

## Proxmox Guide – Splunk

### Pre-requisites

- Proxmox node
- Splunk account

### Splunk Setup

1. In the node, select “Shell” and run the following script:
  - a. `bash -c "$(curl -fsSL https://raw.githubusercontent.com/community-scripts/ProxmoxVE/main/ct/splunk-enterprise.sh)"`
  - b. Script is from: <https://community-scripts.github.io/ProxmoxVE/scripts?id=splunk-enterprise>
  - c. Default setup information:

```

  __/
  ⚙ Using Default Settings on node metronome
  💡 PVE Version 9.1.2 (Kernel: 6.17.2-2-pve)
  ID Container ID: 102
  🖥 Operating System: ubuntu (24.04)
  📦 Container Type: Unprivileged
  💾 Disk Size: 40 GB
  🧠 CPU Cores: 4
  🛠 RAM Size: 8192 MiB
  🚀 Creating a Splunk-Enterprise LXC using the above default settings
  \__/

```

2. Once completed, you’ll be presented with an IP and port to connect to.
3. For the first time login credentials:
  - a. Open the Splunk container in Proxmox and go into the console
  - b. By default you should already be in the directory containing the splunk.creds file

```

root@splunk-enterprise:~# ls
splunk.creds
root@splunk-enterprise:~# cat splunk.creds
Splunk-Credentials

```

- c.
- d. If you cannot locate the splunk.creds file, use a command like readlink to locate the file

```

root@splunk-enterprise:~# readlink -f splunk.creds
/root/splunk.creds

```

- e.

## Connecting Splunk to UniFi Router

1. Login to your router
2. Navigate to Settings>CyberSecure>Traffic Logging
3. Select SIEM Server next to Active Logging
4. Enter in your Splunk server's IP and port, and select what content you want sent to Splunk

The screenshot shows the UniFi Traffic Logging configuration page. The 'Traffic Logging' tab is selected. The 'NetFlow (IPFIX)' option is disabled. 'Flow Logging' is enabled with 'All Traffic' selected. Under 'Additional Flows', 'Gateway DNS' is disabled, 'UniFi Services' is checked, and 'All UniFi Device Management' is disabled. 'Activity Logging (Syslog)' is set to 'SIEM Server'. The 'Contents' section shows a list of log categories: Gateway, Access Points, Switches, Admin Activity, Clients, Critical, Devices, Security Detections, Triggers, Updates, VPN, and Firewall Default Policy. 'Debug Logs' is disabled. The 'Server Address' field is filled with a redacted IP address, and the 'Port' is set to 443. 'Netconsole' is disabled. 'Data Retention' is set to 'Auto'. 'SNMP Monitoring' is disabled with 'Version 1/2C' selected. 'Logging Levels' is set to 'Auto'. At the bottom, there are 'Apply Changes' and 'Cancel' buttons.

- a.
5. Apply your changes