Installation Cisco Secure Endpoint Protection unter Linux

Für die Installation des Cisco Secure Endpoint Protection Client auf ubuntu/debian Systemen liefert Cisco ein deb-Paket aus.

1. Das passende deb-Paket für die eigene Distribution herunterladen

2. Das Paket z.B. mit aptitude als root oder per sudo installieren:
   z.B. sudo apt install ./Downloads/amp_ubuntu-20-04-amd64.deb

3. Anschließend kann der Status des Clients mit dem Aufruf des Kommandozeilentools ampcli geprüft werden. Dazu den folgenden Befehl in der Kommandozeile ausführen:
   /opt/cisco/amp/bin/ampcli status

   Die Ausgabe sollte bei erfolgreicher Installation wie folgt aussehen:

```
Trying to connect...
Connected.
Status:                  Connected
Mode:                    Normal
Scan:                    Ready for scan
Last Scan:               2025-04-03 07:57:28 AM
Policy:                  UNI-Protect (#155)
Command-line:            Enabled
Orbital:                 Disabled
Behavioral Protection:   Protect
Faults:                  None
```

4. Über das Kommandozeilentool kann auch ein sofortiger Virenscan des Systems initiiert werden. Dazu für einen Flash-Scan den folgenden Befehl ausführen:
   /opt/cisco/amp/bin/ampcli scan flash

   oder für einen vollständigen scan:
   /opt/cisco/amp/bin/ampcli scan full

5. Die Logfiles mit Informationen über eventuell gefundenen Bedrohungen befinden sich im Verzeichnis: /var/log/cisco

6. Eine Hilfe für das Kommandozeilentool kann mit dem folgenden Befehl aufgerufen werden:
   /opt/cisco/amp/bin/ampcli help