accounts/passwords.	PCI: Accounts Created on NetApp Filer PCI: Accounts Created on NetApp Filer Audit PCI: Accounts Created on Sidewinder PCI: Accounts Created on Symantec Endpoint Protection PCI: Accounts Created on TIBCO ActiveMatrix Administrator PCI: Accounts Created on TIBCO Administrator PCI: Accounts Created on Windows Servers PCI: Accounts Created on UNIX Servers PCI: Active Directory System Changes PCI: Administrator Logins on Windows Servers PCI: Check Point Management Station Login PCI: Cisco ISE, ACS Accounts Created PCI: DB2 Database Failed Logins PCI: DB2 Database Successful Logins PCI: DB2 Database User Additions and Deletions PCI: Denied VPN Connections - RADIUS PCI: ESX Accounts Activities PCI: ESX Accounts Created PCI: ESX Failed Logins PCI: ESX Logins Succeeded PCI: ESX Logins Failed Unknown User PCI: F5 BIG-IP TMOS Login Failed PCI: F5 BIG-IP TMOS Login Successful PCI: Failed Logins PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: Pulse Connect Secure Successful Logins by User
8.1	Identify all users with a unique username before allowing them to access system components or cardholder data	**Compliance Suite Reports** (Cont.) PCI: HP NonStop Audit Login Failed PCI: HP NonStop Audit Login Successful PCI: i5/OS Network User Login Failed PCI: i5/OS Network User Login Successful PCI: i5/OS Network User Profile Creation PCI: i5/OS User Login Failed

Requirement	Description	Compliance Suite Reports and Alerts
8.5.8	Do not use group, shared, or generic accounts/passwords.	PCI: i5/OS User Login Successful PCI: i5/OS User Profile Creation PCI: Juniper SSL VPN (Secure Access) Failed Logins by User PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Failed Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication Type PCI: LogLogic DSM Logins PCI: LogLogic Management Center Account Activities PCI: LogLogic Management Center Login PCI: Microsoft Operations Manager - Windows Accounts Activities PCI: Microsoft Operations Manager - Windows Accounts Created PCI: Microsoft Operations Manager - Windows Accounts Enabled PCI: Microsoft SQL Server Database Successful Logins PCI: Microsoft SQL Server Database Failed Logins PCI: Microsoft SQL Server Database User Additions and Deletions PCI: NetApp Filer Audit Accounts Enabled PCI: NetApp Filer Audit Login Failed PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer File Activity PCI: NetApp Filer Login Failed PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Oracle Database Failed Logins PCI: Oracle Database Successful Logins PCI: Oracle Database User Additions and Deletions
8.1	Identify all users with a unique username before allowing them to access system components or cardholder data	**Compliance Suite Reports** (Cont.) PCI: RACF Accounts Created PCI: RACF Failed Logins PCI: RACF Successful Logins PCI: Root Logins PCI: Successful Logins

Requirement	Description	Compliance Suite Reports and Alerts
8.5.8	Do not use group, shared, or generic accounts/passwords.	PCI: Sybase ASE Database User Additions and Deletions PCI: Sybase ASE Failed Logins PCI: Sybase ASE Successful Logins PCI: TIBCO ActiveMatrix Administrator Failed Logins PCI: TIBCO ActiveMatrix Administrator Successful Logins PCI: UNIX Failed Logins PCI: vCenter Failed Logins PCI: vCenter Successful Logins PCI: vCenter Orchestrator Failed Logins PCI: vCloud Failed Logins PCI: vCloud Successful Logins PCI: vCloud User Created PCI: VPN Users Accessing Corporate Network PCI: Windows Accounts Enabled **Compliance Suite Alerts** PCI: Accounts Created PCI: Accounts Enabled PCI: Accounts Modified PCI: Active Directory Changes PCI: DB2 Database User Added or Dropped PCI: Guardium SQL Guard Logins PCI: Logins Failed PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: NetApp Authentication Failure PCI: Oracle Database User Added or Deleted PCI: vCenter User Login Failed PCI: vCenter User Login Successful PCI: vCenter Orchestrator Login Failed PCI: vCloud Director Login Failed PCI: vCloud Director Login Success PCI: vCloud User Created

Requirement	Description	Compliance Suite Reports and Alerts
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**Compliance Suite Reports** PCI: Accepted VPN Connections - RADIUS PCI: Account Activities on UNIX Servers PCI: Account Activities on Windows Servers PCI: Active Directory System Changes PCI: Administrator Logins on Windows Servers PCI: Check Point Management Station Login PCI: DB2 Database Successful Logins PCI: DB2 Database User Additions and Deletions PCI: ESX Accounts Activities PCI: ESX Group Activities PCI: ESX Logins Succeeded PCI: F5 BIG-IP TMOS Login Successful PCI: Group Activities on NetApp Filer Audit PCI: Group Activities on Symantec Endpoint Protection PCI: Group Activities on UNIX Servers PCI: Group Activities on Windows Servers PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Successful PCI: HP NonStop Audit Object Changes PCI: HP NonStop Audit Permissions Changed PCI: i5/OS Network User Login Successful PCI: i5/OS Network User Profile Modified PCI: i5/OS Object Permissions Modified PCI: i5/OS User Login Successful PCI: i5/OS User Profile Modifications PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication Type PCI: LogLogic DSM Logins PCI: LogLogic Management Center Account Activities PCI: LogLogic Management Center Login PCI: Microsoft Operations Manager - Windows Accounts Activities

Requirement	Description	Compliance Suite Reports and Alerts
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**Compliance Suite Reports** (Cont.) PCI: Microsoft Operations Manager - Windows Permissions Modified PCI: Microsoft Sharepoint Permissions Changed PCI: Microsoft SQL Server Database Successful Logins PCI: Microsoft SQL Server Database Permission Events PCI: Microsoft SQL Server Database User Additions and Deletions PCI: NetApp Filer Accounts Locked PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Oracle Database Successful Logins PCI: Oracle Database Permission Events PCI: Oracle Database User Additions and Deletions PCI: Permissions Modified on Windows Servers PCI: RACF Accounts Modified PCI: RACF Permissions Changed PCI: RACF Successful Logins PCI: Root Logins PCI: Successful Logins PCI: Sybase ASE Database User Additions and Deletions PCI: Sybase ASE Successful Logins PCI: TIBCO ActiveMatrix Administrator Permission Changes PCI: TIBCO ActiveMatrix Administrator Successful Logins PCI: TIBCO Administrator Permission Changes PCI: vCenter Successful Logins PCI: vCenter User Permission Change PCI: vCloud Successful Logins PCI: Windows Accounts Locked

Requirement	Description	Compliance Suite Reports and Alerts
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**Compliance Suite Alerts** PCI: Accounts Locked PCI: Active Directory Changes PCI: DB2 Database User Added or Dropped PCI: Group Members Added PCI: Groups Created PCI: Groups Deleted PCI: Groups Modified PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Permission Changed PCI: i5/OS Permission or Policy Change PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: Microsoft Operations Manager - Permissions Changed PCI: Microsoft Sharepoint Permission Changed PCI: NetApp Filer NIS Group Update PCI: Oracle Database Permissions Changed PCI: Oracle Database User Added or Deleted PCI: RACF Permissions Changed PCI: TIBCO ActiveMatrix Administrator Permission Changed PCI: vCenter Permission Change PCI: vCenter User Login Successful PCI: vCenter Orchestrator Login Failed PCI: vCloud Director Login Success PCI: vCloud User, Group, or Role Modified PCI: Windows Permissions Changed

Requirement	Description	Compliance Suite Reports and Alerts
8.5.4	Immediately revoke accesses of terminated users.	**Compliance Suite Reports** PCI: Accepted VPN Connections - RADIUS PCI: Account Activities on UNIX Servers PCI: Account Activities on Windows Servers PCI: Accounts Deleted on NetApp Filer PCI: Accounts Deleted on NetApp Filer Audit PCI: Accounts Deleted on Sidewinder PCI: Accounts Deleted on Symantec Endpoint Protection PCI: Accounts Deleted on TIBCO Administrator PCI: Accounts Deleted on UNIX Servers PCI: Accounts Deleted on Windows Servers PCI: Active Directory System Changes PCI: Check Point Management Station Login PCI: Cisco ISE, ACS Accounts Removed PCI: DB2 Database Successful Logins PCI: DB2 Database User Additions and Deletions PCI: ESX Accounts Activities PCI: ESX Accounts Deleted PCI: ESX Group Activities PCI: ESX Logins Succeeded PCI: F5 BIG-IP TMOS Login Successful PCI: Group Activities on NetApp Filer Audit PCI: Group Activities on Symantec Endpoint Protection PCI: Group Activities on TIBCO ActiveMatrix Administrator PCI: Group Activities on UNIX Servers PCI: Group Activities on Windows Servers PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Successful PCI: HP NonStop Audit Object Changes PCI: HP NonStop Audit Permissions Changed PCI: i5/OS Network User Login Successful PCI: i5/OS Network User Profile Deletion PCI: i5/OS Network User Profile Modified

Requirement	Description	Compliance Suite Reports and Alerts
		PCI: i5/OS Object Permissions Modified

Requirement	Description	Compliance Suite Reports and Alerts
8.5.4	Immediately revoke accesses of terminated users.	**Compliance Suite Reports** (Cont.) PCI: i5/OS User Login Successful PCI: i5/OS User Profile Modifications PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication Type PCI: LogLogic DSM Logins PCI: LogLogic Management Center Account Activities PCI: LogLogic Management Center Login PCI: Microsoft Operations Manager - Windows Accounts Activities PCI: Microsoft Operations Manager - Windows Permissions Modified PCI: Microsoft Sharepoint Permissions Changed PCI: Microsoft SQL Server Database Successful Logins PCI: Microsoft SQL Server Database Permission Events PCI: Microsoft SQL Server Database User Additions and Deletions PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Oracle Database Successful Logins PCI: Oracle Database Permission Events PCI: Oracle Database User Additions and Deletions PCI: Permissions Modified on Windows Servers PCI: RACF Accounts Deleted PCI: RACF Accounts Modified PCI: RACF Permissions Changed PCI: RACF Successful Logins PCI: Successful Logins PCI: Sybase ASE Database User Additions and Deletions PCI: Sybase ASE Successful Logins PCI: TIBCO ActiveMatrix Administrator Permission Changes PCI: TIBCO ActiveMatrix Administrator Successful Logins

Requirement	Description	Compliance Suite Reports and Alerts
		PCI: TIBCO Administrator Permission Changes
8.5.4	Immediately revoke accesses of terminated users.	**Compliance Suite Reports** (Cont.) PCI: vCenter Successful Logins PCI: vCenter User Permission Change PCI: vCloud Successful Logins PCI: vCloud User Deleted or Removed PCI: VPN Users Accessing Corporate Network
8.5.4	Immediately revoke accesses of terminated users.	**Compliance Suite Alerts** PCI: Accounts Deleted PCI: Active Directory Changes PCI: DB2 Database User Added or Dropped PCI: Group Members Added PCI: Group Members Deleted PCI: Groups Created PCI: Groups Deleted PCI: Groups Modified PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Permission Changed PCI: i5/OS Permission or Policy Change PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: Microsoft Operations Manager - Permissions Changed PCI: Microsoft Sharepoint Permission Changed PCI: NetApp Filer NIS Group Update PCI: Oracle Database Permissions Changed PCI: Oracle Database User Added or Deleted PCI: RACF Permissions Changed PCI: TIBCO ActiveMatrix Administrator Permission Changed PCI: vCenter Permission Change PCI: vCenter User Login Successful PCI: vCloud Director Login Success PCI: vCloud User, Group, or Role Modified PCI: Windows Permissions Changed

Requirement	Description	Compliance Suite Reports and Alerts
8.5.6	Enable accounts used by vendors for remote maintenance only during the time needed.	**Compliance Suite Reports** PCI: Accepted VPN Connections - RADIUS PCI: Account Activities on Windows Servers PCI: Check Point Management Station Login PCI: DB2 Database Successful Logins PCI: ESX Logins Succeeded PCI: F5 BIG-IP TMOS Login Successful PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Successful PCI: i5/OS Network User Login Successful CI: i5/OS User Login Successful PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication Type PCI: LogLogic DSM Logins PCI: LogLogic Management Center Login PCI: Microsoft SQL Server Database Successful Logins PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer Login Successful PCI: Oracle Database Successful Logins PCI: RACF Successful Logins PCI: Successful Logins PCI: Sybase ASE Successful Logins PCI: vCenter Successful Logins PCI: vCloud Successful Logins PCI: VPN Users Accessing Corporate Network **Compliance Suite Alerts** PCI: Guardium SQL Guard Logins PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: vCenter User Login Successful PCI: vCloud Director Login Success

Requirement	Description	Compliance Suite Reports and Alerts
8.5.9	Change user passwords at least every 90 days.	**Compliance Suite Reports** PCI: Active Directory System Changes PCI: Cisco ISE, ACS Password Changes PCI: F5 BIG-IP TMOS Password Changes PCI: i5/OS DST Password Reset PCI: LogLogic Management Center Password Changes PCI: Microsoft Operations Manager - Windows Password Changes PCI: Microsoft SQL Server Password Changes PCI: NetApp Filer Password Changes PCI: Password Changes on Windows Servers PCI: RACF Password Changed PCI: Symantec Endpoint Protection Password Changes PCI: TIBCO Administrator Password Changes **Compliance Suite Alerts** PCI: Active Directory Changes PCI: Cisco ISE, ACS Passwords Changed PCI: IBM AIX Password Changed PCI: LogLogic Management Center Passwords Changed PCI: Microsoft Operations Manager - Windows Passwords Changed PCI: RACF Passwords Changed PCI: Windows Password Changed
8.5.13	Limit repeated access attempts by locking out the user ID after no more than 6 consecutive failed login attempts.	**Compliance Suite Reports** PCI: Active Directory System Changes PCI: NetApp Filer Accounts Locked PCI: Windows Accounts Locked **Compliance Suite Alerts** PCI: Accounts Locked PCI: Active Directory Changes

Requirement	Description	Compliance Suite Reports and Alerts
8.5.16	Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.	**Compliance Suite Reports** PCI: Check Point Management Station Login PCI: DB2 Database Successful Logins PCI: ESX Logins Succeeded PCI: F5 BIG-IP TMOS Login Successful PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Successful PCI: i5/OS Network User Login Successful PCI: i5/OS User Login Successful PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: LogLogic DSM Logins PCI: LogLogic Management Center Login PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updates PCI: Microsoft SQL Server Database Successful Logins PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Oracle Database Successful Logins PCI: RACF Successful Logins PCI: Successful Logins PCI: Sybase ASE Successful Logins PCI: TIBCO ActiveMatrix Administrator Successful Logins PCI: vCenter Successful Logins PCI: vCloud Successful Logins **Compliance Suite Alerts** PCI: Guardium SQL Guard Logins PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updated PCI: vCenter User Login Successful

Requirement	Description	Compliance Suite Reports and Alerts
		PCI: vCloud Director Login Success

Requirement	Description	Compliance Suite Reports and Alerts
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows (Type - Evolving Requirement): Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	**Compliance Suite Reports** PCI: Accepted VPN Connections - RADIUS PCI: Account Activities on UNIX Servers PCI: Account Activities on Windows Servers PCI: Administrator Logins on Windows Servers PCI: Check Point Management Station Login PCI: DB2 Database Successful Logins PCI: ESX Accounts Activities PCI: ESX Group Activities PCI: ESX Logins Succeeded PCI: F5 BIG-IP TMOS Login Successful PCI: Group Activities on NetApp Filer Audit PCI: Group Activities on Symantec Endpoint Protection PCI: Group Activities on TIBCO ActiveMatrix Administrator PCI: Group Activities on UNIX Servers PCI: Group Activities on Windows Servers PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Successful PCI: i5/OS Network User Login Successful PCI: i5/OS User Login Successful PCI: Juniper SSL VPN (Secure Access) Successful Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication Type PCI: LogLogic DSM Logins PCI: LogLogic Management Center Account Activities PCI: LogLogic Management Center Login PCI: Microsoft Operations Manager - Windows Accounts Activities PCI: Microsoft SQL Server Database Successful Logins PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Oracle Database Successful Logins PCI: Root Logins

Requirement	Description	Compliance Suite Reports and Alerts
		PCI: Successful Logins
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows (Type - Evolving Requirement): Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	**Compliance Suite Reports** (Cont.) PCI: Sybase ASE Successful Logins PCI: TIBCO ActiveMatrix Administrator Successful Logins PCI: vCenter Successful Logins PCI: vCloud Successful Logins **Compliance Suite Alerts** PCI: Guardium SQL Guard Logins PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: vCenter User Login Successful PCI: vCloud Director Login Success
8.8	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 9 Restrict physical access to cardholder data		
9.10	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 10 - Track and monitor all access to network resources and cardholder data		

Requirement	Description	Compliance Suite Reports and Alerts
10.1	Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to each individual user	**Compliance Suite Reports** PCI: Active Directory System Changes PCI: Administrators Activities on Servers PCI: Administrator Logins on Windows Servers PCI: Escalated Privilege Activities on Servers PCI: Root Logins **Compliance Suite Alerts** PCI: Active Directory Changes PCI: Escalated Privileges
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data	**Compliance Suite Reports** PCI: Active Directory System Changes PCI: Administrators Activities on Servers PCI: DB2 Database Failed Logins PCI: Denied VPN Connections - RADIUS PCI: Escalated Privilege Activities on Servers PCI: ESX Failed Logins PCI: ESX Logins Failed Unknown User PCI: F5 BIG-IP TMOS Login Failed PCI: Failed Logins PCI: HP NonStop Audit Login Failed PCI: i5/OS Network User Login Failed PCI: i5/OS User Login Failed PCI: Juniper SSL VPN (Secure Access) Failed Logins by User PCI: Juniper SSL VPN Failed Logins by User PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updates PCI: Microsoft SQL Server Database Failed Logins PCI: NetApp Filer Audit Login Failed PCI: NetApp Filer File Activity PCI: NetApp Filer Login Failed PCI: Pulse Connect Secure Failed Logins by User PCI: Oracle Database Failed Logins PCI: RACF Failed Logins PCI: Sybase ASE Failed Logins PCI: TIBCO ActiveMatrix Administrator Failed Logins

Requirement	Description	Compliance Suite Reports and Alerts
10.2.2	Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges	PCI: Unauthorized Logins PCI: UNIX Failed Logins PCI: vCenter Failed Logins PCI: vCenter Orchestrator Failed Logins PCI: vCloud Failed Logins PCI: VPN Users Accessing Corporate Network
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data	**Compliance Suite Alerts** PCI: Active Directory Changes PCI: Escalated Privileges PCI: Logins Failed PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updated PCI: NetApp Authentication Failure PCI: vCenter User Login Failed PCI: vCenter Orchestrator Login Failed PCI: vCloud Director Login Failed
10.2.2	Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges	
10.2.3	Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails	**Compliance Suite Reports** PCI: LogLogic File Retrieval Errors PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updates PCI: NetApp Filer Audit Logs Cleared PCI: Periodic Review of Log Reports PCI: Periodic Review of User Access Logs PCI: Windows Audit Logs Cleared **Compliance Suite Alerts** PCI: LogLogic File Retrieval Errors PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updated PCI: Windows Audit Log Cleared

Requirement	Description	Compliance Suite Reports and Alerts
10.2.4	Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts	**Compliance Suite Reports** PCI: Active Directory System Changes PCI: Administrators Activities on Servers PCI: DB2 Database Failed Logins PCI: Denied VPN Connections - RADIUS PCI: Escalated Privilege Activities on Servers PCI: ESX Failed Logins PCI: ESX Logins Failed Unknown User PCI: F5 BIG-IP TMOS Login Failed PCI: Failed Logins PCI: HP NonStop Audit Login Failed PCI: i5/OS Network User Login Failed PCI: i5/OS User Login Failed PCI: Juniper SSL VPN (Secure Access) Failed Logins by User PCI: Juniper SSL VPN Failed Logins by User PCI: Microsoft SQL Server Database Failed Logins PCI: NetApp Filer Audit Login Failed PCI: NetApp Filer File Activity PCI: NetApp Filer Login Failed PCI: Pulse Connect Secure Failed Logins by User PCI: Oracle Database Failed Logins PCI: RACF Failed Logins PCI: Sybase ASE Failed Logins PCI: TIBCO ActiveMatrix Administrator Failed Logins PCI: Unauthorized Logins PCI: UNIX Failed Logins PCI: vCenter Failed Logins PCI: vCenter Orchestrator Failed Logins PCI: vCloud Failed Logins PCI: VPN Users Accessing Corporate Network **Compliance Suite Alerts** PCI: Active Directory Changes PCI: Escalated Privileges PCI: Logins Failed PCI: NetApp Authentication Failure

Requirement	Description	Compliance Suite Reports and Alerts
		PCI: vCenter User Login Failed PCI: vCenter Orchestrator Login Failed PCI: vCloud Director Login Failed

Requirement	Description	Compliance Suite Reports and Alerts
10.2.5	Implement automated audit trails for all system components to reconstruct the following events: Use of identification and authentication mechanisms	**Compliance Suite Reports** PCI: Accepted VPN Connections - RADIUS PCI: Administrators Activities on Servers PCI: Check Point Management Station Login PCI: DB2 Database Failed Logins PCI: DB2 Database Successful Logins PCI: Denied VPN Connections - RADIUS PCI: Escalated Privilege Activities on Servers PCI: ESX Failed Logins PCI: ESX Logins Succeeded PCI: ESX Logins Failed Unknown User PCI: F5 BIG-IP TMOS Login Failed PCI: F5 BIG-IP TMOS Login Successful PCI: Failed Logins PCI: Guardium SQL Guard Audit Logins PCI: Guardium SQL Guard Logins PCI: HP NonStop Audit Login Failed PCI: HP NonStop Audit Login Successful PCI: i5/OS Network User Login Failed PCI: i5/OS Network User Login Successful PCI: i5/OS User Login Failed PCI: i5/OS User Login Successful PCI: Juniper SSL VPN (Secure Access) Failed Logins by User PCI: Juniper SSL VPN (Secure Access) Successful Logins by User Name:PCI: Juniper SSL VPN Failed Logins by User PCI: Juniper SSL VPN Successful Logins by User PCI: Logins by Authentication Type PCI: LogLogic DSM Logins PCI: LogLogic Management Center Login PCI: Microsoft SQL Server Database Successful Logins PCI: Microsoft SQL Server Database Failed Logins PCI: NetApp Filer Audit Login Failed PCI: NetApp Filer Audit Login Successful PCI: NetApp Filer File Activity

Requirement	Description	Compliance Suite Reports and Alerts
		PCI: NetApp Filer Login Failed
10.2.5	Implement automated audit trails for all system components to reconstruct the following events: Use of identification and authentication mechanisms	**Compliance Suite Reports** PCI: NetApp Filer Login Successful PCI: Pulse Connect Secure Successful Logins by User PCI: Pulse Connect Secure Failed Logins by User PCI: Oracle Database Failed Logins PCI: Oracle Database Successful Logins PCI: RACF Failed Logins PCI: RACF Successful Logins PCI: Successful Logins PCI: Sybase ASE Failed Logins PCI: Sybase ASE Successful Logins PCI: TIBCO ActiveMatrix Administrator Failed Logins PCI: TIBCO ActiveMatrix Administrator Successful Logins PCI: Unauthorized Logins PCI: UNIX Failed Logins PCI: vCenter Failed Logins PCI: vCenter Successful Logins PCI: vCenter Orchestrator Failed Logins PCI: vCloud Failed Logins PCI: vCloud Successful Logins PCI: VPN Users Accessing Corporate Network **Compliance Suite Alerts** PCI: Escalated Privileges PCI: Guardium SQL Guard Logins PCI: Logins Failed PCI: Logins Succeeded PCI: LogLogic DSM Logins PCI: NetApp Authentication Failure PCI: vCenter User Login Failed PCI: vCenter User Login Successful PCI: vCenter Orchestrator Login Failed PCI: vCloud Director Login Failed PCI: vCloud Director Login Success

Requirement	Description	Compliance Suite Reports and Alerts
10.2.6	Implement automated audit trails for all system components to reconstruct the following events: Initialization of the audit logs	**Compliance Suite Reports** PCI: LogLogic File Retrieval Errors PCI: NetApp Filer Audit Logs Cleared PCI: Periodic Review of Log Reports PCI: Periodic Review of User Access Logs PCI: Windows Audit Logs Cleared **Compliance Suite Alerts** PCI: LogLogic File Retrieval Errors PCI: Windows Audit Log Cleared
10.2.7	Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system-level objects.	**Compliance Suite Reports** PCI: Creation and Deletion of System Level Objects: AIX Audit PCI: Creation and Deletion of System Level Objects: DB2 Database PCI: Creation and Deletion of System Level Objects: HP-UX Audit PCI: Creation and Deletion of System Level Objects: Oracle PCI: Creation and Deletion of System Level Objects: Solaris BSM PCI: Creation and Deletion of System Level Objects: SQL Server PCI: Creation and Deletion of System Level Objects: Windows PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updates **Compliance Suite Alerts** PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updated PCI: Windows Objects Create/Delete
10.3.1	Record at least the following audit trail entries for each event, for all system components: User identification	**Compliance Suite Reports** PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updates **Compliance Suite Alerts** PCI: Microsoft Sharepoint Content Deleted PCI: Microsoft Sharepoint Content Updated PCI: Windows Audit Log Cleared

Requirement	Description	Compliance Suite Reports and Alerts
10.3.2	Record at least the following audit trail entries for all system components for each event: Type of event	
10.3.3	Record at least the following audit trail entries for all system components for each event: Date and time	
10.3.5	Record at least the following audit trail entries for all system components for each event: Origination of event	
10.3.6	Record at least the following audit trail entries for all system components for each event: Identity or name of affected data, system component, or resource	
10.5.1	Limit viewing of audit trails to those with a job-related need	**Compliance Suite Reports** PCI: LogLogic File Retrieval Errors PCI: NetApp Filer Audit Logs Cleared PCI: Periodic Review of Log Reports PCI: Periodic Review of User Access Logs PCI: Windows Audit Logs Cleared **Compliance Suite Alerts** PCI: LogLogic File Retrieval Errors
10.5.2	Protect audit trail files from unauthorized modifications	
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter	

Requirement	Description	Compliance Suite Reports and Alerts
10.5.5	Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)	
10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). (Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6)	
10.7	Retain audit trail history for at least one year, with a minimum of three months available online	**Compliance Suite Reports** PCI: DNS Server Error PCI: LogLogic Disk Full PCI: LogLogic File Retrieval Errors PCI: LogLogic Message Routing Errors PCI: NetApp Filer File System Full PCI: NetApp Filer Snapshot Error **Compliance Suite Alerts** PCI: LogLogic Disk Full PCI: LogLogic Message Routing Errors PCI: LogLogic File Retrieval Errors PCI: NetApp Bad File Handle PCI: NetApp Bootblock Update PCI: NetApp Filer File System Full PCI: NetApp Filer Disk Scrub Suspended PCI: NetApp Filer Snapshot Error

Requirement	Description	Compliance Suite Reports and Alerts
10.8	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts
Requirement 11 - Regularly test security systems and processes		
11.4	Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.	Compliance Suite Reports PCI: Applications Under Attack PCI: Applications Under Attack - Cisco IOS PCI: Applications Under Attack - ISS SiteProtector PCI: Applications Under Attack - SiteProtector PCI: Applications Under Attack - Sourcefire Defense Center PCI: Attack Origins PCI: Attack Origins - Cisco IOS PCI: Attack Origins - ISS SiteProtector PCI: Attack Origins - SiteProtector PCI: Attack Origins - Sourcefire Defense Center PCI: Attack Origins - HIPS PCI: Attacks Detected PCI: Attacks Detected - Cisco IOS PCI: Attacks Detected - ISS SiteProtector PCI: Attacks Detected - PCI: Attacks Detected - Sourcefire Defense Center PCI: Attacks Detected - HIPS **Compliance Suite Alerts** PCI: Anomalous IDS Alerts

Requirement	Description	Compliance Suite Reports and Alerts
11.5	Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.	**Compliance Suite Reports** PCI: Cisco ESA: Attacks by Event ID PCI: Cisco ESA: Attacks Detected PCI: Cisco ESA: Attacks by Threat Name PCI: Cisco ESA: Scans PCI: FortiOS: Attacks by Event ID PCI: FortiOS: Attacks by Threat Name PCI: FortiOS: Attacks Detected PCI: FortiOS DLP Attacks Detected PCI: McAfee AntiVirus: Attacks by Event ID PCI: McAfee AntiVirus: Attacks by Threat Name PCI: McAfee AntiVirus: Attacks Detected PCI: PANOS: Attacks by Event ID
		PCI: PANOS: Attacks by Threat Name PCI: PANOS: Attacks Detected PCI: Symantec AntiVirus: Attacks by Threat Name PCI: Symantec AntiVirus: Attacks Detected PCI: Symantec AntiVirus: Scans PCI: Symantec Endpoint Protection: Attacks by Threat Name PCI: Symantec Endpoint Protection: Attacks Detected PCI: Symantec Endpoint Protection: Scans PCI: TrendMicro Control Manager: Attacks Detected PCI: TrendMicro Control Manager: Attacks Detected by Threat Name PCI: TrendMicro OfficeScan: Attacks Detected PCI: TrendMicro OfficeScan: Attacks Detected by Threat Name PCI: Tripwire Modifications, Additions, and Deletions
11.6	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts

Requirement	Description	Compliance Suite Reports and Alerts
Requirement 12 - Maintain a policy that addresses information security for employees and contractors		
12.2	Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	**Compliance Suite Reports** All PCI reports **Compliance Suite Alerts** All PCI alerts

Requirement	Description	Compliance Suite Reports and Alerts
12.9.5	Implement an incident response plan. Be prepared to respond immediately to a system breach: Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems	**Compliance Suite Reports** PCI: Applications Under Attack PCI: Applications Under Attack - Cisco IOS PCI: Applications Under Attack - ISS SiteProtector PCI: Applications Under Attack - SiteProtector PCI: Attack Origins PCI: Attack Origins - Cisco IOS PCI: Attack Origins - ISS SiteProtector PCI: Attack Origins - SiteProtector PCI: Attack Origins - HIPS PCI: Attacks Detected PCI: Attacks Detected - Cisco IOS PCI: Attacks Detected - ISS SiteProtector PCI: Attacks Detected - SiteProtector PCI: Attacks Detected - HIPS PCI: Cisco ESA: Attacks by Event ID PCI: Cisco ESA: Attacks Detected PCI: Cisco ESA: Attacks by Threat Name PCI: FortiOS: Attacks by Event IDPCI: FortiOS: Attacks by Threat Name PCI: FortiOS: Attacks Detected PCI: FortiOS DLP Attacks Detected PCI: McAfee AntiVirus: Attacks by Event ID PCI: McAfee AntiVirus: Attacks by Threat NamePCI: McAfee AntiVirus: Attacks Detected PCI: PANOS: Attacks by Event ID PCI: PANOS: Attacks by Threat Name PCI: PANOS: Attacks Detected PCI: Symantec AntiVirus: Attacks by Threat Name PCI: Symantec AntiVirus: Attacks Detected PCI: Symantec Endpoint Protection: Attacks by Threat Name PCI: Symantec Endpoint Protection: Attacks Detected PCI: TrendMicro Control Manager: Attacks Detected

Requirement	Description	Compliance Suite Reports and Alerts
12.9.5	Implement an incident response plan. Be prepared to respond immediately to a system breach: Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems	**Compliance Suite Reports** (Cont.) PCI: TrendMicro Control Manager: Attacks Detected by Threat Name PCI: TrendMicro OfficeScan: Attacks Detected PCI: TrendMicro OfficeScan: Attacks Detected by Threat Name PCI: Tripwire Modifications, Additions, and Deletions

Requirement	Description	Compliance Suite Reports and Alerts
12.10.5	Implement an incident response plan. Be prepared to respond immediately to a system breach: Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	**Compliance Suite Reports** PCI: Applications Under Attack PCI: Applications Under Attack - Cisco IOS PCI: Applications Under Attack - ISS SiteProtector PCI: Applications Under Attack - SiteProtector PCI: Applications Under Attack - Sourcefire Defense Center PCI: Attack Origins PCI: Attack Origins - Cisco IOS PCI: Attack Origins - ISS SiteProtector PCI: Attack Origins - SiteProtector PCI: Attack Origins - Sourcefire Defense Center PCI: Attack Origins - HIPS PCI: Attacks Detected PCI: Attacks Detected - Cisco IOS PCI: Attacks Detected - ISS SiteProtector PCI: Attacks Detected - SiteProtector PCI: Attacks Detected - Sourcefire Defense Center PCI: Attacks Detected - HIPS PCI: Cisco ESA: Attacks by Event ID PCI: Cisco ESA: Attacks Detected PCI: Cisco ESA: Attacks by Threat Name PCI: FortiOS: Attacks by Event ID PCI: FortiOS: Attacks by Threat Name PCI: FortiOS: Attacks Detected PCI: FortiOS DLP Attacks Detected PCI: McAfee AntiVirus: Attacks by Event ID PCI: McAfee AntiVirus: Attacks by Threat Name PCI: McAfee AntiVirus: Attacks Detected
		PCI: PANOS: Attacks by Event ID PCI: PANOS: Attacks by Threat Name PCI: PANOS: Attacks Detected PCI: Symantec AntiVirus: Attacks by Threat Name PCI: Symantec AntiVirus: Attacks Detected

Requirement	Description	Compliance Suite Reports and Alerts
12.10.5	Implement an incident response plan. Be prepared to respond immediately to a system breach: Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	**Compliance Suite Reports** (Cont.) PCI: Symantec Endpoint Protection: Attacks by Threat Name PCI: Symantec Endpoint Protection: Attacks Detected PCI: TrendMicro Control Manager: Attacks Detected PCI: TrendMicro Control Manager: Attacks Detected by Threat Name PCI: TrendMicro OfficeScan: Attacks Detected PCI: TrendMicro OfficeScan: Attacks Detected by Threat Name PCI: Tripwire Modifications, Additions, and Deletions

PCI and COBIT 4.0 Control Objectives Mapping

- Introduction to COBIT
- PCI Requirements and COBIT 4.0 Control Objectives Mapping

Introduction to COBIT

COBIT is the IT Governance Institute's IT audit framework used to help achieve SOX compliance and ensure security and availability of IT assets. COBIT supports IT governance by providing a framework to ensure that:

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately

COBIT released the fourth version of its control framework in December 2005. The framework approaches IT controls by looking at all of the information needed to support business requirements and the associated IT resources and processes. COBIT is intended for management, users, and auditors (mostly IT auditors). COBIT is by far the most adopted framework used for regulatory compliance, including Sarbanes-Oxley and Payment Card Industry Data Security Standard. It is no surprise that all of the PCI DSS requirements maps directly to the COBIT IT processes.

PCI Requirements and COBIT 4.0 Control Objectives Mapping

The following table maps the PCI DSS requirements to the COBIT 4.0 framework.

PCI Requirement	Description	COBIT Control Objective	Description
Requirement 1	Install and maintain a firewall configuration to protect data	DS5.10	Network Security
		DS9.3	Configuration Integrity Review
Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters	DS5.3	Identity Management
		DS5.4	User Account Management
Requirement 3	Protect stored data	DS11.6	Security Requirements for Data Management
Requirement 4	Encrypt transmission of cardholder data and sensitive information across public networks	DS11.6	Security Requirements for Data Management
Requirement 5	Use and regularly update anti-virus software	DS5.9	Malicious Software Prevention, Detection and Correction

PCI Requirement	Description	COBIT Control Objective	Description
Requirement 6	Develop and maintain secure systems and applications	AI6.1	Change Standards and Procedures
Requirement 7	Restrict access to data by business need-to-know	PO4.11	Segregation of Duties
		PO7.8	Job Change and Termination
Requirement 8	Assign a unique ID to each person with computer access	DS5.3	Segregation of Duties
		DS5.4	User Account Management
Requirement 9	Restrict physical access to cardholder data	DS12	Manage the Physical Environment
Requirement 10	Track and monitor all access to network resources and cardholder data	AI2.3	Application Control and Auditability
Requirement 11	Regularly test security systems and processes	DS4.5	Testing of IT Continuity
		DS5.5	Security Testing
Requirement 12	Maintain a policy that addresses information security	DS5.2	IT Security Plan