Vendor - Cisco

Product - ACS

Ref	Link
Splunk Add-on	https://splunkbase.splunk.com/app/1811/
Product Manual	https://community.cisco.com/t5/security-documentation/cisco-secure-access-control-system-5-x-configuring-the-external-syslog-servers/ta-p/1143113

Sourcetypes

sourcetype	notes
cisco:acs	Aggregation used

Sourcetype and Index Configuration

key	sourcetype	index	notes
cisco:acs	cisco:acs	netauth	None

Filter type

PATTERN MATCH

Setup and Configuration

 • No special steps required

Options

Variable	default	description
ACS_LISTENER_CISCO_ACS_TCP_PORT	empty string	Enable a TCP port for this specific sourcetype. When configured, overrides port used if no number defined.
ACS_LISTENER_CISCO_ACS_UDP_PORT	empty string	Enable a UDP port for this specific sourcetype. When configured, overrides port used if no number defined.
ACS_ARCHIVE_INDEXOS	no	Enable archive to disk for this specific source
ACS_DEDUP_INDEXOS_HEC	no	When splunk HEC is enabled, globally set to yes to enable the dedup this sourcetype source

Verification

Use the following search to validate events are present

```
index=<asconfigured> sourcetype=cisco:acs
```

Verify timestamp, and host values match as expected