Vendor - Ubiquiti - Unifi

All Ubiquiti Sola firewalls, switches, and access points share a common syslog configuration via the NMS.

- Login to NMS
- Navigate to settings
- Navigate to Site
- Enable Remote syslog server
- Enter hostname and port
- Update `vi /opt/sc4s/local/context/vendor_product_by_source.conf` update the host variable for `f_ubiquiti_unifi_fw` to identify USG firewalls

Product - Unifi Switch and Access Points

Unifi devices are managed using the Network Management Controller

Ref	Link
Splunk Add-on	https://splunkbase.splunk.com/app/4107/
Product Manual	https://help.ubnt.com/

Sourcetypes

sourcetype	notes
ubnt	Used when no sub sourcetype is required by add on
ubnt:config	USG events
ubnt:threat	USG IDS events
ubnt:switch	Unifi Switches
ubnt:wireless	Access Points logs

Sourcetype and Index Configuration

key	sourcetype	index	notes
ubiquiti_unifi	ubnt	netops	none
ubiquiti_unifi_fw	ubnt:config	netops	none
ubiquiti_unifi_login	ubnt:login	netops	none
ubiquiti_unifi_usg	ubnt:usg	netops	none
ubiquiti_unifi_switch	ubnt:switch	netops	none
ubiquiti_unifi_ips	ubnt:threat	netids	none
ubiquiti_unifi_wireless	ubnt:wireless	netops	none

Filter type

MSG Parse: This filter parses message content

Setup and Configuration