# TIBCO LogLogic® Compliance Suite - GPG13 Edition Guide

*Software Release 3.9.0*
*November 2017*
*Document Updated: April 2018*

Two-Second Advantage®

## Important Information

This document contains excerpted portions of the Good Practice Guide 13 ("GPG 13") 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 GPG 13 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 GPG 13 standards, you should consult with an attorney for further legal guidance.

# Contents

# Figures

# 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 - GPG13 Guide*
- *TIBCO LogLogic® Compliance Suite - GPG13 Readme*
- *TIBCO LogLogic® Compliance Suite - GPG13 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 GPG13 Compliance

The provision of an effective framework of Protective Monitoring within Her Majesty's Government's (HMG's) Information and Communication Technology (ICT) systems is an essential element of HMG's information security risk strategy. CESG's Good Practice Guide 13 (GPG13) Protective Monitoring framework has been developed to guide public sector organizations on how to monitor exactly what is going on within their ICT infrastructure in a consistent and effective manner. GPG13 is mandatory for all central and local government, fire, police, health or education authorities.

Protective Monitoring is essentially a set of business processes and support technology that have to be put into place to monitor how ICT systems are used and to assure visibility and accountability for use of HMG's ICT facilities.

# The LogLogic® Compliance Suite - GPG 13 Edition Overview

The LogLogic® Compliance Suite - GPG 13 Edition standard delivers automated process validation, reporting and alerts based on infrastructure data to evidence and enforce business, and IT policies related to compliance. By automating compliance reporting and alerting based on critical infrastructure data collected and stored by TIBCO LogLogic® Log Management Intelligence (LMI) Appliances, the TIBCO LogLogic Compliance Suite removes the complexity and resource requirements for implementing control frameworks like GPG13.

## Protective Monitoring Controls

Log data allows organizations to manage the extreme challenges of meeting major GPG implementation specifications. TIBCO LogLogic's compliance reports and alerts satisfy the following protective monitoring controls:

- **Precise Time Stamps**: ensures that the accounting and auditing logs record accurate time stamps.
- **Recording the Business Traffic crossing a Boundary**: identifies the authorized and non-authorized business traffic across the network boundary by defining a set of alerts and reports.
- **Recording the suspicious activity on the boundary**: identifies the suspicious traffic on the network boundary by defining a set of alerts and reports.
- **Recording on Internal Workstation, server or device status**: identifies the changes in configuration or status of the internal workstations, servers and network devices by defining a set of alerts and reports.
- **Recording the suspicious internal network activity**: Identifies the suspicious internal network activity by defining a set of alerts and reports.
- **Recording activities on network connections**: Identifies temporary connections to the network, such as VPN or wireless connection.
- **Recording user activity on the network**: identifies the suspicious user activity or enable the forensic analysis of the user activity within the network by defining a set of alerts and reports.
- **Recording on data backup process**: ensures that the data backup and recovery process is defined and followed, so that the integrity and availability of the network resource is ensured.
- **Alerts and reports on critical events**: defines set of real-time alerts and reports that identifies the events classified as 'critical' by the organization.
- **Reporting the status of auditing system**: defines a set of alerts and reports to ensure the integrity of the auditing system.
- **Generating management reports**: ensures the production of clean and statistical management reports.
- **Providing a legal framework**: ensures that the protective monitoring activities are performed within the legal framework.

## Control Descriptions

### PMC1 - Accurate time in logs

**Control Description**: Provide a means of providing accurate time in logs and synchronisation between system components with a view to facilitating collation of events between those components. This can be achieved by any or all of the following means:

- Providing a master clock system component which is synchronised to an atomic clock
- Updating device clocks from the master clock using the Network Time Protocol (NTP)
- Record time in logs in a consistent format (Universal Co-ordinated Time (UTC) is recommended)
- As a fallback, checking and updating device clocks on a regular basis (for example, weekly).

Projects should define the error margin for time accuracy according to business requirements. The following issues also must be considered:

- Some devices might not support clock synchronisation and must be manually maintained
- Although recording time in UTC, the human interface should also support local time
- Clocks drift on mobile devices (e.g. Portable Electronic Devices (PEDs)) might require correction upon attachment.

### PMC2 - Recording relating to business traffic crossing a boundary

**Control Description**: The objective of this control is to provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented.

The main requirement is to provide an accountable record of imports and exports executed by internal users and to track cross-boundary information exchange operations and the utilisation of any externally visible interfaces. This includes all checking of cross-boundary movement of information, content checking and quarantining services.

Application based checks can be applied to business traffic to accept legitimate transactions and reject and alert malformed exchanges.

### PMC3 - Recording relating to suspicious behaviour at a boundary

**Control Description**: The objective of this control is to provide reports, monitoring, recording, and analysis of network activity at the boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach the system boundary or other deviation from normal business behaviour.

The main requirement is to receive information from firewalls and other network devices for traffic and traffic trend analysis. This enables detection of common attacks such as port scanning, malformed packets and illicit protocol behaviours.

An intrusion detection service is a recommended defence at the boundary with any untrusted network (for example, the Internet). It might also be a mandated requirement in codes of connection for membership of community of interest networks (such as GSI). Whenever it is implemented then it is recommended it includes a Recordable Report profile of at least B.

### PMC4 - Recording of workstation, server or device status

**Control Description**: The objective of this control is to detect changes to device status and configuration. Changes might occur through accidental or deliberate acts by a user or by subversion of a device by malware (for example, installation of trojan software or so called "rootkits"). It also records indications that are typical of the behaviour of such events (including unexpected and repeated system restarts or addition of unidentified system processes).

It also attempts to detect other unauthorised actions in tightly controlled environments (for example, attachment of USB storage devices). This includes extension to extensive monitoring of any business critical file areas.

### PMC5 - Recording relating to suspicious internal network activity

**Control Description**: The objective of this control is to monitor critical internal boundaries and resources within internal networks to detect suspicious activity that might indicate attacks either by internal users or by external attackers who have penetrated to the internal network.

Likely targets for heightened internal monitoring include:

- core electronic messaging infrastructure (e.g. email servers and directory servers)
- sensitive databases (e.g. HR databases, finance, procurement or contracts and so on.)
- information exchanges with third parties
- project servers and file stores with strict "need to know" requirements

### PMC6 - Recording relating to network connections

**Control Description**: The objective of this control is to monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection.

This includes:

- Environments which are permissive and that support Wireless LANs (WLANs), mobile users and remote working and it includes.
- More restrictive environments in which the attachment of modems and wireless access points are prohibited.

### PMC7 - Recording of session activity by user and workstation

**Control Description**: To monitor user activity and access to ensure they can be made accountable for their actions and to detect unauthorised activity and access that is either suspicious or is in violation of security policy requirements.

This is intended to support accountability requirements such that users can be held to account for actions they perform on ICT systems.

### PMC8 - Recording of data backup status

**Control Description**: To provide a means by which previous known working states of information assets can be identified and recovered from in the event that either their integrity or availability is compromised.

Providing an audit trail of backup and recovery operations is an essential part of the backup process and enables identification of the most reliable source of the prior known good states of the information assets to be recovered in the event of data corruption, deletion or loss.

The need for more sophisticated backup and recovery facilities are generally driven by higher levels of risk to Integrity and Availability properties.

There is a complimentary requirement for online storage failure events to be alerted, this is met by PMC4 Recordable Event 1 (the detection of any server storage failure should be classed as an alertable Critical event).

### PMC9 - Alerting critical events

**Control Description**: To allow critical classes of events to be notified in as close to real-time as is achievable.

The aware level requirement is for console based alerts that can be watched for by duty Security Managers.

It would be expected that extensive projects (with continuous monitoring requirement) would require a Security Operations Centre with summary wall displays (with the most complex scenario implementing redundant monitoring centres).

It should be noted that alerts themselves are recordable events.

Smaller projects can have a solution to fit their size and would typically only require a profile A solution with simple monitoring facilities (a Security Manager workstation). Smaller projects might also consider combination of functions (for example, security and network management) provided this does not conflict with segregation requirements.

Secondary alerting channels might also be supported for projects that cannot provide continuous console manning (for example, SNMP, email, SMS, and so on) through either in hours or out of hours services.

### PMC10 - Reporting on the status of the audit system

**Control Description**: To support means by which the integrity status of the collected accounting data can be verified.

The Aware segment requirements comprise the need to inspect log status on end devices and alerting of log error or other security relevant conditions.

Upper segment requirements expand to include the requirement for log collection and query systems (ultimately served as a resilient solution).

Smaller (especially single location) projects can have a solution to fit their size and would typically only require a profile level A solution without log collection facilities (perhaps assisted by COTS log analysis tools).

### PMC11 - Production of sanitised and statistical management reports

**Control Description**: To provide management feedback on the performance of the protective monitoring system in regard of audit, detection and investigation of information security incidents.

### PMC12 - Providing a legal framework for Protective Monitoring activities

**Control Description**: To ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right.

The most significant aspect of ensuring Protective Monitoring is lawful is ensuring that it is justified. A major part of the evidence for that justification is that the risk management process ensures there is neither too much nor too little.

There are certain aspects of user consent that must be recorded as part of the system implementation. As for the other treatments the degree of rigour and trust in these increased along the scale of increasing segment. It is important to seek legal advice on compliance with the law and wording of all related screen messages and documents. Online electronic sign up might also be supplemented, or alternatively replaced, by manual records of user agreements and monitoring policies.

# TIBCO LogLogic Compliance Suite Setup

Setting up the LogLogic® Compliance Suite - GPG 13 Edition comprises checking that all prerequisites are met before starting the installation process, installing the Compliance Suite file, and enabling the alerts.

See Installing the Compliance Suite and Enabling Compliance Suite Alerts for more details.

## Installing the Compliance Suite

### Prerequisites

Before installing the LogLogic® Compliance Suite - GPG 13 Edition, ensure that you have:

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

The Compliance Suite includes one file containing GPG13 filters, custom reports, and alerts.

- `GPG13.xml` – GPG13 Reports, Search Filters, 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.

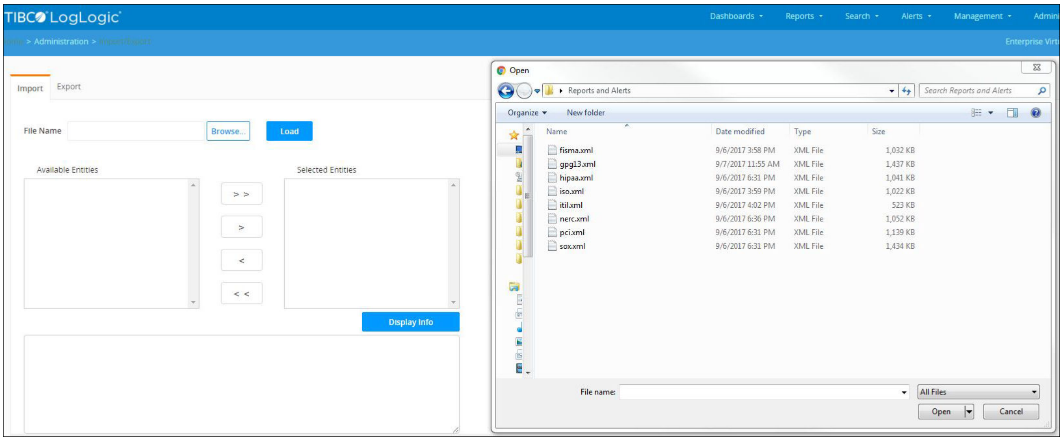
### Procedure

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** .

   The **Import** and **Export** tabs open.
3. 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 is displayed after clicking **Browse** on the **Import** tab.

*Loading a Compliance Suite File*



| Name | Date modified | Type | Size |
|---|---|---|---|
| fisma.xml | 9/6/2017 3:58 PM | XML File | 1,032 KB |
| gpg13.xml | 9/7/2017 11:55 AM | XML File | 1,437 KB |
| hipaa.xml | 9/6/2017 6:31 PM | XML File | 1,041 KB |
| iso.xml | 9/6/2017 3:59 PM | XML File | 1,022 KB |
| itil.xml | 9/6/2017 4:02 PM | XML File | 523 KB |
| nerc.xml | 9/6/2017 6:36 PM | XML File | 1,052 KB |
| pci.xml | 9/6/2017 6:31 PM | XML File | 1,139 KB |
| sox.xml | 9/6/2017 6:31 PM | XML File | 1,434 KB |

c) Click **Load**.

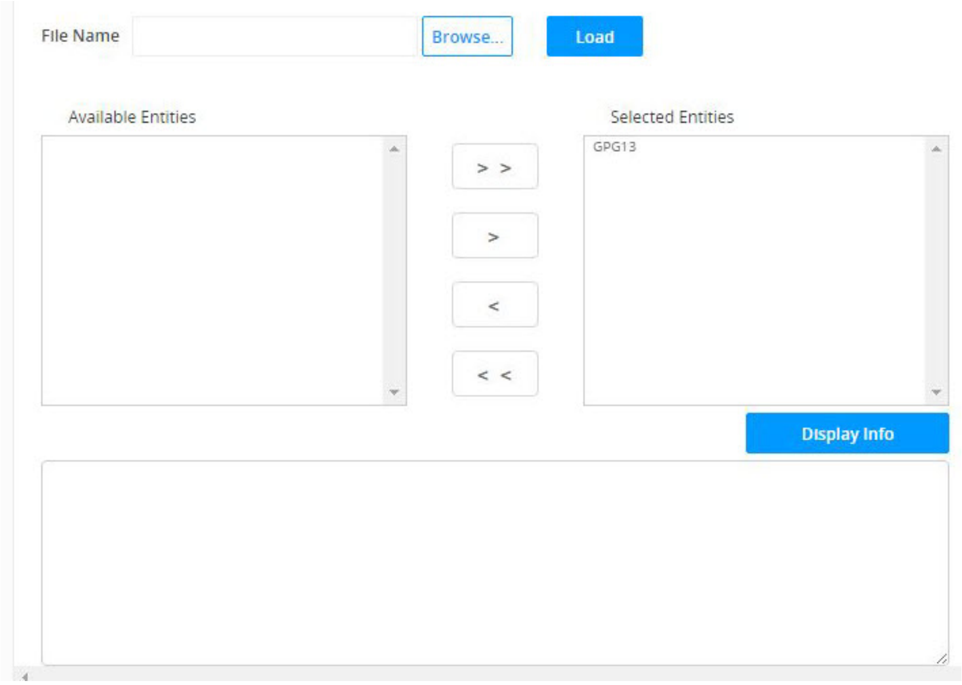
This loads the **Available Entities** from the XML file.

d) Click **Add All Entities**.

> You can also select the specific GPG13 entity from the **Available Entities** text block, and then click **Add Selected Entities**.

The following figure shows all entities of the GPG13 XML file that were selected by clicking **Add All Entities**.

*Selected Entities to be Imported*



GPG13

4. Click **Import**.

An import successfully completed message is displayed 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 LogLogic® Compliance Suite - GPG 13 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

If you have to make modifications based on your business needs, all LogLogic® Compliance Suite - GPG 13 Edition reports are designed to run out-of-the box and be flexible

For a description of all custom reports in this Compliance Suite, see TIBCO LogLogic Reports for GPG13.

- Viewing complaince Suite Reports and Output Data
- Customizing Compliance Suite Reports

### Viewing Compliance Suite Reports and Output Data

By using TIBCO LogLogic LX or MX or ST Appliance, you can view all the Compliance Suite reports for the device and run them as well as view the output data.

**Procedure**

1. Log in to your TIBCO LogLogic LX or MX or ST Appliance as admin.
2. From the navigation menu, select **Reports** > **GPG13** .

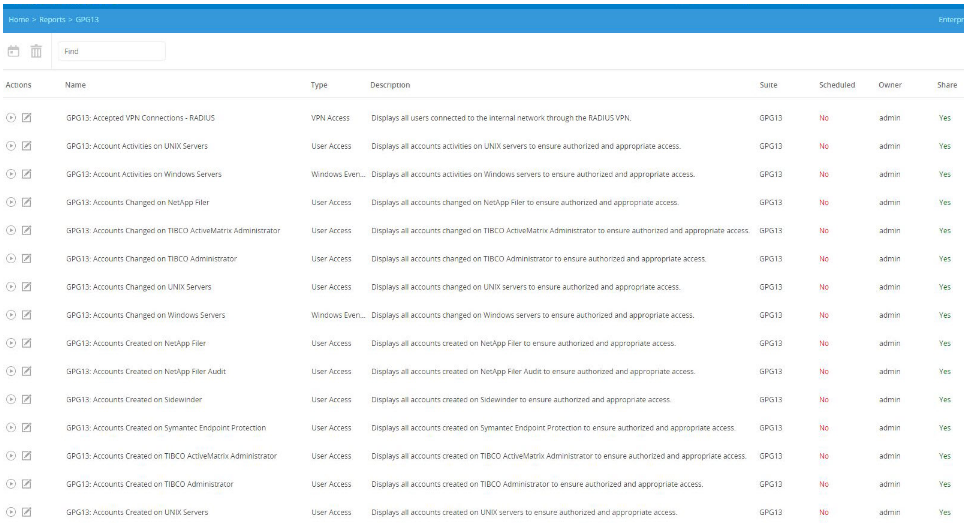
   > You can also access all of your custom reports on the Appliance including the Compliance Suite reports you installed, by selecting **Reports** > **All Saved Reports** .

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 GPG13 XML file.

*Compliance Suite Reports*

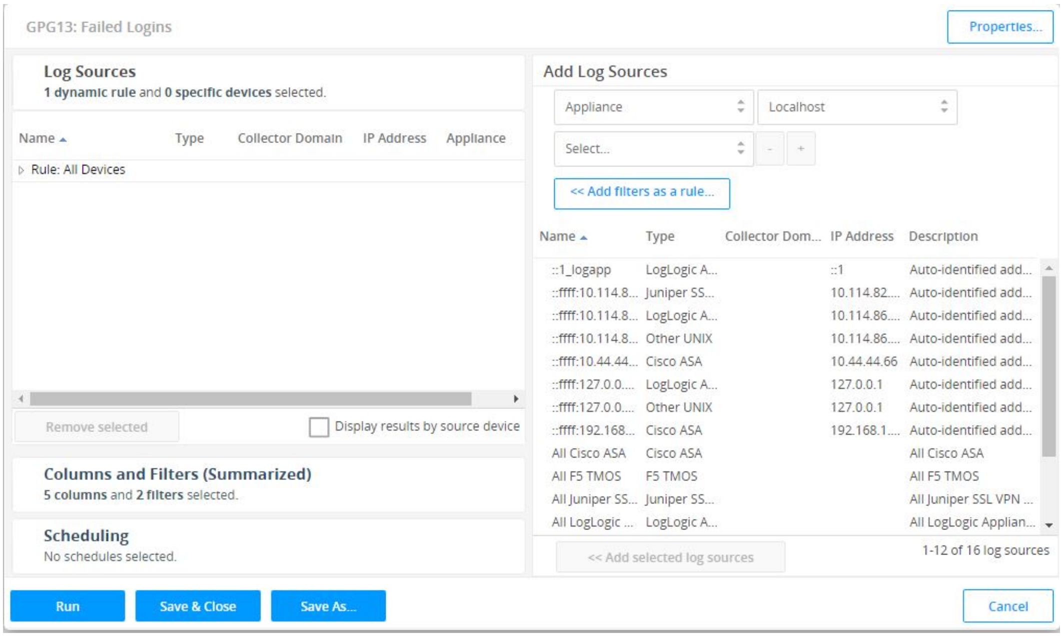


| Actions | Name | Type | Description | Suite | Scheduled | Owner | Share |
|---|---|---|---|---|---|---|---|
| | GPG13: Accepted VPN Connections - RADIUS | VPN Access | Displays all users connected to the internal network through the RADIUS VPN. | GPG13 | No | admin | Yes |
| | GPG13: Account Activities on UNIX Servers | User Access | Displays all accounts activities on UNIX servers to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Account Activities on Windows Servers | Windows Even... | Displays all accounts activities on Windows servers to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Changed on NetApp Filer | User Access | Displays all accounts changed on NetApp Filer to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Changed on TIBCO ActiveMatrix Administrator | User Access | Displays all accounts changed on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Changed on TIBCO Administrator | User Access | Displays all accounts changed on TIBCO Administrator to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Changed on UNIX Servers | User Access | Displays all accounts changed on UNIX servers to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Changed on Windows Servers | Windows Even... | Displays all accounts changed on Windows servers to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Created on NetApp Filer | User Access | Displays all accounts created on NetApp Filer to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Created on NetApp Filer Audit | User Access | Displays all accounts created on NetApp Filer Audit to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Created on Sidewinder | User Access | Displays all accounts created on Sidewinder to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Created on Symantec Endpoint Protection | User Access | Displays all accounts created on Symantec Endpoint Protection to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Created on TIBCO ActiveMatrix Administrator | User Access | Displays all accounts created on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Created on TIBCO Administrator | User Access | Displays all accounts created on TIBCO Administrator to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |
| | GPG13: Accounts Created on UNIX Servers | User Access | Displays all accounts created on UNIX servers to ensure authorized and appropriate access. | GPG13 | No | admin | Yes |

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 **GPG13: Failed Logins** report.

   *Failed Logins Report Details*



GPG13: Failed Logins

Log Sources

1 dynamic rule and 0 specific devices selected.

| Name ▲ | Type | Collector Domain | IP Address | Appliance |
|---|---|---|---|---|
| ▷ Rule: All Devices | | | | |

☐ Display results by source device

Columns and Filters (Summarized)

5 columns and 2 filters selected.

Scheduling

No schedules selected.

| Name ▲ | Type | Collector Dom... | IP Address | Description |
|---|---|---|---|---|
| ::1_logapp | LogLogic A... | | ::1 | Auto-identified add... |
| ::ffff:10.114.8... | Juniper SS... | | 10.114.82.... | Auto-identified add... |
| ::ffff:10.114.8... | LogLogic A... | | 10.114.86.... | Auto-identified add... |
| ::ffff:10.114.8... | Other UNIX | | 10.114.86.... | Auto-identified add... |
| ::ffff:10.44.44... | Cisco ASA | | 10.44.44.66 | Auto-identified add... |
| ::ffff:127.0.0.... | LogLogic A... | | 127.0.0.1 | Auto-identified add... |
| ::ffff:127.0.0.... | Other UNIX | | 127.0.0.1 | Auto-identified add... |
| ::ffff:192.168... | Cisco ASA | | 192.168.1.... | Auto-identified add... |
| All Cisco ASA | Cisco ASA | | | All Cisco ASA |
| All F5 TMOS | F5 TMOS | | | All F5 TMOS |
| All Juniper SS... | Juniper SS... | | | All Juniper SSL VPN ... |
| All LogLogic ... | LogLogic A... | | | All LogLogic Applian... |

1-12 of 16 log sources

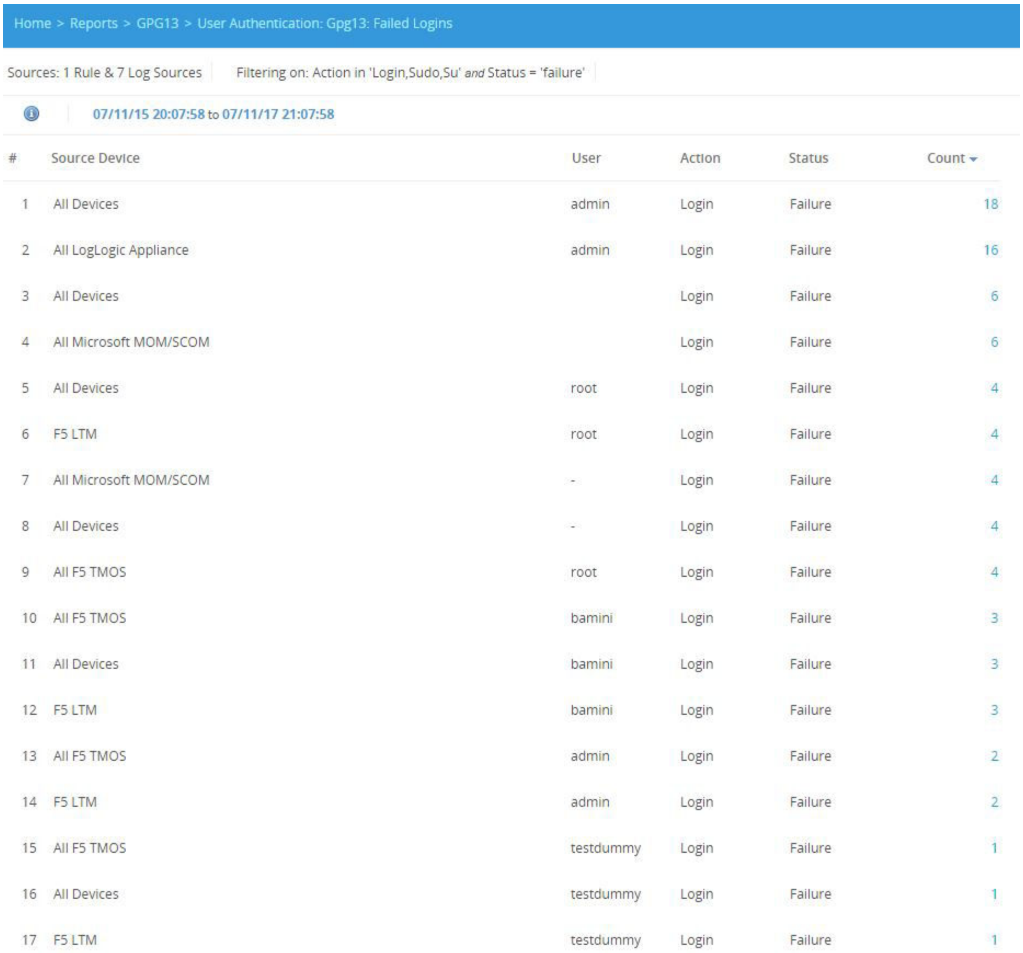
5. Run the report to view the report output data by completing the following steps:
   a) Click **Run**.

   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 **GPG13: Failed Logins** report.

*Failed Logins Report Results*



Home > Reports > GPG13 > User Authentication: Gpg13: Failed Logins

Sources: 1 Rule & 7 Log Sources | Filtering on: Action in 'Login,Sudo,Su' *and* Status = 'failure'

07/11/15 20:07:58 to 07/11/17 21:07:58

| # | Source Device | User | Action | Status | Count |
|---|---|---|---|---|---|
| 1 | All Devices | admin | Login | Failure | 18 |
| 2 | All LogLogic Appliance | admin | Login | Failure | 16 |
| 3 | All Devices |  | Login | Failure | 6 |
| 4 | All Microsoft MOM/SCOM |  | Login | Failure | 6 |
| 5 | All Devices | root | Login | Failure | 4 |
| 6 | F5 LTM | root | Login | Failure | 4 |
| 7 | All Microsoft MOM/SCOM | - | Login | Failure | 4 |
| 8 | All Devices | - | Login | Failure | 4 |
| 9 | All F5 TMOS | root | Login | Failure | 4 |
| 10 | All F5 TMOS | bamini | Login | Failure | 3 |
| 11 | All Devices | bamini | Login | Failure | 3 |
| 12 | F5 LTM | bamini | Login | Failure | 3 |
| 13 | All F5 TMOS | admin | Login | Failure | 2 |
| 14 | F5 LTM | admin | Login | Failure | 2 |
| 15 | All F5 TMOS | testdummy | Login | Failure | 1 |
| 16 | All Devices | testdummy | Login | Failure | 1 |
| 17 | F5 LTM | testdummy | Login | Failure | 1 |

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 LogLogic® Compliance Suite - GPG 13 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.

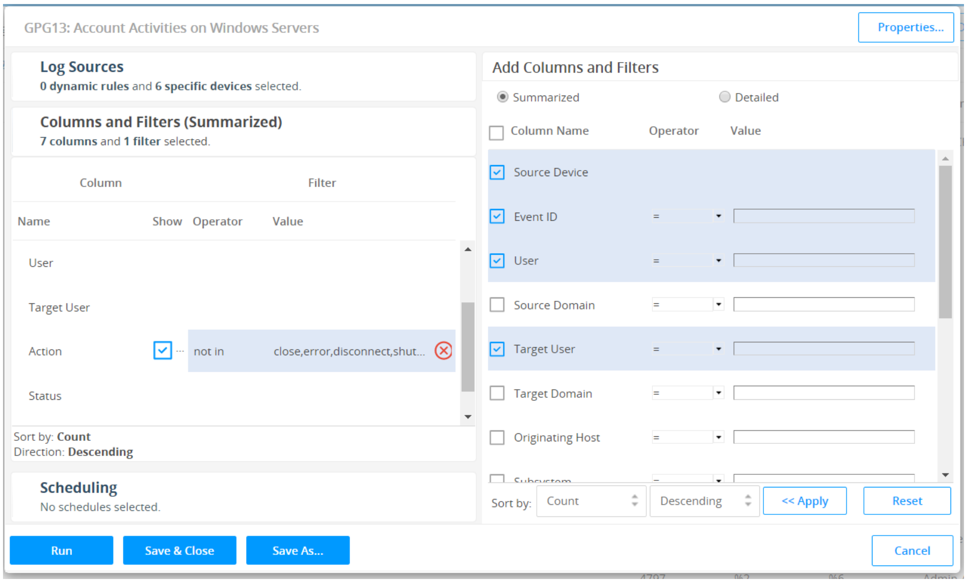
### Procedure

1. Make sure that you are on the **Reports** page and click the **Edit** button for a report you want to modify.
2. Modify the report details (for example, name, description, and so on), 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 image shows the report filters available under **Columns and Filters** options.

*Advanced Options and Update Saved Custom Report Views*



GPG13: Account Activities on Windows Servers

**Log Sources**
0 dynamic rules and 6 specific devices selected.

**Columns and Filters (Summarized)**
7 columns and 1 filter selected.

| Name | Show | Operator | Value |
|---|---|---|---|
| User | | | |
| Target User | | | |
| Action | ☑ | not in | close,error,disconnect,shut... |
| Status | | | |

Sort by: **Count**
Direction: **Descending**

**Scheduling**
No schedules selected.

Add Columns and Filters

● Summarized ○ Detailed

| | Column Name | Operator | Value |
|---|---|---|---|
| ☑ | Source Device | | |
| ☑ | Event ID | = | |
| ☑ | User | = | |
| ☐ | Source Domain | = | |
| ☑ | Target User | = | |
| ☐ | Target Domain | = | |
| ☐ | Originating Host | = | |
| ☐ | Subsystem | = | |

Sort by: Count Descending

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 (for example, **Report Name**, **Report Description**, and so on).

   b) Click **Save & Close**.

   A report saved message is displayed. 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 LogLogic® Compliance Suite - GPG 13 Edition alerts enable you to manage activities helping you to maintain GPG13 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 GPG13.

- Accessing Available Compliance Suite Alerts
- Enabling Compliance Suite Alerts
- Viewing Compliance Suite Alert Results

## Accessing Available Compliance Suite Alerts

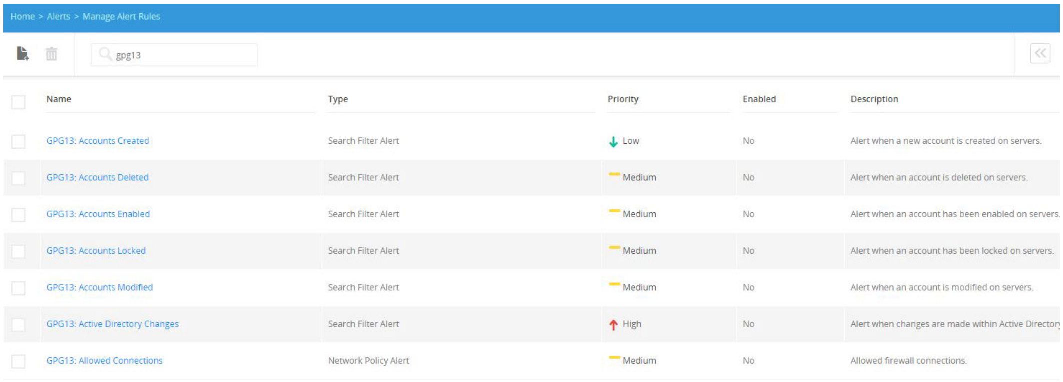
The Compliance Suite package contains a number of alerts that can be easily enabled and modified for your business needs.

### Procedure

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

   The following image shows a cropped list of the Compliance Suite alerts loaded from the GPG13 XML file.

   *Compliance Suite Alerts*

   | ☐ | Name | Type | Priority | Enabled | Description |
   |---|---|---|---|---|---|
   | ☐ | GPG13: Accounts Created | Search Filter Alert | ↓ Low | No | Alert when a new account is created on servers. |
   | ☐ | GPG13: Accounts Deleted | Search Filter Alert | Medium | No | Alert when an account is deleted on servers. |
   | ☐ | GPG13: Accounts Enabled | Search Filter Alert | Medium | No | Alert when an account has been enabled on servers. |
   | ☐ | GPG13: Accounts Locked | Search Filter Alert | Medium | No | Alert when an account has been locked on servers. |
   | ☐ | GPG13: Accounts Modified | Search Filter Alert | Medium | No | Alert when an account is modified on servers. |
   | ☐ | GPG13: Active Directory Changes | Search Filter Alert | ↑ High | No | Alert when changes are made within Active Director |
   | ☐ | GPG13: Allowed Connections | Network Policy Alert | Medium | No | Allowed firewall connections. |

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 have 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 because the default settings are aimed at capturing a broad range of alerts.

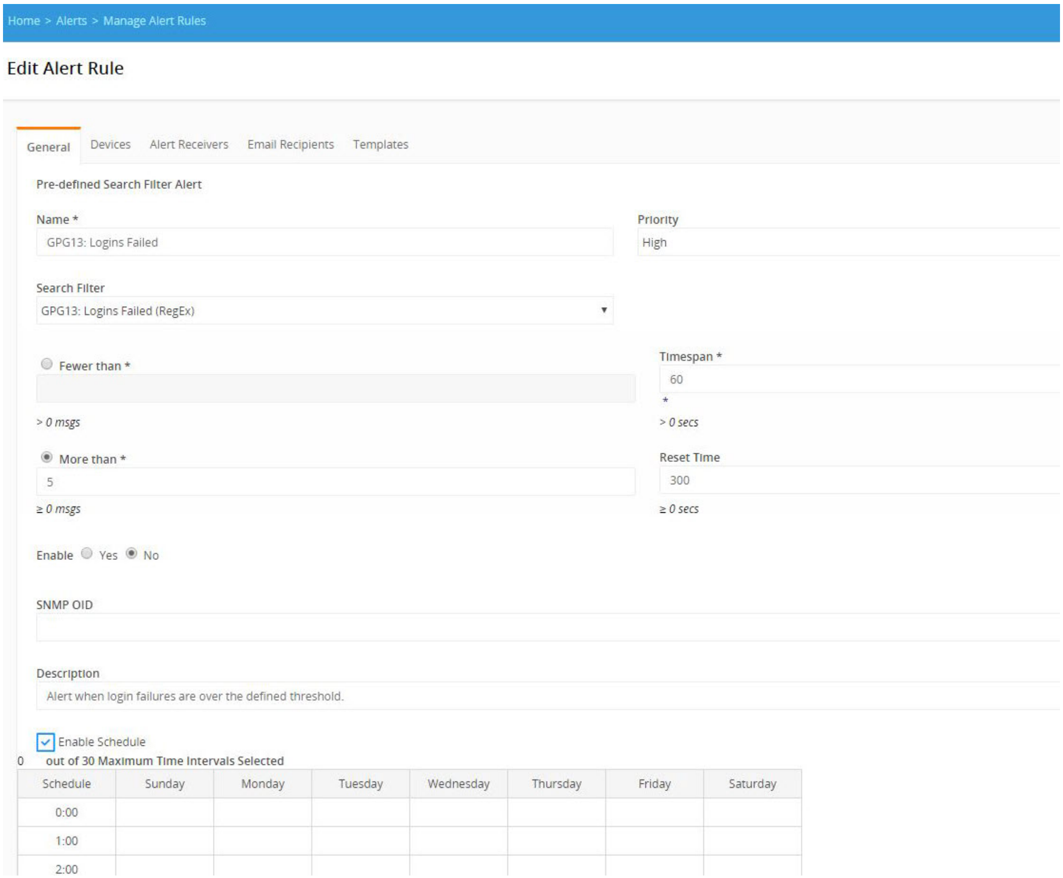
To enable alerts, you must set one of devices to monitor, the SNMP trap receivers, as well as who receives an alert notification, and how they receive it.

### Procedure

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

   The following image shows the **General** tab for the **GPG13: Logins Failed** alert.

*Logins Failed Alert*



Pre-defined Search Filter Alert

Name *: GPG13: Logins Failed

Priority: High

Search Filter: GPG13: Logins Failed (RegEx)

○ Fewer than *

> 0 msgs

● More than *: 5

≥ 0 msgs

Timespan *: 60

> 0 secs

Reset Time: 300

≥ 0 secs

Enable ○ Yes ● No

SNMP OID

Description: Alert when login failures are over the defined threshold.

☑ Enable Schedule

0 out of 30 Maximum Time Intervals Selected

| Schedule | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
|---|---|---|---|---|---|---|---|
| 0:00 | | | | | | | |
| 1:00 | | | | | | | |
| 2:00 | | | | | | | |

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.

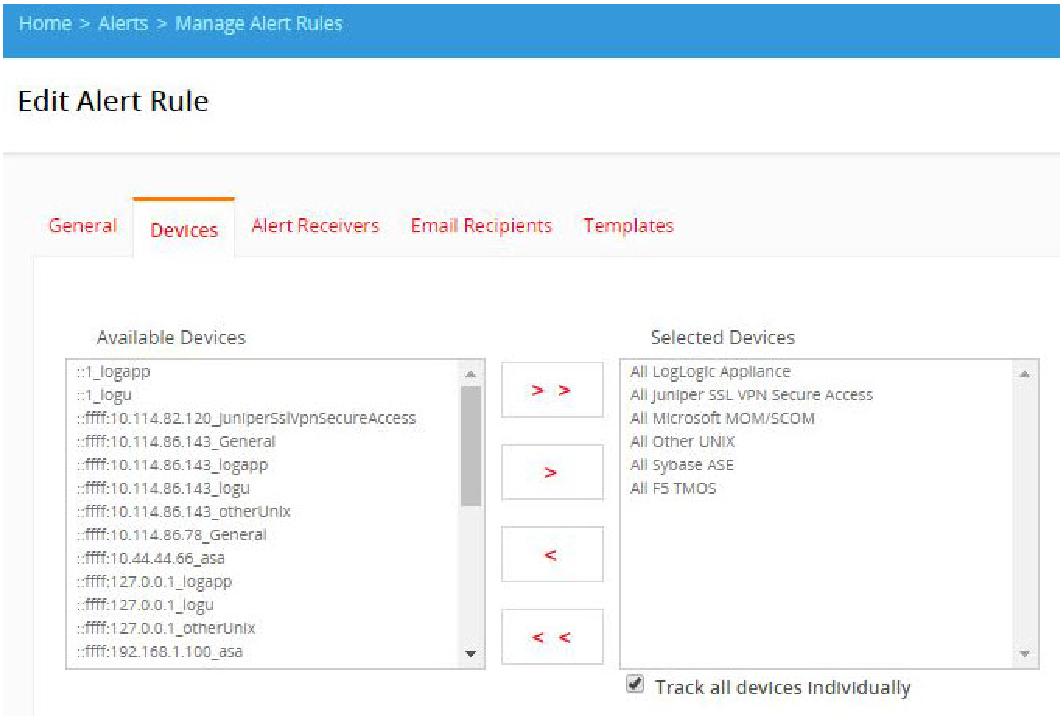
   b) In the **Available Devices** text block, select the appropriate log sources (i.e., devices) you want to monitor and be alerted on when an alert rule is triggered.

   > 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 image shows the **Devices** tab for the selected alert.

*Available and Selected Devices*



Available Devices

::1_logapp
::1_logu
::ffff:10.114.82.120_JuniperSslVpnSecureAccess
::ffff:10.114.86.143_General
::ffff:10.114.86.143_logapp
::ffff:10.114.86.143_logu
::ffff:10.114.86.143_otherUnix
::ffff:10.114.86.78_General
::ffff:10.44.44.66_asa
::ffff:127.0.0.1_logapp
::ffff:127.0.0.1_logu
::ffff:127.0.0.1_otherUnix
::ffff:192.168.1.100_asa

Selected Devices

All LogLogic Appliance
All Juniper SSL VPN Secure Access
All Microsoft MOM/SCOM
All Other UNIX
All Sybase ASE
All F5 TMOS

☑ Track all devices individually

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.

      The **Available Users** text block lists all of the user accounts on the Appliance.
   c) Click **Add All** or **Add Selected User(s)**.
7. Click **Update**.

## Viewing Compliance Suite Alert Results

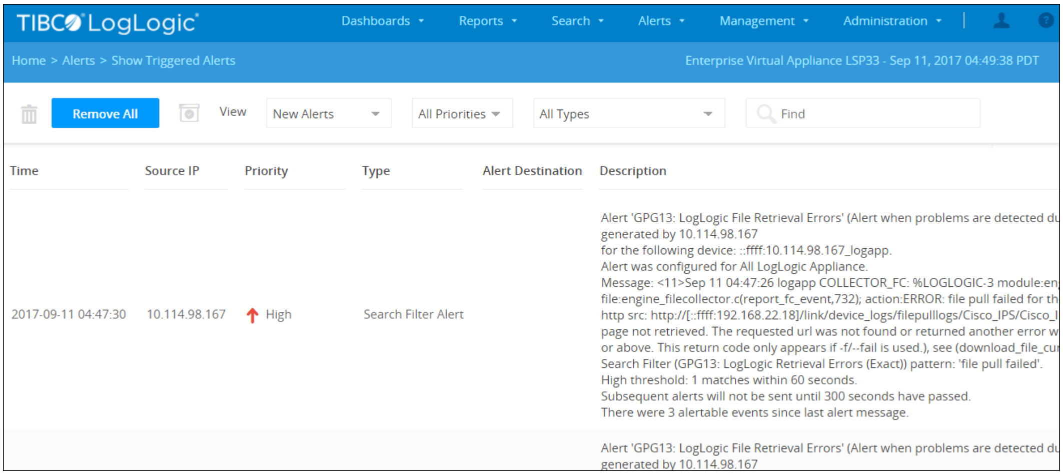
After you have enabled at least one alert, and that alert is triggered, you can view the results.

### Procedure

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

   Following figure shows a cropped version of the **Show Triggered Alert** page.

*Aggregated Alert Log*



| Time | Source IP | Priority | Type | Alert Destination | Description |
|---|---|---|---|---|---|
| 2017-09-11 04:47:30 | 10.114.98.167 | ↑ High | Search Filter Alert | | Alert 'GPG13: LogLogic File Retrieval Errors' (Alert when problems are detected du<br>generated by 10.114.98.167<br>for the following device: ::ffff:10.114.98.167_logapp.<br>Alert was configured for All LogLogic Appliance.<br>Message: <11>Sep 11 04:47:26 logapp COLLECTOR_FC: %LOGLOGIC-3 module:en<br>file:engine_filecollector.c(report_fc_event,732); action:ERROR: file pull failed for th<br>http src: http://[::ffff:192.168.22.18]/link/device_logs/filepulllogs/Cisco_IPS/Cisco_I<br>page not retrieved. The requested url was not found or returned another error w<br>or above. This return code only appears if -f/--fail is used.), see (download_file_cu<br>Search Filter (GPG13: LogLogic Retrieval Errors (Exact)) pattern: 'file pull failed'.<br>High threshold: 1 matches within 60 seconds.<br>Subsequent alerts will not be sent until 300 seconds have passed.<br>There were 3 alertable events since last alert message. |
| | | | | | Alert 'GPG13: LogLogic File Retrieval Errors' (Alert when problems are detected du<br>generated by 10.114.98.167 |

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. Select the check box 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.

# TIBCO LogLogic Reports and Alerts for GPG13

- TIBCO LogLogic Reports for GPG13
- TIBCO LogLogic Alerts for GPG13

## TIBCO LogLogic Reports for GPG13

All TIBCO LogLogic reports can be used to monitor regular user activity, as well as the activity and results of system and network administrators.

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 1 | GPG13: Account Activities on UNIX Servers | Displays all accounts activities on UNIX servers to ensure authorized and appropriate access. |
| 2 | GPG13: Account Activities on Windows Servers | Displays all accounts activities on Windows servers to ensure authorized and appropriate access. |
| 3 | GPG13: Windows Group Members Added | Displays all accounts added to groups on the Windows servers to ensure appropriate access. |
| 4 | GPG13: Accounts Changed on UNIX Servers | Displays all accounts changed on UNIX servers to ensure authorized and appropriate access. |
| 5 | GPG13: Accounts Changed on Windows Servers | Displays all accounts changed on Windows servers to ensure authorized and appropriate access. |
| 6 | GPG13: Accounts Created on UNIX Servers | Displays all accounts created on UNIX servers to ensure authorized and appropriate access. |
| 7 | GPG13: Accounts Created on Windows Servers | Displays all accounts created on Windows servers to ensure authorized and appropriate access. |
| 8 | GPG13: Accounts Deleted on UNIX Servers | Displays all accounts deleted on UNIX servers to ensure authorized and appropriate access. |
| 9 | GPG13: Accounts Deleted on Windows Servers | Displays all accounts deleted on Windows servers to ensure authorized and appropriate access. |
| 10 | GPG13: Windows Accounts Enabled | Displays all accounts enabled on Windows servers to ensure authorized and appropriate access. |
| 11 | GPG13: Network Traffic per Rule - Juniper Firewall | Displays all network traffic flowing through each rule in a network policy to ensure appropriate access. |
| 12 | GPG13: Windows Group Members Deleted | Displays all accounts removed from groups on the Windows servers to ensure appropriate access. |
| 13 | GPG13: Escalated Privilege Activities on Servers | Displays all privilege escalation activities performed on servers to ensure appropriate access. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 14 | GPG-13: F5 BIG-IP TMOS Ports Denied Access | Displays the applications that have been denied access the most by the F5 BIG-IP TMOS. |
| 15 | GPG13: F5 BIG-IP TMOS Restarted | Displays all events when the F5 BIG-IP TMOS has been restarted. |
| 16 | GPG13: Failed Logins | Displays all failed login attempts to review any access violations or unusual activity. |
| 17 | GPG13: Failed Windows Events Summary | Displays summary of all failed access-related Windows events. |
| 18 | GPG13: Files Accessed on Servers | Displays all files accessed on servers to ensure appropriate access. |
| 19 | GPG13: Group Activities on UNIX Servers | Displays all group activities on UNIX servers to ensure authorized and appropriate access. |
| 20 | GPG13: Group Activities on Windows Servers | Displays all group activities on Windows servers to ensure authorized and appropriate access. |
| 21 | GPG13: Groups Created on UNIX Servers | Displays all groups created on UNIX servers to ensure authorized and appropriate access. |
| 22 | GPG13: Groups Created on Windows Servers | Displays all groups created on Windows servers to ensure authorized and appropriate access. |
| 23 | GPG13: Groups Deleted on UNIX Servers | Displays all groups deleted on UNIX servers to ensure authorized and appropriate access. |
| 24 | GPG13: Groups Deleted on Windows Servers | Displays all groups deleted on Windows servers to ensure authorized and appropriate access. |
| 25 | GPG13: Last Activities Performed by Administrators | Displays the latest activities performed by administrators and root users to ensure appropriate access. |
| 26 | GPG13: Last Activities Performed by All Users | Displays the latest activities performed by all users to ensure appropriate access. |
| 27 | GPG13: Logins by Authentication Type | Displays all logins categorized by the authentication type. |
| 28 | GPG13: Windows New Services Installed | Displays a list of new services installed on Windows servers to ensure authorized access. |
| 29 | GPG13: Password Changes on Windows Servers | Displays all password change activities on Windows servers to ensure authorized and appropriate access. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 30 | GPG13: Periodic Review of Log Reports | Displays all review activities performed by administrators to ensure review for any access violations. |
| 31 | GPG13: Periodic Review of User Access Logs | Displays all review activities performed by administrators to ensure review for any access violations. |
| 32 | GPG13: Permissions Modified on Windows Servers | Displays all permission modification activities on Windows Servers to ensure authorized access. |
| 33 | GPG13: Policies Modified on Windows Servers | Displays all policy modification activities on Windows servers to ensure authorized and appropriate access. |
| 34 | GPG13: Windows Programs Accessed | Displays all programs started and stopped on servers to ensure appropriate access. |
| 35 | GPG13: Successful Logins | Displays successful logins to ensure only authorized personnel have access. |
| 36 | GPG13: Trusted Domain Created on Windows Servers | Displays all trusted domains created on Windows servers to ensure authorized and appropriate access. |
| 37 | GPG13: Trusted Domain Deleted on Windows Servers | Displays all trusted domains deleted on Windows servers to ensure authorized and appropriate access. |
| 38 | GPG13: Unauthorized Logins | Displays all logins from unauthorized users to ensure appropriate access to data. |
| 39 | GPG13: Unencrypted Logins | Displays all unencrypted logins to ensure secure access to data. |
| 40 | GPG13: Users Created on Servers | Displays all users created on servers to ensure authorized and appropriate access. |
| 41 | GPG13: Users Removed from Servers | Displays all users removed from servers to ensure timely removal of terminated users. |
| 42 | GPG13: Windows Events by Users | Displays a summary of access-related Windows events by source and target users. |
| 43 | GPG13: Windows Events Summary | Displays a summary of access-related Windows events by count. |
| 44 | GPG13: Active Connections for Cisco PIX | Displays all currently active firewall connections for Cisco PIX. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 45 | GPG13: Active Connections for Cisco ASA | Displays all currently active firewall connections for Cisco ASA. |
| 46 | GPG13: Denied Inbound Connections - Cisco ASA | Displays all inbound connections that have been denied by the Cisco ASA devices. |
| 47 | GPG13: Denied Inbound Connections - Juniper Firewall | Displays all inbound connections that have been denied by the Juniper Firewalls. |
| 48 | GPG13: Denied Outbound Connections - Cisco PIX | Displays all outbound connections that have been denied by the Cisco PIX. |
| 49 | GPG13: Denied Outbound Connections - Juniper Firewall | Displays all outbound connections that have been denied by the Juniper Firewall. |
| 50 | GPG13: Ports Denied Access - Juniper Firewall | Displays the applications that have been denied access the most by the Juniper Firewall. |
| 51 | GPG13: Ports Allowed Access - Cisco PIX | Displays all connections passed through the Cisco PIX by port. |
| 52 | GPG13: Most Active Ports Through Firewall - Cisco PIX | Displays the most active ports used through the Cisco PIX firewall. |
| 53 | GPG13: Network Traffic per Rule - Check Point | Displays all network traffic flowing through each rule in a network policy to ensure appropriate access. |
| 54 | GPG13: Applications Under Attack | Displays all applications under attack as well as the attack signatures. |
| 55 | GPG13: Attackers by Service | Displays all attack source IP address and service ports. |
| 56 | GPG13: Attackers by Signature | Displays all attack source IP address and signatures. |
| 57 | GPG13: Attacks Detected | Displays all IDS attacks detected against servers and applications. |
| 58 | GPG13: Sensors Generating Alerts | Displays the IDS sensors that generated the most alerts. |
| 59 | GPG13: Servers Under Attack | Displays all servers under attack. |
| 60 | GPG13: Source of Attacks | Displays the sources that have initiated the most attacks. |
| 61 | GPG13: Domains Sending the Most Email - Exchange 2000/2003 | Displays the top domains sending email. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 62 | GPG13: Email Recipients Receiving the Most Emails by Count - Exchange 2000/2003 | Displays the email recipients who receiving the most emails by count. |
| 63 | GPG13: Email Recipients Receiving the Most Emails by Size - Exchange 2000/2003 | Displays the email recipients who received the most emails by mail size. |
| 64 | GPG13: Email Senders Sending the Most Emails by Count - Exchange 2000/2003 | Displays the email senders who sent the most emails by count. |
| 65 | GPG13: Email Senders Sending the Most Emails by Size - Exchange 2000/2003 | Displays the email senders who sent the most emails by mail size. |
| 66 | GPG13: Most Active Email Senders - Exchange 2000/2003 | Displays the most active email senders based on activity. |
| 67 | GPG13: Most Used Mail Commands - Exchange 2000/2003 | Displays the most used email protocol commands on Microsoft Exchange servers. |
| 68 | GPG13: Recipient Domains Experiencing Delay - Exchange 2000/2003 | Displays the recipient domains that have experienced the most delivery delays. |
| 69 | | |
| 70 | GPG13: Sender and Recipients Exchanging the Most Emails - Exchange 2000/2003 | Displays the top email sender and recipient combinations. |
| 71 | GPG13: Source IP Sending To Most Recipients - Exchange 2000/2003 | Displays IP addresses that are sending to the most recipients. |
| 72 | GPG13: Active VPN Connections for Cisco VPN Concentrators | Displays all currently active VPN connections for Cisco VPN Concentrators. |
| 73 | GPG13: Active VPN Connections for Nortel Contivity | Displays all currently active VPN connections for Nortel Contivity VPN devices. |
| 74 | GPG13: Bandwidth Usage by User | Displays users who are using the most bandwidth. |
| 75 | GPG13: VPN Connection Average Bandwidth | Displays the average bandwidth for VPN connections. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 76 | GPG13: VPN Connection Average Duration | Displays the average duration of VPN connections. |
| 77 | GPG13: VPN Connection Disconnect Reasons | Displays the disconnect reasons for VPN connections. |
| 78 | GPG13: VPN Connections by Users | Displays users who are made the most connections. |
| 79 | GPG13: Denied Connections by IP Addresses - Check Point | Displays remote IP addresses with the most denied connections from Check Point. |
| 80 | GPG13: VPN Denied Connections by Users | Displays users with the most denied connections. |
| 81 | GPG13: VPN Sessions by Destination IPs | Displays all VPN sessions categorized by destination IP addresses. |
| 82 | GPG13: VPN Sessions by Source IPs | Displays all VPN sessions categorized by source IP addresses. |
| 83 | GPG13: VPN Sessions by Users | Displays all VPN sessions categorized by authenticated users. |
| 84 | GPG13: VPN Users Accessing Corporate Network | Displays all users logging into the corporate network through Virtual Private Network to ensure appropriate access. |
| 85 | GPG13: Allowed URLs by Source IPs | Displays successful access to URLs by source IP addresses. |
| 86 | GPG13: Allowed URLs by Source Users | Displays successful access to URLs by source users. |
| 87 | GPG13: Blocked URLs by Source IPs | Displays URLs that have been blocked by source IP addresses. |
| 88 | GPG13: Blocked URLs by Source Users | Displays URLs that have been blocked by source users. |
| 89 | GPG13: Files Downloaded through the Web | Displays all web-based downloads ensure authorized and appropriate access. |
| 90 | GPG13: Files Uploaded through the Web | Displays all web-based uploads to ensure only authorized data can be uploaded. |
| 91 | GPG13: Peer Servers and Status | Displays all web servers providing data for cache servers and the status of requests. |
| 92 | GPG13: Web URLs Visited | Displays URLs that have been visited. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 93 | GPG13: Users Using the Proxies | Displays users who have been surfing the web through the proxy servers. |
| 94 | GPG13: Web Access from All Users | Displays all web-based access by all users for regular reviews and updates. |
| 95 | GPG13: Web Access to Applications | Displays all web-based access to applications to ensure appropriate and authorized access. |
| 96 | GPG13: NetApp Filer Snapshot Error | Displays events that indicate backup on the NetApp Filer has failed. |
| 97 | GPG13: Cisco Routers and Switches Restart | Displays all Cisco routers and switches restart activities to detect unusual activities. |
| 98 | GPG13: Juniper Firewall Reset Accepted | Displays events that indicate the Juniper Firewall has been reset to its factory default state. |
| 99 | GPG13: Juniper Firewall Reset Imminent | Displays events that indicate the Juniper Firewall is reset to its factory default state. |
| 100 | GPG13: LogLogic File Retrieval Errors | Displays all errors while retrieving log files from devices, servers and applications. |
| 101 | GPG13: LogLogic Message Routing Errors | Displays all log forwarding errors on the LogLogic appliance to ensure all logs are archived properly. |
| 102 | GPG13: Windows Audit Logs Cleared | Displays all audit logs clearing activities on Windows servers to detect access violations or an unusual activity. |
| 103 | GPG13: Windows Servers Restarted | Displays all Windows server restart activities to detect unusual activities. |
| 104 | GPG13: Check Point Configuration Changes | Displays all Check Point audit events related to configuration changes. |
| 105 | GPG13: Check Point Objects Created | Displays all Check Point audit events related to object creation in policies. |
| 106 | GPG13: Check Point Objects Deleted | Displays all Check Point audit events related to policy objects deleted. |
| 107 | GPG13: Check Point Objects Modified | Displays all Check Point audit events related to policy objects modified. |
| 108 | GPG13: Check Point SIC Revoked | Displays all Check Point audit events related to the security certificate being revoked. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 109 | GPG13: Creation and Deletion of System Level Objects: AIX Audit | Displays AIX audit events related to creation and deletion of system-level objects. |
| 110 | GPG13: Creation and Deletion of System Level Objects: DB2 Database | Displays DB2 database events related to creation and deletion of system-level objects. |
| 111 | GPG13: Creation and Deletion of System Level Objects: HP-UX Audit | Displays HP-UX audit events related to creation and deletion of system-level objects. |
| 112 | GPG13: Creation and Deletion of System Level Objects: Oracle | Displays Oracle database events related to creation and deletion of system-level objects. |
| 113 | GPG13: Creation and Deletion of System Level Objects: Solaris BSM | Displays Solaris BSM events related to creation and deletion of system-level objects. |
| 114 | GPG13: Creation and Deletion of System Level Objects: SQL Server | Displays Microsoft SQL Server events related to creation and deletion of system-level objects. |
| 115 | GPG13: Creation and Deletion of System Level Objects: Windows | Displays all Windows events related to creation and deletion of system-level objects. |
| 116 | GPG13: DB2 Database Configuration Changes | Displays DB2 database configuration changes. |
| 117 | GPG13: DB2 Database Successful Logins | Displays successful DB2 database logins. |
| 118 | GPG13: Microsoft SQL Server Database Failed Logins | Displays failed Microsoft SQL Server database logins. |
| 119 | GPG13: Decru DataFort Cryptographic Key Events | Displays events related to cryptographic key handling. |
| 120 | GPG13: Decru DataFort Zeroization Events | Displays events related to Decru DataFort zeroization. |
| 121 | GPG13: i5/OS Access Control List Modifications | Displays i5/OS events related to access control list modification. |
| 122 | GPG13: i5/OS Audit Configuration Changes | Displays all audit configuration changes on i5/OS. |
| 123 | GPG13: i5/OS DST Password Reset | Displays i5/OS events related to the reset of the DST (Dedicated Service Tools) password. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 124 | GPG13: i5/OS Internet Security Management Events | Displays i5/OS events related to Internet Security Management (IPSec/VPN). |
| 125 | GPG13: i5/OS Key Ring File Events | Displays i5/OS key ring file events (cryptographic key management). |
| 126 | GPG13: i5/OS Network Authentication Events | Displays i5/OS network authentication events. |
| 127 | GPG13: i5/OS Object Access | Displays i5/OS events related to object access. |
| 128 | GPG13: i5/OS Object Creation and Deletion | Displays i5/OS events related to object creation and deletion. |
| 129 | GPG13: Ports Denied Access - F5 BIG-IP TMOS | Displays the applications that have been denied access the most by the F5 BIG-IP TMOS. |
| 130 | GPG13: i5/OS Restore Events | Displays i5/OS events related to object, program, and profile restoration. |
| 131 | GPG13: i5/OS Server Security User Information Actions | Displays i5/OS events related to server security user information actions. |
| 132 | GPG13: i5/OS System Management Changes | Displays i5/OS events related to system management changes. |
| 133 | GPG13: i5/OS User Profile Creation, Modification, or Restoration | Displays i5/OS events related to user profile creation, modification, or restoration. |
| 134 | GPG13: Oracle Database Configuration Changes | Displays Oracle database configuration changes. |
| 135 | GPG13: Oracle Database Successful Logins | Displays successful Oracle database logins. |
| 136 | GPG13: Sybase ASE Database Backup and Restoration | Displays Sybase ASE DUMP and LOAD events. |
| 137 | GPG13: Sybase ASE Database Create Events | Displays Sybase ASE events involving the CREATE statement. |
| 138 | GPG13: Sybase ASE Database Data Access | Displays Sybase ASE events involving the SELECT statement. |
| 139 | GPG13: Sybase ASE Database Drop Events | Displays Sybase ASE events involving the DROP statement. |
| 140 | GPG13: Sybase ASE Failed Logins | Displays failed Sybase ASE database logins. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 141 | GPG13: Sybase ASE Successful Logins | Displays successful Sybase ASE database logins. |
| 142 | GPG13: Tripwire Modifications, Additions, and Deletions | Displays system modifications, additions, and deletions detected by Tripwire. |
| 143 | GPG13: Administrator Logins on Windows Servers | Displays all logins with the administrator account on Windows servers. |
| 144 | GPG13: Root Logins | Displays root logins. |
| 145 | GPG13: Unencrypted Network Services - Nortel | Displays Nortel firewall traffic containing unencrypted network services. |
| 146 | GPG13: Microsoft SQL Server Data Access | Displays data access events on Microsoft SQL Server databases. |
| 147 | GPG13: Microsoft SQL Server Database Successful Logins | Displays successful Microsoft SQL Server database logins. |
| 148 | GPG13: Microsoft SQL Server Database Permission Events | Displays events related to Microsoft SQL Server database permission modifications. |
| 149 | GPG13: Microsoft SQL Server Database User Additions and Deletions | Displays Microsoft SQL Server events related to creation and deletion of database users. |
| 150 | GPG13: Microsoft SQL Server Password Changes | Displays password changes for Microsoft SQL Server database accounts. |
| 151 | GPG13: Juniper SSL VPN Successful Logins | Displays successful connections through the Juniper SSL VPN. |
| 152 | GPG13: Denied Inbound Connections - Check Point | Displays all inbound connections that have been denied by the Check Point devices. |
| 153 | GPG13: Unencrypted Network Services - Juniper Firewall | Displays Juniper Firewall traffic containing unencrypted network services. |
| 154 | GPG13: Ports Allowed Access - Juniper Firewall | Displays all connections passed through the Juniper Firewall by port. |
| 155 | GPG13: UNIX Failed Logins | Displays failed UNIX logins for known and unknown users. |
| 156 | GPG13: Ports Denied Access - Cisco ASA | Displays the applications that have been denied access the most by the Cisco ASA. |
| 157 | GPG13: Ports Denied Access - Cisco PIX | Displays the applications that have been denied access the most by the Cisco PIX. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 158 | GPG13: Ports Denied Access - Cisco FWSM | Displays the applications that have been denied access the most by the Cisco FWSM. |
| 159 | GPG13: Active Connections for Cisco FWSM | Displays all currently active firewall connections for Cisco FWSM. |
| 160 | GPG13: Active Directory System Changes | Displays changes made within Active Directory. |
| 161 | GPG13: Symantec AntiVirus: Attacks by Threat Name | Displays Symantec AntiVirus attacks by threat name. |
| 162 | GPG13: Symantec AntiVirus: Attacks Detected | Displays attacks detected by Symantec AntiVirus. |
| 163 | GPG13: Symantec AntiVirus: Updated | Displays updates to Symantec AntiVirus. |
| 164 | GPG13: Symantec AntiVirus: Scans | Displays scans using Symantec AntiVirus. |
| 165 | GPG13: McAfee AntiVirus: Attacks by Event ID | Displays McAfee AntiVirus attacks by Event ID. |
| 166 | GPG13: McAfee AntiVirus: Attacks by Threat Name | Displays McAfee AntiVirus attacks by threat name. |
| 167 | GPG13: McAfee AntiVirus: Attacks Detected | Displays attacks detected by McAfee AntiVirus. |
| 168 | GPG13: Check Point Management Station Login | Displays all login events to the Check Point management station. |
| 169 | GPG13: Cisco Switch Policy Changes | Displays all configuration changes to the Cisco router and switch policies. |
| 170 | GPG13: Cisco Line Protocol Status Changes | Displays all Cisco line protocol up and down events. |
| 171 | GPG13: Cisco Link Status Changes | Displays all Cisco link up and down events. |
| 172 | GPG13: Cisco Peer Reset/Reload | Displays all Cisco Peer reset and reload events. |
| 173 | GPG13: Cisco Peer Supervisor Status Changes | Displays all Cisco Peer Supervisor status changes. |
| 174 | GPG13: Juniper Firewall Escalated Privilege | Displays events related to users having escalated privileges in the Juniper Firewall. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 175 | GPG13: Juniper Firewall Restarted | Displays all Juniper Firewall restart events. |
| 176 | GPG13: Juniper Firewall VPN Tunnel Status Change | Displays events when the Juniper Firewall VPN Tunnel is setup or taken down. |
| 177 | GPG13: Microsoft SQL Server Backup Failed | Displays all Microsoft SQL Server backup failures. |
| 178 | GPG13: Microsoft SQL Server Restore Failed | Displays all Microsoft SQL Server restore failure events. |
| 179 | GPG13: Microsoft SQL Server Schema Corruption | Displays all schema corruption events on Microsoft SQL Server databases. |
| 180 | GPG13: Microsoft SQL Server Shutdown by Reason | Displays all Microsoft SQL Server shutdown events by reason. |
| 181 | GPG13: Windows Software Update Activities | Displays all events related to the system's software or patch update. |
| 182 | GPG13: Windows Software Update Failures | Displays all failed events related to the system's software or patch update. |
| 183 | GPG13: Windows Software Update Successes | Displays all successful events related to the system's software or patch update. |
| 184 | GPG13: Juniper SSL VPN (Secure Access) Successful Logins | Displays all successfull logins through the Juniper SSL VPN (Secure Access). |
| 185 | GPG13: TrendMicro OfficeScan: Attacks Detected | Displays attacks detected by TrendMicro OfficeScan. |
| 186 | GPG13: TrendMicro OfficeScan: Attacks Detected by Threat Name | Displays attacks detected by TrendMicro OfficeScan by threat name. |
| 187 | GPG13: TrendMicro Control Manager: Attacks Detected | Displays attacks detected by TrendMicro Control Manager. |
| 188 | GPG13: TrendMicro Control Manager: Attacks Detected by Threat Name | Displays attacks detected by TrendMicro Control Manager by threat name. |
| 189 | GPG13: Ports Denied Access - Check Point | Displays the applications that have been denied access the most by the Check Point. |
| 190 | GPG13: Ports Denied Access - Fortinet | Displays the applications that have been denied access the most by the Fortinet. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 191 | GPG13: Ports Denied Access - Juniper RT Flow | Displays the applications that have been denied access the most by the Juniper RT Flow. |
| 192 | GPG13: Ports Denied Access - Nortel | Displays the applications that have been denied access the most by the Nortel. |
| 193 | GPG13: Network Traffic per Rule - Nortel | Displays all network traffic flowing through each rule in a network policy to ensure appropriate access. |
| 194 | GPG13: Denied Connections by IP Addresses - Cisco ASA | Displays remote IP addresses with the most denied connections from Cisco ASA. |
| 195 | GPG13: Denied Connections by IP Addresses - Cisco FWSM | Displays remote IP addresses with the most denied connections from Cisco FWSM. |
| 196 | GPG13: Denied Connections by IP Addresses - Cisco PIX | Displays remote IP addresses with the most denied connections from Cisco PIX. |
| 197 | GPG13: Denied Connections by IP Addresses - Nortel | Displays remote IP addresses with the most denied connections from Nortel. |
| 198 | GPG13: Denied Inbound Connections - Cisco FWSM | Displays all inbound connections that have been denied by the Cisco FWSM devices. |
| 199 | GPG13: Denied Inbound Connections - Cisco PIX | Displays all inbound connections that have been denied by the Cisco PIX devices. |
| 200 | GPG13: Denied Outbound Connections - Cisco ASA | Displays all outbound connections that have been denied by the Cisco ASA. |
| 201 | GPG13: Denied Outbound Connections - Cisco FWSM | Displays all outbound connections that have been denied by the Cisco FWSM. |
| 202 | GPG13: Denied Outbound Connections - Check Point | Displays all outbound connections that have been denied by the Check Point. |
| 203 | GPG13: Ports Allowed Access - Check Point | Displays all connections passed through the Check Point by port. |
| 204 | GPG13: Ports Allowed Access - Cisco ASA | Displays all connections passed through the Cisco ASA by port. |
| 205 | GPG13: Ports Allowed Access - Cisco FWSM | Displays all connections passed through the Cisco FWSM by port. |
| 206 | GPG13: Ports Allowed Access - Fortinet | Displays all connections passed through the Fortinet by port. |
| 207 | GPG13: Ports Allowed Access - Juniper RT Flow | Displays all connections passed through the Juniper RT Flow by port. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 208 | GPG13: Ports Allowed Access - Nortel | Displays all connections passed through the Nortel by port. |
| 209 | GPG13: Unencrypted Network Services - Check Point | Displays Check Point firewall traffic containing unencrypted network services. |
| 210 | GPG13: Unencrypted Network Services - Cisco ASA | Displays Cisco ASA firewall traffic containing unencrypted network services. |
| 211 | GPG13: Unencrypted Network Services - Cisco FWSM | Displays Cisco FWSM firewall traffic containing unencrypted network services. |
| 212 | GPG13: Unencrypted Network Services - Cisco PIX | Displays Cisco PIX firewall traffic containing unencrypted network services. |
| 213 | GPG13: Unencrypted Network Services - Fortinet | Displays Fortinet firewall traffic containing unencrypted network services. |
| 214 | GPG13: Unencrypted Network Services - Juniper RT Flow | Displays Juniper RT Flow firewall traffic containing unencrypted network services. |
| 215 | GPG13: Most Active Ports Through Firewall - Check Point | Displays the most active ports used through the Check Point firewall. |
| 216 | GPG13: Most Active Ports Through Firewall - Cisco ASA | Displays the most active ports used through the Cisco ASA firewall. |
| 217 | GPG13: Most Active Ports Through Firewall - Cisco FWSM | Displays the most active ports used through the Cisco FWSM firewall. |
| 218 | GPG13: Most Active Ports Through Firewall - Fortinet | Displays the most active ports used through the Fortinet firewall. |
| 219 | GPG13: Most Active Ports Through Firewall - Juniper Firewall | Displays the most active ports used through the Juniper Firewall. |
| 220 | GPG13: Most Active Ports Through Firewall - Nortel | Displays the most active ports used through the Nortel firewall. |
| 221 | GPG13: Active VPN Connections for RADIUS | Displays all currently active VPN connections for RADIUS Acct Client. |
| 222 | GPG13: Accepted VPN Connections - RADIUS | Displays all users connected to the internal network through the RADIUS VPN. |
| 223 | GPG13: Denied VPN Connections - RADIUS | Displays all users denied access to the internal network by the RADIUS VPN. |
| 224 | GPG13: RACF Accounts Created | Displays all accounts created on RACF servers to ensure authorized and appropriate access. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 225 | GPG13: RACF Accounts Deleted | Displays all accounts deleted on RACF servers to ensure authorized and appropriate access. |
| 226 | GPG13: RACF Accounts Modified | Displays all events when a network user profile has been modified. |
| 227 | GPG13: RACF Successful Logins | Displays successful logins to ensure only authorized personnel have access. |
| 228 | GPG13: RACF Failed Logins | Displays all failed login attempts to review any access violations or unusual activity. |
| 229 | GPG13: RACF Files Accessed | Displays all files accessed on RACF servers to ensure appropriate access. |
| 230 | GPG13: RACF Permissions Changed | Displays all permission modification activities on RACF to ensure authorized access. |
| 231 | GPG13: RACF Password Changed | Displays all password change activities on RACF servers to ensure authorized and appropriate access. |
| 232 | GPG13: RACF Process Started | Displays all processes started on the RACF servers. |
| 233 | GPG13: Email Recipients Receiving the Most Emails by Count - Exchange 2007/10 | Displays the email recipients who receiving the most emails by count. |
| 234 | GPG13: Email Senders Sending the Most Emails by Count - Exchange 2007/10 | Displays the email senders who sent the most emails by count. |
| 235 | GPG13: Email Senders Sending the Most Emails by Size - Exchange 2007/10 | Displays the email senders who sent the most emails by mail size. |
| 236 | GPG13: Microsoft SQL Server Configuration Changes | Displays Microsoft SQL database configuration changes. |
| 237 | GPG13: DB2 Database Backup Failed | Displays all IBM DB2 Database Server backup failures. |
| 238 | GPG13: DB2 Database Failed Logins | Displays all failed login attempts to review any access violations or unusual activity. |
| 239 | GPG13: DB2 Database Restore Failed | Displays all IBM DB2 Database restore failure events. |
| 240 | GPG13: DB2 Database User Additions and Deletions | Displays IBM DB2 Database events related to creation and deletion of database users. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 241 | GPG13: DB2 Database Stop and Start Events | Displays DB2 database events related to starting and stopping the database. |
| 242 | GPG13: Oracle Database Data Access | Displays data access events on Oracle databases. |
| 243 | GPG13: Oracle Database Permission Events | Displays events related to Oracle Server database role and privilege management. |
| 244 | GPG13: Oracle Database Shutdown | Displays Oracle database events related to shutting down the server. |
| 245 | GPG13: Oracle Database User Additions and Deletions | Displays Oracle database events related to creation and deletion of database users. |
| 246 | GPG13: Oracle Database Failed Logins | Displays all failed login attempts to the Oracle database. |
| 247 | GPG13: Guardium SQL Guard Configuration Changes | Displays all configuration changes on the Guardium SQL Guard database. |
| 248 | GPG13: Guardium SQL Guard Data Access | Displays all select statements made on Guardium SQL Server. |
| 249 | GPG13: Guardium SQL Guard Logins | Displays all login attempts to the Guardium SQL Server database. |
| 250 | GPG13: Guardium SQL Guard Startup or Shutdown | Displays all startup and shutdown events on Guardium SQL Server. |
| 251 | GPG13: vCenter Change Attributes | Modification of VMware vCenter and VMware ESX properties. |
| 252 | GPG13: vCenter Datastore Events | Displays create, modify, and delete datastore events on VMware vCenter. |
| 253 | GPG13: vCenter Failed Logins | Failed logins to the VMware vCenter console. |
| 254 | GPG13: vCenter Modify Firewall Policy | Displays changes to the VMware ESX allowed services firewall policy. |
| 255 | GPG13: vCenter Shutdown or Restart of ESX Server | VMware ESX Server is shutdown or restarted from VMware vCenter console. |
| 256 | GPG13: vCenter Successful Logins | Successful logins to the VMware vCenter console. |
| 257 | GPG13: vCenter User Permission Change | A permission role has been added, changed, removed, or applied to a user on VMware vCenter server. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 258 | GPG13: vCenter Virtual Machine Created | Virtual machine has been created from VMware vCenter console. |
| 259 | GPG13: vCenter Virtual Machine Deleted | Virtual machine has been deleted or removed from VMware vCenter console. |
| 260 | GPG13: vCenter Virtual Machine Shutdown | Virtual machine has been shutdown or paused from VMware vCenter console. |
| 261 | GPG13: vCenter Virtual Machine Started | Virtual machine has been started or resumed from VMware vCenter console. |
| 262 | GPG13: vCenter vSwitch Added, Changed or Removed | vSwitch on VMware ESX server has been added, modified or removed from the VMware vCenter console. |
| 263 | GPG13: vCenter Data Move | Entity has been moved within the VMware vCenter infrastructure. |
| 264 | GPG13: vCenter Restart ESX Services | VMware vCenter restarted services running on VMware ESX Server. |
| 265 | GPG13: vCenter Resource Usage Change | Resources have changed on VMware vCenter. |
| 266 | GPG13: vCloud Failed Logins | Failed logins to the VMware vCloud Director console. |
| 267 | GPG13: vCloud Organization Created | Vmware vCloud Director organization created events. |
| 268 | GPG13: vCloud Organization Deleted | VMware vCloud Director organization deleted events. |
| 269 | GPG13: vCloud Organization Modified | VMware vCloud Director organization modified events. |
| 270 | GPG13: vCloud Successful Logins | Successful logins to the VMware vCloud Director console. |
| 271 | GPG13: vCloud User Created | VMware vCloud Director user created events. |
| 272 | GPG13: vCloud User Deleted or Removed | VMware vCloud Director users have been deleted or removed from the system. |
| 273 | GPG13: vCloud vApp Created, Modified, or Deleted | VMWare vCloud Director vApp created, deleted, and modified events. |
| 274 | GPG13: vCloud vDC Created, Modified, or Deleted | VMWare vCloud Director virtual datacenter created, modified, or deleted events. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 275 | GPG13: ESX Accounts Activities | Displays all accounts activities on VMware ESX servers to ensure authorized and appropriate access. |
| 276 | GPG13: ESX Accounts Created | Displays all accounts created on VMware ESX servers to ensure authorized and appropriate access. |
| 277 | GPG13: ESX Accounts Deleted | Displays all accounts deleted on VMware ESX servers to ensure authorized and appropriate access. |
| 278 | GPG13: ESX Failed Logins | Failed VMware ESX logins for known user. |
| 279 | GPG13: ESX Group Activities | Displays all group activities on VMware ESX servers to ensure authorized and appropriate access. |
| 280 | GPG13: ESX Logins Succeeded | Displays successful logins to VMware ESX to ensure only authorized personnel have access. |
| 281 | GPG13: vShield Edge Configuration Changes | Displays changes to VMware vShield Edge policies. |
| 282 | GPG13: ESX Logins Failed Unknown User | Failed VMware ESX logins for unknown user. |
| 283 | GPG13: ESX Kernel log daemon terminating | Displays all VMware ESX Kernel log daemon terminating. |
| 284 | GPG13: ESX Kernel logging Stop | Displays all VMware ESX Kernel logging stops. |
| 285 | GPG13: ESX Syslogd Restart | Displays all VMware ESX syslogd restarts. |
| 286 | GPG13: Denied Connections - Cisco Router | Displays all connections that have been denied by the Cisco Router devices. |
| 287 | GPG13: Ports Denied Access - Cisco Router | Displays the applications that have been denied access the most by the Cisco Router. |
| 288 | GPG13: Sybase ASE Database Configuration Changes | Displays configuration changes to the Sybase database. |
| 289 | GPG13: Sybase ASE Database Startup or Shutdown | Displays all startup and shutdown events for the Sybase database. |
| 290 | GPG13: Sybase ASE Database User Additions and Deletions | Displays Sybase database events related to creation and deletion of database users. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 291 | GPG13: LogLogic DSM Configuration Changes | Displays all configuration changes on the LogLogic DSM database. |
| 292 | GPG13: LogLogic DSM Data Access | Displays all select statements made on LogLogic DSM database. |
| 293 | GPG13: LogLogic DSM Logins | Displays all login attempts to the LogLogic DSM database. |
| 294 | GPG13: LogLogic DSM Startup or Shutdown | Displays all startup and shutdown events on LogLogic DSM database. |
| 295 | GPG13: Microsoft Sharepoint Content Deleted | Displays all events when content has been deleted from Microsoft Sharepoint. |
| 296 | GPG13: Microsoft Sharepoint Content Updates | Displays all events when content is updated within Microsoft Sharepoint. |
| 297 | GPG13: Microsoft Sharepoint Permissions Changed | Displays all user/group permission events to Microsoft Sharepoint. |
| 298 | GPG13: Microsoft Sharepoint Policy Add, Remove, or Modify | Displays all events when a Microsoft Sharepoint policy is added, removed, or modified. |
| 299 | GPG13: Files Downloaded through Proxy | Displays all proxy-based downloads ensure authorized and appropriate access. |
| 300 | GPG13: Files Uploaded through Proxy | Displays all proxy-based uploads to ensure only authorized data can be uploaded. |
| 301 | GPG13: Web URLs Visited through Proxy | Displays URLs that have been visited through a proxy server. |
| 302 | GPG13: Guardium SQL Guard Audit Configuration Changes | Displays all configuration changes on the Guardium SQL Guard Audit database. |
| 303 | GPG13: Guardium SQL Guard Audit Logins | Displays all login attempts to the Guardium SQL Server Audit database. |
| 304 | GPG13: Guardium SQL Guard Audit Startup or Shutdown | Displays all startup and shutdown events on Guardium SQL Audit Server. |
| 305 | GPG13: Guardium SQL Guard Audit Data Access | Displays all select statements made on Guardium SQL Audit Server. |
| 306 | GPG13: Microsoft Operations Manager - Failed Windows Events | Displays summary of all failed access-related Windows events. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 307 | GPG13: Microsoft Operations Manager - Windows Accounts Activities | Displays all accounts activities on Windows servers to ensure authorized and appropriate access. |
| 308 | GPG13: Microsoft Operations Manager - Windows Accounts Changed | Displays all accounts changed on Windows servers to ensure authorized and appropriate access. |
| 309 | GPG13: Microsoft Operations Manager - Windows Accounts Created | Displays all accounts created on Windows servers to ensure authorized and appropriate access. |
| 310 | GPG13: Microsoft Operations Manager - Windows Accounts Enabled | Displays all accounts enabled on Windows servers to ensure authorized and appropriate access. |
| 311 | GPG13: Microsoft Operations Manager - Windows Events by Users | Displays a summary of access-related Windows events by source and target users. |
| 312 | GPG13: Microsoft Operations Manager - Windows Events Summary | Displays a summary of access-related Windows events by count. |
| 313 | GPG13: Microsoft Operations Manager - Windows Password Changes | Displays all password change activities on Windows servers to ensure authorized and appropriate access. |
| 314 | GPG13: Microsoft Operations Manager - Windows Permissions Modified | Displays all permission modification activities on Windows servers to ensure authorized access. |
| 315 | GPG13: Microsoft Operations Manager - Windows Policies Modified | Displays all policy modification activities on Windows servers to ensure authorized and appropriate access. |
| 316 | GPG13: Microsoft Operations Manager - Windows Servers Restarted | Displays all Windows server restart activities to detect unusual activities. |
| 317 | GPG13: Cisco PIX, ASA, FWSM Policy Changed | Displays all configuration changes made to the Cisco PIX, ASA, and FWSM devices. |
| 318 | GPG13: Cisco PIX, ASA, FWSM Failover Performed | Displays all logs related to performing a Cisco PIX, ASA, and FWSM failover. |
| 319 | GPG13: Cisco PIX, ASA, FWSM Failover Disabled | Displays all logs related to disabling Cisco PIX, ASA, and FWSM failover capability. |
| 320 | GPG13: Ports Allowed Access - PANOS | Displays all connections passed through the Palo Alto Networks by port. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 321 | GPG13: Ports Denied Access - PANOS | Displays the applications that have been denied access the most by the Palo Alto Networks. |
| 322 | GPG13: Unencrypted Network Services - PANOS | Displays Palo Alto Networks firewall traffic containing unencrypted network services. |
| 323 | GPG13: PANOS: Attacks by Event ID | Displays Palo Alto Networks attacks by Event ID. |
| 324 | GPG13: PANOS: Attacks by Threat Name | Displays Palo Alto Networks attacks by threat name. |
| 325 | GPG13: PANOS: Attacks Detected | Displays attacks detected by Palo Alto Networks. |
| 326 | GPG13: FortiOS: Attacks by Event ID | Displays FortiOS attacks by Event ID. |
| 327 | GPG13: FortiOS: Attacks Detected | Displays attacks detected by FortiOS. |
| 328 | GPG13: FortiOS: Attacks by Threat Name | Displays FortiOS attacks by threat name. |
| 329 | GPG13: FortiOS DLP Attacks Detected | Displays all DLP attacks detected by FortiOS. |
| 330 | GPG13: Ports Allowed Access - Juniper JunOS | Displays all connections passed through the Juniper JunOS by port. |
| 331 | GPG13: Unencrypted Network Services - Juniper JunOS | Displays Juniper JunOS firewall traffic containing unencrypted network services. |
| 332 | GPG13: Ports Denied Access - Juniper JunOS | Displays the applications that have been denied access the most by the Juniper JunOS. |
| 333 | GPG13: Symantec Endpoint Protection: Scans | Displays scans using Symantec Endpoint Protection. |
| 334 | GPG13: Symantec Endpoint Protection: Updated | Displays updates to Symantec Endpoint Protection. |
| 335 | GPG13: Symantec Endpoint Protection: Attacks by Threat Name | Displays Symantec Endpoint Protection attacks by threat name. |
| 336 | GPG13: Symantec Endpoint Protection: Attacks Detected | Displays attacks detected by Symantec Endpoint Protection. |
| 337 | GPG13: Denied Connections - Cisco NXOS | Displays all connections that have been denied by the Cisco NXOS devices. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 338 | GPG13: Cisco ISE, ACS Configuration Changes | Displays Cisco ISE and Cisco SecureACS configuration changes. |
| 339 | GPG13: Cisco ISE, ACS Password Changes | Displays all password change activities on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access. |
| 340 | GPG13: Cisco ISE, ACS Accounts Created | Displays all accounts created on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access. |
| 341 | GPG13: Cisco ISE, ACS Accounts Removed | Displays all accounts removed on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access. |
| 342 | GPG13: Ports Allowed Access - Cisco Netflow | Displays all connections passed through the Cisco Netflow by port. |
| 343 | GPG13: Unencrypted Network Services - Cisco Netflow | Displays Cisco Netflow traffic containing unencrypted network services. |
| 344 | GPG13: Email Source IP Sending To Most Recipients | Displays IP addresses that are sending to the most recipients using Exchange 2007/10. |
| 345 | GPG13: Sidewinder Configuration Changes | Displays Sidewinder configuration changes. |
| 346 | GPG13: Accounts Created on Sidewinder | Displays all accounts created on Sidewinder to ensure authorized and appropriate access. |
| 347 | GPG13: Accounts Deleted on Sidewinder | Displays all accounts deleted on Sidewinder to ensure authorized and appropriate access. |
| 348 | GPG13: Unencrypted Network Services - Sidewinder | Displays Sidewinder firewall traffic containing unencrypted network services. |
| 349 | GPG13: Denied Connections - Sidewinder | Displays all connections that have been denied by the Sidewinder devices. |
| 350 | GPG13: NetApp Filer Audit Logs Cleared | Displays all audit logs clearing activities on NetApp Filer Audit to detect access violations or unusual activity. |
| 351 | GPG13: Cisco ESA: Attacks by Event ID | Displays Cisco ESA attacks by Event ID. |
| 352 | GPG13: Cisco ESA: Attacks Detected | Displays attacks detected by Cisco ESA. |
| 353 | GPG13: Cisco ESA: Attacks by Threat Name | Displays Cisco ESA attacks by threat name. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 354 | GPG13: Cisco ESA: Updated | Displays updates to Cisco ESA. |
| 355 | GPG13: Cisco ESA: Scans | Displays scans using Cisco ESA. |
| 356 | GPG13: Ports Allowed Access - VMware vShield | Displays all connections passed through the VMware vShield by port. |
| 357 | GPG13: Ports Denied Access - VMware vShield | Displays the applications that have been denied access the most by the VMware vShield Edge. |
| 358 | GPG13: Unencrypted Network Services - VMware vShield | Displays VMware vShield firewall traffic containing unencrypted network services. |
| 359 | GPG13: Denied Connections - VMware vShield | Displays all connections that have been denied by the VMware vShield devices. |
| 360 | GPG13: DHCP Granted/ Renewed Activities on VMware vShield | Displays all DHCP Granted/Renewed activities on VMware vShield Edge. |
| 361 | GPG13: DHCP Granted/ Renewed Activities on Microsoft DHCP | Displays all DHCP Granted/Renewed activities on Microsoft DHCP Server. |
| 362 | GPG13: Applications Under Attack - Cisco IOS | Displays all applications under attack as well as the attack signatures by Cisco IOS. |
| 363 | GPG13: Attacks Detected - Cisco IOS | Displays all IDS attacks detected against servers and applications by Cisco IOS. |
| 364 | GPG13: Attackers by Service - Cisco IOS | Displays all attack source IP address and service ports by Cisco IOS. |
| 365 | GPG13: Attackers by Signature - Cisco IOS | Displays all attack source IP address and signatures by Cisco IOS. |
| 366 | GPG13: Sensors Generating Alerts - Cisco IOS | Displays the IDS sensors that generated the most alerts by Cisco IOS. |
| 367 | GPG13: Servers Under Attack - Cisco IOS | Displays all servers under attack by Cisco IOS. |
| 368 | GPG13: Source of Attacks - Cisco IOS | Displays the sources that have initiated the most attacks by Cisco IOS. |
| 369 | GPG13: Denied Connections - Cisco IOS | Displays all connections that have been denied by the Cisco IOS devices. |
| 370 | GPG13: Ports Allowed Access - Cisco IOS | Displays all connections passed through the Cisco IOS by port. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 371 | GPG13: Ports Denied Access - Cisco IOS | Displays the applications that have been denied access the most by the Cisco IOS. |
| 372 | GPG13: Unencrypted Network Services - Cisco IOS | Displays Cisco IOS firewall traffic containing unencrypted network services. |
| 373 | GPG13: Files Accessed through Juniper SSL VPN (Secure Access) | Displays all files accessed through Juniper SSL VPN (Secure Access). |
| 374 | GPG13: Juniper SSL VPN (Secure Access) Policy Changed | Displays all configuration changes to the Juniper SSL VPN (Secure Access) policies. |
| 375 | GPG13: DNS Server Error | Displays all events when DNS Server has errors. |
| 376 | GPG13: Juniper Firewall Policy Changed | Displays all configuration changes to the Juniper Firewall policies. |
| 377 | GPG13: Accounts Created on TIBCO Administrator | Displays all accounts created on TIBCO Administrator to ensure authorized and appropriate access. |
| 378 | GPG13: Accounts Deleted on TIBCO Administrator | Displays all accounts deleted on TIBCO Administrator to ensure authorized and appropriate access. |
| 379 | GPG13: Unencrypted Network Services - F5 BIG-IP TMOS | Displays F5 BIG-IP TMOS firewall traffic containing unencrypted network services. |
| 380 | GPG13: Denied Connections - F5 BIG-IP TMOS | Displays all connections that have been denied by the F5 BIG-IP TMOS devices. |
| 381 | GPG13: TIBCO Administrator Password Changes | Displays all password change activities on TIBCO Administrator to ensure authorized and appropriate access. |
| 382 | GPG13: TIBCO Administrator Permission Changes | Displays events related to TIBCO Administrator permission modifications. |
| 383 | GPG13: Accounts Changed on TIBCO Administrator | Displays all accounts changed on TIBCO Administrator to ensure authorized and appropriate access. |
| 384 | GPG13: Accounts Changed on NetApp Filer | Displays all accounts changed on NetApp Filer to ensure authorized and appropriate access. |
| 385 | GPG13: Accounts Created on NetApp Filer | Displays all accounts created on NetApp Filer to ensure authorized and appropriate access. |
| 386 | GPG13: Accounts Deleted on NetApp Filer | Displays all accounts deleted on NetApp Filer to ensure authorized and appropriate access. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 387 | GPG13: NetApp Filer File Activity | Displays all file activities on NetApp Filer. |
| 388 | GPG13: NetApp Filer Login Failed | Displays all NetApp Filer login events which have failed. |
| 389 | GPG13: NetApp Filer Login Successful | Displays all NetApp Filer login events which have succeeded. |
| 390 | GPG13: NetApp Filer Password Changes | Displays all password change activities on NetApp Filer to ensure authorized and appropriate access. |
| 391 | GPG13: Accounts Created on NetApp Filer Audit | Displays all accounts created on NetApp Filer Audit to ensure authorized and appropriate access. |
| 392 | GPG13: Accounts Deleted on NetApp Filer Audit | Displays all accounts deleted on NetApp Filer Audit to ensure authorized and appropriate access. |
| 393 | GPG13: Files Accessed on NetApp Filer Audit | Displays all files accessed on NetApp Filer Audit to ensure appropriate access. |
| 394 | GPG13: Group Activities on NetApp Filer Audit | Displays all group activities on NetApp Filer Audit to ensure authorized and appropriate access. |
| 395 | GPG13: NetApp Filer Audit Login Failed | Displays all NetApp Filer Audit login events which have failed. |
| 396 | GPG13: NetApp Filer Audit Login Successful | Displays all NetApp Filer Audit login events which have succeeded. |
| 397 | GPG13: NetApp Filer Audit Policies Modified | Displays all policy modification activities on NetApp Filer Audit to ensure authorized and appropriate access. |
| 398 | GPG13: Domain activities on Symantec Endpoint Protection | Displays all domain activities on Symantec Endpoint Protection. |
| 399 | GPG13: Symantec Endpoint Protection Policy Add, Remove, or Modify | Displays all events when a Symantec Endpoint Protection policy is added, removed, or modified. |
| 400 | GPG13: Symantec Endpoint Protection Configuration Changes | Displays Symantec Endpoint Protection configuration changes. |
| 401 | GPG13: Group Activities on Symantec Endpoint Protection | Displays all group activities on Symantec Endpoint Protection to ensure authorized and appropriate access. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 402 | GPG13: Symantec Endpoint Protection Password Changes | Displays all password change activities on Symantec Endpoint Protection to ensure authorized and appropriate access. |
| 403 | GPG13: Ports Allowed Access - F5 BIG-IP TMOS | Displays all connections passed through the F5 BIG-IP TMOS by port. |
| 404 | GPG13: Accounts Created on Symantec Endpoint Protection | Displays all accounts created on Symantec Endpoint Protection to ensure authorized and appropriate access. |
| 405 | GPG13: Accounts Deleted on Symantec Endpoint Protection | Displays all accounts deleted on Symantec Endpoint Protection to ensure authorized and appropriate access. |
| 406 | GPG13: Applications Under Attack - ISS SiteProtector | Displays all applications under attack as well as the attack signatures by ISS SiteProtector. |
| 407 | GPG13: Attacks Detected - ISS SiteProtector | Displays all IDS attacks detected against servers and applications by ISS SiteProtector. |
| 408 | GPG13: Attackers by Service - ISS SiteProtector | Displays all attack source IP address and service ports by ISS SiteProtector. |
| 409 | GPG13: Attackers by Signature - ISS SiteProtector | Displays all attack source IP address and signatures by ISS SiteProtector. |
| 410 | GPG13: Sensors Generating Alerts - ISS SiteProtector | Displays the IDS sensors that generated the most alerts by ISS SiteProtector. |
| 411 | GPG13: Servers Under Attack - ISS SiteProtector | Displays all servers under attack by ISS SiteProtector. |
| 412 | GPG13: Source of Attacks - ISS SiteProtector | Displays the sources that have initiated the most attacks by ISS SiteProtector. |
| 413 | GPG13: Applications Under Attack - SiteProtector | Displays all applications under attack as well as the attack signatures by SiteProtector. |
| 414 | GPG13: Attacks Detected - SiteProtector | Displays all IDS attacks detected against servers and applications by SiteProtector. |
| 415 | GPG13: Attackers by Service - SiteProtector | Displays all attack source IP address and service ports by SiteProtector. |
| 416 | GPG13: Attackers by Signature - SiteProtector | Displays all attack source IP address and signatures by SiteProtector. |
| 417 | GPG13: Sensors Generating Alerts - SiteProtector | Displays the IDS sensors that generated the most alerts by SiteProtector. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 418 | GPG13: Servers Under Attack - SiteProtector | Displays all servers under attack by SiteProtector. |
| 419 | GPG13: Source of Attacks - SiteProtector | Displays the sources that have initiated the most attacks by SiteProtector. |
| 420 | GPG13: Files Downloaded through Proxy - Microsoft IIS | Displays all proxy-based downloads to ensure authorized and appropriate access on Microsoft IIS. |
| 421 | GPG13: Files Uploaded through Proxy - Microsoft IIS | Displays all proxy-based uploads to ensure only authorized data can be uploaded on Microsoft IIS. |
| 422 | GPG13: Peer Servers and Status - Microsoft IIS | Displays all web servers providing data for cache servers and the status of requests on Microsoft IIS. |
| 423 | GPG13: Web URLs Visited through Proxy - Microsoft IIS | Displays URLs that have been visited through a proxy server on Microsoft IIS. |
| 424 | GPG13: Users Using the Proxies - Microsoft IIS | Displays users who have been surfing the web through the proxy servers on Microsoft IIS. |
| 425 | GPG13: Allowed URLs by Source IPs - Microsoft IIS | Displays successful access to URLs by source IP addresses on Microsoft IIS. |
| 426 | GPG13: Allowed URLs by Source Users - Microsoft IIS | Displays successful access to URLs by source users on Microsoft IIS. |
| 427 | GPG13: Blocked URLs by Source IPs - Microsoft IIS | Displays URLs that have been blocked by source IP addresses on Microsoft IIS. |
| 428 | GPG13: Blocked URLs by Source Users - Microsoft IIS | Displays URLs that have been blocked by source users on Microsoft IIS. |
| 429 | GPG13: Files Downloaded through the Web - Microsoft IIS | Displays all web-based downloads to ensure authorized and appropriate access on Microsoft IIS. |
| 430 | GPG13: Files Uploaded through the Web - Microsoft IIS | Displays all web-based uploads to ensure only authorized data can be uploaded on Microsoft IIS. |
| 431 | GPG13: Web URLs Visited - Microsoft IIS | Displays URLs that have been visited on Microsoft IIS. |
| 432 | GPG13: Web Access to Applications - Microsoft IIS | Displays all web-based access to applications to ensure appropriate and authorized access on Microsoft IIS. |
| 433 | GPG13: Web Access from All Users - Microsoft IIS | Displays all web-based access by all users for regular reviews and updates on Microsoft IIS. |
| 434 | GPG13: vCenter Orchestrator Virtual Machine Created | Virtual machine has been created from VMware vCenter Orchestrator. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 435 | GPG13: vCenter Orchestrator Virtual Machine Deleted | Virtual machine has been deleted from VMware vCenter Orchestrator. |
| 436 | GPG13: vCenter Orchestrator Datastore Events | Displays create, modify, and delete datastore events on VMware vCenter Orchestrator. |
| 437 | GPG13: vCenter Orchestrator Failed Logins | Displays all failed logins for VMWare vCenter Orchestrator. |
| 438 | GPG13: vCenter Orchestrator Data Move | Entity has been moved within the VMware vCenter Orchestrator infrastructure. |
| 439 | GPG13: vCenter Orchestrator Virtual Machine Shutdown | Virtual machine has been shutdown or paused from VMware vCenter Orchestrator console. |
| 440 | GPG13: vCenter Orchestrator Virtual Machine Started | Virtual machine has been started or resumed from VMware vCenter Orchestrator console. |
| 441 | GPG13: vCenter Orchestrator vSwitch Added, Changed or Removed | vSwitch has been added, modified or removed from VMware vCenter Orchestrator console. |
| 442 | GPG13: vCenter Orchestrator Change Attributes | Modification of VMware vCenter Orchestrator properties. |
| 443 | GPG13: Allowed URLs by Source IPs - F5 BIG-IP TMOS | Displays successful access to URLs by source IP addresses on F5 BIG-IP TMOS. |
| 444 | GPG13: Allowed URLs by Source Users - F5 BIG-IP TMOS | Displays successful access to URLs by source users on F5 BIG-IP TMOS. |
| 445 | GPG13: Blocked URLs by Source IPs - F5 BIG-IP TMOS | Displays URLs that have been blocked by source IP addresses on F5 BIG-IP TMOS. |
| 446 | GPG13: Blocked URLs by Source Users - F5 BIG-IP TMOS | Displays URLs that have been blocked by source users on F5 BIG-IP TMOS. |
| 447 | GPG13: Files Downloaded through the Web - F5 BIG-IP TMOS | Displays all web-based downloads ensure authorized and appropriate access on F5 BIG-IP TMOS. |
| 448 | GPG13: Files Uploaded through the Web - F5 BIG-IP TMOS | Displays all web-based uploads to ensure only authorized data can be uploaded on F5 BIG-IP TMOS. |
| 449 | GPG13: Web URLs Visited - F5 BIG-IP TMOS | Displays URLs that have been visited on F5 BIG-IP TMOS. |
| 450 | GPG13: 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. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 451 | GPG13: Web Access from All Users - F5 BIG-IP TMOS | Displays all web-based access by all users for regular reviews and updates on F5 BIG-IP TMOS. |
| 452 | GPG13: F5 BIG-IP TMOS Login Failed | Displays all F5 BIG-IP TMOS login events which have failed. |
| 453 | GPG13: F5 BIG-IP TMOS Login Successful | Displays all F5 BIG-IP TMOS login events which have succeeded. |
| 454 | GPG13: F5 BIG-IP TMOS Password Changes | Displays all password change activities on F5 BIG-IP TMOS to ensure authorized and appropriate access. |
| 455 | GPG13: Files Uploaded through Proxy - Blue Coat | Displays all proxy-based uploads to ensure only authorized data can be uploaded on Blue Coat. |
| 456 | GPG13: Files Downloaded through Proxy - Blue Coat | Displays all proxy-based downloads to ensure authorized and appropriate access on Blue Coat. |
| 457 | GPG13: Peer Servers and Status - Blue Coat | Displays all web servers providing data for cache servers and the status of requests on Blue Coat. |
| 458 | GPG13: Users Using the Proxies - Blue Coat | Displays users who have been surfing the web through the proxy servers on Blue Coat. |
| 459 | GPG13: Web URLs Visited through Proxy - Blue Coat | Displays URLs that have been visited through a proxy server on Blue Coat. |
| 460 | GPG13: Attacks Detected - HIPS | Displays all IPS attacks detected against servers and applications. |
| 461 | GPG13: Servers Under Attack - HIPS | Displays all servers under attack. |
| 462 | GPG13: Source of Attacks - HIPS | Displays the sources that have initiated the most attacks. |
| 463 | GPG13: HP NonStop Audit Configuration Changes | Displays all audit configuration changes on HP NonStop. |
| 464 | GPG13: HP NonStop Audit Login Failed | Displays all HP NonStop Audit login events which have failed. |
| 465 | GPG13: HP NonStop Audit Login Successful | Displays all HP NonStop Audit login events which have succeeded. |
| 466 | GPG13: HP NonStop Audit Object Access | Displays HP NonStop Audit events related to object access. |
| 467 | GPG13: HP NonStop Audit Object Changes | Displays HP NonStop Audit events related to object changes. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 468 | GPG13: HP NonStop Audit Permissions Changed | Displays all permission modification activities on HP NonStop Audit to ensure authorized access. |
| 469 | GPG13: LogLogic Management Center Account Activities | Displays all accounts activities on LogLogic management center to ensure authorized and appropriate access. |
| 470 | GPG13: LogLogic Management Center Restore Activities | Displays all restore activities on LogLogic management center. |
| 471 | GPG13: LogLogic Management Center Backup Activities | Displays all backup activities on LogLogic management center. |
| 472 | GPG13: LogLogic Management Center Login | Displays all login events to the LogLogic management center. |
| 473 | GPG13: LogLogic Management Center Password Changes | Displays all password change activities on LogLogic management center to ensure authorized and appropriate access. |
| 474 | GPG13: LogLogic Management Center Upgrade Success | Displays all successful events related to the system's upgrade. |
| 475 | GPG13: LogLogic Universal Collector Configuration Changes | Displays LogLogic universal collector configuration changes. |
| 476 | GPG13: Sensors Generating Alerts - Sourcefire Defense Center | Displays the IDS sensors that generated the most alerts by Sourcefire Defense Center. |
| 477 | GPG13: Servers Under Attack - Sourcefire Defense Center | Displays all servers under attack by Sourcefire Defense Center. |
| 478 | GPG13: Source of Attacks - Sourcefire Defense Center | Displays the sources that have initiated the most attacks by Sourcefire Defense Center. |
| 479 | GPG13: Applications Under Attack - Sourcefire Defense Center | Displays all applications under attack as well as the attack signatures by Sourcefire Defense Center. |
| 480 | GPG13: Attackers by Service - Sourcefire Defense Center | Displays all attack source IP address and service ports by Sourcefire Defense Center. |
| 481 | GPG13: Attackers by Signature - Sourcefire Defense Center | Displays all attack source IP address and signatures by Sourcefire Defense Center. |
| 482 | GPG13: Attacks Detected - Sourcefire Defense Center | Displays all IDS attacks detected against servers and applications by Sourcefire Defense Center. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 483 | GPG13: Ports Allowed Access - Sidewinder | Displays all connections passed through the Sidewinder by port. |
| 484 | GPG13: Ports Denied Access - Sidewinder | Displays the applications that have been denied access the most by the Sidewinder. |
| 485 | GPG13: Files Downloaded through Proxy - Cisco WSA | Displays all proxy-based downloads to ensure authorized and appropriate access on Cisco WSA. |
| 486 | GPG13: Files Uploaded through Proxy - Cisco WSA | Displays all proxy-based uploads to ensure only authorized data can be uploaded on Cisco WSA. |
| 487 | GPG13: Peer Servers and Status - Cisco WSA | Displays all web servers providing data for cache servers and the status of requests on Cisco WSA. |
| 488 | GPG13: Users Using the Proxies - Cisco WSA | Displays users who have been surfing the web through the proxy servers on Cisco WSA. |
| 489 | GPG13: Web Access to Applications - PANOS | Displays all web-based access to applications to ensure appropriate and authorized access on Palo Alto Networks. |
| 490 | GPG13: Web URLs Visited - PANOS | Displays URLs that have been visited on Palo Alto Networks. |
| 491 | GPG13: Web Access from All Users - PANOS | Displays all web-based access by all users for regular reviews and updates on Palo Alto Networks. |
| 492 | GPG13: Files Accessed through PANOS | Displays all files accessed through Palo Alto Networks. |
| 493 | GPG13: Web Access to Applications - Fortinet | Displays all web-based access to applications to ensure appropriate and authorized access on Fortinet. |
| 494 | GPG13: Web URLs Visited - Fortinet | Displays URLs that have been visited on Fortinet. |
| 495 | GPG13: Web Access from All Users - Fortinet | Displays all web-based access by all users for regular reviews and updates on Fortinet. |
| 496 | GPG13: NetApp Filer Audit Group Members Deleted | Displays all accounts removed from groups on the NetApp Filer Audit to ensure appropriate access. |
| 497 | GPG13: Groups Created on NetApp Filer Audit | Displays all groups created on NetApp Filer Audit to ensure authorized and appropriate access. |
| 498 | GPG13: Groups Deleted on NetApp Filer Audit | Displays all groups deleted on NetApp Filer Audit to ensure authorized and appropriate access. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 499 | GPG13: NetApp Filer Audit Accounts Enabled | Displays all accounts enabled on NetApp Filer Audit to ensure authorized and appropriate access. |
| 500 | GPG13: NetApp Filer Audit Group Members Added | Displays all accounts added to groups on the NetApp Filer Audit to ensure appropriate access. |
| 501 | GPG13: Accounts Changed on TIBCO ActiveMatrix Administrator | Displays all accounts changed on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access. |
| 502 | GPG13: Accounts Created on TIBCO ActiveMatrix Administrator | Displays all accounts created on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access. |
| 503 | GPG13: Accounts Deleted on TIBCO ActiveMatrix Administrator | Displays all accounts deleted on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access. |
| 504 | GPG13: Group Activities on TIBCO ActiveMatrix Administrator | Displays all group activities on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access. |
| 505 | GPG13: Groups Created on TIBCO ActiveMatrix Administrator | Displays all groups created on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access. |
| 506 | GPG13: Groups Deleted on TIBCO ActiveMatrix Administrator | Displays all groups deleted on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access. |
| 507 | GPG13: TIBCO ActiveMatrix Administrator Failed Logins | Displays all TIBCO ActiveMatrix Administrator login events which have failed. |
| 508 | GPG13: TIBCO ActiveMatrix Administrator Permission Changes | Displays events related to TIBCO ActiveMatrix Administrator permission modifications. |
| 509 | GPG13: TIBCO ActiveMatrix Administrator Successful Logins | Displays successful logins to TIBCO ActiveMatrix Administrator to ensure only authorized personnel have access. |
| 510 | GPG13: Files Accessed Through Pulse Connect Secure | Displays all files accessed through Pulse Connect Secure. |
| 511 | GPG13: Sensors Generating Alerts - FireEye MPS | Displays the IDS sensors that generated the most alerts by FireEye MPS. |
| 512 | GPG13: Servers under Attacks - FireEye MPS | Displays all servers under attack by FireEye MPS. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 513 | GPG13: Source of Attacks - FireEye MPS | Displays the sources that have initiated the most attacks by FireEye MPS |
| 514 | GPG13: Applications Under Attack - FireEye MPS | Displays all applications under attack as well the attack signatures by FireEye MPS. |
| 515 | GPG13: Attackers by Signature - FireEye MPS | Displays all attack source IP address and signatures by FireEye MPS. |
| 516 | GPG13: Attackers by Service - FireEye MPS | Displays all attack source IP address and service ports by FireEye MPS. |
| 517 | GPG13: Files Downloaded via Proxy | Displays all proxy-based downloads to ensure authorized and appropriate access on Cisco WSA. |
| 518 | GPG13: Files Downloaded via Proxy - Blue Coat | Displays all proxy-based downloads to ensure authorized and appropriate access on Blue Coat. |
| 519 | GPG13: Files Downloaded via Proxy - Cisco WSA | Displays all proxy-based downloads to ensure authorized and appropriate access on Cisco WSA |
| 520 | GPG13: Files Downloaded via Proxy - Microsoft IIS | Displays all proxy-based downloads to ensure authorized and appropriate access on Microsoft IIS. |
| 521 | GPG13: Files Downloaded via the Web | Displays all web-based downloads ensure authorized and appropriate access. |
| 522 | GPG13: Files Downloaded via the Web - F5 BIG-IP TMOS | Displays all web-based downloads ensure authorized and appropriate access on F5 BIG-IP TMOS. |
| 523 | GPG13: Files Downloaded via the Web - Microsoft IIS | Displays all web-based downloads ensure authorized and appropriate access on Microsoft IIS. |
| 524 | GPG13: Files Uploaded via Proxy | Displays all proxy-based uploads to ensure only authorized data can be uploaded. |
| 525 | GPG13: Files Uploaded via Proxy - Blue Coat | Displays all proxy-based uploads to ensure only authorized data can be uploaded on Blue Coat. |
| 526 | GPG13: Files Uploaded via Proxy - Cisco WSA | Displays all proxy-based uploads to ensure only authorized data can be uploaded on Cisco WSA. |
| 527 | GPG13: Files Uploaded via Proxy - Microsoft IIS | Displays all proxy-based uploads to ensure only authorized data can be uploaded on Microsoft IIS. |
| 528 | GPG13: Files Uploaded via the web | Displays all web-based uploads to ensure only authorized data can be uploaded. |

| Serial Number | TIBCO LogLogic Report | Description |
|---|---|---|
| 529 | GPG13: Files Uploaded via the Web - F5 BIG-IP TMOS | Displays all web-based uploads to ensure only authorized data can be uploaded on F5 BIG-IP TMOS. |
| 530 | GPG13: Files Uploaded via the Web - Microsoft IIS | Displays all web-based uploads to ensure only authorized data can be uploaded on Microsoft IIS. |
| 531 | GPG13: FireEye MPS: Attacks by Event ID | Displays FireEye MPS attacks by Event ID. |
| 532 | GPG13: FireEye MPS: Attacks by Threat Name | Displays FireEye MPS attacks by threat name. |
| 533 | GPG13: FireEye MPS: Attacks Detected | Displays attacks detected by FireEye MPS. |
| 534 | GPG13: Pulse Connect Secure Failed Logins | Displays a report of all failed logins at the Pulse Connect Secure. |
| 535 | GPG13: Pulse Connect Secure Policy Change | Displays all configuration changes to the Pulse Connect Secure policies. |
| 536 | GPG13: Pulse Connect Secure Successful Logins | Displays all successfull logins through the Pulse Connect Secure. |
| 537 | GPG13: Web URLs Visited via Proxy | Displays URLs that have been visited via a proxy server. |
| 538 | GPG13: Web URLs Visited via Proxy - Blue Coat | Displays URLs that have been visited via a proxy server on Blue Coat. |
| 539 | GPG13: Web URLs Visited via Proxy - Cisco WSA | Displays URLs that have been visited via a proxy server on Cisco WSA. |
| 540 | GPG13: Web URLs Visited via Proxy - Microsoft IIS | Displays URLs that have been visited via a proxy server on Microsoft IIS. |

## TIBCO LogLogic Alerts for GPG13

The following table lists the alerts included in the LogLogic® Compliance Suite - GPG 13 Edition.

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 1 | GPG13: Accounts Created | Alerts when a new account is created on servers. |
| 2 | GPG13: Accounts Deleted | Alerts when an account is deleted on servers. |
| 3 | GPG13: Accounts Enabled | Alerts when an account has been enabled on servers. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 4 | GPG13: Accounts Locked | Alerts when an account has been locked on servers. |
| 5 | GPG13: Accounts Modified | Alerts when an account is modified on servers. |
| 6 | GPG13: Active Directory Changes | Alerts when changes are made within Active Directory. |
| 7 | GPG13: Allowed Connections | Allowed firewall connections. |
| 8 | GPG13: Check Point Policy Changed | Alerts when a Check Point firewall's policy has been modified. |
| 9 | GPG13: Cisco ISE, ACS Configuration Changed | Alerts when configuration changes are made to the Cisco ISE or Cisco SecureACS. |
| 10 | GPG13: Cisco ISE, ACS Passwords Changed | Alerts when a user changes their password via Cisco ISE or Cisco SecureACS. |
| 11 | GPG13: Cisco PIX, ASA, FWSM Commands Executed | Alerts when a Cisco PIX, ASA, or FWSM commands are executed. |
| 12 | GPG13: Cisco PIX, ASA, FWSM Failover Disabled | Alerts when a Cisco PIX, ASA, or FWSM HA configuration is disabled. |
| 13 | GPG13: Cisco PIX, ASA, FWSM Failover Errors | Alerts when an error has occurred during PIX, ASA, or FWSM failover. |
| 14 | GPG13: Cisco PIX, ASA, FWSM Failover Performed | Alerts when a failover has occurred on the Cisco PIX, ASA, or FWSM devices. |
| 15 | GPG13: Cisco PIX, ASA, FWSM Fragment Database Limit | Alerts when the fragment database count has been reached on Cisco PIX, ASA, or FWSM devices. |
| 16 | GPG13: Cisco PIX, ASA, FWSM Logon Failure | Alerts when login attempt to the Cisco PIX, ASA, or FWSM devices fails. |
| 17 | GPG13: Cisco PIX, ASA, FWSM Logon Success | Alerts when a login attempt to the Cisco PIX, ASA, or FWSM firewall is successful. |
| 18 | GPG13: Cisco PIX, ASA, FWSM NAT Failure | Failures in Network Address Translation (NAT) on the Cisco PIX, ASA, or FWSM. |
| 19 | GPG13: Cisco PIX, ASA, FWSM Policy Changed | Alerts when a Cisco PIX, ASA, or FWSM firewall policy has been modified. |
| 20 | GPG13: Cisco PIX, ASA, FWSM Protocol Failure | Alerts when possible network protocol failures on the Cisco PIX, ASA, or FWSM devices. |
| 21 | GPG13: System Restarted | Alerts when system has been restarted. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 22 | GPG13: Cisco PIX, ASA, FWSM Routing Failure | Alerts when routing failure occurred in the Cisco PIX, ASA, or FWSM devices. |
| 23 | GPG13: Cisco PIX, ASA, FWSM Shun Added | Alerts when a shun rule has been added to the PIX, ASA, or FWSM configuration. |
| 24 | GPG13: Cisco PIX, ASA, FWSM Shun Deleted | Alerts when a shun rule has been removed from the PIX, ASA, or FWSM configuration. |
| 25 | GPG13: Cisco PIX, ASA, FWSM VPN Tunnel Creation | Alerts when a VPN tunnel has been created on the Cisco PIX, ASA, or FWSM devices. |
| 26 | GPG13: Cisco PIX, ASA, FWSM VPN Tunnel Teardown | Alerts when a VPN tunnel has been removed on the Cisco PIX, ASA, or FWSM devices. |
| 27 | GPG13: Cisco Switch Card Insert | Alerts when a card module is inserted into a switch. |
| 28 | GPG13: Cisco Switch Device Reload | Alerts when a command to reload a Cisco switch has been executed. |
| 29 | GPG13: Cisco Switch Device Restart | Alerts when a router or switch has been rebooted. |
| 30 | GPG13: Cisco Switch HA Failure (ver) | Alerts when a HA setup has version incompatibility issues. |
| 31 | GPG13: Cisco Switch Interface Change | Alerts when network interfaces are going up or down. |
| 32 | GPG13: Cisco Switch Interface Down | Alerts when Cisco switch interface is going down. |
| 33 | GPG13: Cisco Switch Interface Up | Alerts when the Cisco switch interface is back up. |
| 34 | GPG13: Cisco Switch Policy Changed | Alerts when Cisco router or switch configuration has been modified. |
| 35 | GPG13: DB2 Database Backup Failed | Alerts when a DB2 database backup fails. |
| 36 | GPG13: DB2 Database Configuration Change | Alerts when a configuration is changed on a DB2 database. |
| 37 | GPG13: DB2 Database Restore Failed | Alerts when a database restore fails on a DB2 database. |
| 38 | GPG13: DB2 Database Started or Stopped | Alerts when a DB2 database is started or stopped. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 39 | GPG13: DB2 Database User Added or Dropped | Alerts when a user is added or dropped from a DB2 database. |
| 40 | GPG13: Disallowed Services | Disallowed firewall services. |
| 41 | GPG13: DNS Server Shutdown | Alerts when DNS Server has been shutdown. |
| 42 | GPG13: DNS Server Started | Alerts when DNS Server has been started. |
| 43 | GPG13: Escalated Privileges | Alerts when a user or program has escalated the privileges. |
| 44 | GPG13: Excessive IDS Attack | IDS anomalies using message volume threshold alerts. |
| 45 | GPG13: Group Members Added | Alerts when new members are added to user groups. |
| 46 | GPG13: Group Members Deleted | Alerts when members are removed from user groups. |
| 47 | GPG13: Groups Created | Alerts when new user groups are created. |
| 48 | GPG13: Groups Deleted | Alerts when a user group is deleted. |
| 49 | GPG13: Groups Modified | Alerts when a user group has been modified. |
| 50 | GPG13: Guardium SQL Guard Config Changes | Alerts when a configuration is changed on Guardium SQL Database. |
| 51 | GPG13: Guardium SQL Guard Data Access | Alerts when a select statement is made on Guardium SQL Database. |
| 52 | GPG13: Guardium SQL Guard Logins | Alerts when a user logs into the Guardium SQL Database. |
| 53 | GPG13: Guardium SQL Guard Startup or Shutdown | Alerts when the Guardium SQL Database is started or stopped. |
| 54 | GPG13: HP NonStop Audit Configuration Changed | Alerts when configuration changes are made to the HP NonStop Audit. |
| 55 | GPG13: HP NonStop Audit Permission Changed | Alerts on HP NonStop Audit permission changed events. |
| 56 | GPG13: i5/OS Network Profile Changes | Alerts when any changes are made to an i5/OS network profile. |
| 57 | GPG13: i5/OS Permission or Policy Change | Alerts when policies or permissions are changed on the i5/OS. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 58 | GPG13: i5/OS Server or Service Status Change | Alerts when the i5/OS is restarted or a service stops or starts. |
| 59 | GPG13: i5/OS Software Updates | Alerts when events related to the i5/OS software updates. |
| 60 | GPG13: i5/OS User Profile Changes | Alerts when a user profile is changed on the i5/OS. |
| 61 | GPG13: IBM AIX Password Changed | Alerts when an account password is changed on IBM AIX servers. |
| 62 | GPG13: Juniper Firewall HA State Change | Alerts when Juniper Firewall has changed its failover state. |
| 63 | GPG13: Juniper Firewall Logon Failure | Alerts when login attempt to the Juniper Firewall fails. |
| 64 | GPG13: Juniper Firewall Logon Success | Alerts when login attempt to the Juniper Firewall is successful. |
| 65 | GPG13: Juniper Firewall Peer Missing | Alerts when a Juniper Firewall HA peer is missing. |
| 66 | GPG13: Juniper Firewall Policy Changes | Alerts when Juniper Firewall configuration is changed. |
| 67 | GPG13: Juniper Firewall Policy Out of Sync | Alerts when the Juniper Firewall's policy is out of sync. |
| 68 | GPG13: Juniper Firewall System Reset | Alerts when the Juniper Firewall has been reset to system default. |
| 69 | GPG13: Juniper VPN Policy Change | Alerts when Juniper VPN policy or configuration change. |
| 70 | GPG13: Logins Failed | Alerts when login failures are over the defined threshold. |
| 71 | GPG13: Logins Succeeded | Alerts when successful logins are over the defined threshold. |
| 72 | GPG13: LogLogic Disk Full | Alerts when the LogLogic appliance's disk is near full. |
| 73 | GPG13: LogLogic DSM Configuration Changes | Alerts when a configuration is changed on LogLogic DSM database. |
| 74 | GPG13: LogLogic DSM Data Access | Alerts when a select statement is made on LogLogic DSM database. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 75 | GPG13: LogLogic DSM Logins | Alerts when a user logs into the LogLogic DSM database. |
| 76 | GPG13: LogLogic DSM Startup or Shutdown | Alerts when the LogLogic DSM database is started or stopped. |
| 77 | GPG13: LogLogic File Retrieval Errors | Alerts when problems are detected during log file retrieval. |
| 78 | GPG13: LogLogic Management Center Backed Up or Restored | Alerts on backup and restore events to the LogLogic management center. |
| 79 | GPG13: LogLogic Management Center Passwords Changed | Alerts when users have changed their passwords. |
| 80 | GPG13: LogLogic Management Center Upgrade Succeeded | Alerts for successful events related to the system's upgrade. |
| 81 | GPG13: LogLogic Message Routing Errors | Alerts when problems are detected during message forwarding. |
| 82 | GPG13: LogLogic Universal Collector Configuration Changed | Alerts when configuration changes are made to the LogLogic universal collector. |
| 83 | GPG13: Microsoft Operations Manager - Permissions Changed | Alerts when user or group permissions have been changed. |
| 84 | GPG13: Microsoft Operations Manager - Windows Passwords Changed | Alerts when users have changed their passwords. |
| 85 | GPG13: Microsoft Operations Manager - Windows Policies Changed | Alerts when Windows policies changed. |
| 86 | GPG13: Microsoft Sharepoint Content Deleted | Alerts on Microsoft Sharepoint content deleted events. |
| 87 | GPG13: Microsoft Sharepoint Content Updated | Alerts on Microsoft Sharepoint content updated events. |
| 88 | GPG13: Microsoft Sharepoint Permission Changed | Alerts on Microsoft Sharepoint permission changed events. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 89 | GPG13: Microsoft Sharepoint Policies Added, Removed, Modified | Alerts on Microsoft Sharepoint policy additions, deletions, and modifications. |
| 90 | GPG13: Microsoft SQL Server Backup Failed | Alerts when Microsoft SQL Server backup process has failed. |
| 91 | GPG13: Microsoft SQL Server Restore Failed | Alerts when Microsoft SQL Server restore process failed. |
| 92 | GPG13: Microsoft SQL Server Shutdown | Alerts when Microsoft SQL Server has been shutdown. |
| 93 | GPG13: Neoteris Files Accessed | Identifies all files being accessed through the Juniper SSL VPN. |
| 94 | GPG13: NetApp Authentication Failure | Alerts when NetApp authentication failure events occur. |
| 95 | GPG13: NetApp Bad File Handle | Alerts when a bad file handle is detected on a NetApp device. |
| 96 | GPG13: NetApp Bootblock Update | Alerts when the bootblock has been updated on a NetApp Filer. |
| 97 | GPG13: NetApp Filer Audit Policies Changed | Alerts when NetApp Filer Audit policies changed. |
| 98 | GPG13: NetApp Filer Disk Failure | Alerts when a disk fails on a NetApp Filer. |
| 99 | GPG13: NetApp Filer Disk Inserted | Alerts when a disk is inserted into the NetApp Filer. |
| 100 | GPG13: NetApp Filer Disk Missing | Alerts when a disk is missing on the NetApp Filer device. |
| 101 | GPG13: NetApp Filer Disk Pulled | Alerts when a RAID disk has been pulled from the Filer device. |
| 102 | GPG13: NetApp Filer Disk Scrub Suspended | Alerts when the disk scrubbing process has been suspended. |
| 103 | GPG13: NetApp Filer File System Full | Alerts when the file system is full on the NetApp Filer device. |
| 104 | GPG13: NetApp Filer NIS Group Update | Alerts when the NIS group has been updated on the Filer device. |
| 105 | GPG13: NetApp Filer Snapshot Error | Alerts when an error has been detected during a NetApp Filer snapshot. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 106 | GPG13: NetApp Filer Unauthorized Mounting | Alerts when an unauthorized mount event occurs. |
| 107 | GPG13: Oracle Database Configuration Change | Alerts when an ALTER or an UPDATE command is executed on Oracle DBs. |
| 108 | GPG13: Oracle Database Data Access | Alerts when Oracle tables are accessed. |
| 109 | GPG13: Oracle Database Permissions Changed | Alerts when permissions are changed on Oracle databases. |
| 110 | GPG13: Oracle Database Shutdown | Alerts when an Oracle database is shutdown. |
| 111 | GPG13: Oracle Database User Added or Deleted | Alerts when a user is added or deleted from an Oracle database. |
| 112 | GPG13: Policy Violation | Alerts when the firewall policy is violated. |
| 113 | GPG13: RACF Files Accessed | Alerts when files are accessed on the RACF servers. |
| 114 | GPG13: RACF Passwords Changed | Alerts when users have changed their passwords. |
| 115 | GPG13: RACF Permissions Changed | Alerts when user or group permissions have been changed. |
| 116 | GPG13: RACF Process Started | Alerts whenever a process is run on a RACF server. |
| 117 | GPG13: Sidewinder Configuration Changed | Alerts when configuration changes are made to the Sidewinder. |
| 118 | GPG13: Sybase ASE Database Backed Up or Restored | Alerts on backup and restore events to the Sybase ASE Database. |
| 119 | GPG13: Sybase ASE Database Config Changes | Alerts on Sybase ASE Database configuration change events. |
| 120 | GPG13: Sybase ASE Database Data Access | Alerts on Sybase ASE Database data access events. |
| 121 | GPG13: Sybase ASE Database Started | Alerts on Sybase ASE Database start events. |
| 122 | GPG13: Sybase ASE Database Stopped | Alerts on Sybase ASE Database stop events. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 123 | GPG13: Symantec Endpoint Protection Configuration Changed | Alerts when configuration changes are made to the Symantec Endpoint Protection. |
| 124 | GPG13: Symantec Endpoint Protection Policy Add, Delete, Modify | Alerts on Symantec Endpoint Protection additions, deletions, and modifications. |
| 125 | GPG13: System Anomalies | Detects and alerts any anomalies based on past log patterns. |
| 126 | GPG13: System Restarted | Alerts when systems such as routers and switches have restarted. |
| 127 | GPG13: TIBCO ActiveMatrix Administrator Permission Changed | Alerts on TIBCO ActiveMatrix Administrator permission changed events. |
| 128 | GPG13: vCenter Create Virtual Machine | Alerts when virtual machine has been created from VMware vCenter console. |
| 129 | GPG13: vCenter Data Move | Alerts when entity has been moved within the VMware vCenter infrastructure. |
| 130 | GPG13: vCenter Datastore Event | Alerts on create, modify, and delete datastore events on VMware vCenter. |
| 131 | GPG13: vCenter Delete Virtual Machine | Alerts when a virtual machine has been deleted or removed from VMware vCenter console. |
| 132 | GPG13: vCenter Firewall Policy Change | Alerts when changes to the VMware ESX allowed services firewall policy. |
| 133 | GPG13: vCenter Orchestrator Create Virtual Machine | Alerts when a virtual machine has been created from VMware vCenter Orchestrator console. |
| 134 | GPG13: vCenter Orchestrator Data Move | Alerts when an entity is moved within the VMware vCenter Orchestrator infrastructure. |
| 135 | GPG13: vCenter Orchestrator Datastore Events | Alerts on create, modify, and delete datastore events on VMware vCenter Orchestrator. |
| 136 | GPG13: vCenter Orchestrator Delete Virtual Machine | Alerts when a virtual machine has been deleted or removed from VMware vCenter Orchestrator console. |
| 137 | GPG13: vCenter Orchestrator Login Failed | Alerts when logins to the VMware vCenter Orchestrator console fail. |
| 138 | GPG13: vCenter Orchestrator Virtual Machine Shutdown | Alerts when a virtual machine has been shutdown or paused from VMware vCenter Orchestrator console. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 139 | GPG13: vCenter Orchestrator Virtual Machine Started | Alerts when a virtual machine has been started or resumed from VMware vCenter Orchestrator console. |
| 140 | GPG13: vCenter Orchestrator vSwitch Add, Modify or Delete | Alerts when a vSwitch on VMware ESX server has been added, modified or removed from vCenter Orchestrator. |
| 141 | GPG13: vCenter Permission Change | Alerts when a permission role has been added, changed, removed, or applied on VMware vCenter. |
| 142 | GPG13: vCenter Restart ESX Services | Alerts when VMware vCenter restarted services running on VMware ESX Server. |
| 143 | GPG13: vCenter Shutdown or Restart ESX | Alerts when VMware ESX Server is shutdown from vCenter console. |
| 144 | GPG13: vCenter User Login Failed | Alerts on failed logins to the VMware vCenter console. |
| 145 | GPG13: vCenter User Login Successful | Alerts on successful logins to the VMware vCenter console. |
| 146 | GPG13: vCenter Virtual Machine Shutdown | Alerts when virtual machine has been shutdown or paused from VMware vCenter console. |
| 147 | GPG13: vCenter Virtual Machine Started | Alerts when virtual machine has been started or resumed from VMware vCenter console. |
| 148 | GPG13: vCenter vSwitch Add, Modify or Delete | Alert when vSwitch on VMware ESX server has been added, modified or removed from vCenter. |
| 149 | GPG13: vCloud Director Login Failed | Alerts on failed logins to the VMware vCloud Director console. |
| 150 | GPG13: vCloud Director Login Success | Alerts on successful logins to the VMware vCloud Director console. |
| 151 | GPG13: vCloud Organization Created | Alerts when organization successfully created on VMware vCloud Director. |
| 152 | GPG13: vCloud Organization Deleted | Alerts when organization successfully deleted on VMware vCloud Director. |
| 153 | GPG13: vCloud Organization Modified | Alerts when organization successfully modified on VMware vCloud Director. |
| 154 | GPG13: vCloud User Created | Alerts when a user successfully created on VMware vCloud Director. |
| 155 | GPG13: vCloud User, Group, or Role Modified | Alerts when VMware vCloud Director user, group, or role has been modified. |

| Serial Number | TIBCO LogLogic Alert | Description |
|---|---|---|
| 156 | GPG13: vCloud vApp Created, Deleted, or Modified | Alerts when VMware vCloud Director vApp has been created, deleted, or modified. |
| 157 | GPG13: vCloud vDC Created, Modified, or Deleted | Alerts when VMware vCloud Director Virtual Datacenters have been created, deleted, or modified. |
| 158 | GPG13: vShield Edge Configuration Change | Alerts when configuration changes to VMware vShield Edge policies. |
| 159 | GPG13: Windows Audit Log Cleared | Alerts when audit logs on Windows servers have been cleared. |
| 160 | GPG13: Windows Files Accessed | Show files accessed on the Windows servers. |
| 161 | GPG13: Windows Passwords Changed | Alerts when users have changed their passwords. |
| 162 | GPG13: Windows Permissions Changed | Alerts when user or group permissions have been changed. |
| 163 | GPG13: Windows Policies Changed | Alerts when Windows policies have been changed. |
| 164 | GPG13: Windows Programs Accessed | Alerts when a program is accessed on a Windows server. |
| 165 | GPG13: System Restarted | Alerts when system has been restarted. |
| 166 | GPG13: Windows Software Updates | Alerts when events related to the Windows' software updates. |
| 167 | GPG13: Windows Software Updates Failed | Alerts when failed events related to the software updates. |
| 168 | GPG13: Windows Software Updates Succeeded | Alerts for successful events related to the software updates. |
| 169 | GPG13: Anomalous IDS Alert | Alerts when IDS anomalies are above or below defined threshold. |
| 170 | GPG13: Pulse Connect Secure Policy Change Alert | Displays alert when Pulse Connect Secure policy or configuration change |

## GPG13 reports and alerts and corresponding controls

The following section lists the GPG13 alerts and reports and the corresponding controls.

GPG13 alerts and corresponding controls

GPG13 reports and corresponding controls

## GPG13 alerts and corresponding controls

The following section lists the GPG13 alerts and the corresponding controls.

| Serial number | Alert Name | Compliance Mapping |
|---|---|---|
| 1 | GPG13: Accounts Created | PMC3, PMC4, PMC5, PMC6 |
| 2 | GPG13: Accounts Deleted | PMC3, PMC4, PMC5, PMC6 |
| 3 | GPG13: Accounts Enabled | PMC3, PMC4, PMC5, PMC6 |
| 4 | GPG13: Accounts Locked | PMC3, PMC4, PMC5, PMC6 |
| 5 | GPG13: Accounts Modified | PMC3, PMC4, PMC5, PMC6 |
| 6 | GPG13: Active Directory Changes | PMC4 |
| 7 | GPG13: Active Directory Changes | PMC4 |
| 8 | GPG13: Allowed Connections | PMC2, PMC3, PMC5 |
| 9 | GPG13: Anomalous IDS Alerts | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 10 | GPG13: Check Point Policy Changed | PMC3, PMC4, PMC5, PMC6 |
| 11 | GPG13: Cisco ISE, ACS Configuration Changed | PMC4, PMC5, PMC7 |
| 12 | GPG13: Cisco ISE, ACS Passwords Changed | PMC4, PMC5, PMC8 |
| 13 | GPG13: Cisco PIX, ASA, FWSM Commands Executed | PMC4, PMC5, PMC9 |
| 14 | GPG13: Cisco PIX, ASA, FWSM Failover Disabled | PMC4, PMC5, PMC10 |
| 15 | GPG13: Cisco PIX, ASA, FWSM Failover Errors | PMC3, PMC4, PMC5, PMC6 |
| 16 | GPG13: Cisco PIX, ASA, FWSM Failover Performed | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 17 | GPG13: Cisco PIX, ASA, FWSM Logon Failure | PMC5, PMC6, PMC7 |
| 18 | GPG13: Cisco PIX, ASA, FWSM Logon Success | PMC5, PMC6, PMC8 |

| Serial number | Alert Name | Compliance Mapping |
|---|---|---|
| 19 | GPG13: Cisco PIX, ASA, FWSM Policy Changed | PMC3, PMC4, PMC5, PMC6 |
| 20 | GPG13: System Restarted | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 21 | GPG13: Cisco PIX, ASA, FWSM Routing Failure | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 22 | GPG13: Cisco Switch Device Reload | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 23 | GPG13: Cisco Switch Device Restart | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 24 | GPG13: Cisco Switch HA Failure (ver) | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 25 | GPG13: Cisco Switch Interface Change | PMC4, PMC5, PMC7 |
| 26 | GPG13: Cisco Switch Policy Changed | PMC3, PMC4, PMC5, PMC6 |
| 27 | GPG13: DB2 Database Backup Failed | PMC4, PMC7, PMC8 |
| 28 | GPG13: DB2 Database Configuration Change | PMC4, PMC5, PMC7 |
| 29 | GPG13: DB2 Database Restore Failed | PMC4, PMC5, PMC7, PMC8 |
| 30 | GPG13: DB2 Database Started or Stopped | PMC4, PMC5, PMC7 |
| 31 | GPG13: Escalated Privileges | PMC4, PMC7 |
| 32 | GPG13: Excessive IDS Attack | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 33 | GPG13: Group Members Added | PMC3, PMC4, PMC5, PMC6 |
| 34 | GPG13: Group Members Deleted | PMC3, PMC4, PMC5, PMC6 |
| 35 | GPG13: Groups Created | PMC3, PMC4, PMC5, PMC6 |
| 36 | GPG13: Groups Deleted | PMC3, PMC4, PMC5, PMC6 |
| 37 | GPG13: Groups Modified | PMC3, PMC4, PMC5, PMC6 |

| Serial number | Alert Name | Compliance Mapping |
|---|---|---|
| 38 | GPG13: Guardium SQL Guard Config Changes | PMC4, PMC5, PMC7 |
| 39 | GPG13: Guardium SQL Guard Data Access | PMC4, PMC5, PMC7 |
| 40 | GPG13: Guardium SQL Guard Logins | PMC5, PMC7 |
| 41 | GPG13: Guardium SQL Guard Startup or Shutdown | PMC5, PMC7, PMC9 |
| 42 | GPG13: HP NonStop Audit Configuration Changed | PMC4, PMC5, PMC7 |
| 43 | GPG13: HP NonStop Audit Permission Changed | PMC4, PMC5, PMC7 |
| 44 | GPG13: i5/OS Network Profile Changes | PMC3, PMC4, PMC5, PMC6 |
| 45 | GPG13: i5/OS Permission or Policy Change | PMC3, PMC4, PMC5, PMC6 |
| 46 | GPG13: i5/OS Server or Service Status Change | PMC4, PMC5 |
| 47 | GPG13: i5/OS User Profile Changes | PMC5, PMC7, PMC8 |
| 48 | GPG13: IBM AIX Password Changed | PMC5, PMC7 |
| 49 | GPG13: Juniper Firewall HA State Change | PMC3, PMC5, PMC6 |
| 50 | GPG13: Juniper Firewall Logon Failure | PMC3, PMC6 |
| 51 | GPG13: Juniper Firewall Logon Success | PMC3, PMC6 |
| 52 | GPG13: Juniper Firewall Policy Changes | PMC3, PMC4, PMC5, PMC6 |
| 53 | GPG13: Juniper Firewall System Reset | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 54 | GPG13: Juniper VPN Policy Change | PMC3, PMC4, PMC5, PMC6 |

| Serial number | Alert Name | Compliance Mapping |
|---|---|---|
| 55 | GPG13: Logins Failed | PMC3, PMC4, PMC5, PMC6 |
| 56 | GPG13: Logins Succeeded | PMC2, PMC3, PMC7 |
| 57 | GPG13: LogLogic Disk Full | PMC10 |
| 58 | GPG13: LogLogic DSM Configuration Changes | PMC4, PMC5, PMC10 |
| 59 | GPG13: LogLogic DSM Data Access | PMC5, PMC10 |
| 60 | GPG13: LogLogic DSM Logins | PMC5 |
| 61 | GPG13: LogLogic DSM Startup or Shutdown | PMC5 |
| 62 | GPG13: LogLogic File Retrieval Errors | PMC4, PMC5, PMC10 |
| 63 | GPG13: LogLogic Management Center Backed Up or Restored | PMC4, PMC5 |
| 64 | GPG13: LogLogic Message Routing Errors | PMC4, PMC5, PMC10 |
| 65 | GPG13: LogLogic Universal Collector Configuration Changed | PMC4, PMC5, PMC10 |
| 66 | GPG13: Microsoft Operations Manager - Permissions Changed | PMC5, PMC7 |
| 67 | GPG13: Microsoft Operations Manager - Windows Passwords Changed | PMC5, PMC7 |
| 68 | GPG13: Microsoft Operations Manager - Windows Policies Changed | PMC5, PMC7 |
| 69 | GPG13: Microsoft Sharepoint Permission Changed | PMC4, PMC5, PMC7 |
| 70 | GPG13: Microsoft Sharepoint Policies Added, Removed, Modified | PMC4, PMC5, PMC7 |
| 71 | GPG13: Microsoft SQL Server Backup Failed | PMC4, PMC7, PMC8 |

| Serial number | Alert Name | Compliance Mapping |
|---|---|---|
| 72 | GPG13: Microsoft SQL Server Restore Failed | PMC4, PMC5, PMC7, PMC8 |
| 73 | GPG13: Microsoft SQL Server Shutdown | PMC5, PMC7 |
| 74 | GPG13: NetApp Authentication Failure | PMC5 |
| 75 | GPG13: NetApp Filer Audit Policies Changed | PMC4, PMC5 |
| 76 | GPG13: NetApp Filer File System Full | PMC5 |
| 77 | GPG13: NetApp Filer NIS Group Update | PMC5 |
| 78 | GPG13: NetApp Filer Snapshot Error | PMC4, PMC5, PMC8 |
| 79 | GPG13: Oracle Database Configuration Change | PMC4, PMC5, PMC7 |
| 80 | GPG13: Oracle Database Data Access | PMC5, PMC7 |
| 81 | GPG13: Oracle Database Permissions Changed | PMC5, PMC7 |
| 82 | GPG13: Oracle Database Shutdown | PMC5, PMC7, PMC9 |
| 83 | GPG13: Oracle Database User Added or Deleted | PMC5, PMC7 |
| 84 | GPG13: Pulse Connect Secure Policy Change | PMC3, PMC4, PMC5, PMC6 |
| 85 | GPG13: RACF Files Accessed | PMC4, PMC5 |
| 86 | GPG13: RACF Passwords Changed | PMC5 |
| 87 | GPG13: RACF Permissions Changed | PMC5 |
| 88 | GPG13: RACF Process Started | PMC5 |
| 89 | GPG13: Sidewinder Configuration Changed | PMC2, PMC3, PMC4, PMC5, PMC6 |

| Serial number | Alert Name | Compliance Mapping |
|---|---|---|
| 90 | GPG13: Sybase ASE Database Backed Up or Restored | PMC4, PMC5, PMC7, PMC8 |
| 91 | GPG13: Sybase ASE Database Config Changes | PMC4, PMC5, PMC7 |
| 92 | GPG13: Sybase ASE Database Data Access | PMC5, PMC7 |
| 93 | GPG13: Sybase ASE Database Started | PMC5, PMC7 |
| 94 | GPG13: Sybase ASE Database Stopped | PMC5, PMC7 |
| 95 | GPG13: Symantec Endpoint Protection Configuration Changed | PMC3, PMC4, PMC5, PMC6 |
| 96 | GPG13: Symantec Endpoint Protection Policy Add, Delete, Modify | PMC3, PMC5, PMC6 |
| 97 | GPG13: TIBCO ActiveMatrix Administrator Permission Changed | PMC4, PMC7 |
| 98 | GPG13: vCenter Data Move | PMC7 |
| 99 | GPG13: vCenter Datastore Event | PMC7, PMC8 |
| 100 | GPG13: vCenter Delete Virtual Machine | PMC7 |
| 101 | GPG13: vCenter Firewall Policy Change | PMC3, PMC4 |
| 102 | GPG13: vCenter Orchestrator Datastore Events | PMC7, PMC8 |
| 103 | GPG13: vCenter Orchestrator Delete Virtual Machine | PMC7 |
| 104 | GPG13: vCenter Orchestrator Login Failed | PMC7 |
| 105 | GPG13: vCenter Orchestrator Virtual Machine Shutdown | PMC7 |
| 106 | GPG13: vCenter Permission Change | PMC7 |

| Serial number | Alert Name | Compliance Mapping |
|---|---|---|
| 107 | GPG13: vCenter Restart ESX Services | PMC4, PMC9 |
| 108 | GPG13: vCenter Shutdown or Restart ESX | PMC4, PMC9 |
| 109 | GPG13: vCenter User Login Failed | PMC7 |
| 110 | GPG13: vCenter User Login Successful | PMC7 |
| 111 | GPG13: vCenter Virtual Machine Shutdown | PMC7 |
| 112 | GPG13: vCenter Virtual Machine Started | PMC7 |
| 113 | GPG13: vCloud Director Login Failed | PMC7 |
| 114 | GPG13: vCloud Director Login Success | PMC7 |
| 115 | GPG13: vCloud Organization Modified | PMC7 |
| 116 | GPG13: vCloud User Created | PMC7 |
| 117 | GPG13: vCloud User, Group, or Role Modified | PMC7 |
| 118 | GPG13: vCloud vApp Created, Deleted, or Modified | PMC7 |
| 119 | GPG13: vCloud vDC Created, Modified, or Deleted | PMC7 |
| 120 | GPG13: vShield Edge Configuration Change | PMC3, PMC4, PMC5, PMC6 |
| 121 | GPG13: Windows Audit Log Cleared | PMC7 |
| 122 | GPG13: Windows Files Accessed | PMC7 |
| 123 | GPG13: Windows Passwords Changed | PMC5, PMC7 |

| Serial number | Alert Name | Compliance Mapping |
|---|---|---|
| 124 | GPG13: Windows Permissions Changed | PMC5, PMC7 |
| 125 | GPG13: Windows Policies Changed | PMC3, PMC4, PMC5, PMC6 |
| 126 | GPG13: Windows Programs Accessed | PMC4, PMC7 |
| 127 | GPG13: System Restarted | PMC4, PMC9 |

## GPG13 reports and corresponding controls

The following section lists the GPG13 reports and the corresponding controls.

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 1 | GPG13: Accepted VPN Connections - RADIUS | PMC2, PMC3, PMC6 |
| 2 | GPG13: Account Activities on UNIX Servers | PMC4, PMC7, PMC9 |
| 3 | GPG13: Account Activities on Windows Servers | PMC4, PMC7, PMC9 |
| 4 | GPG13: Accounts Changed on NetApp Filer | PMC5 |
| 5 | GPG13: Accounts Changed on UNIX Servers | PMC7 |
| 6 | GPG13: Accounts Changed on Windows Servers | PMC7 |
| 7 | GPG13: Accounts Created on NetApp Filer | PMC5 |
| 8 | GPG13: Accounts Created on NetApp Filer Audit | PMC5 |
| 9 | GPG13: Accounts Created on Sidewinder | PMC3, PMC5 |
| 10 | GPG13: Accounts Created on Symantec Endpoint Protection | PMC3, PMC5 |
| 11 | GPG13: Accounts Created on UNIX Servers | PMC7 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 12 | GPG13: Accounts Created on Windows Servers | PMC7 |
| 13 | GPG13: Accounts Deleted on NetApp Filer | PMC5 |
| 14 | GPG13: Accounts Deleted on NetApp Filer Audit | PMC5 |
| 15 | GPG13: Accounts Deleted on Sidewinder | PMC3, PMC5 |
| 16 | GPG13: Accounts Deleted on Symantec Endpoint Protection | PMC3, PMC5 |
| 17 | GPG13: Accounts Deleted on UNIX Servers | PMC7 |
| 18 | GPG13: Accounts Deleted on Windows Servers | PMC7 |
| 19 | GPG13: Active Connections for Cisco ASA | PMC3, PMC5, PMC6 |
| 20 | GPG13: Active Connections for Cisco FWSM | PMC3, PMC5, PMC6 |
| 21 | GPG13: Active Connections for Cisco PIX | PMC3, PMC5, PMC6 |
| 22 | GPG13: Active Directory System Changes | PMC4 |
| 23 | GPG13: Active VPN Connections for Cisco VPN Concentrators | PMC3, PMC6 |
| 24 | GPG13: Active VPN Connections for Nortel Contivity | PMC3, PMC6 |
| 25 | GPG13: Active VPN Connections for RADIUS | PMC3, PMC6 |
| 26 | GPG13: Administrator Logins on Windows Servers | PMC7, PMC9 |
| 27 | GPG13: Allowed URLs by Source IPs | PMC2 |
| 28 | GPG13: Allowed URLs by Source IPs - F5 BIG-IP TMOS | PMC2 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 29 | GPG13: Allowed URLs by Source IPs - Microsoft IIS | PMC2 |
| 30 | GPG13: Allowed URLs by Source Users | PMC2 |
| 31 | GPG13: Allowed URLs by Source Users - F5 BIG-IP TMOS | PMC2 |
| 32 | GPG13: Allowed URLs by Source Users - Microsoft IIS | PMC2 |
| 33 | GPG13: Applications Under Attack | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 34 | GPG13: Applications Under Attack - Cisco IOS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 35 | GPG13: Applications Under Attack - FireEye MPS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 36 | GPG13: Applications Under Attack - ISS SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 37 | GPG13: Applications Under Attack - SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 38 | GPG13: Applications Under Attack - Sourcefire Defense Center | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 39 | GPG13: Attackers by Service | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 40 | GPG13: Attackers by Service - Cisco IOS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 41 | GPG13: Attackers by Service - FireEye MPS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 42 | GPG13: Attackers by Service - ISS SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 43 | GPG13: Attackers by Service - SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 44 | GPG13: Attackers by Service - Sourcefire Defense Center | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 45 | GPG13: Attackers by Signature | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 46 | GPG13: Attackers by Signature - Cisco IOS | PMC3, PMC4, PMC5, PMC6, PMC9 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 47 | GPG13: Attackers by Signature - FireEye MPS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 48 | GPG13: Attackers by Signature - ISS SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 49 | GPG13: Attackers by Signature - SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 50 | GPG13: Attackers by Signature - Sourcefire Defense Center | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 51 | GPG13: Attacks Detected | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 52 | GPG13: Attacks Detected - Cisco IOS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 53 | GPG13: Attacks Detected - HIPS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 54 | GPG13: Attacks Detected - ISS SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 55 | GPG13: Attacks Detected - SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 56 | GPG13: Attacks Detected - Sourcefire Defense Center | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 57 | GPG13: Bandwidth Usage by User | PMC2 |
| 58 | GPG13: Blocked URLs by Source IPs | PMC2 |
| 59 | GPG13: Blocked URLs by Source IPs - F5 BIG-IP TMOS | PMC2 |
| 60 | GPG13: Blocked URLs by Source IPs - Microsoft IIS | PMC2 |
| 61 | GPG13: Blocked URLs by Source Users | PMC2 |
| 62 | GPG13: Blocked URLs by Source Users - F5 BIG-IP TMOS | PMC2 |
| 63 | GPG13: Blocked URLs by Source Users - Microsoft IIS | PMC2 |
| 64 | GPG13: Check Point Configuration Changes | PMC3, PMC4, PMC5, PMC6, PMC9 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 65 | GPG13: Check Point Management Station Login | PMC3, PMC5 |
| 66 | GPG13: Check Point Objects Created | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 67 | GPG13: Check Point Objects Deleted | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 68 | GPG13: Check Point Objects Modified | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 69 | GPG13: Check Point SIC Revoked | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 70 | GPG13: Cisco ESA: Attacks by Event ID | PMC3, PMC4, PMC5, PMC6 |
| 71 | GPG13: Cisco ESA: Attacks by Threat Name | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 72 | GPG13: Cisco ESA: Attacks Detected | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 73 | GPG13: Cisco ESA: Scans | PMC3, PMC4, PMC5, PMC6 |
| 74 | GPG13: Cisco ESA: Updated | PMC3, PMC4, PMC5, PMC6 |
| 75 | GPG13: Cisco ISE, ACS Accounts Created | PMC3, PMC4, PMC5, PMC6 |
| 76 | GPG13: Cisco ISE, ACS Accounts Removed | PMC3, PMC4, PMC5, PMC6 |
| 77 | GPG13: Cisco ISE, ACS Configuration Changes | PMC3, PMC4, PMC5, PMC6 |
| 78 | GPG13: Cisco ISE, ACS Password Changes | PMC3, PMC5, PMC6 |
| 79 | GPG13: Cisco Line Protocol Status Changes | PMC3, PMC4, PMC6 |
| 80 | GPG13: Cisco Link Status Changes | PMC3, PMC4, PMC6, PMC9 |
| 81 | GPG13: Cisco Peer Reset/Reload | PMC3, PMC4, PMC6 |
| 82 | GPG13: Cisco Peer Supervisor Status Changes | PMC3, PMC4, PMC6 |
| 83 | GPG13: Cisco PIX, ASA, FWSM Failover Disabled | PMC3, PMC4, PMC5, PMC6 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 84 | GPG13: Cisco PIX, ASA, FWSM Failover Performed | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 85 | GPG13: Cisco PIX, ASA, FWSM Policy Changed | PMC3, PMC4, PMC5, PMC6 |
| 86 | GPG13: Cisco Routers and Switches Restart | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 87 | GPG13: Cisco Switch Policy Changes | PMC3, PMC4, PMC5, PMC6 |
| 88 | GPG13: Creation and Deletion of System Level Objects: AIX Audit | PMC4, PMC5, PMC7 |
| 89 | GPG13: Creation and Deletion of System Level Objects: DB2 Database | PMC4, PMC5, PMC7 |
| 90 | GPG13: Creation and Deletion of System Level Objects: HP-UX Audit | PMC4, PMC5, PMC7 |
| 91 | GPG13: Creation and Deletion of System Level Objects: Oracle | PMC4, PMC5, PMC7 |
| 92 | GPG13: Creation and Deletion of System Level Objects: Solaris BSM | PMC4, PMC5, PMC7 |
| 93 | GPG13: Creation and Deletion of System Level Objects: SQL Server | PMC4, PMC5, PMC7 |
| 94 | GPG13: Creation and Deletion of System Level Objects: Windows | PMC4, PMC7 |
| 95 | GPG13: DB2 Database Backup Failed | PMC4, PMC7, PMC8 |
| 96 | GPG13: DB2 Database Configuration Changes | PMC4, PMC5, PMC7 |
| 97 | GPG13: DB2 Database Failed Logins | PMC5, PMC7 |
| 98 | GPG13: DB2 Database Restore Failed | PMC4, PMC5, PMC7, PMC8 |
| 99 | GPG13: DB2 Database Stop and Start Events | PMC4, PMC5, PMC7 |
| 100 | GPG13: DB2 Database Successful Logins | PMC5, PMC7 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 101 | GPG13: DB2 Database User Additions and Deletions | PMC5, PMC7 |
| 102 | GPG13: Decru DataFort Cryptographic Key Events | PMC5, PMC7 |
| 103 | GPG13: Decru DataFort Zeroization Events | PMC2, PMC3, PMC5, PMC7 |
| 104 | GPG13: Denied Connections - Cisco IOS | PMC2, PMC3, PMC5, PMC6 |
| 105 | GPG13: Denied Connections - Cisco NXOS | PMC2, PMC3, PMC5, PMC6 |
| 106 | GPG13: Denied Connections - Cisco Router | PMC2, PMC3, PMC5, PMC6 |
| 107 | GPG13: Denied Connections - F5 BIG-IP TMOS | PMC2, PMC3, PMC5, PMC6 |
| 108 | GPG13: Denied Connections - Sidewinder | PMC2, PMC3, PMC6 |
| 109 | GPG13: Denied Connections - VMware vShield | PMC2, PMC3, PMC6 |
| 110 | GPG13: Denied Connections by IP Addresses - Check Point | PMC2, PMC3, PMC5, PMC6 |
| 111 | GPG13: Denied Connections by IP Addresses - Cisco ASA | PMC2, PMC3, PMC5, PMC6 |
| 112 | GPG13: Denied Connections by IP Addresses - Cisco FWSM | PMC2, PMC3, PMC5, PMC6 |
| 113 | GPG13: Denied Connections by IP Addresses - Cisco PIX | PMC2, PMC3, PMC5, PMC6 |
| 114 | GPG13: Denied Connections by IP Addresses - Nortel | PMC2, PMC3, PMC6 |
| 115 | GPG13: Denied Inbound Connections - Check Point | PMC2, PMC3, PMC5, PMC6 |
| 116 | GPG13: Denied Inbound Connections - Cisco ASA | PMC2, PMC3, PMC5, PMC6 |
| 117 | GPG13: Denied Inbound Connections - Cisco FWSM | PMC2, PMC3, PMC5, PMC6 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 118 | GPG13: Denied Inbound Connections - Cisco PIX | PMC2, PMC3, PMC5, PMC6 |
| 119 | GPG13: Denied Inbound Connections - Juniper Firewall | PMC2, PMC3, PMC5, PMC6 |
| 120 | GPG13: Denied Outbound Connections - Check Point | PMC2, PMC3, PMC5 |
| 121 | GPG13: Denied Outbound Connections - Cisco ASA | PMC2, PMC3, PMC5 |
| 122 | GPG13: Denied Outbound Connections - Cisco FWSM | PMC2, PMC3, PMC5 |
| 123 | GPG13: Denied Outbound Connections - Cisco PIX | PMC2, PMC3, PMC5 |
| 124 | GPG13: Denied Outbound Connections - Juniper Firewall | PMC2, PMC3, PMC5 |
| 125 | GPG13: Denied VPN Connections - RADIUS | PMC2, PMC3, PMC6 |
| 126 | GPG13: DHCP Granted/Renewed Activities on Microsoft DHCP | PMC4, PMC6 |
| 127 | GPG13: DHCP Granted/Renewed Activities on VMware vShield | PMC4, PMC6 |
| 128 | GPG13: DNS Server Error | PMC4 |
| 129 | GPG13: Domain activities on Symantec Endpoint Protection | PMC4, PMC5 |
| 130 | GPG13: Escalated Privilege Activities on Servers | PMC4, PMC7 |
| 131 | GPG13: ESX Accounts Activities | PMC4 |
| 132 | GPG13: ESX Accounts Created | PMC4 |
| 133 | GPG13: ESX Accounts Deleted | PMC4 |
| 134 | GPG13: ESX Failed Logins | PMC4 |
| 135 | GPG13: ESX Group Activities | PMC4 |
| 136 | GPG13: ESX Kernel log daemon terminating | PMC4, PMC9 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 137 | GPG13: ESX Kernel logging Stop | PMC4 |
| 138 | GPG13: ESX Syslogd Restart | PMC4 |
| 139 | GPG13: F5 BIG-IP TMOS Login Failed | PMC3, PMC5 |
| 140 | GPG13: F5 BIG-IP TMOS Login Successful | PMC3, PMC5 |
| 141 | GPG13: F5 BIG-IP TMOS Password Changes | PMC3, PMC5 |
| 142 | GPG13: F5 BIG-IP TMOS Ports Denied Access | PMC3, PMC5, PMC6 |
| 143 | GPG13: F5 BIG-IP TMOS Restarted | PMC3, PMC4, PMC5, PMC9 |
| 144 | GPG13: Failed Logins | PMC5, PMC6, PMC7 |
| 145 | GPG13: Failed Windows Events Summary | PMC4 |
| 146 | GPG13: Files Accessed on NetApp Filer Audit | PMC4, PMC5 |
| 147 | GPG13: Files Accessed on Servers | PMC4, PMC5 |
| 148 | GPG13: Files Accessed through Juniper SSL VPN (Secure Access) | PMC2, PMC3, PMC4, PMC6 |
| 149 | GPG13: Files Accessed through PANOS | PMC2, PMC3, PMC4, PMC5, PMC6 |
| 150 | GPG13: Files Accessed Through Pulse Connect Secure | PMC2, PMC3, PMC4, PMC6 |
| 151 | GPG13: Files Downloaded via Proxy | PMC2, PMC4 |
| 152 | GPG13: Files Downloaded via Proxy - Blue Coat | PMC2, PMC4 |
| 153 | GPG13: Files Downloaded via Proxy - Cisco WSA | PMC2, PMC4 |
| 154 | GPG13: Files Downloaded via Proxy - Microsoft IIS | PMC2, PMC4 |
| 155 | GPG13: Files Downloaded via the Web | PMC2, PMC4 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 156 | GPG13: Files Downloaded via the Web - F5 BIG-IP TMOS | PMC2, PMC4 |
| 157 | GPG13: Files Downloaded via the Web - Microsoft IIS | PMC2, PMC4 |
| 158 | GPG13: Files Uploaded via Proxy | PMC2, PMC4 |
| 159 | GPG13: Files Uploaded via Proxy - Blue Coat | PMC2, PMC4 |
| 160 | GPG13: Files Uploaded via Proxy - Cisco WSA | PMC2, PMC4 |
| 161 | GPG13: Files Uploaded via Proxy - Microsoft IIS | PMC2, PMC4 |
| 162 | GPG13: Files Uploaded via the Web | PMC2, PMC4 |
| 163 | GPG13: Files Uploaded via the Web - F5 BIG-IP TMOS | PMC2, PMC4 |
| 164 | GPG13: Files Uploaded via the Web - Microsoft IIS | PMC2, PMC4 |
| 165 | GPG13: FireEye MPS: Attacks by Event ID | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 166 | GPG13: FireEye MPS: Attacks by Threat Name | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 167 | GPG13: FireEye MPS: Attacks Detected | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 168 | GPG13: FortiOS DLP Attacks Detected | PMC4, PMC5, PMC6, PMC9 |
| 169 | GPG13: FortiOS: Attacks by Event ID | PMC4, PMC5, PMC6, PMC9 |
| 170 | GPG13: FortiOS: Attacks by Threat Name | PMC4, PMC5, PMC6, PMC9 |
| 171 | GPG13: FortiOS: Attacks Detected | PMC4, PMC5, PMC6, PMC9 |
| 172 | GPG13: Group Activities on NetApp Filer Audit | PMC4, PMC5 |
| 173 | GPG13: Group Activities on Symantec Endpoint Protection | PMC4, PMC5, PMC6 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 174 | GPG13: Group Activities on UNIX Servers | PMC7 |
| 175 | GPG13: Group Activities on Windows Servers | PMC7 |
| 176 | GPG13: Groups Created on UNIX Servers | PMC7 |
| 177 | GPG13: Groups Created on Windows Servers | PMC7 |
| 178 | GPG13: Groups Deleted on UNIX Servers | PMC7 |
| 179 | GPG13: Groups Deleted on Windows Servers | PMC7 |
| 180 | GPG13: Guardium SQL Guard Audit Configuration Changes | PMC4, PMC5, PMC7 |
| 181 | GPG13: Guardium SQL Guard Audit Data Access | PMC4, PMC5, PMC7 |
| 182 | GPG13: Guardium SQL Guard Audit Logins | PMC5, PMC7 |
| 183 | GPG13: Guardium SQL Guard Audit Startup or Shutdown | PMC5, PMC7, PMC9 |
| 184 | GPG13: Guardium SQL Guard Configuration Changes | PMC4, PMC5, PMC7 |
| 185 | GPG13: Guardium SQL Guard Data Access | PMC4, PMC5, PMC7 |
| 186 | GPG13: Guardium SQL Guard Logins | PMC5, PMC7 |
| 187 | GPG13: Guardium SQL Guard Startup or Shutdown | PMC5, PMC7, PMC9 |
| 188 | GPG13: HP NonStop Audit Configuration Changes | PMC4, PMC5, PMC7 |
| 189 | GPG13: HP NonStop Audit Login Failed | PMC5, PMC7 |
| 190 | GPG13: HP NonStop Audit Login Successful | PMC5, PMC7 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 191 | GPG13: HP NonStop Audit Object Access | PMC4, PMC5, PMC7 |
| 192 | GPG13: HP NonStop Audit Object Changes | PMC4, PMC5, PMC7 |
| 193 | GPG13: HP NonStop Audit Permissions Changed | PMC4, PMC5, PMC7 |
| 194 | GPG13: i5/OS Access Control List Modifications | PMC4, PMC5, PMC7 |
| 195 | GPG13: i5/OS Audit Configuration Changes | PMC4, PMC5, PMC7 |
| 196 | GPG13: i5/OS Internet Security Management Events | PMC4, PMC5, PMC9 |
| 197 | GPG13: i5/OS Key Ring File Events | PMC7 |
| 198 | GPG13: i5/OS Network Authentication Events | PMC5, PMC6, PMC7 |
| 199 | GPG13: i5/OS Object Access | PMC4, PMC5, PMC7 |
| 200 | GPG13: i5/OS Object Creation and Deletion | PMC7 |
| 201 | GPG13: i5/OS Restore Events | PMC8 |
| 202 | GPG13: i5/OS Server Security User Information Actions | PMC4, PMC5, PMC7 |
| 203 | GPG13: i5/OS System Management Changes | PMC4, PMC5 |
| 204 | GPG13: i5/OS User Profile Creation, Modification, or Restoration | PMC5, PMC7, PMC8 |
| 205 | GPG13: Juniper Firewall Escalated Privilege | PMC3, PMC5, PMC6 |
| 206 | GPG13: Juniper Firewall Policy Changed | PMC3, PMC4, PMC5, PMC6 |
| 207 | GPG13: Juniper Firewall Reset Accepted | PMC3, PMC5, PMC6 |
| 208 | GPG13: Juniper Firewall Reset Imminent | PMC3, PMC5, PMC6 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 209 | GPG13: Juniper Firewall Restarted | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 210 | GPG13: Juniper Firewall VPN Tunnel Status Change | PMC3, PMC4, PMC5, PMC6 |
| 211 | GPG13: Juniper SSL VPN (Secure Access) Policy Changed | PMC3, PMC4, PMC6 |
| 212 | GPG13: Juniper SSL VPN (Secure Access) Successful Logins | PMC3, PMC6 |
| 213 | GPG13: Juniper SSL VPN Successful Logins | PMC3, PMC6 |
| 214 | GPG13: Last Activities Performed by Administrators | PMC4, PMC5, PMC7 |
| 215 | GPG13: Last Activities Performed by All Users | PMC4, PMC5, PMC7 |
| 216 | GPG13: Logins by Authentication Type | PMC5, PMC7 |
| 217 | GPG13: LogLogic DSM Configuration Changes | PMC4, PMC5, PMC10 |
| 218 | GPG13: LogLogic DSM Data Access | PMC5, PMC10 |
| 219 | GPG13: LogLogic DSM Logins | PMC5 |
| 220 | GPG13: LogLogic DSM Startup or Shutdown | PMC5 |
| 221 | GPG13: LogLogic File Retrieval Errors | PMC4, PMC5, PMC10 |
| 222 | GPG13: LogLogic Management Center Account Activities | PMC5 |
| 223 | GPG13: LogLogic Management Center Backup Activities | PMC5 |
| 224 | GPG13: LogLogic Management Center Login | PMC5 |
| 225 | GPG13: LogLogic Management Center Restore Activities | PMC4, PMC5 |
| 226 | GPG13: LogLogic Message Routing Errors | PMC4, PMC5, PMC10 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 227 | GPG13: LogLogic Universal Collector Configuration Changes | PMC4, PMC5, PMC10 |
| 228 | GPG13: McAfee AntiVirus: Attacks by Event ID | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 229 | GPG13: McAfee AntiVirus: Attacks by Threat Name | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 230 | GPG13: McAfee AntiVirus: Attacks Detected | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 231 | GPG13: Microsoft Operations Manager - Failed Windows Events | PMC4, PMC5, PMC7, PMC8 |
| 232 | GPG13: Microsoft Operations Manager - Windows Accounts Activities | PMC4, PMC5, PMC7 |
| 233 | GPG13: Microsoft Operations Manager - Windows Accounts Changed | PMC5, PMC7 |
| 234 | GPG13: Microsoft Operations Manager - Windows Accounts Created | PMC5, PMC7 |
| 235 | GPG13: Microsoft Operations Manager - Windows Accounts Enabled | PMC5, PMC7 |
| 236 | GPG13: Microsoft Operations Manager - Windows Events by Users | PMC5, PMC7 |
| 237 | GPG13: Microsoft Operations Manager - Windows Events Summary | PMC5, PMC7 |
| 238 | GPG13: Microsoft Operations Manager - Windows Password Changes | PMC5, PMC7 |
| 239 | GPG13: Microsoft Operations Manager - Windows Permissions Modified | PMC5, PMC7 |
| 240 | GPG13: Microsoft Operations Manager - Windows Policies Modified | PMC5, PMC7 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 241 | GPG13: Microsoft Operations Manager - Windows Servers Restarted | PMC4, PMC5, PMC9 |
| 242 | GPG13: Microsoft Sharepoint Content Deleted | PMC4, PMC5 |
| 243 | GPG13: Microsoft Sharepoint Content Updates | PMC4, PMC5 |
| 244 | GPG13: Microsoft Sharepoint Permissions Changed | PMC4, PMC5, PMC7 |
| 245 | GPG13: Microsoft Sharepoint Policy Add, Remove, or Modify | PMC4, PMC5, PMC7 |
| 246 | GPG13: Microsoft SQL Server Backup Failed | PMC4, PMC5, PMC7, PMC8 |
| 247 | GPG13: Microsoft SQL Server Configuration Changes | PMC4, PMC5, PMC7 |
| 248 | GPG13: Microsoft SQL Server Data Access | PMC5, PMC7 |
| 249 | GPG13: Microsoft SQL Server Database Failed Logins | PMC5, PMC7 |
| 250 | GPG13: Microsoft SQL Server Database Permission Events | PMC5, PMC7 |
| 251 | GPG13: Microsoft SQL Server Database Successful Logins | PMC5, PMC7 |
| 252 | GPG13: Microsoft SQL Server Database User Additions and Deletions | PMC5, PMC7 |
| 253 | GPG13: Microsoft SQL Server Password Changes | PMC5, PMC7 |
| 254 | GPG13: Microsoft SQL Server Restore Failed | PMC4, PMC5, PMC7, PMC8 |
| 255 | GPG13: Microsoft SQL Server Schema Corruption | PMC4, PMC5, PMC7, PMC9 |
| 256 | GPG13: Microsoft SQL Server Shutdown by Reason | PMC5, PMC7 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 257 | GPG13: Most Active Email Senders - Exchange 2000/2003 | PMC5 |
| 258 | GPG13: Most Active Ports Through Firewall - Check Point | PMC3, PMC5 |
| 259 | GPG13: Most Active Ports Through Firewall - Cisco ASA | PMC3, PMC5 |
| 260 | GPG13: Most Active Ports Through Firewall - Cisco FWSM | PMC3, PMC5 |
| 261 | GPG13: Most Active Ports Through Firewall - Cisco PIX | PMC3, PMC5 |
| 262 | GPG13: Most Active Ports Through Firewall - Fortinet | PMC3, PMC5 |
| 263 | GPG13: Most Active Ports Through Firewall - Juniper Firewall | PMC3, PMC5 |
| 264 | GPG13: Most Active Ports Through Firewall - Nortel | PMC3, PMC5 |
| 265 | GPG13: NetApp Filer Audit Accounts Enabled | PMC5 |
| 266 | GPG13: NetApp Filer Audit Group Members Added | PMC5 |
| 267 | GPG13: NetApp Filer Audit Group Members Deleted | PMC5 |
| 268 | GPG13: NetApp Filer Audit Login Failed | PMC5 |
| 269 | GPG13: NetApp Filer Audit Login Successful | PMC5 |
| 270 | GPG13: NetApp Filer Audit Logs Cleared | PMC5 |
| 271 | GPG13: NetApp Filer Audit Policies Modified | PMC4, PMC5 |
| 272 | GPG13: NetApp Filer File Activity | PMC5 |
| 273 | GPG13: NetApp Filer Login Failed | PMC5 |
| 274 | GPG13: NetApp Filer Login Successful | PMC5 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 275 | GPG13: NetApp Filer Password Changes | PMC5 |
| 276 | GPG13: NetApp Filer Snapshot Error | PMC4, PMC5, PMC8 |
| 277 | GPG13: Network Traffic per Rule - Check Point | PMC2, PMC3, PMC5 |
| 278 | GPG13: Network Traffic per Rule - Juniper Firewall | PMC2, PMC3, PMC5 |
| 279 | GPG13: Network Traffic per Rule - Nortel | PMC2, PMC3, PMC5 |
| 280 | GPG13: Oracle Database Configuration Changes | PMC2 PMC3 PMC4 PMC5 PMC7 |
| 281 | GPG13: Oracle Database Data Access | PMC5, PMC7 |
| 282 | GPG13: Oracle Database Failed Logins | PMC5, PMC7 |
| 283 | GPG13: Oracle Database Permission Events | PMC5, PMC7 |
| 284 | GPG13: Oracle Database Shutdown | PMC5, PMC7, PMC9 |
| 285 | GPG13: Oracle Database Successful Logins | PMC5, PMC7 |
| 286 | GPG13: Oracle Database User Additions and Deletions | PMC5, PMC7 |
| 287 | GPG13: PANOS: Attacks by Event ID | PMC3, PMC4, PMC5, PMC6 |
| 288 | GPG13: PANOS: Attacks by Threat Name | PMC3, PMC4, PMC5, PMC6 |
| 289 | GPG13: PANOS: Attacks Detected | PMC3, PMC4, PMC5, PMC6 |
| 290 | GPG13: Password Changes on Windows Servers | PMC7 |
| 291 | GPG13: Peer Servers and Status | PMC2, PMC4 |
| 292 | GPG13: Peer Servers and Status - Blue Coat | PMC2, PMC4 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 293 | GPG13: Peer Servers and Status - Cisco WSA | PMC2, PMC4 |
| 294 | GPG13: Peer Servers and Status - Microsoft IIS | PMC2, PMC4 |
| 295 | GPG13: Periodic Review of Log Reports | PMC4, PMC5, PMC7 |
| 296 | GPG13: Periodic Review of User Access Logs | PMC4, PMC5, PMC7 |
| 297 | GPG13: Permissions Modified on Windows Servers | PMC4, PMC5, PMC7 |
| 298 | GPG13: Policies Modified on Windows Servers | PMC4, PMC5, PMC7 |
| 299 | GPG13: Ports Allowed Access - Check Point | PMC2, PMC3, PMC5 |
| 300 | GPG13: Ports Allowed Access - Cisco ASA | PMC2, PMC3, PMC5 |
| 301 | GPG13: Ports Allowed Access - Cisco FWSM | PMC2, PMC3, PMC5 |
| 302 | GPG13: Ports Allowed Access - Cisco IOS | PMC2, PMC3, PMC5 |
| 303 | GPG13: Ports Allowed Access - Cisco Netflow | PMC2, PMC3, PMC5 |
| 304 | GPG13: Ports Allowed Access - Cisco PIX | PMC2, PMC3, PMC5 |
| 305 | GPG13: Ports Allowed Access - F5 BIG-IP TMOS | PMC2, PMC3, PMC5 |
| 306 | GPG13: Ports Allowed Access - Fortinet | PMC2, PMC3, PMC5 |
| 307 | GPG13: Ports Allowed Access - Juniper Firewall | PMC2, PMC3, PMC5 |
| 308 | GPG13: Ports Allowed Access - Juniper JunOS | PMC2, PMC3, PMC5 |
| 309 | GPG13: Ports Allowed Access - Juniper RT Flow | PMC2, PMC3, PMC5 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 310 | GPG13: Ports Allowed Access - Nortel | PMC2, PMC3, PMC5 |
| 311 | GPG13: Ports Allowed Access - PANOS | PMC2, PMC3, PMC5 |
| 312 | GPG13: Ports Allowed Access - Sidewinder | PMC2, PMC3, PMC5 |
| 313 | GPG13: Ports Allowed Access - VMware vShield | PMC2, PMC3, PMC5 |
| 314 | GPG13: Ports Denied Access - Check Point | PMC2, PMC3, PMC5, PMC6 |
| 315 | GPG13: Ports Denied Access - Cisco ASA | PMC2, PMC3, PMC5, PMC6 |
| 316 | GPG13: Ports Denied Access - Cisco FWSM | PMC2, PMC3, PMC5, PMC6 |
| 317 | GPG13: Ports Denied Access - Cisco IOS | PMC2, PMC3, PMC5, PMC6 |
| 318 | GPG13: Ports Denied Access - Cisco PIX | PMC2, PMC3, PMC5, PMC6 |
| 319 | GPG13: Ports Denied Access - Cisco Router | PMC2, PMC3, PMC5, PMC6 |
| 320 | GPG13: Ports Denied Access - Fortinet | PMC2, PMC3, PMC5, PMC6 |
| 321 | GPG13: Ports Denied Access - Juniper Firewall | PMC2, PMC3, PMC5, PMC6 |
| 322 | GPG13: Ports Denied Access - Juniper JunOS | PMC2, PMC3, PMC5, PMC6 |
| 323 | GPG13: Ports Denied Access - Juniper RT Flow | PMC2, PMC3, PMC5, PMC6 |
| 324 | GPG13: Ports Denied Access - Nortel | PMC2, PMC3, PMC5, PMC6 |
| 325 | GPG13: Ports Denied Access - PANOS | PMC2, PMC3, PMC5, PMC6 |
| 326 | GPG13: Ports Denied Access - Sidewinder | PMC2, PMC3, PMC5, PMC6 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 327 | GPG13: Ports Denied Access - VMware vShield | PMC2, PMC3, PMC5, PMC6 |
| 328 | GPG13: Pulse Connect Secure Failed Logins | PMC3, PMC6 |
| 329 | GPG13: Pulse Connect Secure Policy Change | PMC3, PMC4, PMC6 |
| 330 | GPG13: Pulse Connect Secure successful logins | PMC3, PMC6 |
| 331 | GPG13: RACF Accounts Created | PMC5, PMC7 |
| 332 | GPG13: RACF Accounts Deleted | PMC5, PMC7 |
| 333 | GPG13: RACF Accounts Modified | PMC5, PMC7 |
| 334 | GPG13: RACF Failed Logins | PMC5, PMC6 |
| 335 | GPG13: RACF Files Accessed | PMC4, PMC5 |
| 336 | GPG13: RACF Password Changed | PMC5 |
| 337 | GPG13: RACF Permissions Changed | PMC5 |
| 338 | GPG13: RACF Process Started | PMC5 |
| 339 | GPG13: RACF Successful Logins | PMC5, PMC7 |
| 340 | GPG13: Root Logins | PMC7 |
| 341 | GPG13: Sensors Generating Alerts | PMC2, PMC3, PMC5, PMC6 |
| 342 | GPG13: Sensors Generating Alerts - Cisco IOS | PMC2, PMC3, PMC5, PMC6 |
| 343 | GPG13: Sensors Generating Alerts - FireEye MPS | PMC2, PMC3, PMC5, PMC6 |
| 344 | GPG13: Sensors Generating Alerts - ISS SiteProtector | PMC2, PMC3, PMC5, PMC6 |
| 345 | GPG13: Sensors Generating Alerts - SiteProtector | PMC2, PMC3, PMC5, PMC6 |
| 346 | GPG13: Sensors Generating Alerts - Sourcefire Defense Center | PMC2, PMC3, PMC5, PMC6 |
| 347 | GPG13: Servers Under Attack | PMC3, PMC4, PMC5, PMC6, PMC9 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 348 | GPG13: Servers Under Attack - Cisco IOS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 349 | GPG13: Servers Under Attack - FireEye MPS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 350 | GPG13: Servers Under Attack - HIPS | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 351 | GPG13: Servers Under Attack - ISS SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 352 | GPG13: Servers Under Attack - SiteProtector | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 353 | GPG13: Servers Under Attack - Sourcefire Defense Center | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 354 | GPG13: Sidewinder Configuration Changes | PMC2, PMC3, PMC4, PMC5, PMC6 |
| 355 | GPG13: Source of Attacks | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 356 | GPG13: Source of Attacks - Cisco IOS | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 357 | GPG13: Source of Attacks - FireEye MPS | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 358 | GPG13: Source of Attacks - HIPS | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 359 | GPG13: Source of Attacks - ISS SiteProtector | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 360 | GPG13: Source of Attacks - SiteProtector | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 361 | GPG13: Source of Attacks - Sourcefire Defense Center | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 362 | GPG13: Successful Logins | PMC2 PMC3 PMC7 |
| 363 | GPG13: Sybase ASE Database Backup and Restoration | PMC4, PMC5, PMC7, PMC8 |
| 364 | GPG13: Sybase ASE Database Configuration Changes | PMC4, PMC5, PMC7 |
| 365 | GPG13: Sybase ASE Database Create Events | PMC5, PMC7 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 366 | GPG13: Sybase ASE Database Data Access | PMC5, PMC7 |
| 367 | GPG13: Sybase ASE Database Drop Events | PMC5, PMC7 |
| 368 | GPG13: Sybase ASE Database Startup or Shutdown | PMC5, PMC7 |
| 369 | GPG13: Sybase ASE Database User Additions and Deletions | PMC5, PMC7 |
| 370 | GPG13: Sybase ASE Failed Logins | PMC5, PMC7 |
| 371 | GPG13: Sybase ASE Successful Logins | PMC5, PMC7 |
| 372 | GPG13: Symantec AntiVirus: Attacks by Threat Name | PCM2PMC3, PMC4, PMC5, PMC6, PMC9 |
| 373 | GPG13: Symantec AntiVirus: Attacks Detected | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 374 | GPG13: Symantec AntiVirus: Scans | PMC3, PMC5, PMC6 |
| 375 | GPG13: Symantec AntiVirus: Updated | PMC3, PMC4, PMC5, PMC6 |
| 376 | GPG13: Symantec Endpoint Protection Configuration Changes | PMC3, PMC4, PMC5, PMC6 |
| 377 | GPG13: Symantec Endpoint Protection Password Changes | PMC3, PMC5, PMC6 |
| 378 | GPG13: Symantec Endpoint Protection Policy Add, Remove, or Modify | PMC3, PMC5, PMC6 |
| 379 | GPG13: Symantec Endpoint Protection: Attacks by Threat Name | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 380 | GPG13: Symantec Endpoint Protection: Attacks Detected | PMC3, PMC4, PMC5, PMC6, PMC9 |
| 381 | GPG13: Symantec Endpoint Protection: Scans | PMC3, PMC5, PMC6 |
| 382 | GPG13: Symantec Endpoint Protection: Updated | PMC3, PMC4, PMC5, PMC6 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 383 | GPG13: TIBCO ActiveMatrix Administrator Failed Logins | PMC7 |
| 384 | GPG13: TIBCO ActiveMatrix Administrator Permission Changes | PMC4, PMC7 |
| 385 | GPG13: TIBCO ActiveMatrix Administrator Successful Logins | PMC7 |
| 386 | GPG13: TIBCO Administrator Password Changes | PMC7 |
| 387 | GPG13: TIBCO Administrator Permission Changes | PMC7 |
| 388 | GPG13: TrendMicro Control Manager: Attacks Detected | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 389 | GPG13: TrendMicro Control Manager: Attacks Detected by Threat Name | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 390 | GPG13: TrendMicro OfficeScan: Attacks Detected | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 391 | GPG13: TrendMicro OfficeScan: Attacks Detected by Threat Name | PMC2, PMC3, PMC4, PMC5, PMC6, PMC9 |
| 392 | GPG13: Tripwire Modifications, Additions, and Deletions | PMC2 PMC3 PMC4 PMC5 PMC7 |
| 393 | GPG13: Trusted Domain Deleted on Windows Servers | PMC7 |
| 394 | GPG13: Unauthorized Logins | PMC2, PMC6 |
| 395 | GPG13: Unencrypted Logins | PMC2, PMC6 |
| 396 | GPG13: Unencrypted Network Services - Check Point | PMC3, PMC6 |
| 397 | GPG13: Unencrypted Network Services - Cisco ASA | PMC3, PMC6 |
| 398 | GPG13: Unencrypted Network Services - Cisco FWSM | PMC3, PMC6 |
| 399 | GPG13: Unencrypted Network Services - Cisco IOS | PMC3, PMC6 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 400 | GPG13: Unencrypted Network Services - Cisco Netflow | PMC3, PMC6 |
| 401 | GPG13: Unencrypted Network Services - Cisco PIX | PMC3, PMC6 |
| 402 | GPG13: Unencrypted Network Services - F5 BIG-IP TMOS | PMC3, PMC6 |
| 403 | GPG13: Unencrypted Network Services - Fortinet | PMC3, PMC6 |
| 404 | GPG13: Unencrypted Network Services - Juniper Firewall | PMC3, PMC6 |
| 405 | GPG13: Unencrypted Network Services - Juniper JunOS | PMC3, PMC6 |
| 406 | GPG13: Unencrypted Network Services - Juniper RT Flow | PMC3, PMC6 |
| 407 | GPG13: Unencrypted Network Services - Nortel | PMC3, PMC6 |
| 408 | GPG13: Unencrypted Network Services - PANOS | PMC3, PMC6 |
| 409 | GPG13: Unencrypted Network Services - Sidewinder | PMC3, PMC6 |
| 410 | GPG13: Unencrypted Network Services - VMware vShield | PMC3, PMC6 |
| 411 | GPG13: UNIX Failed Logins | PMC7 |
| 412 | GPG13: Users Created on Servers | PMC7 |
| 413 | GPG13: Users Removed from Servers | PMC7 |
| 414 | GPG13: Users Using the Proxies | PMC2 |
| 415 | GPG13: Users Using the Proxies - Blue Coat | PMC2 |
| 416 | GPG13: Users Using the Proxies - Cisco WSA | PMC2 |
| 417 | GPG13: Users Using the Proxies - Microsoft IIS | PMC2 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 418 | GPG13: vCenter Change Attributes | PMC4 |
| 419 | GPG13: vCenter Datastore Events | PMC8 |
| 420 | GPG13: vCenter Modify Firewall Policy | PMC3, PMC4 |
| 421 | GPG13: vCenter Orchestrator Change Attributes | PMC4, PMC7 |
| 422 | GPG13: vCenter Orchestrator Data Move | PMC7 |
| 423 | GPG13: vCenter Orchestrator Datastore Events | PMC7, PMC8 |
| 424 | GPG13: vCenter Orchestrator Failed Logins | PMC7 |
| 425 | GPG13: vCenter Orchestrator Virtual Machine Created | PMC7 |
| 426 | GPG13: vCenter Orchestrator Virtual Machine Deleted | PMC7 |
| 427 | GPG13: vCenter Orchestrator Virtual Machine Shutdown | PMC7 |
| 428 | GPG13: vCenter Orchestrator Virtual Machine Started | PMC7 |
| 429 | GPG13: vCenter Shutdown or Restart of ESX Server | PMC4, PMC9 |
| 430 | GPG13: vCenter Successful Logins | PMC7 |
| 431 | GPG13: vCenter User Permission Change | PMC7 |
| 432 | GPG13: vCenter Virtual Machine Created | PMC7 |
| 433 | GPG13: vCenter Virtual Machine Deleted | PMC7 |
| 434 | GPG13: vCenter Virtual Machine Shutdown | PMC7 |
| 435 | GPG13: vCenter Virtual Machine Started | PMC7 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 436 | GPG13: vCloud Failed Logins | PMC7 |
| 437 | GPG13: vCloud Organization Created | PMC7 |
| 438 | GPG13: vCloud Organization Deleted | PMC7 |
| 439 | GPG13: vCloud Organization Modified | PMC7 |
| 440 | GPG13: vCloud Successful Logins | PMC7 |
| 441 | GPG13: vCloud User Created | PMC7 |
| 442 | GPG13: vCloud User Deleted or Removed | PMC7 |
| 443 | GPG13: vCloud vApp Created, Modified, or Deleted | PMC7 |
| 444 | GPG13: vCloud vDC Created, Modified, or Deleted | PMC7 |
| 445 | GPG13: VPN Connection Average Bandwidth | PMC3 |
| 446 | GPG13: VPN Connection Average Duration | PMC3 |
| 447 | GPG13: VPN Connection Disconnect Reasons | PMC2 PMC3 |
| 448 | GPG13: VPN Connections by Users | PMC2 PMC3 |
| 449 | GPG13: VPN Denied Connections by Users | PMC2 PMC3 |
| 450 | GPG13: VPN Sessions by Destination IPs | PMC2 PMC3 |
| 451 | GPG13: VPN Sessions by Source IPs | PMC2 PMC3 |
| 452 | GPG13: VPN Sessions by Users | PMC2 PMC3 |
| 453 | GPG13: VPN Users Accessing Corporate Network | PMC2 PMC3 |
| 454 | GPG13: vShield Edge Configuration Changes | PMC3, PMC4, PMC5, PMC6 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 455 | GPG13: Web Access from All Users | PMC2 PMC3 |
| 456 | GPG13: Web Access from All Users - F5 BIG-IP TMOS | PMC2 PMC3 |
| 457 | GPG13: Web Access from All Users - Fortinet | PMC2 PMC3 |
| 458 | GPG13: Web Access from All Users - Microsoft IIS | PMC2 PMC3 |
| 459 | GPG13: Web Access from All Users - PANOS | PMC2 PMC3 |
| 460 | GPG13: Web Access to Applications | PMC2 PMC3 |
| 461 | GPG13: Web Access to Applications - F5 BIG-IP TMOS | PMC2 |
| 462 | GPG13: Web Access to Applications - Fortinet | PMC2 |
| 463 | GPG13: Web Access to Applications - Microsoft IIS | PMC2 |
| 464 | GPG13: Web Access to Applications - PANOS | PMC2 |
| 465 | GPG13: Web URLs Visited | PMC2 |
| 466 | GPG13: Web URLs Visited - F5 BIG-IP TMOS | PMC2 |
| 467 | GPG13: Web URLs Visited - Fortinet | PMC2 |
| 468 | GPG13: Web URLs Visited - Microsoft IIS | PMC2 |
| 469 | GPG13: Web URLs Visited - PANOS | PMC2 |
| 470 | GPG13: Web URLs Visited via Proxy | PMC2 |
| 471 | GPG13: Web URLs Visited via Proxy - Blue Coat | PMC2 |
| 472 | GPG13: Web URLs Visited via Proxy - Cisco WSA | PMC2 |
| 473 | GPG13: Web URLs Visited via Proxy - Microsoft IIS | PMC2 |

| Sr. no | Report Name | Compliance Mapping |
|---|---|---|
| 474 | GPG13: Windows Accounts Enabled | PMC7 |
| 475 | GPG13: Windows Audit Logs Cleared | PMC7 |
| 476 | GPG13: Windows Events by Users | PMC7 |
| 477 | GPG13: Windows Events Summary | PMC4, PMC7, PMC8 |
| 478 | GPG13: Windows Group Members Added | PMC7 |
| 479 | GPG13: Windows Group Members Deleted | PMC7 |
| 480 | GPG13: Windows New Services Installed | PMC4, PMC7 |
| 481 | GPG13: Windows Programs Accessed | PMC4, PMC7 |
| 482 | GPG13: Windows Servers Restarted | PMC4, PMC9 |
| 483 | GPG13: Windows Software Update Successes | PMC4 |