# Table of Contents

**Introduction** ................................................................. 1  
About PCI DSS ................................................................. 1  
About Splunk App for PCI Compliance .............................. 1  
How this app works with Splunk Enterprise Security ............. 3  
Get support and find information about Splunk software ......... 3

**Prepare for your deployment** .............................................. 4  
Understand the Splunk App for PCI Compliance .................. 4  
Identify data sources ....................................................... 5  
Deployment options ....................................................... 7

**Add data** ........................................................................... 14  
Data management overview ................................................. 14  
Using technology add-ons with the Splunk App for PCI Compliance ................................................................. 17

**Install the app** ................................................................. 19  
Install prerequisites ........................................................ 19  
Install the Splunk App for PCI Compliance ......................... 19  
Install technology add-ons ................................................. 21

**Configure the app** ............................................................ 23  
Steps to configure the Splunk App for PCI Compliance .......... 23  
Configure assets ............................................................ 23  
Configure identities ......................................................... 25  
Configure Primary Functions list ...................................... 27  
Configure Prohibited Traffic list ...................................... 28  
Configure Interesting Services list ................................... 29  
Configure Interesting Processes list .................................. 31  
Configure Interesting Ports list ......................................... 32  
Customize the menu bar in Splunk App for PCI Compliance ...... 33  
Configure and deploy indexes ....................................... 38  
Configure users and roles .............................................. 39

**Configure reports** ............................................................ 48  
Reports in the Splunk App for PCI Compliance ................. 48  
Firewall Rule Activity ................................................... 49  
Network Traffic Activity ............................................... 51  
Default Account Access ............................................... 52  
Insecure Authentication Attempts .................................... 54
# Table of Contents

**Configure reports**
- PCI System Inventory ................................................................. 56
- Primary Functions ........................................................................ 59
- Prohibited Services ..................................................................... 61
- System Misconfigurations ......................................................... 64
- Weak Encrypted Communication ............................................... 65
- Wireless Network Misconfigurations .......................................... 66
- Credit Card Data Found ............................................................... 67
- Endpoint Product Deployment ..................................................... 68
- Endpoint Product Versions ......................................................... 70
- Malware Activity ......................................................................... 72
- Malware Signature Updates ......................................................... 73
- Update Service Status ................................................................. 74
- System Update Status ................................................................ 76
- Anomalous System Uptime .......................................................... 77
- PCI Command History ............................................................... 78
- PCI Resource Access .................................................................. 79
- Endpoint Changes ....................................................................... 80
- System Time Synchronization .................................................... 82
- Privileged User Activity .............................................................. 83
- PCI Asset Logging ...................................................................... 84
- Vulnerability Scan Details .......................................................... 85
- Rogue Wireless Access Point Protection .................................... 86
- IDS/IPS Alert Activity ................................................................. 88

**Configure correlation searches** .................................................. 90
- Configure correlation searches ................................................... 90
- Create new correlation searches ................................................. 98
- Notable events ............................................................................ 100
- Configure Incident Workflow .................................................... 103

**Upgrade your existing deployment** ........................................... 110
- Plan the upgrade ........................................................................ 110
- Upgrade the Splunk App for PCI Compliance ............................ 111

**Resources** ............................................................................... 117
- Troubleshoot your deployment ................................................ 117
- FAQ ......................................................................................... 118
Introduction

About PCI DSS

The Payment Card Industry Data Security Standard, or PCI DSS, is an industry standard for all organizations that handle cardholder data. This data can include credit cards, debit cards, ATM cards, and point of sale (POS) cards. The standard protects cardholder data and minimizes the possibility of cardholder data theft and/or loss. PCI DSS requires that all merchants, service providers, and financial institutions meet minimum levels of security and monitoring of the systems in their cardholder data environment (CDE).

The Data Security Standard is made up of 12 requirements that businesses are expected to comply with. These requirements consist of security policies, procedures, and guidelines for storage, processing, and transmission of cardholder data. Any business that stores, processes, or transmits payment cardholder data is required to regularly monitor its CDE in accordance with the PCI DSS standard. See PCI Security Standards Council for more details about the PCI Data Security Standard.

About Splunk App for PCI Compliance

Install the Splunk App for PCI Compliance in a Splunk deployment that captures information from applications, systems, and devices in the PCI cardholder data environment.

Use the Splunk App for PCI Compliance to do the following tasks:

- Capture, monitor, and report on data from enterprise devices, systems, and applications in the cardholder data environment.
- Monitor access attempts to PCI assets.
- Monitor traffic between PCI domains.
- Identify vulnerabilities found on PCI assets.
- Notify administrators of malware found on PCI assets.
- Investigate and resolve compliance issues.
- Enable PCI compliance managers to monitor and report on PCI DSS compliance by producing views and reports of significant activity.

The Splunk App for PCI Compliance includes the following:
• **Incident Review and Response.** Use the incident management framework to alert, assign, evaluate risk, and respond to potential security incidents. The notable events allow compliance managers to view, respond, and audit the response to issues discovered in the cardholder data environment.

• **Compliance Reports.** Report-based views for each of the relevant compliance controls. Each report includes filters to specify specific parameters to evaluate different data views, so compliance managers can evaluate the cardholder data environment (CDE) as needed or required by a compliance auditor.

• **PCI Requirement Scorecards.** New compliance scorecards provide an overview of compliance for each major PCI requirement. This view shows the current real-time compliance status and a historical trend of compliance over the last 365 days. Compliance managers can use this dashboard to see where they are having compliance issues, and drill down to see reports or incidents.

• **Asset and Identity Correlation.** Asset and identity correlation facilitates compliance reporting against specific assets in the PCI cardholder data environment and users with access to the PCI assets. This allows compliance managers to monitor the cardholder data environment and provide the necessary user and asset context to support incident response.

• **Audit Review and Reporting.** Everything that a compliance manager does within the Splunk App for PCI Compliance solution can be audited. This provides an audit trail of all activity to provide proof to auditors that the environment is being monitored and issues responded to on an ongoing basis.

• **Data Normalization.** The Splunk App for PCI Compliance relies on data added to the Splunk platform indexers using add-ons that are compliant with the Splunk Common Information Model (CIM).

• **Correlation Searches.** Correlation searches create notable events on Incident Review that correspond to common threats to monitor in a cardholder data environment.
How this app works with Splunk Enterprise Security

The Splunk App for PCI Compliance 4.x.x and Splunk Enterprise Security use the same framework and share certain components so that they work together without duplicating efforts.

- The Splunk App for PCI Compliance (for Splunk Enterprise) includes the Splunk Enterprise Security framework to provide functionality such as correlation searches, notable events, asset and identity correlation, and others. The Splunk App for PCI Compliance (for Splunk Enterprise) creates indexes and data model accelerations in the same way as Splunk Enterprise Security.
- The Splunk App for PCI Compliance (for Splunk Enterprise Security) functions as an add-on with Splunk Enterprise Security and uses the same indexes, data models, and framework as Splunk Enterprise Security. If you have Splunk Enterprise Security in your deployment, install the Splunk App for PCI Compliance (for Splunk Enterprise Security).

For specifics about what you install and where, see Install prerequisites.

Get support and find information about Splunk software

If you have questions about the Splunk App for PCI Compliance, file a case using the Splunk Support Portal.

If your Splunk deployment is large or complex, talk to a member of the Splunk Professional Services team to assist you in deploying the Splunk App for PCI Compliance.

More information about the Splunk App for PCI Compliance

View questions and answers tagged with pci for potentially helpful information about the Splunk App for PCI Compliance.

- Splunk Answers (PCI Compliance-specific)
Prepare for your deployment

Understand the Splunk App for PCI Compliance

You can add data from the PCI cardholder data environment (CDE) using add-ons installed on Splunk forwarders. The forwarders send data to the indexers. After the data arrives at the indexers, the indexers perform custom categorization and field extractions and store the data. The Splunk App for PCI Compliance installed on a search head searches the indexed data and returns results, populating dashboards and providing administrators with an overview of their CDE.

- The Splunk App for PCI Compliance (for Splunk Enterprise) includes the domain add-on (DA-ESS-PCICompliance) and supporting add-ons (SA-*) and technology add-ons (TA-*) that make up the Enterprise Security framework.
- The Splunk App for PCI Compliance (for Splunk Enterprise Security) includes only the DA-ESS-PCICompliance domain add-on.

Several lookup files included in the add-ons that make up the Splunk App for PCI Compliance or the Enterprise Security framework are necessary for configuring the Splunk App for PCI Compliance.

<table>
<thead>
<tr>
<th>Name</th>
<th>File Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI Views</td>
<td>Splunk_DA-ESS_PCICompliance/lookups/pci_views.csv</td>
<td>List of reports and mapping to main PCI DSS requirement.</td>
</tr>
<tr>
<td>Expected Views</td>
<td>SA-AuditAndDataProtection/lookups/expected_views.csv</td>
<td>Views that are tracked for auditing.</td>
</tr>
<tr>
<td>Prohibited Traffic</td>
<td>SA-NetworkProtection/lookups/prohibited_traffic.csv</td>
<td>Traffic that generates notable events when detected.</td>
</tr>
<tr>
<td>Identities</td>
<td>SA-IdentityManagement/lookups/identities.csv</td>
<td></td>
</tr>
</tbody>
</table>
### Identify data sources

Before you install, configure, and deploy the Splunk App for PCI Compliance, identify the data sources to be monitored in your cardholder data environment.

The following table shows the main data sources to gather information from before deploying the app.

<table>
<thead>
<tr>
<th>Source</th>
<th>Example data</th>
<th>How data is used</th>
<th>Why it is important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data sources</td>
<td>Firewall data from Nessus.</td>
<td>Used in the dashboard.</td>
<td>Information about access attempts.</td>
</tr>
<tr>
<td>Asset information</td>
<td>List of servers in deployment.</td>
<td>Used by correlation searches.</td>
<td>Identify assets to monitor and report on.</td>
</tr>
</tbody>
</table>

#### Name | File Location | Description
---|---------------|------------------
Assets | SA-IdentityManagement/lookups/assets.csv | List of identities used for identity correlation.
Categories List | SA-IdentityManagement/lookups/categories.csv | Categories that apply to assets and identities.
PCI Domains List | SA-IdentityManagement/lookups/pci_domains.csv | List of PCI domain labels.
Urgency Matrix | SA-ThreatIntelligence/lookups/urgency.csv | List of defined urgency levels.
<table>
<thead>
<tr>
<th>Source</th>
<th>Example data</th>
<th>How data is used</th>
<th>Why it is important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity information</td>
<td>For example, verified users.</td>
<td>Used by correlation searches, notable events, reports.</td>
<td>Monitor expected users.</td>
</tr>
</tbody>
</table>

Data from these sources and the search-time knowledge applied to the data to normalize it for use in the app create a real-time view into the state of PCI compliance in your cardholder data environment.

Additional data to collect might include the following:

- information from enterprise devices, systems, and applications in the cardholder data environment
- access attempts to PCI assets
- traffic between PCI domains
- vulnerabilities identified on PCI assets
- notification of malware found on PCI assets
- notification of compliance issues

The app uses this information to populate the dashboards, views, and reports that are available in the Splunk App for PCI Compliance. The app also provides trended views of areas over time, a breakdown of issues by PCI requirement, and visibility in the incident status. Any of this information can be presented in the form of a report.

**Data sources**

Identify all of the data sources in your PCI cardholder data environment.

<table>
<thead>
<tr>
<th>Data source</th>
<th>Type of data collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>operating system logs</td>
<td>log files</td>
</tr>
<tr>
<td>network device logs</td>
<td>log files</td>
</tr>
<tr>
<td>security logs (anti-malware solutions)</td>
<td>log files</td>
</tr>
<tr>
<td>vulnerability management solutions</td>
<td>Common Vulnerabilities and Exposures (CVE) information</td>
</tr>
<tr>
<td>application logs</td>
<td>application specific notification (for Windows, for Unix)</td>
</tr>
</tbody>
</table>

For each data source, identify the mapping (technology add-ons) needed to
normalize the data for use with the Splunk App for PCI Compliance.

**Asset information**

See [Identify assets](#) in the *Installation and Configuration Manual*.

**Identity Information**

See [Identify system identities](#) in the *Installation and Configuration Manual*.

**Deployment options**

Splunk App for PCI Compliance is available as a standalone app, or as a content addition to Splunk Enterprise Security.

- If you have Splunk Enterprise Security 5.0 or later installed, install the [Splunk App for PCI Compliance (for Splunk Enterprise Security)](#).
- If you do not have Splunk Enterprise Security 5.0 or later installed, install the [Splunk App for PCI Compliance (for Splunk Enterprise)](#).

**Common deployment architectures**

This topic covers how to integrate the Splunk App for PCI Compliance into common Splunk Enterprise architectures:

- Single instance deployment
- Distributed deployment

**Single instance deployment**

You can install the [Splunk App for PCI Compliance (for Splunk Enterprise)](#) on a single Splunk platform instance. A single instance serves as both search head and indexer, providing both search and storage capability. A single instance deployment can support one or two users running concurrent searches.

You can also install the [Splunk App for PCI Compliance (for Splunk Enterprise Security)](#) along with Splunk Enterprise Security on a single Splunk platform instance, but a distributed deployment is recommended.
Distributed deployment

A distributed Splunk Enterprise deployment is recommended for the Splunk App for PCI Compliance. A dedicated search head provides the web interface and search management, while a collection of indexers provide improved search performance by distributing the workload of searches across multiple nodes. Multiple indexers also allow for the distribution of incoming data from the forwarders and the workload of processing that data.

You can install this app on a search head cluster and run it with an indexer cluster.

Search Head considerations

Install the Splunk App for PCI Compliance on one dedicated search head or search head cluster. Install only Common Information Model (CIM)-compatible add-ons on a search head or search head cluster with this app.

Install the Splunk App for PCI Compliance (for Splunk Enterprise Security) on the same search head as Splunk Enterprise Security. If you install PCI Compliance with Splunk Enterprise Security, follow the hardware recommendations for Splunk Enterprise Security.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Requirement</th>
<th>Additional Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU cores</td>
<td>16</td>
<td>Additional cores needed depending on search concurrency, search type, and number of users.</td>
</tr>
<tr>
<td>Memory</td>
<td>16GB RAM</td>
<td>Add additional memory to address search concurrency, number of enabled correlation searches, and the size of the asset and identity tables.</td>
</tr>
</tbody>
</table>

- All real-time searches in the app use the indexed real-time setting for improved indexing performance. Reverting the configuration reduces overall indexing capacity. See About real-time searches and reports in the Search Manual. To review the performance implications, see Expected performance and known limitations of real-time searches and reports” in the Search Manual.
- Splunk App for PCI Compliance requires the KV Store. For more information about KV Store, including the system requirements, see About the app key value store in the Admin Manual.
- If you enable the Monitoring Console on a Splunk App for PCI Compliance search head, it must remain in standalone mode. For more information on
when and how to configure the Monitoring Console for use in a distributed environment, see Which instance should host the console?.

**Search head clustering**

You can install the Splunk App for PCI Compliance on a search head cluster and run it with an indexer cluster. Splunk App for PCI Compliance supports installation on Linux-based search head clusters only. Review the requirements and differences of search head clustering.

- For details on search head clustering architecture, see Search head clustering architecture in the *Distributed Search Manual*.
- A search head cluster requires the KV store feature for data synchronization among search cluster members. For a list of requirements, see System requirements and other deployment considerations for search head clusters in the *Distributed Search Manual*.
- Configure the search head to forward all data to the indexers. See Forward search head data to the indexer layer in the *Distributed Search manual*.

**Indexer considerations**

Indexing is an I/O-intensive process. The indexers require sufficient disk I/O to ingest and parse data efficiently while responding to search requests. For the latest IOPS requirements to run Splunk Enterprise, see Reference Hardware: Indexer in the *Capacity Planning Manual*.

Using the Splunk App for PCI Compliance (for Splunk Enterprise Security) on the same search head as Splunk Enterprise Security introduces added indexer load of 15%. This results in reduced throughput capacity of 85GB, compared with 100GB per day when using Splunk Enterprise Security by itself. If you install PCI Compliance with Splunk Enterprise Security, follow the hardware recommendations for Splunk Enterprise Security.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Requirement</th>
<th>Additional Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU cores</td>
<td>16</td>
<td>Additional cores needed depending on search concurrency, search type, and number of users.</td>
</tr>
<tr>
<td>Memory</td>
<td>32GB RAM</td>
<td>Add additional memory to address search concurrency, number of enabled correlation searches, and the size of the asset and identity tables.</td>
</tr>
</tbody>
</table>
A collection of indexers can serve more than one search head. Additional search heads using the same indexers affects the total performance, and reduces the resources available to the search infrastructure. Always increase the number of indexers to scale with increases in search load and search concurrency.

Because the Splunk App for PCI Compliance uses the same framework as Splunk Enterprise Security, the Performance test results are useful to review. Data model usage and correlation search load are the two largest factors in sizing the Splunk App for PCI Compliance. Changing correlation search counts and data model usage may require additional indexers.

Indexes

Splunk App for PCI Compliance (for Splunk Enterprise) defines custom indexes for event storage. For more information about the indexes required, see Configure and deploy indexes. The Splunk App for PCI Compliance (for Enterprise Security) relies on the custom indexes defined by Splunk Enterprise Security.

Indexer clustering

Splunk App for PCI Compliance supports both single site and multisite cluster architectures. See The basics of indexer cluster architecture and Multisite cluster architecture in the Managing Indexers and Clusters Manual.

A single site or multisite indexer cluster architecture may have one search head or a search head cluster with a running instance of the Splunk App for PCI Compliance. Additional, single instance search heads cannot run this app.

Data model accelerations

Splunk App for PCI Compliance accelerates data models to provide dashboard panel and correlation search results. Data model acceleration uses the indexers for processing and storage, placing the accelerated data alongside each index. To calculate the additional storage needed on the indexers based on the total volume of data, use the following formula: accelerated data model storage/year = data volume per day * 3.4

This formula assumes that you are using the recommended retention rates for the accelerated data models.

Example: If you process 100GB/day of data volume for use with this app, you need approximately 340GB more space available across all of the indexers to
allow for up to one year of data model retention and source retention.

The storage used for data model acceleration is not added to index sizing calculations for maintenance tasks such as bucket rolling and free space checks.

Splunk Enterprise 6.1.0 and later implements new configuration parameters for data model acceleration tasks. See Advanced configurations for persistently accelerated data models in the *Knowledge Manager Manual*.

**TSIDX reduction compatibility**

A retention policy for an index’s TSIDX files is available in Splunk Enterprise 6.4.x. For more information on TSIDX reduction, see Reduce tsidx disk usage in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual. Setting a retention policy for the TSIDX files does not effect data model acceleration retention.

Some searches provided with the Splunk App for PCI compliance do not work on buckets with reduced TSIDX files.

<table>
<thead>
<tr>
<th>Panel/Search Name</th>
<th>Default time range</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarder Audit panel: Event Count Over Time by Host</td>
<td>-30d</td>
<td>Set the TSIDX retention to a value greater then the time range, or reduce the default time range for the search to a value under the TSIDX retention value.</td>
</tr>
<tr>
<td>Saved Search: Audit - Event Count Over Time By Top 10 Hosts</td>
<td>-30d</td>
<td>Set the TSIDX retention to a value greater then the time range, or reduce the default time range for the search to a value under the TSIDX retention value.</td>
</tr>
<tr>
<td>Saved Search: Audit - Events Per Day - Lookup Gen</td>
<td>-1d</td>
<td>Set the TSIDX retention to a value greater then the default time range.</td>
</tr>
<tr>
<td>Saved Search: Endpoint - Index Time Delta 2 - Summary Gen</td>
<td>-1d</td>
<td>Set the TSIDX retention to a value greater then the default time range.</td>
</tr>
</tbody>
</table>
Deploying add-ons

Deploy add-ons to forwarders and indexers to distribute index-time knowledge.

- If you use a distributed deployment without index or search head clusters, use the deployment server. For information about the deployment server configuration and use, see About deployment server and forwarder management in the *Updating Splunk Enterprise Instances Manual*.
- If you use indexer clustering, see Manage common configurations across all cluster peers and Manage app deployment across all cluster peers in the *Managing Indexers and Clusters Manual*.
- If you use search head clustering, use the search head cluster deployer to distribute configurations across the set of search head cluster members. See Use the deployer to distribute apps and configuration updates in the *Distributed Search Manual*.
  - To facilitate using the deployer to manage configuration files with hashed passwords, the captain replicates its *Splunk.secret* file to all other cluster members during initial deployment of the cluster. For more information, see Deploy secure passwords across multiple servers in the *Securing Splunk Enterprise Manual*.
- Splunk App for PCI Compliance includes the Distributed Configuration Management tool to gather the *indexes.conf* and index-time *props.conf* and *transforms.conf* settings from all enabled apps and add-ons on the search head and assemble them into one add-on.

Virtualized hardware

Installing Splunk App for PCI Compliance in a virtualized environment requires the same memory and CPU allocation as an installation in a non-virtualized environment. You must reserve all CPU and memory resources, with no oversubscription of hardware.

In a virtualized environment, test the storage IOPS across all Splunk platform indexer nodes simultaneously. The results from every node must conform to the Reference Hardware IOPS specified in the *Capacity Planning Manual*.

Insufficient storage performance is a common cause for poor search response and timeouts when scaling the Splunk platform in a virtualized environment.

Deploying with other apps

For optimal performance, install the Splunk App for PCI Compliance on a dedicated search head. The dedicated search head should not have any other
apps installed, and use indexers that have only the necessary Common
Information Model-compatible technology add-ons. In some cases, it might be
necessary to install other apps on the same search head or instance as the
Splunk App for PCI Compliance. Apps compatible with the Splunk App for PCI
Compliance are documented as CIM-compatible. Splunk apps and other add-ons
that are not CIM-compatible could prevent PCI Compliance searches and
dashboards from functioning properly.

If you have Splunk Enterprise Security, you can install the Splunk App for PCI
Compliance (for Splunk Enterprise Security) on the same search head. Test and
consider the data volume that you process in your environment before doing so.

Splunk App for PCI Compliance and the SA-VMNetAppUtils component of the
Splunk Add-on for VMware cannot be installed on the same search head.
Conflicts with identically-named files can prevent some parts of Splunk App for
PCI Compliance from working correctly.

Remote data collection

Use forwarders to collect data from remote systems. See Using forwarding
agents. A node where a forwarder is installed is a collection point for one or more
data sources. The technology add-ons for those data sources should be installed
on the forwarder, ensuring that the data is properly tagged. To manage and
distribute technology add-ons across many forwarders, use the Splunk
deployment server or a third party software distribution system. See About
deployment server. If Splunk Enterprise Security is already installed and the
technology add-ons are already collecting data on a specific node, this node can
act as a forwarder.
Add data

Data management overview

The Splunk App for PCI Compliance works with Splunk software and supports all CIM-compliant data ingestion methods. After the app is installed and configured, solution administrators can start to add data to the Splunk deployment.

The Splunk App for PCI Compliance requires considerations when determining how to get data from the various sources. When you set up a data input for the Splunk App for PCI Compliance, make sure the data is correctly mapped using a technology add-on so that the data is normalized and assigned the correct source type.

Considerations for data inputs with PCI compliance

You can use each of the main approaches for Splunk data inputs (monitoring files, monitoring network ports, monitoring Windows and Unix data, and deploying custom scripted inputs) with the Splunk App for PCI Compliance. Some approaches work better than others because the input data must be assigned the correct source type.

- **Monitoring files**: Deploy a forwarder on each system where you want to monitor files and source type the file inputs on the forwarder. If there is a large number of forwarders with identical configurations, use the deployment server to set up and manage the logging sources across your forwarders.

- **Monitoring network ports**: You can send data to a forwarder or directly to an indexer on any TCP or UDP port. Be careful when sending data from multiple sources over the same port. See the Get data from TCP and UDP ports section in Getting Data In.

- **Monitoring Windows data**: To implement Windows eventlog monitoring, deploy a forwarder on each system. If there is a large number of forwarders with identical configurations, use the Splunk Enterprise deployment server to set up and manage the logging sources across your forwarders.

- **Scripted inputs**: A scripted input is a flexible input type that collects data from API's and remote data interfaces. See Get data from APIs and other
remote data interfaces through scripted inputs in *Getting Data In*.

**Source typing**

Set the correct source type for data to be properly processed by Splunk platform and used by the Splunk App for PCI Compliance. The app works with all types of inputs. Technology add-ons provide search-time knowledge to map data.

For more information about automatic source typing, see Why source types matter in *Getting Data In*.

**Identify assets**

To get the most out of the Splunk App for PCI Compliance, you must provide information about the assets, which are the devices and systems in the environment. The asset list includes a number of fields used by the dashboards and correlation searches in the app. Splunk App for PCI Compliance still functions without an asset list, but the functionality for some dashboards and features is incomplete.

Some of the important fields in the asset list include:

- **ip, mac, nt_host, dns, owner** - Asset information. These fields are used to provide details about current assets in the Splunk App for PCI Compliance.

- **priority** - Assets by priority. This field is used to determine the urgency of the notable events associated with security incidents.

- **category** - Asset category. This field is used to define systems in-scope for PCI and/or contain cardholder data. Categories are configurable and are defined in a separate category list. Used by many Splunk for PCI Compliance dashboards to filter the view. Common examples are compliance and security standards governing the asset, or functional categories (such as server, domain_controller, and so on). An asset can be included in multiple categories by assigning a bar-delimited list of categories in the asset list, For example, `pci|cardholder|server`. See Set up asset categories.

- **pci_domain** - This field is used to specify the network zone the asset is found within. An asset can be included in multiple PCI domains by assigning a pipe-delimited list of domains in the asset list. The following values are supported by default:
trust
trust|wireless
trust|cardholder
trust|dmz
untrust

- **bunit** - Assets by business unit. Used by many Splunk for PCI Compliance dashboards to restrict the view. A free-form field that can be used to specify the business unit the asset is part of.

This can be done by using the asset list, a comma-separated values (CSV) lookup file with contextual information about your systems, information that cannot be gathered from events themselves. Augmenting events with additional asset information helps security analysts and incident investigators. Populate the asset list either by building an automated capture from an existing asset database or by populating the file manually. See Configure assets for more about how to add asset data to the asset list.

**Identify system identities**

The Splunk App for PCI Compliance needs to have information about the identities who use the system. Create an identity list, which is a list of account names, legal names, nicknames, alternate names, and phone numbers within your organization. The identity list provides information used to correlate identities (individuals) with both events and assets.

The identity list includes a number of fields that are used by the dashboards and correlation searches in PCI Compliance. Splunk App for PCI Compliance still functions without an identity list, but the functionality for some dashboards and features is incomplete. Some of the important fields in the identity list include:

- **Identities by Priority**: Used to determine the urgency of the notable events associated with security incidents involving identities.

- **Identities by Business Unit**: Used by many PCI Compliance dashboards to restrict the view to a particular business unit. A free-form field that can be used to specify to which the business unit the identity belongs.

- **Identities by Category**: Used by many PCI Compliance dashboards to restrict the view. Categories are configurable and are defined in a separate category list. Common examples are compliance and security standards governing the identity, or functional categories (such as server, domain_controller, and so on.). You can include an identity in multiple
categories by assigning a bar-delimited list of categories in the identity list (for example, "pci|cardholder|server")

- **Identities**: Used to view details of the current identities in the system.

Identities are defined in CSV lookup table located under the **Identity Management** add-on in the

```
$SPLUNK_HOME/etc/apps/SA-IdentityManagement/lookups/identities.csv
```
directory. Populate this file with the identity information for your infrastructure. The CSV file can be constructed manually or populated by a script that pulls the information from an existing identity table or database. See Configure identities for more about how to add identity data to the identity list.

**Using technology add-ons with the Splunk App for PCI Compliance**

This topic provides instruction on using predefined technology add-on feeds to gather data from common compliance data sources.

**Normalize data at search time**

To derive information from the types of data monitored in your cardholder data environment, Splunk platform parses, indexes, and normalizes data so that it can be used by apps in searches, views, and reports. The data is normalized by tagging it.

For example, one firewall add-on might report an incident as a "failed attempt" while another one might report an incident as "unsuccessful". When the data is normalized, it is mapped to a field in the common information model, such as "failed". The "failed" field can be used as part of searches, filters, views, reports, and so on. Additional tagging and search-time information, such as correlating asset information with events, is provided by technology add-ons.

**Technology add-ons and data inputs**

The Splunk App for PCI Compliance data inputs are closely connected with technology add-ons, mapping data for use in the app. Manage apps to configure or add technology add-ons to your configuration.

1. Select **Apps > Manage Apps**.
2. Click **Edit properties** for the app you want to configure.
3. Configure the app and click **Save**.

You can also select one of the other available options to find more apps or install an app from a file.

For each data source:

- **Identify the technology add-on**: Identify the technology and determine the corresponding technology add-on. If the Splunk App for PCI Compliance does not ship with default support for your type of data or data source, you might be able to find an add-on on Splunkbase. You can also create your own add-ons.

- **Customize the technology add-on where necessary**: Each technology add-on provided with the Splunk App for PCI Compliance comes with a README file, located in the root of the add-on folder in `$SPLUNK_HOME/etc/apps`. The README details any changes you need to make to the add-on to configure it for your deployment. For example, you might need to specify the location or source of the data, choose whether the data is located in a file or in a database, and so on.

- **Install the technology add-on**: You must install the technology add-on on each search head that handles the data. You must also install technology add-ons that perform index-time processing on each indexer and forwarder. If technology add-ons exist as part of a Splunk Enterprise Security installation on the same search head, they are shared with the Splunk App for PCI Compliance.

- **Configure the server, device, or technology where necessary**: In some cases, you might need to enable logging or data collection for the device or application and/or configure the output for collection by Splunk software. Consult the documentation for that technology for details.

- **Set up a Splunk data input and set the source type where necessary**: The Splunk App for PCI Compliance supports all Splunk data input methods, including network inputs, file monitoring, and scripted inputs. The README file in the technology add-on directory describes which input types are supported for this particular technology. The README file also includes the source type associated with the data and tells you whether or not you need to explicitly specify the source type when you set up the data input.
Install the app

Install prerequisites

Make sure you have sufficient hardware, the appropriate system software, the correct version of Splunk platform, and the necessary add-ons for your deployment. See the Deployment options.

This table summarizes the installation options for this app, along with the compatible software versions.

<table>
<thead>
<tr>
<th>Splunk App for PCI Compliance version</th>
<th>Compatible Splunk platform version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk App for PCI Compliance (for Splunk Enterprise)</td>
<td>7.2.x, 7.3.x, 8.x stand-alone release. See <a href="https://splunkbase.splunk.com/app/1143">https://splunkbase.splunk.com/app/1143</a>.</td>
</tr>
<tr>
<td>Splunk App for PCI Compliance (for Splunk Enterprise Security)</td>
<td>6.0.0 with content pack 4.0.0 DA-ESS_PCI. See <a href="https://splunkbase.splunk.com/app/2897/">https://splunkbase.splunk.com/app/2897/</a>.</td>
</tr>
</tbody>
</table>

Only install the Splunk App for PCI Compliance for Enterprise Security with Splunk Enterprise Security. See the following for more information:

- How this app works with Splunk Enterprise Security
- Understand the Splunk App for PCI Compliance

See Install the Splunk App for PCI Compliance for installation instructions.

Install the Splunk App for PCI Compliance

Before you install the app, make sure you have satisfied the install prerequisites for both Splunk Enterprise and the Splunk App for PCI Compliance. See Install prerequisites in this manual.
Download the app

1. Browse to splunk.com and log in with your Splunk.com ID. You must be a licensed Splunk App for PCI Compliance customer to download the product.
2. Download the Splunk App for PCI Compliance from Splunkbase.
   1. If you have Splunk Enterprise Security installed, install the Splunk App for PCI Compliance (for Splunk Enterprise Security).
   2. If you do not have Splunk Enterprise Security installed, install the Splunk App for PCI Compliance (for Splunk Enterprise).
3. Choose Download, and save the app file to your desktop.
4. Log in to the search head as an administrator.

Install the app

1. On the Splunk Enterprise search page, select Apps > Manage Apps and click Install App from File.
   Caution: Install the Splunk App for PCI Compliance (for Splunk Enterprise Security) on the same instance as Splunk Enterprise Security. If you do not install it on the same instance as Splunk Enterprise Security, the Splunk App for PCI Compliance (for Splunk Enterprise Security) will not work.
2. Select Choose File and browse to the Splunk App for PCI Compliance product file.
3. Select Upload to begin the installation.
4. Click Set up now to begin the installation.

Set up the App

1. Click Setup next to Splunk App for PCI Compliance in Manage Apps.
2. Click Start then wait until it completes the entire installation.
3. Restart your instance of Splunk platform.
4. Access Splunk Web from https and log in.

Add data

You can add data to the Splunk App for PCI compliance in two ways.

- Use data from preconfigured add-ons such as TA-bluecoat.
- Create custom add-ons to capture specific data in your environment.
Configure the app

To configure the app, click Configure in the menu bar. Follow the Steps to configure in this manual to begin setting up the Splunk App for PCI Compliance for your cardholder data environment.

Install technology add-ons

The Splunk App for PCI Compliance solution includes predefined technology add-ons to work with the data you want to monitor. The add-ons provide the feeds to get data from different sources, and provide search-time knowledge maps to normalize the data for use within the app. Technology add-ons ensure that the data is correctly consumed by the Splunk App for PCI Compliance.

Steps for installing technology add-ons

Configure or add technology add-ons to your deployment.

Find technology add-ons

To find a technology add-on to add:

1. Click Apps > Manage Apps.
2. Click Browse more apps.
3. Browse list of apps.

Before you install a new add-on, make sure the add-on is compatible with the Splunk App for PCI Compliance.

Add a technology add-on from a local file

To add a technology add-on locally:

1. Click Apps> Manage Apps.
2. Click Install app from file.
3. In the Upload an app panel, browse for the app, select it, then click Upload.
Edit an existing add-on

To edit an existing add-on:

1. Click Apps > Manage Apps.
2. Select the app from the list.
3. Click Edit Properties for the app you want to configure.
4. Click Save.

Update technology add-ons

A newer version of a technology add-on used by the Splunk App for PCI Compliance might be available on Splunkbase.

Update the app from within Splunk Enterprise

To check for a newer version, go to Manage Apps from the Splunk menu. If there is an updated version of a technology add-on, there will be a link similar to this: 4.6.0|Update to 4.6.3 in the Version column. You need to be logged in to Splunk.com to download the technology add-on.

1. To update your existing technology add-on with the newer one, click the link in the version column.
2. Click Update to get the newer version.
3. Click Restart.

Update the app manually

1. Go to Splunkbase and find the new version of the add-on. Download the add-on to your desktop or local directory.
2. Install the add-on by navigating to Manage Apps > Install app from file from the Splunk Home page.
3. Browse to the add-on location and select the add-on.
4. Select Upgrade app so that the newer version of the add-on overwrites the older one.
5. Click Upload.
6. Click Restart.

See Using technology add-ons in this manual.
Configure the app

Steps to configure the Splunk App for PCI Compliance

After you install the Splunk App for PCI Compliance, you need to configure the app for your deployment. Most of the configuration options can be found in the Configuration dashboard.

Click Configure > Data Enrichment > Asset and Identity Management in the menu bar from anywhere in the app to configure the Splunk App for PCI Compliance.

1. Configure the asset table
2. Configure the identity table
3. Configure the provided reports. As you configure reports, you configure your domains.
4. Enable the correlation searches

You can also Add a custom report.

Configure assets

The asset list provides external information about the devices on your system, such as the asset priority, owner, and business unit. It also provides the geographic location of the asset and the DNS and Windows machine name of the asset. You can search on any of these fields from the asset list and use them while you are investigating events.

When an event contains a field that PCI Compliance identifies as belonging to a host or device, Splunk App for PCI Compliance looks up the device in the asset list and generates new fields that contain the information from the asset list. The asset information provides PCI Compliance with contextual information about the systems involved in an event or related to a notable event that can allow a security analyst or incident investigator to identify additional asset information such as asset priority, categories, business unit, owner, and other information.

Maintain the asset list to allow assets to be correlated with events. See Asset and Identity Correlation in the User Manual.
Register asset and identity data

You have choices for registering asset and identity data:

- Manually register asset and identity data in Asset and Identity Manager
- Use LDAP to register data in Asset and Identity Manager


Set up asset categories

After formatting an asset list as a lookup, the following identity categories are specific to PCI. See Format an asset or identity list as a lookup in Splunk Enterprise Security.

The category list specifies a list of categories that can be used for the category field in the asset list. The relationship between the pci_domain field and the category field is the single most important factor in determining asset management and PCI compliance in a cardholder data environment. The PCI compliance analyst needs a list of all assets that reside in a trusted zone, to monitor and report on these assets as a group and tell them apart from any assets that are not in a trusted zone.

The asset table fields category and pci_domain can be used to determine your PCI compliance scoping for assets.

- Use the category field to distinguish assets relevant for PCI compliance from other assets.
- Use the pci_domain field to identify the PCI domain-relevant details about PCI compliance assets.

<table>
<thead>
<tr>
<th>Asset table field</th>
<th>Valid values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pci_domain</td>
<td>wireless, trust, untrust, cardholder, dmz</td>
<td>Separate valid values with a pipe if multiple values apply to a single asset. For example, trust</td>
</tr>
<tr>
<td>category</td>
<td>cardholder, pci</td>
<td>Separate valid values with a pipe if multiple values apply to a single asset. Use cardholder to define the cardholder data environment for PCI</td>
</tr>
</tbody>
</table>
compliance. For example, people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data. Use \texttt{pci} to identify a network component, server, or application included in or connected to the cardholder data environment.

<table>
<thead>
<tr>
<th>Asset table field</th>
<th>Valid values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>compliance. For example, people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data. Use \texttt{pci} to identify a network component, server, or application included in or connected to the cardholder data environment.</td>
</tr>
</tbody>
</table>

Verify that your asset data was added to the Splunk App for PCI Compliance

Check the Asset Center dashboard.

Configure identities

Set up the identity list to enrich the data in the Splunk App for PCI Compliance. The identity list provides information about the users in your cardholder data environment, such as the user name, first and last name, and email address. Some of these fields, such as priority, watchlist, and endDate are used for dashboard charts and to calculate the urgency of notable events associated with identities. Other fields, such as "business unit" and "category", are used by the filters at the top of the dashboards. You can search on any of these fields from the identity list and use them while investigating events.

When an event contains a field that the Splunk App for PCI Compliance identifies as belonging to a specific identity, the app looks up the identity in the identities list and generates new fields that contain the information from the identities list. The identity information provides the app with contextual information about the identities involved in an event or related to a notable event that can allow a PCI compliance analyst or incident investigator to identify additional identity information such as priority, categories, business unit, watchlist, and other information.

Maintain the identity list to allow identities to be correlated with events. See Asset and Identity Correlation in the \textit{User Manual}.

Register asset and identity data

You have choices for registering asset and identity data:
• Manually register asset and identity data in Asset and Identity Manager
• Use LDAP to register data in Asset and Identity Manager


Set up identity categories

After formatting an identity list as a lookup, the following identity categories are specific to PCI. See Format an asset or identity list as a lookup in Splunk Enterprise Security.

The category list specifies a list of categories that you can use for the category field in the identities list. The category list can be any set of categories you choose. Common examples are compliance and security standards, such as PCI, governing the identities, or functional categories such as officer, pci-analyst, and others. Assign user categories to identities to further enrich your data.

These user categories are available in the Splunk App for PCI Compliance.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cardholder</td>
<td>cardholder user</td>
</tr>
<tr>
<td>contractor</td>
<td>contractor user</td>
</tr>
<tr>
<td>default</td>
<td>default user</td>
</tr>
<tr>
<td>intern</td>
<td>temporary intern user</td>
</tr>
<tr>
<td>officer</td>
<td>user who is an officer of the company</td>
</tr>
<tr>
<td>pci</td>
<td>PCI analyst or PCI compliance manager</td>
</tr>
<tr>
<td>privileged</td>
<td>user with additional privileges</td>
</tr>
<tr>
<td>sox</td>
<td>Sarbanes?Oxley user</td>
</tr>
</tbody>
</table>

You can edit this list by navigating to Configure > Content Management and selecting the Categories lookup.

Verify that your identity data was added to the Splunk App for PCI Compliance

Check the Identity Center dashboard.
Configure Primary Functions list

The PCI DSS requires that systems include only one primary function. To report systems that might be in violation of this requirement, solution administrators and compliance managers can populate a list to define the primary services. Use this information to determine violations.

View the Primary Functions service and ports list:

1. Select Configure > Content > Content Management.
2. Click the Primary Functions lookup. The Primary Functions lookup file (primary_functions.csv) appears in a lookup editor.

```
process,service,transport,port,is_primary,function
,,,,Application (name)
splunkd,,,false,splunk
slapd,,,true,Authentication
,*,true,Authentication
,*,636,true,Authentication
mysql,,,true,Database
,mysql,,,true,Database
,*,3306,true,Database
named,,,true,Domain Name Service (DNS)
named,,,true,Domain Name Service (DNS)
,*,53,true,Domain Name Service (DNS)
...
```

The first line in the file describes the fields in the file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>process</td>
<td>Process name.</td>
<td>ssh</td>
</tr>
<tr>
<td>service</td>
<td>Type of service.</td>
<td>sshd</td>
</tr>
<tr>
<td>transport</td>
<td>The transport protocol.</td>
<td>TCP</td>
</tr>
<tr>
<td>port</td>
<td>Port number.</td>
<td>8000</td>
</tr>
<tr>
<td>is_primary</td>
<td>Does the service provide a primary function?</td>
<td>true or false</td>
</tr>
<tr>
<td>function</td>
<td>The function provided by the service/process.</td>
<td>database</td>
</tr>
</tbody>
</table>

Add to, or modify this list using the editor. Click Save when you are done.

There is no file checking or verification for this editor, so any typo might break the lookup file.
Configure Prohibited Traffic list

The PCI data security standards requires that systems in a cardholder data environment only include services necessary on the system. Using the **Prohibited Traffic** list, PCI compliance solutions administrators can define a list of prohibited services that they do not expect to see on systems within the environment.

To view the **Prohibited Traffic** list, do the following:

1. Select **Configure > Content > Content Management**.
2. Click the **Prohibited Traffic** lookup. The Prohibited Traffic lookup file (prohibited_traffic.csv) appears in the lookup editor.

```
transport,src,srcc_pci_domain,dest,dest_pci_domain,dest_port,is_prohibited,is_secure,note
*,*,cardholder,*,untrust,*,true,false,deny_all_cardholder_to_untrust
*,*,untrust,*,cardholder,*,true,false,deny_all_untrust_to_cardholder
*,*,wireless,*,cardholder,80,true,false,deny_http_wireless_to_cardholder
icmp,*,untrust,*,dmz,*,false,,permit_icmp_untrust_to_dmz
tcp,*,untrust,*,dmz,80,false,permit_tcp80_untrust_to_dmz
tcp,*,untrust,*,dmz,443,false,true,permit_tcp443_untrust_to_dmz
udp,*,untrust,*,dmz,500,false,true,permit_udp500_untrust_to_dmz
udp,*,untrust,*,dmz,4500,false,true,permit_udp4500_untrust_to_dmz
tcp,*,untrust,*,dmz,1723,false,true,permit_tcp1723_untrust_to_dmz
udp,*,untrust,*,dmz,1701,false,true,permit_udp1701_untrust_to_dmz
udp,*,*,cardholder,514,false,,permit_udp514_dmz_to_cardholder
tcp,*,*,cardholder,443,false,permit_tcp443_dmz_to_cardholder
tcp,*,trust,*,trust,22,false,true,permit_tcp22_inside_trust
tcp,*,trust,*,trust,80,false,permit_tcp80_inside_trust
```

The first line in the file describes the fields in the file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>transport</td>
<td>The transport protocol.</td>
<td>TCP</td>
</tr>
<tr>
<td>src</td>
<td>The host that is the source of the activity. Use a wildcard * to match all hosts.</td>
<td>ACME_host_002</td>
</tr>
<tr>
<td>src_pci_domain</td>
<td>The source domain of the activity.</td>
<td>cardholder</td>
</tr>
<tr>
<td>dest</td>
<td>The host that is the destination of the activity. Use a wildcard * to match all hosts.</td>
<td>ACME_host_001</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>dest_pci_domain</td>
<td>The source domain of the activity.</td>
<td>cardholder</td>
</tr>
<tr>
<td>dest_port</td>
<td>The destination port of the activity.</td>
<td>80</td>
</tr>
<tr>
<td>is_prohibited</td>
<td>Is the service/traffic/port prohibited?</td>
<td>true false</td>
</tr>
<tr>
<td>is_secure</td>
<td>Is the traffic for the given service encrypted (secure)?</td>
<td>true false</td>
</tr>
<tr>
<td>note</td>
<td>A description about the traffic or activity.</td>
<td>permit_icmp_untrust_to_dmz</td>
</tr>
<tr>
<td>src_category</td>
<td>Category of the source</td>
<td>pci_cardholder</td>
</tr>
<tr>
<td>dest_category</td>
<td>Category of the source</td>
<td>pci_cardholder</td>
</tr>
</tbody>
</table>

Add to, or modify this list using the editor. Click **Save** when you are done.

There is no file checking or verification for this editor, so any typo might break the lookup file.

### Configure Interesting Services list

For PCI DSS, some services are required to be running within the PCI environment. This might include a patch service like Windows Update service or other services that should be on the systems within the environment.

View the "Interesting Services" list and view the current list of required services.

1. Select **Configure > Content > Content Management**.
2. Click the **Interesting Services** lookup. The Interesting Services lookup file *(interesting_services.csv)* appears in the lookup editor.

```
app,dest,dest_pci_domain,is_required,is_prohibited,is_secure,note
portmap,*,*,false,true,,Unix RPC portmapper service is prohibited.
xinetd,*,*,false,true,,Unix xinetd services are prohibited.
Fax,*,*,false,true,,Windows Fax service is prohibited.
RemoteRegistry,*,*,false,true,,Windows remote registry service is prohibited.
SNMPTRAP,*,*,false,true,,Windows SNMP trap service is prohibited.
ssh,*,*,false,false,true,Unix Secure shell is permitted.
W32Time,*,*,true,false,,Windows time service is required.
wuauserv,*,*,true,false,,Windows automatic update service is required.
```
The first line in the file describes the fields in the file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>The application that is the source of the activity.</td>
<td>Win32Time</td>
</tr>
<tr>
<td>dest</td>
<td>The host that is the destination of the activity. Use a wildcard * to match all hosts.</td>
<td>ACME_host_*</td>
</tr>
<tr>
<td>dest_pci_domain</td>
<td>The source domain of the activity.</td>
<td>cardholder</td>
</tr>
<tr>
<td>is_required</td>
<td>Should the given service be required to be running?</td>
<td>true, false</td>
</tr>
<tr>
<td>is_prohibited</td>
<td>Is the service prohibited?</td>
<td>true, false</td>
</tr>
<tr>
<td>is_secure</td>
<td>Is the traffic for the given service encrypted?</td>
<td>true, false</td>
</tr>
<tr>
<td>note</td>
<td>A description about the app or service.</td>
<td>Windows time service is required.</td>
</tr>
</tbody>
</table>

Add to or modify this list using the editor. Click Save when you are done.

There is no file checking or verification for this editor, so any typo might break the lookup file.

**Configure secure and insecure services**

Many services are considered insecure and should never be run within a cardholder data environment. The Splunk App for PCI Compliance populates a list of insecure services by default, but a solution administrator or compliance manager might need to modify this list.

Modify the "Interesting Services" list.

1. Select Configure > Content > Content Management.
2. Click Interesting Services. The Interesting Services lookup file (interesting_services.csv) opens in the editor.
3. Modify this list to identify secure and insecure services.
4. Click Save when you are done.
There is no file checking or verification for this editor, so any typo might break the lookup file.

**Configure Interesting Processes list**

The PCI DSS requires that processes in the PCI domain be tracked. To report on systems that might be in violation of this requirement, solution administrators and compliance managers can populate a list to define interesting processes. You can use this information to determine violations.

View the list.

1. Select **Configure > Content Management**.
2. Click the "Interesting Processes" list. In the **Lookup** editor, the interesting Processes lookup file (*interesting_processes.csv*) appears.

The first line in the file describes the fields in the file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>The application that is the source of the activity.</td>
<td>Win32Time</td>
</tr>
<tr>
<td>dest</td>
<td>The host that is the destination of the activity. Use a wildcard * to match all hosts.</td>
<td>ACME_host_001</td>
</tr>
<tr>
<td>dest_PCI_Domain</td>
<td>The source domain of of the activity.</td>
<td>cardholder</td>
</tr>
<tr>
<td>is_required</td>
<td>Should the given service be required to be running?</td>
<td>true, false</td>
</tr>
<tr>
<td>is_prohibited</td>
<td>Is the service/traffic/port prohibited?</td>
<td>true, false</td>
</tr>
<tr>
<td>is_secure</td>
<td>Is the traffic for the given service encrypted?</td>
<td>true, false</td>
</tr>
<tr>
<td>note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
telnetd,*,*,false,true,false,The telnet application is prohibited because of insecure authentication.
```

The telnet application is prohibited because of insecure authentication.
The telnet application is prohibited because of insecure authentication.

Add to or modify this list using the editor. Click Save when you are done.

There is no file checking or verification for this editor, so any typo might break the lookup file.

### Configure Interesting Ports list

**Interesting Ports** contains a list of TCP and UDP ports that are required, prohibited, or insecure in your deployment. The PCI DSS requires that network ports on servers in the PCI domain be tracked. Solutions administrators should set a policy defining the allowed and disallowed ports.

1. Review the "Interesting Ports" list.
2. Edit the list, changing the fields and adding new entries based on the policy definition.
3. Enable the correlation search that will trigger an alert.

### Interesting Ports list lookup fields

1. Select **Configure > Content Management**.
2. Choose the "Interesting Ports" list. In the **Lookup** editor, the lookup file `interesting_ports.csv` appears. The first line in the file is the header that describes the fields in the file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>The application or service name.</td>
<td>Win32Time</td>
</tr>
<tr>
<td>dest</td>
<td>The destination host for the network service. Accepts a wildcard. Use only a wildcard to match all hosts.</td>
<td>DARTH*, 10.10.1.100, my_host, etc.</td>
</tr>
<tr>
<td>dest_pci_domain</td>
<td>The PCI domain. Accepts a wildcard.</td>
<td>trust, untrust, etc.</td>
</tr>
<tr>
<td>dest_port</td>
<td>The destination port number. Accepts a wildcard.</td>
<td>443, 3389, 5900, etc.</td>
</tr>
<tr>
<td>transport</td>
<td>The transport protocol. Accepts a wildcard.</td>
<td>tcp udp</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>is_required</td>
<td>Is the service required to be running? Alert if not present.</td>
<td>true, false</td>
</tr>
<tr>
<td>is_prohibited</td>
<td>Is the service/traffic/port prohibited from running? Alert if present.</td>
<td>true, false</td>
</tr>
<tr>
<td>is_secure</td>
<td>Is the service traffic encrypted?</td>
<td>true, false</td>
</tr>
<tr>
<td>note</td>
<td>A brief description of the service and use case.</td>
<td>Unencrypted telnet services are insecure.</td>
</tr>
</tbody>
</table>

Add to or modify this list using the editor. Click **Save** when you are done.

- There is no file checking for this editor. A typo might break the lookup file and generate a lookup error.
- Use a search to review the user and time the lookup file was edited.
  
  **Example:** `index=_internal edit  
  uri_path="/en-US/app/SplunkPCIComplianceSuite/pci_lookups_edit"`
- A lookup does not accept regular expressions.

**Example interesting ports configuration**

You can update the Interesting Ports list to allow an open connection on the loopback port for the mail server, but alert you if email is received on any trusted server. Create a lookup table entry as follows:

```
mail,127.0.0.1,*,25,tcp,false,false,false, Any host can communicate with itself on TCP port 25 in all domains. Please don't bug me if it does.
mail,*,trust,25,tcp,false,true,false, Alert me if any host in the Trust domain is open on TCP port 25.
```

**Customize the menu bar in Splunk App for PCI Compliance**

Customize the menu bar in Splunk App for PCI Compliance with the Edit Navigation view. Add new **dashboards**, reports, **views**, links to filtered dashboards, or links to the web to your menu bar. You must have Splunk App for PCI Compliance administrator privileges to make changes to the menu bar navigation.
You can add views to the menu bar as part of a collection that groups several views together or as an individual item on the menu bar. For example, Incident Review is an individual dashboard in the menu bar, and each report domain, such as R1: Network Traffic is a collection.

Splunk App for PCI Compliance persists customizations you made to the navigation from previous versions.

**Check for updated views**

Views and collections that are new, updated, or deprecated in the version of the app that you have installed are highlighted with small icons that indicate the relevant changes.

After installing a new version of Splunk App for PCI Compliance or a new version of an app that provides views and collections for use in Splunk App for PCI Compliance, visit the Edit Navigation view to check for updates in those views and collections.

1. On the Splunk App for PCI Compliance menu bar, select **Configure > General > Navigation**.
2. If any content has been updated, the message "Some content updates available" appears at the top of the navigation editor.
3. Look for icons on the views on the editor pane to find content that has been added, updated, or deprecated. These same icons also appear in the Add a New View and Add a New Collection menus.

**Set a default view for Splunk App for PCI Compliance**

To see a specific view or link when you or another user opens Splunk App for PCI Compliance, set a default view.

1. On the Splunk App for PCI Compliance menu bar, select **Configure > General > Navigation**.
2. Locate the view or link that you want to be the default view.
3. Click the checkmark icon that appears when you mouse over the view to Set this as the default view.
4. Click **Save** to save your changes
5. Click **OK** to refresh the page and view your changes.
Edit the existing menu bar navigation

1. On the Splunk App for PCI Compliance menu bar, select Configure >
   General > Navigation.
2. Click and drag views or collections of views to change the location of the
   views or collections of views in the menu.
3. Click the X next to a view or collection to remove it from the menu.
4. Click the ☐️ icon to edit the name of a collection.
5. Click the ☐️ icon to add a divider and visually separate items in a collection.
6. Click Save to save your changes
7. Click OK to refresh the page and view your changes.

Add a single view to the menu bar

You can add a new view to the menu bar without adding it to a collection.

1. On the Splunk App for PCI Compliance menu bar, select Configure >
   General > Navigation.
2. Click Add a New View.
3. Leave View Options set to the default of View.
4. Click Select a View from Unused Views.
5. Select a dashboard or view from the list.
6. Click Save. The dashboard appears on the navigation editor.
7. If you are finished adding items to the menu, click Save to save your
   changes
8. Click OK to refresh the page and view your changes.

Add a collection to the menu bar

Use a collection to organize several views or links together in the menu bar.

1. On the Splunk App for PCI Compliance menu bar, select Configure >
   General > Navigation.
2. Click Add a New Collection.
3. Type a Name. For example, Audit.
4. Click Save. The collection appears on the navigation editor.

You must add a view or link to the collection before it appears in the menu
navigation.
Configure a custom report

The Splunk App for PCI Compliance provides reports for different aspects of your PCI compliance. Each report (or dashboard) in the Splunk App for PCI Compliance has an XML file, such as `pci_malware_activity.xml`, that describes the information used in the report, which notable events provide the data, and how that data is displayed. These reports are included as part of the app.

To add a custom report to your deployment, you need to first create the XML file for your report. See About the Dashboard Editor in the *Dashboards and Visualizations* manual.

**Choose the domain that the report applies to**

A report is associated, or categorized, with a domain within the app. In the Splunk App for PCI Compliance, these categories are shown in the *Reports* tab. The categories include:

- R1: Network Traffic
- R2: Default Configuration
- R3: Protect Data at Rest

To have the new report show up in the correct place in the app navigation (or correct location in the menu bar), you must choose the category domain that the report applies to.

**Add the report to the navigation menu bar**

To add your custom report to the app, you need to add it to the navigation. You must associate the new report with a domain.

Add views to an existing collection. In this case, each PCI domain is a collection.

1. On the Splunk App for PCI Compliance menu bar, select **Configure > General > Navigation**.
2. Locate the collection that you want to add views to.
3. Click the icon.
4. Leave **View Options** set to the default of **View**.
5. Click **Select a View** from **Unused Views**.
6. Select a view from the list.
7. Click **Save**. The view appears on the navigation editor.
8. If you are finished adding items to the menu, click **Save** to save your changes.
9. Click OK to refresh the page and view your changes.

**Add a link to the menu bar**

You can add a link to the menu bar of Splunk App for PCI Compliance. For example, add a link to a specifically-filtered view of Incident Review or to an external ticketing system.

*Create a link in the menu to an external system or webpage*

1. On the Splunk App for PCI Compliance menu bar, select **Configure > General > Navigation**.
2. Click **Add a New View** to add it to the menu, or locate an existing collection and click the icon to add the link to an existing collection of views.
3. Select **Link** from **View Options**.
4. Type a **Name** to appear on the Splunk App for PCI Compliance menu. For example, Splunk Answers.
5. Type a link. For example, https://answers.splunk.com/
6. Click **Save**.
7. If you are finished adding items to the menu, click **Save** to save your changes.
8. Click **OK** to refresh the page and view your changes.

**Restore the default navigation**

To restore the default navigation of the Splunk App for PCI Compliance menu bar:

1. On the Splunk App for PCI Compliance menu bar, select **Configure > General > Navigation**.
2. In the upper right corner, click **Restore Default Configuration**.
3. Click **OK** to confirm.
4. Scroll to the bottom of page and click **Save**.

**Email a report**

You can configure the Splunk App for PCI compliance to email a report by attaching the report to the email as an HTML file or by including it inline in the email body. See Define actions for your scheduled report with the Edit Schedule dialog in the *Reporting Manual*.
Configure and deploy indexes

Splunk App for PCI Compliance implements custom indexes for event storage. The indexes are defined across the apps provided with Splunk App for PCI Compliance.

- In a single instance deployment, the installation of Enterprise Security creates the indexes in the default path for data storage.
- In a Splunk Cloud deployment, customers work with Splunk Support to set up, manage, and maintain their cloud index parameters. See Manage Splunk Cloud indexes in the *Splunk Cloud User Manual*.
- In a distributed deployment, create the indexes on all Splunk platform indexers or search peers.

Index configuration

The indexes defined in Splunk App for PCI Compliance do not provide configuration settings to address:

- Multiple storage paths
- Accelerated data models
- Data retention
- Bucket sizing
- Use of volume parameters.

For detailed examples of configuring indexes, see indexes.conf.example in the Splunk Enterprise *Admin Manual*.

Indexes by app

<table>
<thead>
<tr>
<th>App context</th>
<th>Index</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA-ESS-AccessProtection</td>
<td>gia_summary</td>
<td>Summary index used by the Geographically Improbable Access panel on the Access Anomalies dashboard.</td>
</tr>
<tr>
<td>DA-ESS-ThreatIntelligence</td>
<td>ioc</td>
<td>Unused in this release.</td>
</tr>
<tr>
<td></td>
<td>threat_activity</td>
<td>Contains events that result from a threat list match.</td>
</tr>
<tr>
<td>SA-AuditAndDataProtection</td>
<td>audit_summary</td>
<td>Audit and Data Protection summary index.</td>
</tr>
<tr>
<td>App context</td>
<td>Index</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SA-EndpointProtection</td>
<td>endpoint_summary</td>
<td>Endpoint protection summary index.</td>
</tr>
<tr>
<td></td>
<td>notable</td>
<td>Contains the notable events.</td>
</tr>
<tr>
<td>SA-ThreatIntelligence</td>
<td>notable_summary</td>
<td>Contains a stats summary of notable events used on select dashboards.</td>
</tr>
<tr>
<td></td>
<td>risk</td>
<td>Contains the risk modifier events.</td>
</tr>
<tr>
<td>SA-NetworkProtection</td>
<td>whois</td>
<td>WHOIS data index.</td>
</tr>
<tr>
<td>Splunk_SA_CIM</td>
<td>cim_summary</td>
<td>Unused in this release.</td>
</tr>
<tr>
<td></td>
<td>cim_modactions</td>
<td>Contains the adaptive response action events.</td>
</tr>
</tbody>
</table>

Add-ons can include custom indexes defined in an `indexes.conf` file.

**Index deployment**

Splunk App for PCI Compliance includes a tool to gather the `indexes.conf` and `index-time props.conf` and `transforms.conf` settings from all enabled apps and add-ons on the search head and assemble them into one add-on. For more details, see Deploy add-ons included with Splunk Enterprise Security in this manual.

**Configure users and roles**

Splunk App for PCI Compliance uses the access control system integrated with the Splunk platform. The Splunk platform authorization allows you to add users, assign users to roles, and assign those roles custom capabilities to provide granular, role-based access control for your organization.

**Configuring user roles**

Splunk App for PCI Compliance adds three roles to the default roles provided by Splunk platform. The new roles allow a Splunk administrator to assign access to specific functions in ES based on a user’s access requirements. Assign all Splunk App for PCI Compliance users appropriate roles in order to perform their duties. There are three categories of users.
<table>
<thead>
<tr>
<th>User</th>
<th>Description</th>
<th>Splunk PCI role</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI Compliance Manager</td>
<td>Reviews PCI Compliance Posture, Protection Centers, and Audit dashboards in order to understand current PCI Compliance Posture of the organization. PCI Compliance Managers generally do not configure the product or manage incidents.</td>
<td>pci_user</td>
</tr>
<tr>
<td>PCI Compliance Analyst</td>
<td>Uses PCI Compliance Posture and Incident Review dashboards to manage and investigate PCI compliance incidents. PCI Compliance Analyst are also responsible for reviewing Protection Centers and providing direction on what constitutes a PCI compliance incident. Generally, they define the thresholds used by correlation searches and dashboards. A PCI Compliance Analyst needs to be able to edit correlation searches and create suppressions.</td>
<td>pci_analyst</td>
</tr>
<tr>
<td>PCI Compliance Administrator</td>
<td>Installs and maintains Splunk Enterprise and Splunk Apps. This user is responsible for configuring workflow, new data sources, tuning of rules, and troubleshooting the application.</td>
<td>admin or sc_admin</td>
</tr>
</tbody>
</table>

Each Splunk App for PCI Compliance custom role inherits from Splunk platform roles and adds capabilities specific to the PCI app. Not all of the three roles custom to the Splunk App for PCI Compliance can be assigned to users.

<table>
<thead>
<tr>
<th>Splunk PCI role</th>
<th>Inherits from Splunk platform role</th>
<th>Added Splunk PCI capabilities</th>
<th>Can be assigned to users</th>
</tr>
</thead>
<tbody>
<tr>
<td>pci_user</td>
<td>user</td>
<td>real-time search, list search head clustering</td>
<td>Yes. Replaces the user role for PCI users.</td>
</tr>
<tr>
<td>pci_analyst</td>
<td>user, pci_user, power</td>
<td>Inherits pci_user and adds the capabilities to create, edit, and own notable events and perform all</td>
<td>Yes. Replaces the power role for PCI users.</td>
</tr>
</tbody>
</table>
transitions, and create and modify investigations.

<table>
<thead>
<tr>
<th>Splunk PCI role</th>
<th>Inherits from Splunk platform role</th>
<th>Added Splunk PCI capabilities</th>
<th>Can be assigned to users</th>
</tr>
</thead>
<tbody>
<tr>
<td>pci_admin</td>
<td>user, pci_user, power, pci_analyst</td>
<td>Inherits pci_analyst and adds several other capabilities.</td>
<td>No. You must use a Splunk platform admin role to administer a Splunk App for PCI Compliance installation.</td>
</tr>
</tbody>
</table>

See the capabilities specific to Splunk App for PCI Compliance for more details about which capabilities are assigned to which roles by default.

The Splunk platform admin role inherits all unique PCI capabilities. In a Splunk Cloud deployment, the Splunk platform admin role is named sc_admin. Use the admin or sc_admin role to administer a Splunk App for PCI Compliance installation.

<table>
<thead>
<tr>
<th>Splunk platform role</th>
<th>Inherits from role</th>
<th>Added capabilities</th>
<th>Accepts user assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>user, pci_user, power, pci_analyst, pci_admin</td>
<td>All</td>
<td>Yes.</td>
</tr>
<tr>
<td>sc_admin</td>
<td>user, pci_user, power, pci_analyst, pci_admin</td>
<td>All</td>
<td>Yes.</td>
</tr>
</tbody>
</table>

**Role inheritance**

All role inheritance is preconfigured in Splunk App for PCI Compliance. If the capabilities of any role are changed, other inheriting roles will receive the changes. For more information about roles, see the Splunk platform documentation.

- For Splunk Enterprise, see Add and edit roles in *Securing Splunk Enterprise*.
- For Splunk Cloud, see Manage Splunk Cloud roles in *Splunk Cloud User Manual*. 

41
Add capabilities to a role

Capabilities control the level of access that roles have to various features in the Splunk App for PCI Compliance. Use the Permissions page in the Splunk App for PCI Compliance to review and change the capabilities assigned to a role.

1. On the Splunk App for PCI Compliance menu bar, select Configure > General > Permissions.
2. Find the role you want to update.
3. Find the ES Component you want to add.
4. Select the check box for the component for the role.
5. Save.

Capabilities specific to Splunk App for PCI Compliance

Splunk App for PCI Compliance uses custom capabilities to control access to PCI-specific features.

Add capabilities on the permissions page in Splunk App for PCI Compliance to make sure that the proper access control lists (ACLs) are updated. The permissions page makes the ACL changes for you. If you add these custom capabilities on the Splunk platform settings page, you must update the ACLs yourself.

<table>
<thead>
<tr>
<th>Function in ES</th>
<th>Description</th>
<th>Capability</th>
<th>pci_user</th>
<th>pci_analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new notable events</td>
<td>Create ad-hoc notable events from search results. See Manually create a notable event.</td>
<td>edit_notable_events</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Edit advanced search schedule settings</td>
<td>Edit the schedule priority and schedule window of correlation searches on Content</td>
<td>edit_search_schedule_priority, edit_search_schedule_window</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function in ES</td>
<td>Description</td>
<td>Capability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit correlation searches</td>
<td>Edit correlation searches on Content Management. See Configure correlation searches.</td>
<td>edit_correlationsearches schedule_search</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit Distributed Configuration Management</td>
<td>Use distributed configuration management.</td>
<td>edit_modinput_es_deployment_manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit ES navigation</td>
<td>Make changes to the Splunk App for PCI Compliance navigation.</td>
<td>edit_es_navigation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit glass tables</td>
<td>Create and modify glass tables. Not relevant for the Splunk App for PCI Compliance.</td>
<td>edit_glasstable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit identity lookup configuration</td>
<td>Manage the configuration of identity lookups and restrict asset and identity correlation. Not relevant for the Splunk App for PCI Compliance.</td>
<td>edit_identitylookup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit Incident Review</td>
<td>Make changes to Incident Review</td>
<td>edit_log_review_settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function in ES</td>
<td>Description</td>
<td>Capability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>settings</td>
<td>See Customize Incident Review.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit lookups</td>
<td>Make changes to lookup table files.</td>
<td>edit_lookups, edit_managed_configurations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit statuses</td>
<td>Make changes to the statuses available to select for investigations and notable events. See Managing and monitoring notable event statuses.</td>
<td>edit_reviewstatuses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit notable event suppressions</td>
<td>Create and edit notable event suppressions. See Create and manage notable event suppressions.</td>
<td>edit_suppressions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit notable events</td>
<td>Make changes to notable events, such as assigning them.</td>
<td>edit_notable_events, transition_reviewstatus-X_to_Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit per-panel filters</td>
<td>Create and manage per-panel filters for dashboards.</td>
<td>edit_per_panel_filters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit intelligence</td>
<td>Create and modify</td>
<td>edit_modinput_threatlist, edit_modinput_threat_intelligence_manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function in ES</td>
<td>Description</td>
<td>Capability</td>
<td>pci_user</td>
<td>pci_analyst</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Edit threat intelligence collections</td>
<td>Upload threat intelligence and perform CRUD operations on threat intelligence collections using the REST API. Not relevant for Splunk App for PCI Compliance.</td>
<td>edit_threat_intel_collections</td>
<td></td>
</tr>
<tr>
<td>Manage all investigations</td>
<td>Allows the role to view and make changes to all investigations.</td>
<td>manage_all_investigations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Own notable events</td>
<td>Allows the role to be an owner of notable events. See Notable Events.</td>
<td>can_own_notable_events</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search-driven lookups</td>
<td>Create lookup tables that can be populated by a search.</td>
<td>edit_managed_configurations schedule_search</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage your investigations</td>
<td>Create and edit</td>
<td>edit_timelines</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
investigations. Roles with this capability can make changes to investigations on which they are a collaborator. See Investigations in Splunk Enterprise Security.

<table>
<thead>
<tr>
<th>Function in ES</th>
<th>Description</th>
<th>Capability</th>
<th>pci_user</th>
<th>pci_analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Manager</td>
<td>Manage credentials and certificates for Splunk Enterprise Security and other apps. Cannot be set on the Permissions page.</td>
<td>admin_all_objects list_storage_passwords list_app_certs edit_app_certs delete_app_certs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Adjust the concurrent searches for a role**

Splunk platform defines a limit on concurrently running searches for the user and power roles by default. You may want to change those concurrent searches for some roles.

1. On the Splunk App for PCI Compliance menu bar, select **Configure > General > General Settings**.
2. Review the limits for roles and change them as desired.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Disk Quota (admin)</td>
<td>The maximum disk space (MB) a user with the admin role can use to store search job results.</td>
</tr>
<tr>
<td>Item Description</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Search Jobs Quota (admin)</td>
<td>The maximum number of concurrent searches for users with the admin role.</td>
</tr>
<tr>
<td>Search Jobs Quota (power)</td>
<td>The maximum number of concurrent searches for users with the power role.</td>
</tr>
</tbody>
</table>

To change the limits for roles other than admin and power, edit the authorize.conf file to update the default search quota. See the authorize.conf.example in the Admin manual.

### Configure the roles to search multiple indexes

Splunk platform stores ingested data sources in multiple indexes. Distributing data into multiple indexes allows you to use role-based access control and vary retention policies for data sources. Splunk platform configures all roles to search only the main index by default. See About configuring role-based user access.

To allow roles in Splunk App for PCI Compliance to search additional indexes, assign the indexes that contain relevant security data to the relevant roles.

1. Select **Settings > Access Controls**.
2. Click **Roles**.
3. Click the role name that you want to allow to search additional indexes.
4. Select the desired **Indexes searched by default** and **Indexes** that this role can search. Do not include summary indexes, as this can cause a search and summary index loop.
5. Save your changes.
6. Repeat for additional roles as needed.

If you do not update the roles with the correct indexes, searches and other knowledge objects that rely on data from unassigned indexes will not update or display results.

For more information on the reasons for multiple indexes, see Why have multiple indexes? in Managing Indexers and Clusters of Indexers.
Configure reports

Reports in the Splunk App for PCI Compliance

This section contains information on how to configure reports in the Splunk App for PCI Compliance to get correct data flowing into the app.

The Splunk App for PCI Compliance includes reports that you can configure for best results. For each report, there is a description, configuration information, and troubleshooting steps. Use the links in the table to go to the information for a specific report.

<table>
<thead>
<tr>
<th>R1: Network Traffic</th>
<th>R2: Default Configurations</th>
<th>R3: Protect Data At Rest</th>
</tr>
</thead>
</table>
| • Firewall Rule Activity  
  • Network Traffic Activity  
  • Prohibited Services | • Default Account Access  
  • Insecure Authentication Attempts  
  • PCI System Inventory  
  • Primary Functions  
  • Prohibited Services  
  • System Misconfigurations  
  • Wireless Network Misconfigurations | Credit Card Data Found |
| R4: Protect Data in Motion | R5: Antimalware Protection | R6: Patch Update Protection |
| Credit Card Data Found | • Endpoint Product Deployment  
  • Endpoint Product Versions  
  • Malware Activity  
  • Malware Signature Updates | • Anomalous System Uptime  
  • Default Account Access  
  • Patch Service Status |
<table>
<thead>
<tr>
<th>R1: Network Traffic</th>
<th>R2: Default Configurations</th>
<th>R3: Protect Data At Rest</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• System Patch Status</td>
</tr>
<tr>
<td>R7: Access Monitoring</td>
<td>R8: Activity Accountability</td>
<td>R10: Cardholder Data Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Endpoint Changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PCI Asset Logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PCI Resource Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Privileged User Activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• System Time Synchronization</td>
</tr>
</tbody>
</table>

- PCI Command History
- PCI Resource Access

- Default Account Access
- PCI Resource Access

- Endpoint Changes
- Vulnerability Scan Details
- IDS/IPS Alert Activity

**Firewall Rule Activity**

This report provides a six month view of firewall rule usage to help identify unneeded, outdated, or incorrect rules. This report ensures that all rules allow only authorized services and ports that match business justifications. Compliance managers might run this report more frequently to avoid unnecessary risks and avoid opening potential security holes.
Relevant data sources

Relevant data resources include firewalls that produce rule ID information.

How to configure this report

1. Index the firewall activity data that includes a rule ID in Splunk platform.
2. Map the data to the following Common Information Model fields:
   - action, dvc, rule, transport, src, dest. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the data with "network" and "communicate".

CIM-compliant add-ons for these data sources perform this step for you.

Report description

The data in the Firewall Rule Activity report is populated by the Network – Communication Rule Tracker – Lookup Gen, a lookup that runs against the communication_rule_tracker CSV file. This file is created by the Network – Communication Rule Tracker – Lookup Gen lookup. Review the lookup generating search to learn more about the search schedule and time range.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Verify that...</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall data has been indexed in Splunk platform.</td>
<td><code>tag=network tag=communicate</code> or <code>communicate</code></td>
<td>Returns data from your network device(s).</td>
</tr>
<tr>
<td>The data fields are normalized to the CIM.</td>
<td><code>communicate</code></td>
<td>Returns data in communication_rule_tracker. Each field contains the correct, expected data.</td>
</tr>
<tr>
<td>The communication rule tracker is populated.</td>
<td><code>inputlookup append=t communication_rule_tracker</code> or <code>communication_rule_tracker</code></td>
<td>Returns data in communication_rule_tracker.</td>
</tr>
</tbody>
</table>
**Additional Information**

The communication rule tracker file is located at
$SPLUNK_HOME/etc/apps/SA-NetworkProtection/lookups.

**Network Traffic Activity**

This report provides a six month view of network traffic activity between PCI domains. This report looks at traffic data produced by firewalls, routers, switches, and any other device that produces network traffic data. You can modify and customize the report by using different filters.

**Relevant data sources**

Relevant data sources for this report include any device that creates network traffic activity, such as firewalls.

**How to configure this report**

1. Index firewall activity data in Splunk platform.
2. Map the data to the following **Common Information Model** fields.  
   host, action, dvc, rule, transport, src, src_port, dest, dest_port, vendor_product.  
   CIM-compliant add-ons for these data sources perform this step for you.
3. Set the category column for each asset in the **Asset** table to **pci** or **cardholder**.
4. Set the pci_domain column for each asset in the **Asset** table to (dmz|trust|untrust|cardholder|wireless).
5. Set the is_secure and is_prohibited columns of the prohibited traffic list to {true|false}.

Mapping examples:

- The action field shows either allowed or blocked traffic.
- The eventtypes for traffic-related data are tagged with communicate and network

**Report description**

The **Network Traffic Activity** report relies on the Network Traffic data model.
Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have data from your network devices.</td>
<td><code>sourcetype=&lt;your_sourcetype_for_your_data&gt;</code></td>
<td>Returns data from your network devices.</td>
</tr>
<tr>
<td>Verify that network activity data has been indexed in Splunk platform.</td>
<td><code>tag=network tag=communicate</code> or <code>communicate</code></td>
<td>Returns all network traffic data from your network devices.</td>
</tr>
<tr>
<td>Verify that the fields are normalized to the Common Information Model.</td>
<td><code>communicate</code></td>
<td>fields sourcetype, action, dvc, rule, transport, src, dest</td>
</tr>
</tbody>
</table>

**Default Account Access**

This report provides a six-month rolling view of attempts to access cardholder systems using default user accounts. This report looks at all activity by accounts categorized in the identity table with `tag=default`. A default list of accounts is provided in the identity table, which can be edited from the Content Management page.

**Relevant data sources**

Relevant data sources for this report includes Windows Security, Unix SSH, and any other application, system, or device that produces authentication data. The report looks at data in the the Authentication data model.
How to configure this report

1. Index authentication data from a device, application, or system in Splunk platform.
2. Map the data to the following Common Information Model fields: host, action, app, src, src_user, dest, user. CIM-compliant add-ons for these data sources perform this step for you.
3. Set the category column of the Identity table to default for all accounts that are considered default accounts.

Report description

The data in the Default Account Access report is populated by the Authentication data model.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have data from your network devices.</td>
<td>sourcetype=&lt;your_sourcetype_for_your_data&gt;</td>
<td>Returns data from your network devices.</td>
</tr>
<tr>
<td>Verify that authentication data is indexed in Splunk platform.</td>
<td>tag=authentication or <code>authentication</code></td>
<td>Returns all default account activity data from your devices.</td>
</tr>
<tr>
<td>Verify that default user accounts are tagged properly.</td>
<td><code>default_user_accounts</code></td>
<td>Returns all a list of all default account activity.</td>
</tr>
<tr>
<td>Verify that authentication attempts for default users are returned.</td>
<td><code>default_user_accounts</code> <code>authentication</code></td>
<td>Returns a list of all default account authentication activity.</td>
</tr>
</tbody>
</table>
Verify that authentication data is normalized to the Common Information Model properly.

`authentication` | fields sourcetype, action, app, src, src_user, dest, user

Returns a list of events and the specific default account activity fields of data populated from your devices.

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that authentication data is normalized to the Common Information Model properly.</td>
<td><code>authentication</code></td>
<td>fields sourcetype, action, app, src, src_user, dest, user</td>
</tr>
</tbody>
</table>

**Additional information**

The report displays all attempts from users in either the `src_user` or `user` fields.

The assets table includes user information for default accounts such as root, network service, and other accounts that can produce a lot of data. Customers might not want to include that data in the report. They can modify the assets table to exclude particular users.

**Insecure Authentication Attempts**

This report looks at attempts to access cardholder systems using insecure protocols and services. Use this report to identify the source of the insecure authentication attempts so they can be evaluated and eliminated if they pose a risk to the cardholder system.

If remote administration is not done with secure authentication and encrypted communications, sensitive administrative or operational level information like administrator passwords could be revealed to an eavesdropper. PCI DSS requires that you use only secure technologies to log into cardholder systems.

**Relevant data sources**

Relevant data sources for this report include any device that produces clear text or other insecure authentication activity, such as Windows Security, telnet, and others.
How to configure this report

1. Index authentication data from a device, application, or system in Splunk platform.
2. Map the data to the following Common Information Model fields: host, action, app, src, src_user, dest, user. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag authentication messages that pass credentials in the clear or are considered insecure with either "cleartext" or "insecure".

Report description

The data in the Insecure Authentication Attempts report is populated by the Authentication data model.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that authentication data is returned.</td>
<td><code>tag=authentication</code> or <code>authentication</code></td>
<td>Returns all authentication activity data from your network device(s).</td>
</tr>
<tr>
<td>Verify that clear text authentication attempts are returned.</td>
<td><code>tag=cleartext tag=insecure</code></td>
<td>Returns all clear text authentication data.</td>
</tr>
<tr>
<td>Verify that insecure authentication attempts are returned.</td>
<td><code>tag=authentication tag=insecure</code></td>
<td>Returns all insecure authentication attempts.</td>
</tr>
<tr>
<td>Verify that all insecure and clear text authentication data is</td>
<td><code>authentication</code></td>
<td>tags outputfield=tag</td>
</tr>
</tbody>
</table>
normalized to the Common Information Model properly.

### Additional information

Windows login events with `LoginType=8` are often seen in this report. These login events are clear text login attempts. Other examples include telnet login events, rsh, rexec, and so on.

### PCI System Inventory

This report provides visibility into software that is running on PCI assets. Monitor this report on a daily basis to ensure that no unexpected services or applications are being run. Unexpected software components should be investigated further.

Maintaining a current list of all software components running in the PCI compliant environment enables an organization to define risk exposure and devise adequate controls. Without an automated inventory, some system components could be inadvertently excluded from the organization’s configuration standards.

### Relevant data sources

Relevant data sources for this report include service, process, and port data such as the Splunk Add-on for Unix and Linux or the Splunk Add-on for Microsoft Windows.

### How to configure this report

1. Index process, service, and/or port data in Splunk platform.
2. Map the data to the following Common Information Model fields. Map services fields to `dest, StartMode`. Map process fields to `dest, process`. Map port fields to `dest, dest_port, transport`. CIM-compliant add-ons for these data sources perform this step for you.
**Report description**

The data in the 'PCI Inventory' report is populated by three lookups. One lookup is generated by the [Endpoint - Local Processes - Lookup Gen saved search](#), a second by the [Endpoint - Services Tracker - Lookup Gen saved search](#), and the third by the [Endpoint - Listening Ports Tracker - Lookup Gen saved search](#). The `localprocesses_tracker`, `services_tracker` macros correlate process data with the asset and identity tables to pull in additional information.

This report includes three searches: [Endpoint - Local Processes - Lookup Gen](#), [Endpoint - Services Tracker - Lookup Gen](#), and [Endpoint - Listening Ports Tracker - Lookup Gen](#).

**Useful searches for troubleshooting**

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that service, process, and/or port information has been indexed.</td>
<td><code>sourcetype=&lt;expected_sourcetype&gt;</code></td>
<td>Returns data from service, process, and/or port. For example, <code>sourcetype=WMI:Service</code>.</td>
</tr>
<tr>
<td>Verify that the service data has been normalized at search time correctly.</td>
<td>`sourcetype=&quot;*:Service&quot;</td>
<td>table dest, <code>StartMode</code></td>
</tr>
<tr>
<td></td>
<td><code>service</code></td>
<td>table dest, <code>StartMode</code></td>
</tr>
<tr>
<td>Verify that the process data has been normalized at search time correctly.</td>
<td>`sourcetype=&quot;*:LocalProcesses&quot;</td>
<td>table dest, process</td>
</tr>
<tr>
<td>Verify that the port data has been normalized at search time correctly.</td>
<td>`tag=listening_tag=port</td>
<td>table dest,dest_port,transport`</td>
</tr>
<tr>
<td></td>
<td><code>listeningports</code></td>
<td>table dest,dest_port,transport</td>
</tr>
<tr>
<td>Troubleshooting Task</td>
<td>Search/Action</td>
<td>Expected Result</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Verify that the service tracker file is getting created correctly.</td>
<td>`</td>
<td>inputlookup append=T services_tracker`</td>
</tr>
<tr>
<td></td>
<td>`</td>
<td><code>services_tracker</code>'`</td>
</tr>
<tr>
<td>Verify that the process tracker file is getting created correctly.</td>
<td>`</td>
<td>inputlookup append=T localprocesses_tracker`</td>
</tr>
<tr>
<td></td>
<td>`</td>
<td><code>localprocesses_tracker</code>'`</td>
</tr>
<tr>
<td>Verify that the port tracker file is getting created correctly.</td>
<td>`</td>
<td>inputlookup append=T listeningports_tracker`</td>
</tr>
<tr>
<td></td>
<td>`</td>
<td><code>listeningports_tracker</code>'</td>
</tr>
<tr>
<td>Verify that the Interesting Services, Interesting Processes, and/or Interesting Ports lookups are populated with expected prohibited values.</td>
<td>Open the relevant lists in <strong>Configure &gt; Content Management</strong> and verify that the is_prohibited column is set to &quot;true/false&quot;.</td>
<td></td>
</tr>
</tbody>
</table>

**Additional information**

This report uses default source types that ship with the Splunk add-on for *nix and the Splunk add-on for Windows.

Tracker files for this report are located:

- `$SPLUNK_HOME/etc/apps/SA-EndpointProtection/lookups/listeningports_tracker.csv`
- `$SPLUNK_HOME/etc/apps/SA-EndpointProtection/lookups/services_tracker.csv`
- `$SPLUNK_HOME/etc/apps/SA-EndpointProtection/lookups/localprocesses_tracker.csv`
Primary Functions

This report looks at cardholder systems that have multiple primary functions active. The data in the Primary Functions report is generated from a lookup file (assets.csv) populated by the user. This report looks at process data, service data, and port/protocol data to determine what functions are running on a system and displays them in the result. Use this report to identify systems where multiple primary functions might be running or where unexpected services could be in use.

Systems within the PCI cardholder environment should be implemented with only a single primary function to prevent functions that require different security levels from coexisting on the same server. The PCI requirement ensures that your system configuration standards and related processes minimize the potential for introducing security weaknesses to the system.

Relevant data sources

Relevant data sources for this report include service, process, and port data such as the Splunk Add-on for Unix and Linux or the Splunk Add-on for Microsoft Windows.

How to configure this report

1. Index process, service, and/or port data in Splunk platform.
2. Map the data to the following Common Information Model fields. Map services fields to dest, StartMode. Map process fields to dest, process. Map port fields: dest, dest_port, transport. CIM-compliant add-ons for these data sources perform this step for you.
3. Configure the Primary Functions list with the functions desired.

Report description

The data in the Primary Functions report is populated by three lookups. One lookup is generated by the Endpoint - Local Processes - Lookup Gen saved search, a second by the Endpoint - Services Tracker - Lookup Gen saved search, and the third by the Endpoint - Listening Ports Tracker- Lookup Gen saved search. The localprocesses_tracker, services_tracker macros correlate process data with the asset and identity tables to pull in additional information.

This report includes three searches: Endpoint - Local Processes - Lookup Gen, Endpoint - Services Tracker - Lookup Gen, and Endpoint - Listening Ports
Tracker - Lookup Gen.

Review each lookup generating search to learn more about the search schedule and time range.

The primary functions list can be found at Configure > Content Management and clicking the Primary Functions lookup. The primary functions CSV can be found at $SPLUNK_HOME/etc/apps/SA-EndpointProtection/lookups/primary_functions.csv.

### Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that service, process, and/or port information has been indexed.</td>
<td>sourcetype=&lt;expected_st&gt;</td>
<td>Returns data from your expected source type.</td>
</tr>
<tr>
<td>Verify that the service data has been normalized at search time correctly.</td>
<td>Windows: sourcetype=&quot;*Services&quot;</td>
<td>Returns a table of service data.</td>
</tr>
<tr>
<td>or Nix: sourcetype=&quot;Unix:Service&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>or listeningports</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>table dest, StartMode</td>
<td>table dest, start_mode</td>
</tr>
<tr>
<td>Verify that the process data has been normalized at search time correctly.</td>
<td>sourcetype=&quot;*:LocalProcess&quot;</td>
<td>Returns a table of process data.</td>
</tr>
<tr>
<td>or table dest, process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify that the port data has been normalized at search time correctly.</td>
<td>tag=listening tag=port</td>
<td>Returns a table of port data.</td>
</tr>
<tr>
<td>or <code>listeningports</code></td>
<td>table dest,dest_port,transport</td>
<td>table dest,dest_port,transport</td>
</tr>
<tr>
<td>or</td>
<td><code>listeningports_tracker</code></td>
<td><code>listeningports_tracker</code></td>
</tr>
<tr>
<td>Verify that the service tracker file is getting created correctly.</td>
<td>inputlookup append=T</td>
<td>Returns data in the services tracker file.</td>
</tr>
<tr>
<td>services_tracker</td>
<td><code>services_tracker</code></td>
<td><code>services_tracker</code></td>
</tr>
<tr>
<td>or</td>
<td><code>services_tracker</code></td>
<td><code>services_tracker</code></td>
</tr>
<tr>
<td>Verify that the process tracker file is getting created correctly.</td>
<td>inputlookup append=T</td>
<td>Returns data in the process tracker file.</td>
</tr>
<tr>
<td>localprocesses_tracker</td>
<td><code>localprocesses_tracker</code></td>
<td><code>localprocesses_tracker</code></td>
</tr>
<tr>
<td>or</td>
<td><code>localprocesses_tracker</code></td>
<td><code>localprocesses_tracker</code></td>
</tr>
<tr>
<td>Verify that the port tracker file is getting created correctly.</td>
<td>inputlookup append=T</td>
<td>Returns data in the port tracker file.</td>
</tr>
<tr>
<td>listeningports_tracker</td>
<td><code>listeningports_tracker</code></td>
<td><code>listeningports_tracker</code></td>
</tr>
<tr>
<td>or</td>
<td><code>listeningports_tracker</code></td>
<td><code>listeningports_tracker</code></td>
</tr>
<tr>
<td>or</td>
<td><code>primary_functions_tracker</code></td>
<td><code>primary_functions_tracker</code></td>
</tr>
</tbody>
</table>
Verify that the primary functions tracker is created correctly.

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Returns data in the primary functions tracker.</td>
</tr>
</tbody>
</table>

**Additional information**

This report uses default source types that ship with the Splunk add-on for Windows and the Splunk add-on for *nix.

Tracker files for this report are located:

- `$SPLUNK_HOME/etc/apps/SA-EndpointProtection/lookups/listeningports_tracker.csv`
- `$SPLUNK_HOME/etc/apps/SA-EndpointProtection/lookups/services_tracker.csv`
- `$SPLUNK_HOME/etc/apps/SA-EndpointProtection/lookups/localprocesses_tracker.csv`

**Prohibited Services**

This report looks at prohibited services data produced by the `services_tracker` lookup. It reports on systems with prohibited services installed and running. Compromises often happen because of unused or insecure service and ports on systems within the cardholder environment or systems that have a communication path to cardholder systems.

These services and ports can have known vulnerabilities. A security hardening policy should be defined that clearly defines what services and protocols are allowed to run on each system. Organizations should test those systems periodically to ensure that they are patched appropriately and unauthorized services are disabled.

**Relevant data sources**

Relevant data sources for this report include service, process, and port data such as the Splunk Add-on for Unix and Linux or the Splunk Add-on for Microsoft Windows.

**How to configure this report**

1. Index process, service, or port data in Splunk platform.
2. Map the data to the following **Common Information Model** fields. Map services fields to `dest`, `StartMode`. Map process fields to `dest`, `process`. Map port fields: `dest`, `dest_port`, `transport`. CIM-compliant add-ons for these data sources perform this step for you.

3. Configure the `is_prohibited` column in the **Interesting [ports|processes|ports]** lists with any service, process, or port considered prohibited.

**Report description**

The data in the **Prohibited Services** report is populated by three `services_tracker` lookups. One lookup is generated by the **Endpoint - Local Processes Tracker - Lookup Gen** saved search, a second by the **Endpoint - Services Tracker - Lookup Gen** saved search, and the third by the **Endpoint - Listening Ports Tracker- Lookup Gen** saved search. The `localprocesses_tracker`, `services_tracker` macros correlate process data with the asset and identity tables to pull in additional information.

This report includes three searches: **Endpoint - Local Processes - Lookup Gen**, **Endpoint - Services Tracker - Lookup Gen**, and **Endpoint - Listening Ports Tracker- Lookup Gen**.

Review each lookup generating search to learn more about the search schedule and time range.

**Useful searches for troubleshooting**

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that service, process, and/or port information has been indexed.</td>
<td><code>sourcetype=&lt;expected_st&gt;</code></td>
<td>Returns data from service, process, and/or port. For example, <code>sourcetype=WMI:Service</code>.</td>
</tr>
<tr>
<td>Verify that the service data has been normalized at search time correctly.</td>
<td>`sourcetype=&quot;Service&quot;</td>
<td>table dest, StartMode<code> or ``service</code></td>
</tr>
<tr>
<td>Verify that the process data has been normalized at</td>
<td>`sourcetype=&quot;*:LocalProcess&quot;</td>
<td>table dest, process`</td>
</tr>
<tr>
<td>Troubleshooting Task</td>
<td>Search/Action</td>
<td>Expected Result</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>search time correctly.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify that the port data has been normalized at search time correctly.</td>
<td>tag=listening tag=port</td>
<td>table dest,dest_port,transport or <code>listeningports</code></td>
</tr>
<tr>
<td>Verify that the service tracker file is getting created correctly.</td>
<td></td>
<td>inputlookup append=T services_tracker or <code>services_tracker</code></td>
</tr>
<tr>
<td>Verify that the process tracker file is getting created correctly.</td>
<td></td>
<td>inputlookup append=T localprocesses_tracker or <code>localprocesses_tracker</code></td>
</tr>
<tr>
<td>Verify that the port tracker file is getting created correctly.</td>
<td></td>
<td>inputlookup append=T localprocesses_tracker or <code>listeningports_tracker</code></td>
</tr>
<tr>
<td>Verify that the Interesting Services, Interesting Processes, and/or Interesting Ports lookups are populated with expected prohibited values.</td>
<td>Open the lists in <strong>Configure &gt; Content Management</strong> and click **Interesting [ ports</td>
<td>processes</td>
</tr>
</tbody>
</table>

**Additional information**

This report uses default source types that ship with the Splunk Add-on for Unix and Linux and the Splunk Add-on for Microsoft Windows.

Tracker files for this report are located:

- `$SPLUNK_HOME/etc/apps/SA-EndpointProtection/lookups/listeningports_tracker.csv`
- `$SPLUNK_HOME/etc/apps/SA-EndpointProtection/lookups/services_tracker.csv`
System Misconfigurations

This report provides a view of all identified system misconfigurations on PCI-relevant assets in your cardholder environment. Use this report to compare the identified misconfigurations with the defined hardening policy to determine the level of risk to the asset.

Malicious individuals often use vendor default configuration settings to compromise systems and applications. These settings are well known in hacker communities and leave systems highly vulnerable to attack. This report ensures your organization's system configuration standards and related processes specifically address security settings and parameters that have known security implications.

Relevant data sources

Relevant data for this report includes data from configuration assessment tools that identify a misconfigured setting on an endpoint.

How to configure this report

1. Index misconfiguration data in Splunk platform.
2. Map the data to the following Common Information Model fields. `host, ids_type, category, signature, severity, src, dest, vendor_product`. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag misconfiguration events with "misconfiguration".

Report description

The data in the system misconfiguration report is populated by the IDS Attack and Vulnerabilities CIM data models

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that data is present.</td>
<td><code>ids_attack</code></td>
</tr>
<tr>
<td>Troubleshooting Task</td>
<td>Search/Action</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Verify that fields are normalized and available.</td>
<td><code>ids_attack</code></td>
</tr>
</tbody>
</table>

### Additional information

This report uses default source types from the Splunk Add-on for Unix and Linux and the Splunk Add-on for Microsoft Windows.

### Weak Encrypted Communication

This report looks at network data to identify network sessions encrypted with SSL or weak or insecure versions of the TLS protocol. Track SSL and TLS sessions in the PCI network and identify those encrypted by insecure SSL and TLS versions. Network traffic that uses those encryption protocols could be insecure and in violation of the PCI standard.

### Relevant data sources

Relevant data sources for this report include any log source that tracks SSL and TLS sessions. For example, firewall data, IDS and IPS devices, streaming data from Splunk Stream, or other network capture apps.

### How to configure this report

1. Index network data into Splunk platform.
2. Map the data to the following **Common Information Model** fields. Map the SSL or TLS version from the network traffic data to the `ssl_version` dataset in the Certificates data model. CIM-compliant add-ons for network traffic data sources perform this step for you.

### Report description

The data in the **Weak Encrypted Communications** report is populated by data from the **Certificates** data model and notable events that result from the
Wireless Network Misconfigurations

The report tracks misconfigurations found on wireless network devices. This report provides visibility into data collected from IDS/IPS, NAC, network scanners, and other sources of data. This report displays a list of misconfigurations found on wireless access devices. Use this report to view the misconfiguration information and continuously monitor the data to identify devices that are not configured properly.

Implementation and/or exploitation of wireless technology within a network is one of the most common paths for malicious users to gain access to the network and cardholder data. Corporate controlled or rogue access devices that are not configured with appropriate security configurations can allow an attacker to invisibly enter the network and put cardholder data at risk.

**Note:** This report does not display unencrypted traffic directly, only misconfigurations that indicate the possible transmission or side-channel leakage of unencrypted traffic. For a full traffic report, see Network Traffic Activity in the Installation and Configuration Manual.

**Relevant data sources**

Relevant data sources include misconfiguration data found by wireless network monitoring products or IDS systems. Relevant data sources also include data collected from IDS/IPS, NAC, network scanners, and other similar sources of data.

**How to configure this report**

1. Index network misconfiguration data in Splunk platform.
2. Map the data to the following **Common Information Model** fields: `host`, `ids_type`, `category`, `signature`, `severity`, `src`, `dest`, `vendor_product`. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag wireless misconfiguration events with misconfiguration and wireless.
Report description

The data in the Wireless System Misconfiguration report is populated by the IDS Attack and Vulnerabilities data models.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that data is present.</td>
<td><code>tag=misconfiguration tag=wireless</code></td>
</tr>
<tr>
<td>Verify that fields are normalized and available.</td>
<td><code>ids_attack</code></td>
</tr>
</tbody>
</table>

Credit Card Data Found

This report looks at credit card data, found in motion or at rest, from IDS, IPS, and DLP systems to provide visibility into potentially unauthorized transmissions of credit card data over the network or to unauthorized removable storage devices. Use this report to identify the source of the transmission so it can be further investigated and fixed.

The cardholder data environment should be monitored for unauthorized egress transmission of credit card data using IDS, IPS, and DLP-based technologies. PCI requires that cardholder data be protected from unauthorized access or distribution.

Relevant data sources

Relevant data sources for this report include alerts from IDS, IPS, or DLP solutions and alerts from the Luhn-based algorithm detection method implemented in the Splunk Enterprise Security framework and used by the Splunk App for PCI Compliance.
How to configure this report

Make sure the activity data you are monitoring conforms to the Common Information Model.

1. Index DLP, IDS, IPS, or other data that indicates discovery of credit card data in Splunk platform.
2. Map the data to the following Common Information Model fields: **src**, **dest**, **dvc**, **signature**. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the relevant events with "pii".

Report description

The data in the Unauthorized Credit Card Transmissions report is populated by the IDS Attack data model.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that data is present.</td>
<td><code>ids_attack</code></td>
<td>search tag=pii tag=ids tag=attack</td>
</tr>
<tr>
<td>Verify that fields are normalized and available.</td>
<td><code>ids_attack</code></td>
<td>search tag=pii tag=ids tag=attack</td>
</tr>
</tbody>
</table>

Additional information

This report uses default source types.

Endpoint Product Deployment

This report provides a summary and detail view of all PCI assets and the most current product versions installed. Use this report to identify any assets that are
not using the current antimalware product versions and take appropriate measures to ensure that systems are updated. Review this report at least once per day. Review this report more frequently if you are collecting data from antimalware solutions more frequently.

PCI DSS requires that assets within the cardholder data environment have antimalware technology installed and working to protect against viruses, worms, trojans, and other malware-based threats. The best antimalware software has limited effectiveness if it does not have the current antivirus product versions.

### Relevant data sources

Relevant data sources for this report include antivirus activity, endpoint version data, or endpoint product signature data. This report looks at endpoint protection deployment activity data produced by firewalls, routers, switches, and any other device that produces endpoint data.

### How to configure this report

1. Index endpoint product version data, signature data, or activity data from an antivirus or other endpoint protection software.
2. Map the data to the following Common Information Model fields: `dest`, `product_version`, `vendor_product`. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the activity data with with "malware", "operation", and "attack".

### Report description

The data in the Endpoint Product Deployment report is populated by a lookup that runs against the `malware_operation_tracker` CSV file. This file is created by the Endpoint - Malware Operations Tracker - Lookup Gen lookup.

Review each lookup generating search to learn more about the search schedule and time range.

### Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that malware activity data is present.</td>
<td><code>tag=malware tag=attack</code></td>
<td>Returns malware</td>
</tr>
<tr>
<td>Troubleshooting Task</td>
<td>Search/Action</td>
<td>Expected Result</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Verify that malware activity data fields are normalized.</td>
<td><code>malware</code></td>
<td>table _time, host, action, category, signature, dest, dest_nt_domain, user, vendor_product</td>
</tr>
<tr>
<td>Verify that the endpoint operations tracker file has been populated as expected.</td>
<td><code>malware_operations_tracker</code></td>
<td>inputlookup append=T</td>
</tr>
</tbody>
</table>

**Additional information**

The following lookup is also used:

- **Search**: Endpoint - Malware Operations Tracker - Lookup Gen, which populates the lookup `malware_operations_tracker` and creates a CSV file, `malware_operations_tracker.csv`.

**Endpoint Product Versions**

This report provides a summary and detail view of all PCI assets and the most current product versions installed. Use this report to identify any assets that are not using the current antimalware product versions and take appropriate measures to ensure these systems are updated.

PCI DSS requires that assets within the cardholder data environment have antimalware technology installed and working to protect against viruses, worms, trojans, and other malware-based threats. The best antimalware software has limited effectiveness if it does not have the current antivirus product versions.

Review this report at least once per day, or more frequently if you are collecting data from antimalware solutions more frequently.
Relevant data sources

Relevant data sources for this report include endpoint engine version information, such as antivirus, endpoint protection, and others.

How to configure this report

1. Index endpoint product version data from an antivirus software. Not all antivirus solutions provide this information in the log data.
2. Map the data to the following Common Information Model fields: \texttt{dest}, \texttt{product_version}, \texttt{vendor_product}. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the activity data with "malware", "operations", and "attack".

Report description

The data in the Endpoint Product Versions report is populated by \texttt{malware_operations_tracker} lookup. This lookup is created by the Endpoint - Malware Operations Tracker - Lookup Gen saved search.

Review each lookup generating search to learn more about the search schedule and time range.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that data is present.</td>
<td>tag=malware tag=operations</td>
<td>Returns endpoint application version activity data.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available as expected.</td>
<td>tag=malware tag=operations</td>
<td>Returns a table of the endpoint application version fields.</td>
</tr>
<tr>
<td>Verify that the endpoint operations tracker file has been populated as expected.</td>
<td></td>
<td>Returns data in the malware_operations_tracker.</td>
</tr>
</tbody>
</table>
Malware Activity

This report looks at malware activity data on cardholder systems produced by antimalware solutions or any other device that produces malware activity data. It looks at data from IDS, IPS, and DLP systems, to provide visibility into potentially unauthorized transmissions of credit card data over the network or to unauthorized removable storage devices.

Use this report to identify the source of the transmission so it can be further investigated and fixed. The cardholder data environment should be monitored for unauthorized transmission of credit card data using IDS, IPS, and DLP based technologies. PCI requires that cardholder data be protected from unauthorized access or distribution.

Relevant data sources

Relevant data sources include alerts from IDS, IPS, or DLP solutions and alerts from the Luhn-based algorithm detection method implemented in the Splunk Enterprise Security framework and used by the Splunk App for PCI Compliance.

How to configure this report

Make sure the activity data you are monitoring conforms to the malware sections of the Common Information Model.

1. Index malware activity data from antivirus software in Splunk platform.
2. Map the data to the following Common Information Model fields:
   action, category, signature, dest, dest_nt_domain, user,
   file_name, file_path, file_hash. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the activity data with "malware" and "attack".

Report description

The data in the Malware Activity report is populated by the Malware data model.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Verify that data is present.

<table>
<thead>
<tr>
<th>tag=malware</th>
<th>tag=attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns malware activity data.</td>
<td></td>
</tr>
</tbody>
</table>

Verify that fields are normalized and available as expected.

<table>
<thead>
<tr>
<th><code>malware</code></th>
<th>table _time,host,action,category,signature,dest, dest_nt_domain,user,vendor_product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns a table of events and the specific malware activity fields for malware activity data.</td>
<td></td>
</tr>
</tbody>
</table>

**Malware Signature Updates**

This report uses the information from the antimalware solution to display a list of the systems within the PCI environment that are updating their signatures appropriately. Use this report to identify systems that have not updated their malware signatures as required.

The best antimalware software has limited effectiveness if it does not have current signatures or if it is not active in the network or on an individual's computer. The PCI standard requires that the antimalware tools are current, which includes the signatures used to detect localized threats.

**Relevant data sources**

Relevant data sources for this report include endpoint signature version information such as antivirus, endpoint protection, and others. This report looks at malware signature updates data produced by firewalls, routers, switches, and any other device configured to produce malware data.

**How to configure this report**

1. Index endpoint product version data from an antivirus software.
2. Not all antivirus (AV) solutions provide this information in the log data.
3. Map the data to the following Common Information Model fields. signature_version, dest, vendor_product. CIM-compliant add-ons for these data sources perform this step for you.
4. Tag the malware signature data with "malware", and "operations".
Report description

The data in the **Malware Signature Updates** report is populated by a lookup against the `malware_operations_tracker` CSV file. This tracker is populated by the **Malware Operations Tracker - Lookup Gen** saved search. Review each lookup generating search to learn more about the search schedule and time range.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that data is present.</td>
<td><code>tag=malware tag=operations</code></td>
<td>Returns malware signature update activity data.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available as expected.</td>
<td>`tag=malware tag=operations</td>
<td>table signature_version,dest,vendor`</td>
</tr>
<tr>
<td>Verify that the endpoint operations tracker file has been populated as expected.</td>
<td><code>inputlookup append=T \malware_operations_tracker</code></td>
<td>Returns a table of the data in the endpoint product signature tracker file.</td>
</tr>
</tbody>
</table>

Update Service Status

This report collects data on the patch service on cardholder systems and uses the information from the antimalware solution to display a list of the systems within the PCI environment that are updating their signatures appropriately. Use this report to identify systems that have not updated their malware signatures as required.

The best antimalware software has limited effectiveness if it does not have current signatures or if it is not active in the network or on an individual's computer. The PCI DSS standard requires that the antimalware tools are current, which includes the signatures used to detect localized threats.
Relevant data sources

Relevant data sources for this report include patch service data such as the Splunk Add-on for Unix and Linux or the Splunk Add-on for Microsoft Windows.

How to configure this report

1. Index service data from the systems monitored in Splunk platform.
2. Map the service data to use the following Common Information Model fields. dest, StartMode. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the update service data by applying a tag of automatic and update.
4. Set the should_update column of the assets table to true for any asset that should be evaluated for patch service status.
5. Configure the Interesting Services list to include the name of the service that should be evaluated and set the is_required field to true. Use the dest and dest_pci_domain fields to determine what systems should be evaluated.

Report description

The data in the Update Service Status report is populated by a lookup against the services_tracker CSV. This tracker is populated by the Endpoint - Services Tracker - Lookup Gen saved search.

Review each lookup generating search to learn more about the search schedule and time range.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that patch service data is available.</td>
<td>sourcetype=&quot;*:Service&quot;</td>
<td>stats count by dest</td>
</tr>
<tr>
<td>Verify that fields are normalized and</td>
<td>sourcetype=&quot;*:Service&quot;</td>
<td>table, dest</td>
</tr>
</tbody>
</table>
System Update Status

This report collects information on the patch status of cardholder systems and provides visibility into the current patch state for systems within the PCI cardholder data environment. Use this report to identify systems that are not patched according to policy.

Many attacks use widely published exploits that can be avoided if systems are patched appropriately. PCI DSS requires that systems and applications are protected by installing the latest vendor-supplied patches. Splunk software uses the data from your patch management solution to generate this report.

**Relevant data sources**

Relevant data sources for this report include patch activity data from the native operating system or a patch management tool such as Windows Update.

**How to configure this report**

1. Index patch activity data from the systems to be monitored.
2. Map the patch data to use the following Common Information Model fields: `signature_id`, `signature`, `status`. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the patch activity data with "update", and "status".
4. Set the `should_update` column of the assets table to true for any asset that should be evaluated for patch activity.

**Report description**

The data in the **System Update Status** report is populated by the Updates data model.
Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that patch activity data is available in Splunk Enterprise.</td>
<td>tag=update tag=status</td>
<td>Returns system patch status data.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available as expected.</td>
<td>tag=update tag=status</td>
<td>table signature_id, signature, status or <code>system_update</code></td>
</tr>
<tr>
<td>Verify that the system update tracker is populated as expected.</td>
<td><code>system_update_tracker</code></td>
<td>Returns data in the system_update_tracker.</td>
</tr>
</tbody>
</table>

Anomalous System Uptime

This report provides a list of servers that have not had been rebooted in 30 days or more. Use this report to identify systems that might be vulnerable to attack.

Systems often need to be rebooted after patches are applied. Systems that have not been rebooted might still be vulnerable to compromise. PCI DSS requires that high and/or critical patches be applied within 30 days.

Relevant data sources

Relevant data sources for this report include uptime data extracted through scripts from Windows, Unix, or other hosts.

How to configure this report

1. Index uptime information captured through scripts from relevant hosts.
2. Map the uptime data to the following Common Information Model fields: dest, uptime. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the uptime data with "uptime", "performance", and "os".
4. Set the should_timesync column to true for assets in the asset table that should synchronize their clocks.
Report description

The Anomalous System Update report is populated by the Performance data model and the asset table.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that uptime data is available in Splunk platform.</td>
<td>tag=uptime tag=os tag=performance</td>
<td>Returns uptime data.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available as expected.</td>
<td>tag=uptime tag=os tag=performance</td>
<td>Returns uptime data fields.</td>
</tr>
</tbody>
</table>

PCI Command History

This report provides visibility into the commands that are run on PCI assets. Monitor this report on a daily basis to ensure that no excessively privileged commands are being run. You should investigate unexpected commands further.

When configuring privileged IDs on systems, make sure you assign individuals only the least privileges needed for the task at hand. Assigning least privileges helps prevent users without sufficient training from incorrectly or accidentally changing operational configuration or altering security settings. Least privilege can also help to minimize the amount of damage from unauthorized access to a privileged ID.

Relevant data sources

Bash history collected by the Splunk Add-on for Unix and Linux.

How to configure this report

1. Index bash history data in Splunk platform.
2. Populate the fields: bash_command, bash_user, and bash_user_root.

Report description
The data in the PCI Command History report is populated by a search against the bash_history sourcetype, `sourcetype=bash_history`.

**Useful searches for troubleshooting**

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that data is present.</td>
<td><code>sourcetype=bash_history</code></td>
<td>Data is present.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available.</td>
<td><code>table bash_user</code> <code>bash_user_root</code> <code>bash_command</code></td>
<td>Fields are available and match the data model.</td>
</tr>
</tbody>
</table>

**Additional information**

This report uses default source types that ship with the Splunk Add-on for Unix and Linux.

**PCI Resource Access**

This report collects data on access attempts to PCI resources in the cardholder data environment and provides the compliance manager with visibility into all authentication attempts. Use this report to identify access attempts by users to ensure that access to cardholder data is legitimate.

You should limit access to resources in the PCI cardholder data environment to only those whose jobs require such access. This limits the risk that an account with access to cardholder data is compromised. PCI DSS requires that all authentication attempts to systems, applications, and devices in the cardholder data environment be monitored for appropriate and legitimate access.

**Relevant data sources**

Relevant data sources for this report include authentication data from any system, application, or device in the cardholder data environment.

**How to configure this report**

1. Index all authentication attempts to applications, systems, or devices into Splunk platform.
2. Map the data to the following **Common Information Model** fields: `host, action, app, src, src_user, dest, user`. CIM-compliant add-ons for
these data sources perform this step for you.
3. Tag the authentication data with "authentication".
4. Add the pci category to all PCI assets in the asset table.

**Report description**

The data in the **PCI Resource Access** report is populated by the Authentication data model.

**Useful searches for troubleshooting**

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have data from your system, application, or device.</td>
<td>sourcetype=&lt;expected_st&gt;</td>
<td>Returns data from your network device, or devices.</td>
</tr>
<tr>
<td>Verify that the authentication data is tagged correctly.</td>
<td>tag=authentication or <code>authentication</code></td>
<td>Returns authentication data.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available as expected.</td>
<td><code>authentication</code></td>
<td>table _time, host, action, app, src, src_user, dest, user</td>
</tr>
</tbody>
</table>

**Additional information**

- The report displays all attempts from users in either the src_user or user fields.
- The identity table includes service accounts that appear as users, such as root, and network service.
- Remove the accounts entirely from the identity table in **Configure > Content Management** and opening the Identities lookup.

**Endpoint Changes**

This report collects information on system changes discovered on cardholder systems. It shows a list of all changes identified using Splunk FSChange, Splunk platform file integrity tools, and other change data captured within Splunk platform. Use this report to identify anomalous or unexpected changes to system objects, critical system files, configuration files, or content files that are being monitored.
PCI DSS requires that you monitor systems for changes to system level objects, critical system files, configuration files, or content files on systems within the cardholder data environment. Compare these files and objects periodically to ensure that the integrity of these files is preserved.

**Relevant data sources**

Relevant data sources for this report include change data, inclusive to file integrity changes such as fschange, OSSEC, Tripwire, and others.

**How to configure this report**

1. Index endpoint change data in Splunk platform.
2. Map the data to the following **Common Information Model** fields:
   
   action, dest, object, object_category, object_path, status, user.
   
   CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the endpoint change data with "endpoint", and "change".

**Report description**

The data in the **Endpoint Changes** report is populated by the Change Analysis data model.

**Useful searches for troubleshooting**

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have data from your network device(s).</td>
<td>sourcetype=&lt;expected_st&gt;</td>
<td>Returns data from your network device(s).</td>
</tr>
<tr>
<td>Verify that endpoint change data is being indexed in Splunk platform.</td>
<td>tag=endpoint tag=change</td>
<td>Returns endpoint change data.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available as expected.</td>
<td>tag=endpoint tag=change</td>
<td>Returns a table of endpoint change data.</td>
</tr>
<tr>
<td></td>
<td>fillnull value=unknown action, dest, object, object_category, object_path, status, user or <code>endpoint_change</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>action,dest,object,object_category,object_path,status,user</td>
<td></td>
</tr>
</tbody>
</table>
System Time Synchronization

This report looks at system time synchronization data and provides a list of all assets that are not synchronizing as expected to a centralized time server. Use this report to identify these systems so you can further investigate and fix them.

Time synchronization technology such as Network Time Protocol (NTP) is used to keep system clocks synchronized across a network. This allows for log correlation between systems and establishes a clear sequence of events when necessary. PCI DSS requires that systems in the cardholder data environment be synchronized.

Relevant data sources

Relevant data sources for this report include NTP failure and success data.

How to configure this report

1. Index NTP synchronization data or other data that can be used to indicate a successful time synchronization attempt in Splunk platform. No specific fields of information are needed to determine synchronization.
2. Tag the successful synchronization data with "time", "synchronize", "os", and "performance".
3. Configure the should_timesync column of the assets that should synchronize in the asset table.

Report description

The data in the System Time Synchronization report is populated by the Performance data model and the asset table.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search Command</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that time synchronization data is in Splunk platform.</td>
<td>tag=time tag=synchronize tag=os tag=performance</td>
<td>Returns time synchronization data.</td>
</tr>
<tr>
<td>Troubleshooting Task</td>
<td>Search Command</td>
<td>Expected Result</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>or <code>time_sync</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify successful time sync data.</td>
<td><code>time_sync(success)</code></td>
<td>Returns successful time sync data.</td>
</tr>
<tr>
<td>Verify successful time sync data fields.</td>
<td><code>time_sync(success)</code></td>
<td>Returns successful time sync data fields.</td>
</tr>
</tbody>
</table>

**Additional information**

Windows NTP produces messages 35 and 37 that indicate a synchronization attempt. Windows does not synchronize in a predictable, determinate way. This can cause false positives if you configured the report with short time frames.

**Privileged User Activity**

This report shows raw events associated with privileged user activity and provides you with a report of all administrative activity. Use this report to evaluate privileged user accounts and review the activity to identify potential security threats that can lead to potential cardholder data compromise.

Accounts with increased privileges, such as the administrator and root accounts, can have an impact on the security or operational functionality of a system. PCI DSS requires that all actions taken by individuals using administrative credentials be monitored for misuse and abuse.

**Relevant data sources**

Relevant data sources for this report include any data that includes a privileged user account reference.

**How to configure this report**

1. Index privileged activity from all systems, applications, and devices.
2. Add a category of privileged to all privileged user identities in the identity table.
3. Tag specific events as being privileged using "privileged", and "authentication".
Report description

The data in the Privileged User Activity report is populated by the identity table.

Useful searches and Troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have data from your system, application, or device.</td>
<td>sourcetype=&lt;expected_st&gt;</td>
<td>Returns data from your systems, applications, and/or devices.</td>
</tr>
<tr>
<td>Verify that all privileged activity is returned.</td>
<td>tag=privileged</td>
<td>Returns privileged user activity data.</td>
</tr>
<tr>
<td>Verify that all privileged user activity fields are populated.</td>
<td>tag=privileged</td>
<td>table event_id host sourcetype src_user user eventtype</td>
</tr>
</tbody>
</table>

PCI Asset Logging

This report provides a list of all PCI assets that have stopped logging their data to Splunk platform or that have never logged data to Splunk platform. Use this report to ensure that all PCI assets are logging their data to Splunk platform. Use this report to repair any systems that are non-compliant in their logging configurations.

PCI DSS requires that audit logs from systems, applications, and devices in the cardholder data environment be promptly backed up to a central log server. Splunk platform functions as this central log server and monitors the data flow from all PCI assets.

Relevant data sources

Relevant data sources for this report include Splunk platform and audit logs.

How to configure this report

You do not have to configure this report. It uses Splunk platform metadata and the assets table to create results.
Report description

The data in the PCI Asset Logging report is populated by a lookup that runs against the assets.csv file. You create the asset table. See Configure assets in this manual.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have data from your network device(s).</td>
<td>sourcetype=&lt;expected_st&gt;</td>
<td>Returns data from your network device(s).</td>
</tr>
<tr>
<td>Verify that metadata is accessible and data exists for the hosts from which data is collected.</td>
<td><code>host_eventcount</code></td>
<td>Returns host metadata.</td>
</tr>
<tr>
<td>Verify that metadata is successfully joined with the asset table.</td>
<td><code>asset_eventcount</code></td>
<td>Returns PCI asset logging data.</td>
</tr>
<tr>
<td>Verify that PCI asset logging fields are populated.</td>
<td><code>metadata type=hosts index=*</code></td>
<td>Returns table of PCI asset logging fields fields.</td>
</tr>
</tbody>
</table>

Vulnerability Scan Details

Report on vulnerabilities discovered on PCI assets. This report looks at vulnerability scan details data produced by firewalls, routers, switches, and any other device that produces vulnerability data.

Vulnerability scans of the cardholder data environment expose potential vulnerabilities in networks that could be found and exploited by malicious individuals. When these weaknesses are identified, the organization should correct them and repeat the vulnerability scan to verify that they have corrected the vulnerabilities.

This report shows all vulnerabilities identified for selected assets. Use this report to identify specific high and/or critical vulnerabilities on cardholder systems that need to be fixed.
Relevant data sources

Relevant data sources for this report includes any vulnerability data.

How to configure this report

1. Index vulnerability scan results in Splunk platform.
2. Map the vulnerability data to the following **Common Information Model** fields: category, severity, signature, dest, os. If you want, you can map additional fields: cve, bugtraq, cert, msft, mskb, xref, cvss.
3. Tag the successful synchronization data with "vulnerability" and "report".

Report description

The data in the **Vulnerability Scan Details** report is populated by the Vulnerabilities data model.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have data from your network devices.</td>
<td>sourcetype=&lt;expected_st&gt;</td>
<td>Returns data from your network devices.</td>
</tr>
<tr>
<td>Verify that vulnerability data is in Splunk platform.</td>
<td>tag=vulnerability tag=report or <code>vulnerability</code></td>
<td>Returns vulnerability data.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available at search time.</td>
<td><code>vulnerability</code></td>
<td>Returns a table of the vulnerability data fields.</td>
</tr>
</tbody>
</table>

Rogue Wireless Access Point Protection

This report gathers data on unauthorized wireless access points found on the network. It uses the data generated by IDS/IPS systems, network scan results, or Network Access Control (NAC) logs to report on any rogue access device detections. Use this report to see any discovered rogue access devices and
more deeply explore the network, user activity, or system activity to further investigate the access points.

Implementation and/or exploitation of wireless technology within a network is one of the most common paths for malicious users to gain access to the network and cardholder data. If a wireless device or network is installed without a company’s knowledge, it can allow an attacker to easily and invisibly enter the network. PCI compliance requires that organizations test for the presence of wireless access devices on the network at least once every three months. More frequent testing is recommended.

**Relevant data sources**

Relevant data sources for this report include IDS/IPS systems, network scan results, or Network Access Control (NAC) logs.

**How to configure this report**

1. Index wireless access detection data in Splunk platform.
2. Map the wireless access detection data to the following Common Information Model fields: `dvc`, `ids_type`, `category`, `signature`, `severity`, `src`, `dest`.
3. Tag the successful synchronization data with "rogue", "wireless", "ids", and "attack".

**Report description**

The data in the Rogue Wireless Access Point Protection report is populated by the Intrusion Detection data model.

**Useful searches for troubleshooting**

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have rogue wireless access point data.</td>
<td><code>sourcetype=&lt;expected_st&gt;</code></td>
<td>Returns rogue wireless access point data.</td>
</tr>
<tr>
<td>Verify that wireless access tag=rogue tag=wireless tag=ids tag=attack</td>
<td></td>
<td>Returns rogue</td>
</tr>
<tr>
<td>Troubleshooting Task</td>
<td>Search/Action</td>
<td>Expected Result</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>data from an IDS, network scan, or network scan is in Splunk platform.</td>
<td>search tag=rogue tag=wireless tag=pci tag=ids tag=attack</td>
<td>wireless access point protection data.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available at search time.</td>
<td>search tag=rogue tag=wireless tag=pci tag=ids tag=attack</td>
<td>Returns rogue wireless access point protection data fields.</td>
</tr>
<tr>
<td>Verify that the ids attack tracker file is populated.</td>
<td>inputlookup ids_attack_tracker or <code>ids_attack_tracker</code></td>
<td>Returns data in the ids attack tracker.</td>
</tr>
</tbody>
</table>

### IDS/IPS Alert Activity

Intrusion detection and/or prevention systems (IDS/IPS) compare inbound and outbound network traffic against known signatures and/or behaviors of thousands of compromise types (hacker tools, Trojans and other malware). This report collects data on unauthorized wireless access points found on the network and provides a summarized view of the intrusion activity involving an asset in the PCI domain. Use this report to identify attack trends and behavior that could indicate a more significant threat.

Intrusion detection and/or prevention systems can be configured to either alert or stop the intrusion attempt. Without a proactive approach to unauthorized activity detection using these tools, attacks on (or misuse of) PCI resources could go unnoticed in real time. PCI requires that the alerts generated by these tools be monitored so that attempted intrusions can be stopped before they happen.

### Relevant data sources

Relevant data sources for this report include IDS/IPS systems, network scan results, or Network Access Control (NAC) logs.
How to configure this report

1. Index IDS/IPS alert data in Splunk platform.
2. Map the IDS/IPS data to the following **Common Information Model** fields: dvc, ids_type, category, signature, severity, src, dest. CIM-compliant add-ons for these data sources perform this step for you.
3. Tag the successful synchronization data with "ids" and "attack".

Report description

The data in the **IDS/IPS** report is populated by the Intrusion Detection data model.

Useful searches for troubleshooting

<table>
<thead>
<tr>
<th>Troubleshooting Task</th>
<th>Search/Action</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that IDS/IPS data has been indexed in Splunk platform.</td>
<td><code>tag=ids tag=attack</code> or <code>ids_attack</code></td>
<td>Returns IDS/IPS data.</td>
</tr>
<tr>
<td>Verify that fields are normalized and available at search time.</td>
<td><code>ids_attack</code></td>
<td>Returns a table of IDS/IPS data fields.</td>
</tr>
</tbody>
</table>
Configure correlation searches

Configure correlation searches

A correlation search scans multiple data sources for defined patterns. When the search finds a pattern, it performs an adaptive response action such as creating a notable event.

Correlation searches can search many types of data sources, including events from any security domain (access, identity, endpoint, network), asset lists, identity lists, threat intelligence, and other data in Splunk platform. The searches then aggregate the results of an initial search with functions in SPL, and take action in response to events that match the search conditions with an adaptive response action. Configure correlation searches to update the settings associated with how they run.

Enable correlation searches

Enable correlation searches to start running adaptive response actions and receiving notable events. Splunk App for PCI Compliance installs with all correlation searches disabled so that you can choose the searches that are most relevant to your use cases.

1. Select Configure > Content Management.
2. Filter on a type of Correlation Search.
3. Locate the name of the correlation search you want to enable.
4. In the Actions column, click Enable to enable the searches that you want to enable.
5. After you enable correlation searches, click “Back to PCI Compliance” in the menu bar.

For details about the correlation searches shipped with the Splunk App for PCI Compliance, see Search View Matrix in the User Manual.

Change correlation search scheduling

Change the default search type of a correlation search from real-time to scheduled. Splunk App for PCI Compliance uses indexed real-time searches by default.
1. From the **Content Management** page, locate the correlation search you want to change.
2. In the **Actions** column, click **Change to scheduled**.

**Editing correlation searches**

You can make changes to correlation searches to fit your environment. For example, modify the thresholds used in the search, change the response actions that result from a successful correlation, or change how often the search runs. Modifying a correlation search does not affect existing notable events.

- Click the name of a correlation search on the **Content Management** page to edit it.

If you modify the start time and end time for the correlation search, use relative time modifiers. See Specify time modifiers in your search in the Splunk Enterprise Search Manual.

**Edit the correlation search in guided mode**

You can edit some correlation searches in guided mode. Not all correlation searches support guided search editing. If a search appears grayed-out and has the option to **Edit search manually** or **Edit search in guided mode**, the search was built in guided mode and can be edited in guided mode. If a search can be edited in the search box and only has the option to **Edit search in guided mode**, editing the search in guided mode overwrites the existing search.

1. Click **Edit search in guided mode** to open the guided search creation wizard.
2. Review the search elements in the correlation search, making changes if you want.
3. Save the search.

**Throttle the number of response actions generated by a correlation search**

Set up throttling to limit the number of response actions generated by a correlation search. When a correlation search matches an event, it triggers a response action.

By default, every result returned by the correlation search generates a response action. Typically, you may only want one alert of a certain type. You can use
throttling to prevent a correlation search from creating more than one alert. Some response actions allow you to specify a maximum number of results in addition to throttling. See Set up adaptive response actions in Splunk App for PCI Compliance.

1. Select Configure > Content Management.
2. Click the title of the correlation search you want to edit.
3. Type a Window duration. During this window, any additional event that matches any of the Fields to group by will not create a new alert. After the window ends, the next matching event will create a new alert and apply the throttle conditions again.
4. Type the Fields to group by to specify which fields to use when matching similar events. If a field listed here matches a generated alert, the correlation search will not create a new alert. You can define multiple fields, and available fields depend on the search fields that the correlation search returns.
5. Save the correlation search.

Throttling applies to any type of correlation search response action and occurs before notable event suppression.

**Allow non-admins to edit correlation searches**

If you want non-admins to edit correlation searches, add the edit correlation searches capability to a different role in Splunk App for PCI Compliance.

1. Select Configure > General > Permissions.
2. Locate the role that you want to allow to edit correlation searches.
3. Select the check box for Edit Correlation Searches for that role.
4. Click Save.

**Correlation searches migration to savedsearches.conf**

Starting in the Splunk App for PCI Compliance version 3.4.0, correlationsearches.conf is no longer used to define correlation searches. Instead, savedsearches.conf uniquely identifies correlation searches using the action.correlationsearch.enabled=1 parameter. The correlationsearches.conf file is deprecated.

For stability, the Threat - Correlation Searches - Lookup Gen saved search continues to use the contents of both correlationsearches.conf and savedsearches.conf to populate the correlationsearches KV Store collection used by Incident Review.
Changes the Splunk App for PCI Compliance makes at upgrade

When you upgrade to the Splunk App for PCI Compliance version 3.4.0, the Splunk App for PCI Compliance migrates all correlation searches in your environment, including custom correlation searches. The confcheck_es_correlationmigration.py script migrates all entries in correlationsearches.conf into updated entries in savedsearches.conf. The migration can take up to five minutes to complete after the upgrade.

During the upgrade, the Splunk App for PCI Compliance continues to create notable events without interruption.

Changes you have to make after upgrade

After upgrading to the Splunk App for PCI Compliance version 3.4.0, you have to make additional changes.

- Check for searches that did not migrate successfully and migrate the correlationsearches.conf entries manually using the parameter definitions below.

  • Update searches that call the correlationsearches REST endpoint.

    - For example, a search that displays a list of correlation searches in your environment would change from

      | rest splunk_server=local
      /services/alerts/correlationsearches | rename eai:acl.app as app, title as csearch_name | table app security_domain csearch_name description

      to

      | rest splunk_server=local count=0 /services/saved/searches | where match('action.correlationsearch.enabled', "1|[Tt][Tt][Rr][Uu][Ee]") | rename eai:acl.app as app, title as csearch_name, action.correlationsearch.label as csearch_label, action.notable.param.security_domain as security_domain | table csearch_name, csearch_label, app, security_domain, description

Both the correlationsearches.conf and savedsearches.conf files are used to populate the KV Store collection used by Incident Review. Custom search macros that reference that KV Store collection continue to work as before, but consider updating them anyway.
**correlationsearches.conf parameter translation to savedsearches.conf**

All `correlationsearches.conf` parameters now exist in `savedsearches.conf` and the `correlationsearches.conf` file has been deprecated. Do not update it directly except to manually migrate correlation search definitions.

**Identification parameters for correlation searches**

New parameters identify whether a saved search is a correlation search and the name of the correlation search.

<table>
<thead>
<tr>
<th><code>correlationsearches.conf</code> parameter in pre-3.4.0 versions</th>
<th><code>savedsearches.conf</code> parameter starting in 3.4.0</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td><code>action.correlationsearch=0</code></td>
<td>This is an internal parameter and can be ignored.</td>
</tr>
<tr>
<td>A stanza for the search exists</td>
<td><code>action.correlationsearch.enabled=1</code></td>
<td>This parameter identifies a saved search as a correlation search.</td>
</tr>
<tr>
<td><code>rule_name</code></td>
<td><code>action.correlationsearch.label</code></td>
<td>This parameter provides the name of the correlation search.</td>
</tr>
<tr>
<td><code>description</code></td>
<td><code>description</code></td>
<td>This parameter provides the description of the correlation search.</td>
</tr>
</tbody>
</table>
Notable event parameters for correlation searches

The `action.notable` parameter identifies a notable event associated with a correlation search. The parameters that describe additional details associated with the notable event now exist in the `savedsearches.conf` file.

<table>
<thead>
<tr>
<th>correlationsearches.conf parameter in pre-3.4.0 versions</th>
<th>savedsearches.conf parameter starting in 3.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>security_domain</td>
<td><code>action.notable.param.security_domain</code></td>
</tr>
<tr>
<td>severity</td>
<td><code>action.notable.param.severity</code></td>
</tr>
<tr>
<td>rule_title</td>
<td><code>action.notable.param.rule_title</code></td>
</tr>
<tr>
<td>rule_description</td>
<td><code>action.notable.param.rule_description</code></td>
</tr>
<tr>
<td>nes_fields</td>
<td><code>action.notable.param.nes_fields</code></td>
</tr>
<tr>
<td>drilldown_name</td>
<td><code>action.notable.param.drilldown_name</code></td>
</tr>
<tr>
<td>drilldown_search</td>
<td><code>action.notable.param.drilldown_search</code></td>
</tr>
<tr>
<td>default_status</td>
<td><code>action.notable.param.default_status</code></td>
</tr>
<tr>
<td>default_owner</td>
<td><code>action.notable.param.default_owner</code></td>
</tr>
</tbody>
</table>

Related search parameters for correlation searches

Searches related to a correlation search, such as the context-generating searches associated with a correlation search that uses extreme search, are now part of a JSON blob `action.correlationsearch.related_searches` parameter.

<table>
<thead>
<tr>
<th>correlationsearches.conf parameter in pre-3.4.0 versions</th>
<th>savedsearches.conf parameter starting in 3.4.0</th>
</tr>
</thead>
</table>
| related_search_name = Endpoint - Emails By Source - Context Gen | `action.correlationsearch.related_searches = [\n"Endpoint - Emails By Source - Context Gen",
"Endpoint - Emails By Destination Count - Context Gen"
]` |
**Example correlation search stanzas from this version and previous versions**

The savedsearches.conf stanza for a correlation search looks as follows starting in 3.4.0.

```
[Access - Concurrent App Accesses - Rule]
action.correlationsearch = 0
action.correlationsearch.enabled = 1
action.correlationsearch.label = Concurrent Login Attempts Detected
action.email.sendresults = 0
action.notable = 0
action.notable.param.security_domain = access
action.notable.param.severity = medium
action.notable.param.rule_title = Concurrent Access Event Detected For $user$
action.notable.param.rule_description = Concurrent access attempts to $app1$ by $user$ from two different sources ( $src1$, $src2$ ) have been detected.
action.notable.param.nes_fields = user
action.notable.param.drilldown_name = View access attempts by $user$
action.notable.param.drilldown_search = | datamodel Authentication
Authentication search | search Authentication.user="$user$"
action.risk = 1
action.risk.param._risk_object = user
action.risk.param._risk_object_type = user
action.risk.param._risk_score = 20
alert.suppress = 1
alert.suppress.fields = user
alert.suppress.period = 86300s
alert.track = false
cron_schedule = 10 * * * *
description = Alerts on concurrent access attempts to an app from different hosts. These are good indicators of shared passwords and potential misuse.
disabled = True
dispatch.earliest_time = -70m
dispatch.latest_time = -5m
enableSched = 1
is_visible = false
request.ui_dispatch_app = SplunkEnterpriseSecuritySuite
search = | tstats `summariesonly` count from datamodel=Authentication.Authentication by _time,Authentication.app,Authentication.src,Authentication.user span=1s | `drop_dm_object_name("Authentication")` | eventstats dc(src) as src_count by app,user | search src_count>1 | sort 0 + _time | streamstats current=t window=2 earliest(_time) as previous_time,earliest(src) as previous_src by app,user | where (src!=previous_src) | eval time_diff=abs(_time-previous_time) | where
```
In previous versions of the Splunk App for PCI Compliance, the savedsearches.conf and correlationsearches.conf definitions for the same correlation search looks as follows. savedsearches.conf

```bash
[Access - Concurrent App Accesses - Rule]
action.email.sendresults = 0
action.risk = 1
action.risk.param._risk_object = user
action.risk.param._risk_object_type = user
action.risk.param._risk_score = 20
alert.suppress = 1
alert.suppress.fields = user
alert.suppress.period = 86300s
alert.track = false
cron_schedule = 10 * * * *
disabled = True
dispatch.earliest_time = -70m@m
dispatch.latest_time = -5m@m
enableSched = 1
is_visible = false
request.ui_dispatch_app = SplunkEnterpriseSecuritySuite
search = | tstats `summariesonly` count from datamodel=Authentication.Authentication by _time,Authentication.app,Authentication.src,Authentication.user span=1s | `drop_dm_object_name("Authentication")` | eventstats dc(src) as src_count by app,user | search src_count>1 | sort 0 + _time | streamstats current=t window=2 earliest(_time) as previous_time,earliest(src) as previous_src by app,user | (src!=previous_src) | eval time_diff=abs(_time-previous_time) | where time_diff<300
```
correlationsearches.conf

```bash
[Access - Concurrent App Accesses - Rule]
security_domain = access
severity = medium
rule_name = Concurrent Login Attempts Detected
description = Alerts on concurrent access attempts to an app from different hosts. These are good indicators of shared passwords and potential misuse.
rule_title = Concurrent Access Event Detected For $user$
rule_description = Concurrent access attempts to $app1$ by $user$ from two different sources( $src1$, $src2$ ) have been detected.
nes_fields = user
drilldown_name = View access attempts by $user$
drilldown_search = | datamodel Authentication Authentication search | search Authentication.user="$user$"
default_owner =
default_status =
```
Create new correlation searches

You can create your own correlation searches to create notable events that you want to have stored in the notable index and to appear on the Incident Review dashboard.

Create a custom correlation search using the Content Management page. For this example, create a correlation search for Splunk_DA-ESS_PCICompliance.

1. Select Configure > Content Management.
2. Select Create new content > Correlation Search.
3. Type a search name. Include a domain in the search name if you want.
4. Set the Application Context as PCI Compliance.
5. Create a search with the guided search wizard.
6. Fill out the rest of the fields on the page.
7. Click Save.

For assistance creating correlation searches, see Create a correlation search in Splunk Enterprise Security Tutorials.

Configure thresholds for correlation searches

Correlation searches use thresholds to set the number of security events of a specified type that must occur to trigger a notable event. You can configure the thresholds for these searches based on the typical number of events in your environment.

For example, the Malware Outbreak Detected correlation search triggers when the number of new infections within the last 24 hours exceeds the threshold, alerting you when an organization-wide issue is developing. However, this correlation search may need to be adjusted to reflect the size and load of your environment. A large enterprise might consider ten new infections within a 24-hour period an outbreak, whereas a small company might consider only 3 new infections an outbreak. The threshold sets the number of infections that correlation search considers noteworthy.

Threshold settings are best configured after developing a baseline of security events. Index two weeks of data before finalizing the baseline settings. Thresholds need to be adjusted over time as the network changes.
Add governance to a correlation search

Map new or existing correlation searches to the relevant PCI DSS controls by adding governance to the search.

This step requires file system access on the server. Splunk Cloud customers must work with Splunk Support to map a new correlation search to the relevant PCI DSS controls.

Perform these steps in the same directory as the savedsearches.conf file where the search exists. For example,
/Applications/splunk/etc/apps/Splunk_DA-ESS_PCICompliance/local

1. Create a governance.conf file.
   /Applications/splunk/etc/apps/Splunk_DA-ESS_PCICompliance/local/governance.conf

2. Copy the stanza for the custom correlation search from the savedsearches.conf file and paste it into the governance.conf file.
   [PCI - 1.3.3 - Unauthorized or Insecure Communication Permitted ? Rule]
   compliance.0.governance = pci
   compliance.0.control = 1.3.3

3. Add a compliance control mapping by adding a governance and control line under the correlation search stanza. For example, this correlation search applies for all systems in your environment.
   [PCI - 1.3.3 - Unauthorized or Insecure Communication Permitted ? Rule]
   compliance.0.governance = pci
   compliance.0.control = 1.3.3

4. (Optional) Add a tag value to specify a tag that must be present in the notable event in order for the governance and control mapping to be applied. For example, the results of this correlation search matter for PCI compliance only if the deleted account is related to PCI.
   [Access - Account Deleted - Rule]
   compliance.0.governance = pci
   compliance.0.control = 8.5
   compliance.0.tag = pci

5. (Optional) Add additional compliance control mappings, incrementing the number to indicate an additional mapping. For example, this results of this search are relevant for both the 1.3.3 control and the 1.3.2 control.
   [PCI - 1.3.3 - Unauthorized or Insecure Communication Permitted ? Rule]
   compliance.0.governance = pci
   compliance.0.control = 1.3.3
   compliance.1.governance = pci
   compliance.1.control = 1.3.2

6. Save the file. The results take effect the next time the correlation search matches and creates a notable event.
Notable events must contain a tag value for governance to be applied based on the tag field. Notable events can contain a tag value if:

- The correlation search results contain a tag field. For example, `values(Authentication.tag) as tag` is contained in the correlation search syntax.
- The correlation search results contain a field that is correlated with the asset and identity lookups, and the lookup contains a category value for the asset or identity.

### Notable events

When a [correlation search](#) included in the Splunk App for PCI Compliance (or added by a user) identifies an event or pattern of events, it creates a notable event. Correlation searches filter the IT security data and correlate across events to identify a particular type of incident (or pattern of events) and then create notable events. The app includes pre-configured correlation searches to create notable events, and lets you add your own.

Correlation searches run at regular intervals (for example, every hour) or continuously in real-time and search events for a particular pattern or type of activity. The notable event is stored in a dedicated notable index, which is implemented as a summary index in Splunk Enterprise. The [Incident Review](#) dashboard is used to view and act on notable events. A notable event might be a single event of high importance, such as any activity from a known web attacker, or an aggregate of multiple events that together warrant review, such as a high number of authentication failures on a single host followed by a successful authentication.

When notable events are created, relevant information from the asset list is combined with the event information. To help to further identify important patterns, correlation searches are each assigned a "severity" of informational, low, medium, high, or critical. Notable events are assigned an "urgency", based on the severity of the event and the priority of the asset corresponding to the event.
- If event severity is informational, the event urgency is informational, regardless of asset priority.
- If asset priority is unknown or low and event severity is unknown, low, or medium, the event urgency is low.
- If asset priority is unknown or low and event severity is high, the event urgency is medium.
- If asset priority is unknown or low and event severity is critical, the event urgency is high.
- If asset priority is medium and event severity is unknown or low, the event urgency is low.
- If asset priority is medium and event severity is medium, the event urgency is medium.
- If asset priority is medium and event severity is high, the event urgency is high.
- If asset priority is medium and event severity is critical, the event urgency is critical.
- If asset priority is high and event severity is unknown, low, or medium, the event urgency is medium.
- If asset priority is high and event severity is high, the event urgency is high.
- If asset priority is critical and event severity is unknown or low, the event urgency is medium.
- If asset priority is critical and event severity is medium, the event urgency is high.
- If asset priority is critical and event severity is high or critical, the event urgency is critical.

Correlation searches do not use the calculated severity described if the events being searched contain a severity field.

**How to suppress notable events**

In some cases, you might want to prevent certain types of notable events from appearing on the **Incident Review** dashboard or contributing to alert thresholds. To do this, you need to create a notable event suppression. See **Suppressing notable events** in this manual.
Manually create a notable event

You can manually create a notable event from an indexed event, or create one from scratch.

Note: By default, only administrators can manually create notable events. To grant other users this capability, see Configure user and roles in the Installation and Upgrade Manual.

Create a notable event from an existing event

You can create a notable event from any indexed event using the Event Actions menu. Do not create a notable event from notable events on the Incident Review dashboard.

1. From an event, view the event details and click Event Actions.
2. Select Create notable event.
3. Enter a Title for the event.
4. (Optional) Select a security Domain.
5. (Optional) Select an Urgency level.
6. (Optional) Select an Owner.
7. (Optional) Select a Status.
8. Enter a Description for the event that describes why you created the notable event or what needs to be investigated.
9. Save the new notable event. The Incident Review dashboard displays with your new notable event.

Note: A notable event created in this way includes tracking fields such as Owner and Status, but does not include the unique fields or links created when a notable event is generated by a correlation search alert action.

Create a notable event from scratch

Create a notable event based on observations, a finding from a security system outside Splunk software, or something else.

1. Select Configure > Incident Management > New Notable Event.
2. Enter a Title for the event.
3. (Optional) Select a security Domain.
4. (Optional) Select an Urgency level.
5. (Optional) Select an Owner.
6. (Optional) Select a Status.
7. Enter a **Description** for the event that describes why you created the notable event or what needs to be investigated.

8. Save the new notable event. The **Incident Review** dashboard displays with your new notable event.

**Configure Incident Workflow**

Notable event statuses are used to manage the workflow of notable events in the Splunk App for PCI Compliance. Most users do not need to change these settings from the default. The workflow status of a notable event enables you to manage PCI compliance workflow and events.

The default incident workflow is for a new event to be changed from **Unassigned** to **Assigned** and the status changed from **New** to **In Progress**. From there, the PCI compliance analyst can troubleshoot the issue. If there is some action that needs to be taken, the status might be changed to **Pending**, or it might go straight to **Resolved**. To move from **Resolved** to **Closed** the event must then be verified by another party (admin).

**Change notable event settings**

Navigate to **Configure > Incident Management** in Splunk App for PCI Compliance to make various configuration changes to notable events.

- Review the default notable event statuses and add, remove or change a status as desired. See Managing and monitoring notable event statuses in this topic.
- Review existing or create new **Notable event suppressions**.
- Customize Incident Review to allow an urgency override or enforce comment usage.

**Managing and monitoring notable event statuses**

An analyst assigns a status to a notable event to communicate the state of the notable event in the investigation workflow. The status aligns with the stages of an investigation, and can be used to review and report on the progress of a notable event investigation on the Incident Review Audit dashboard.

To see the available statuses for notable events, select **Configure > Incident Management > Status Configuration** and select the **Notable** tab.
<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Can be edited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unassigned</td>
<td>A notable event has not been assigned.</td>
<td>No</td>
</tr>
<tr>
<td>New (default)</td>
<td>A notable event has not been reviewed.</td>
<td>No</td>
</tr>
<tr>
<td>In Progress</td>
<td>An investigation or response to the notable event is in progress.</td>
<td>Yes</td>
</tr>
<tr>
<td>Pending</td>
<td>A notable event closure is pending some action.</td>
<td>Yes</td>
</tr>
<tr>
<td>Resolved</td>
<td>A notable event has been resolved and awaits verification.</td>
<td>Yes</td>
</tr>
<tr>
<td>Closed</td>
<td>A notable event has been resolved and verified.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Every notable event is assigned a status of **New** by default when it is created by a correlation search. You can customize notable event statuses to match an existing workflow at your organization.

**Edit notable event statuses**

Change the available statuses for notable events.

1. On the Splunk App for PCI Compliance toolbar, select **Configure > Incident Management > Status Configuration**.
2. Select a notable event status on the **Notable** tab.
3. Change the **Label** or **Description** as desired.

You cannot edit the "'Unassigned'" and "'New'" statuses because they are defaults used when creating notable events.

**Manage notable event status history**

Notable events are associated with users, statuses, and comments. Changes made to status names affect only the name of a status, not the status ID assigned to the notable event in the notable index.

If you change the name of a default notable event status, the name will change for both past and future notable events. For example, if you rename pending to waiting for customer, all notable events with a status of pending will then have a status of waiting for customer. The status ID assigned to the notable events will remain the same.
**Notable event status transitions**

The status names represent the steps required in investigating a notable event. Status transitions define the path of a notable event investigation.

An analyst assigned a notable event will change the status of the notable event as the investigation progresses. To change the current status on a notable event:

- The analyst must be a member of a role that has permission to change a status. Notable event status transitions are available to the `ess_analyst` and `ess_admin` roles by default.
- The follow-on status must allow a transition from the current status. Every status can transition to any other status by default. For example, a notable event in a `New` status can transition directly to any other status including `Closed`.

**Restricting status transitions**

You can define a transition workflow and limit which status can transition to another status, creating a predefined path for the notable event investigation workflow. By default, no transition path is defined or required and every status can transition to every other status.

**Prerequisites**

- In order to edit status transitions, you must have the `pci_analyst` role or your role must be assigned the `Edit Statuses` permission. For more information about user roles and capabilities, see Configure user and roles in the *Installation and Upgrade Manual*.
- Define the status workflow for notable event investigations. Determine which statuses to require, and whether analysts should follow a specific sequence of statuses before completing the investigation workflow. Determine whether any roles can bypass the full workflow.

**Restrict notable event status transitions**

1. On the Splunk App for PCI Compliance toolbar, select **Configure > Incident Management > Status Configuration**.
2. Select a notable event status on the Notable tab.
3. In Status Transitions, modify the **To Status** fields.
   1. To define which roles are allowed to transition a notable event to the selected status, choose the **Authorization** field and add or remove roles.
2. To remove a transition an event to the selected status, choose **Unselect All**.
4. Save the changes.
5. Test the changes to the status workflow. If any transitions required adding or removing roles, test with credentials assigned to each role.

**Add a new status**

Add a new status to the notable event investigation workflow. If you restrict status transitions, determine where this status fits in the workflow.

1. Define the status workflow for notable events.
   1. Determine where the new status is needed in the workflow.
   2. Determine whether any roles will be allowed to bypass the new status in the workflow.
2. On the Splunk App for PCI Compliance toolbar, open **Configure > Incident Management > Status Configuration**.
3. On the **Notable** tab, select **New**.
4. Add a label. This is the **Status** field value used on the Incident Review dashboard and for notable event status reporting. For example, Waiting on ITOps.
5. Add a description. The description is only referenced in the Notable Event Status page. For example, Waiting on another department.
6. (Optional) Select **Default status**. Choose only if you are replacing the **New** status for notable events.
7. (Optional) Select **End status**. Choose when adding an additional **Closed** status for notable events.
8. Define the Status Transitions by modifying the **To Status** fields.
   1. Review the status workflow and determine which statuses a notable event can transition to.
   2. Select the **Authorization** field and add the roles allowed to transition a notable event to the selected status.
9. Save the changes.
   For example, the "Waiting on ITOps" status occurs after "New" and "In Progress", but before "Pending." It is not a required status and can be skipped over to choose "Pending." Edit the Status Transitions in "Waiting on ITOps" for "Pending," "Resolved," and "Closed" and add the roles **pci_admin** and **pci_analyst** added under Authorization.
10. Edit the statuses that will precede the new status in the workflow, and add the roles allowed to perform the transition.
   For example, a notable event can be given a status of "Waiting on ITOps" from a status of "New" and "In Progress." Edit the Status Transitions in both "New" and "In Progress" adding the **pci_admin** and **pci_analyst**
Create and manage notable event suppressions

You can hide notable events from the Incident Review dashboard by creating a notable event suppression.

A suppression is a search filter that hides additional notable events from view, and is used to stop excessive or unwanted numbers of notable events from appearing on the Incident Review dashboard. Notable events that meet the search conditions are still created and added to the notable index. Suppressed notable events continue to contribute to notable event counts on the Security Posture and auditing dashboards.

To prevent notable events that meet certain conditions from being created, see Throttle the number of response actions generated by a correlation search.

You can create a suppression filter in two ways.

- Create a suppression from Incident Review. See Suppress a notable event.
- Create a suppression from the Configure menu. See Create a suppression from Notable Event Suppressions.

Create a suppression from Notable Event Suppressions

1. Select Configure > Incident Management > Notable Event Suppressions.
2. Click Create New Suppression.
3. Enter a Name and Description for the suppression filter.
4. Enter a Search to use to find notable events to be suppressed.
5. Set the Expiration Time. This defines a time limit for the suppression filter. If the time limit is met, the suppression filter is disabled.
**Edit notable event suppressions**

1. Select **Configure > Incident Management > Notable Event Suppressions**.
2. Select a notable event suppression to open the **Edit Notable Event Suppression** page.
3. Edit the **Description** and **Search** fields used for the suppression filter.

**Disable notable event suppressions**

1. Select **Configure > Incident Management > Notable Event Suppressions**.
2. Select **Disable** in the **Status** column for the notable event suppression.

**Remove a notable event suppression**

1. From the Splunk platform toolbar, select **Settings > Event types**.
2. Search for the the suppression event: `notable_suppression-<suppression_name>`. 
3. Select **delete** in the **Actions** column for the notable event suppression.

**Audit notable event activity**

You can audit analyst incident review activity on the Incident Review Audit dashboard. Audit notable event suppressions with the Suppression Audit dashboard.

**How urgency is assigned to notable events**

Notable events are assigned an urgency level that is a combination of the severity of the correlation search and the priority assignment of the relevant asset or identity. You can use the **Urgency** field to prioritize the investigation of notable events.

![Urgency Table](image)

You can change the urgency calculation defaults in Splunk App for PCI Compliance.
1. Select **Configure > Content Management**.
2. Choose the **Urgency Levels** lookup. An editable, color coded table representing the urgency lookup file displays.
3. In any row where the **priority** or **severity** is listed as "unknown," review the assigned **Urgency**.
4. (Optional) Edit the table and change the **Urgency**.
5. Save the changes

When calculating the severity level, a notable event displays a default of "low" urgency when an asset or identity is categorized as "unknown." The "unknown" classification typically represents an object that has no match in the asset and identities system.

A notable event is assigned an **unknown** urgency level if the **severity** value assigned by the correlation search or in a triggering event is not recognized by ES. This indicates an error in the severity value provided by the correlation search syntax. Verify that the correlation search severity is unknown, informational, low, medium, high, or critical.
Upgrade your existing deployment

Plan the upgrade

Plan your upgrade of the Splunk App for PCI Compliance. You must be familiar with the app and have administrative knowledge of the Splunk platform to complete the upgrade.

Minimum requirements for upgrade

- Make sure your hardware and software versions are compatible with the new version by reviewing the Deployment options.
- Review the Known Issues and Release Notes in the Release Notes to understand the new features and functionality.

Planning the upgrade

The Splunk App for PCI Compliance upgrade process assumes the following:

- You have an installation of the Splunk App for PCI Compliance 3.0.x and the required add-ons in a single-instance Splunk deployment or on a dedicated search head in a distributed Splunk deployment.
- You are running Splunk Enterprise 6.6.x or later on a supported Linux or Windows system

Order of operations for upgrading

1. Review this topic and any linked items to view the changes in the latest release.
2. Upgrade Splunk platform instances.
3. If installing the Splunk App for PCI Compliance (for Splunk Enterprise Security), upgrade the Splunk Enterprise Security search head instance.
5. Review, upgrade, and deploy add-ons.

Search head clustering considerations

Upgrading a Splunk App for PCI Compliance deployment on a search head cluster is a multi-step process. The recommended procedure is detailed in
Upgrading the Splunk App for PCI Compliance on a search head cluster in this manual.

**Using the Splunk App for PCI Compliance installer**

Splunk App for PCI Compliance supports upgrading from the previous minor version of the app. Performing a full backup of the search head is recommended as the upgrade process will not backup the existing installation before upgrading.

- The upgrade of the Splunk App for PCI Compliance on a search head will not complete if apps or add-ons included in the Splunk App for PCI Compliance package are managed by a deployment server. Before beginning an upgrade, remove the `deploymentclient.conf` containing references to the deployment server and restart Splunk services.
- The upgrade process will overwrite all prior or current versions of apps and add-ons, and it will inherit any configuration changes and files saved in the app `/local` and `/lookups` paths.
- The upgrade process will not overwrite a newer version of an app or add-on.
- An app or add-on that was disabled in the prior version will remain disabled after the upgrade.

**Upgrading distributed add-ons**

A copy of the latest add-ons are included with the Splunk App for PCI Compliance. When upgrading the Splunk App for PCI Compliance, review and deploy all add-ons to indexers and forwarders as required. The Splunk App for PCI Compliance installation process does not automatically upgrade or migrate any configurations deployed to the indexers or forwarders.

Any customizations made to the prior versions of an add-on must be manually migrated.

**Upgrade the Splunk App for PCI Compliance**

This topic describes how to upgrade an installed version of the Splunk App for PCI Compliance version 3.0 or later to the latest release.

To review the migration steps for a 2.x version of the Splunk App for PCI Compliance, see the instructions in Upgrade Splunk App for PCI Compliance in the version 3.0.x *Installation and Upgrade Manual.*
Order of operations for upgrading

1. Review the planning topic.
2. Upgrade Splunk platform instances.
4. Download the Splunk App for PCI Compliance.
5. Install the latest version of the Splunk App for PCI Compliance.
6. Set up the Splunk App for PCI Compliance.
7. Validate the upgrade.

To install the Splunk App for PCI Compliance on a search head cluster, see Upgrade Splunk App for PCI Compliance on a search head cluster.

Review the planning topic

Review the planning topic and back up your system before you upgrade.

1. See Plan the upgrade in this manual.
2. Perform a full backup of the search head or your single instance deployment.

Download the Splunk App for PCI Compliance

Obtain the new version of the Splunk App for PCI Compliance.

1. Download the version of the Splunk App for PCI Compliance that you are upgrading.
   1. Splunk App for PCI Compliance (for Splunk Enterprise).
2. Download the app and save the product file to your desktop.
3. Log in to the PCI instance or search head as an administrator.

Install the latest version of the Splunk App for PCI Compliance

1. On the Splunk platform search page, select Apps > Manage Apps and select Install App from File.
2. Select Upgrade app to start the upgrade.
3. Select **Choose File** and browse to the Splunk App for PCI Compliance product file.
4. Click **Upload** to begin the installation.
5. Select **Set up now** to begin the Splunk App for PCI Compliance setup.

Run the setup procedure promptly after the upload completes. If the setup procedure is not run promptly after the upload completes, errors display in the Splunk App for PCI Compliance.

**Set up the Splunk App for PCI Compliance**

1. Select **Start**.
2. The **Splunk App for PCI Compliance Post-Install Configuration** page indicates the upgrade status as it moves through the stages of installation.
3. Choose to exclude selected add-ons from being installed, or install and disable them. When the setup is done, the page will prompt you to restart Splunk platform services.
4. Select **Restart Splunk** to finish the installation.

**Validate the upgrade**

The Splunk App for PCI Compliance upgrade process is now complete. Objects disabled during the upgrade process will automatically be enabled. Validate success of the upgrade.

1. On the Splunk App for PCI Compliance menu bar, Select **Audit > ES Configuration Health**.
2. Select a version of **4.0.x** to match the 3.0.x version of the Splunk App for PCI Compliance that you are upgrading from. For example, if you are upgrading from Splunk App for PCI Compliance version 3.0.2, select 4.0.2 as your previous version.
3. Review potential conflicts and changes to the default settings. For more information, see ES Configuration Health in the Splunk Enterprise Security User Manual.

**Upgrade Splunk App for PCI Compliance on a search head cluster**

Upgrade the Splunk App for PCI Compliance (for Splunk Enterprise) on a search head cluster. Review the instructions before beginning the upgrade.
**Prerequisites**

Upgrade Splunk platform on all search head instances as required. For more information on upgrading the Splunk platform instances that make up a search head cluster, see Upgrade a search head cluster in the *Distributed Search Manual*.

**Prepare a staging instance**

The staging instance is used to compare the deployer’s copy of the Splunk App for PCI Compliance with the latest release. If you have a clean testing or QA instance in your environment, you may use that instance for staging the upgrade if no other apps are installed.

1. Prepare a single instance of Splunk Enterprise to use for staging an upgrade. This instance is for staging only, and should not connect to indexers or search peers.
2. Copy the Splunk App for PCI Compliance (for Splunk Enterprise) installation from the deployer instance path `$SPLUNK_HOME/etc/shcluster/apps` to the staging instance path `$SPLUNK_HOME/etc/apps`. The deployer’s copy of the Splunk App for PCI Compliance represents the prior release, and includes configuration settings that are deployed to the search head cluster. It does not include the runtime knowledge object changes replicated between the search head cluster nodes.

**Upgrade staging to the latest version of the Splunk App for PCI Compliance**

Follow the upgrade steps.

1. Review the planning topic.
2. Download the Splunk App for PCI Compliance.
3. Install the latest version of the Splunk App for PCI Compliance.
4. Set up the Splunk App for PCI Compliance.
5. Validate the upgrade

After the upgrade is complete, reconcile customized configurations.

1. Reconcile configurations and settings in the deployed version of the Splunk App for PCI Compliance with the latest release.
2. Remove deprecated apps and add-ons. The upgrade process automatically disables deprecated apps and add-ons and displays an alert in **Messages** on the staging instance to identify the deprecated items.
**Migrate the upgraded instance to the deployer**

Migrate the upgraded contents from the staging instance to the deployer and deploy the upgraded version to the search head cluster members.

1. On the staging instance, copy `$SPLUNK_HOME/etc/apps` to `$SPLUNK_HOME/etc/shcluster/apps` on the deployer.
2. On the deployer, remove any deprecated apps or add-ons in `$SPLUNK_HOME/etc/shcluster/apps` that were noted during the upgrade on staging.

**Deploy the changes to the cluster members**

On the deployer, deploy the Splunk App for PCI Compliance while retaining lookup file content created on the cluster members. Use the `preserve-lookups true` switch. See Maintain lookup files across app upgrades in the Splunk Enterprise Distributed Search Manual.

**Validate the configuration on the search cluster**

After the deployer distributes the upgraded version of the Splunk App for PCI Compliance to the search head cluster members, compare the cluster-replicated knowledge objects to the latest Splunk App for PCI Compliance installation.

1. On each search head cluster member, open the Splunk App for PCI Compliance and select Audit > ES Configuration Health.
2. Select a version of 4.x.x to match whichever version of Splunk App for PCI Compliance 3.x.x you are upgrading from.
3. Review any changes.

**Migrate an existing search head to a search cluster**

A Splunk App for PCI Compliance installation on a single instance or search head pool member cannot be added to a search head cluster.

Migrate Splunk App for PCI Compliance configurations to a search head cluster.

1. Identify any custom configurations and modifications in the previous Splunk App for PCI Compliance installation.
2. Implement a new search head cluster.
3. Deploy the latest version of the Splunk App for PCI Compliance on the search head cluster.
4. Review and migrate the customized configurations to the search head cluster deployer for replication to the cluster members.
5. Shut down the old Splunk App for PCI Compliance search head.

For more information on settings migration, see Migrate from a standalone search head to a search head cluster in the Splunk Enterprise Distributed Search Manual.

For assistance in planning a Splunk App for PCI Compliance deployment migration, contact the Splunk Professional Services team.
Resources

Troubleshoot your deployment

This section provides tips for troubleshooting possible issues with your Splunk App for PCI Compliance deployment.

Other required apps

Splunk platform implements some of its functionality through separate apps. Do not disable any of these apps:

- learned
- search
- launcher
- user-prefs

General performance

Where appropriate, you can improve performance of the Splunk App for PCI Compliance and reduce hardware requirements by limiting the indexes used by the app.

If the Splunk App for PCI Compliance is limited to a subset of indexes, all of the indexes it searches require admin access, as described in Set up multiple indexes in Managing Indexers and Clusters of Indexers.

By default the search head searches the "main" index.

Measuring system performance

You can use IOZone on Windows to measure system performance. IOzone will output the data in IOPS if the "-O" argument is specified.

Below is an example of IOzone invocation to store results in an Excel spreadsheet with IOPS:

```bash
iozone -s 4g -r 2k -r 4k -r 8k -r 16k -r 32k -O -b results.xls
```
Performance on UNIX systems

The search head that is hosting the Splunk App for PCI Compliance should be configured for high performance. UNIX systems should check the ulimit setting in particular, as this can artificially limit the operating system’s capacity.

Other performance impacts include the Linux swappiness setting. Consult with your UNIX systems administrator for high performance build recommendations.

Other troubleshooting tips

- Verify that you have the minimum version of Splunk Enterprise installed. See Install Prerequisites in this manual for more information.
- Disable other apps on the search head you are using for the Splunk App for PCI Compliance. If you are using Splunk add-ons for Cisco, disable the saved searches. See the FAQ for details.

FAQ

Why are the scorecards not active if notable events exist?

If correlation searches are working and creating notable events, but the notable events do not appear on scorecards in the Splunk App for PCI Compliance, check two things.

Potential cause: Notable events could be suppressed by a suppression rule.

1. Open the Notable Event Suppression Audit page to determine if suppressions are preventing notable events from appearing.
2. You can also compare the results from these two searches.

`notable`

`notable` | search NOT `suppression`

Potential resolution: Review any suppression rules that exist to confirm that they are accurate and should be enabled or disabled.
Potential cause: For custom correlation searches, notable events could exist but not be linked to a governance and control value in `governance.conf`.

1. Compare the results from these two searches.

```shell
`notable`

`notable` | search (`get_governance(pci)`)
```

Potential resolution: Link the correlation searches to `governance.conf` entries. See Configure correlation searches.

**Cisco add-ons**

You can install various Splunk Add-on for Cisco products on the search head with the Splunk App for PCI Compliance and partially disable them to prevent load.

* To disable the searches, go to **Settings > Searches and Reports**, select the app name and disable all searches.
* To disable their dashboards, go to **Settings > User Interface > Views**, select the app name and disable all views.

This applies to these add-ons:

* Splunk Add-on for Cisco IPS
* Splunk Add-on for Cisco ESA
* Splunk Add-on for Cisco WSA
* Splunk Add-on for Cisco ASA