# Cisco Secure Endpoint Linux Connector on Debian-based systems

## Contents



This article describes the changes and steps administrators can take to deploy the Cisco Secure Endpoint Linux connector on Debian-based systems:

- Debian 10 and newer.
- Ubuntu 18.04 and newer.

## Minimum OS Requirements

Consult the Cisco Secure Endpoint Linux Connector OS Compatibility article for OS Compatibility.

## Environment Setup

The Linux connector on Debian-based systems uses eBPF for file and network monitoring. The machine must have the correct linux-headers software package installed otherwise the connector will raise fault 11 (Missing System Dependency) and run in a degraded state without file and network monitoring. Guidance for resolving this fault can be found the in the Linux Kernel-Devel Fault article.

### Dependencies

The Linux connector depends on system packages that are included in the base installation of Debian-based systems, but if a dependency is missing the following message will appear:

```
ciscoampconnector depends on <package_name>; however: Package <package_name> is not installed.
```

Use the following command to install any missing dependencies required by the Linux connector:

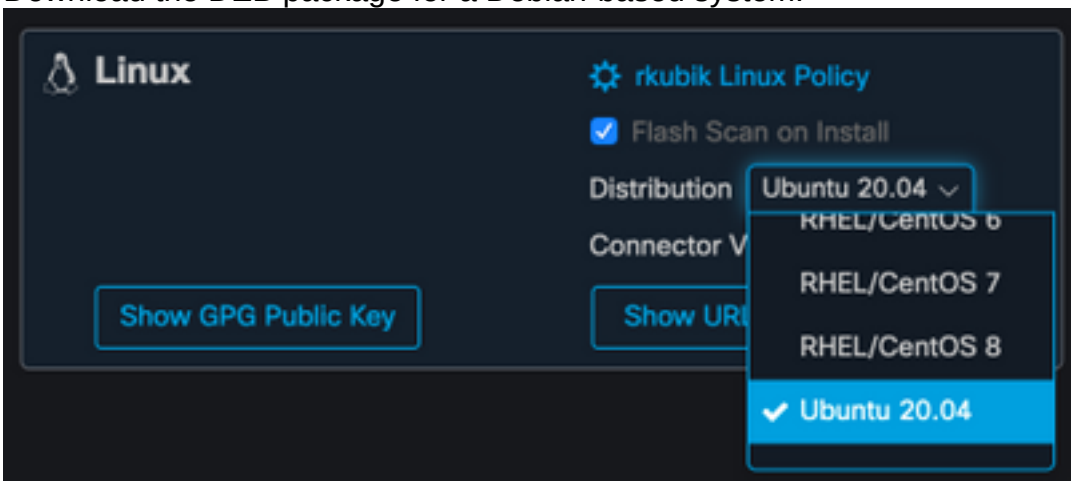
```
sudo apt install <package_name>
```

## Verifying the DEB package

The Linux connector DEB package contains a signature to verify that the downloaded software package belongs to Cisco.

## Downloading the DEB package

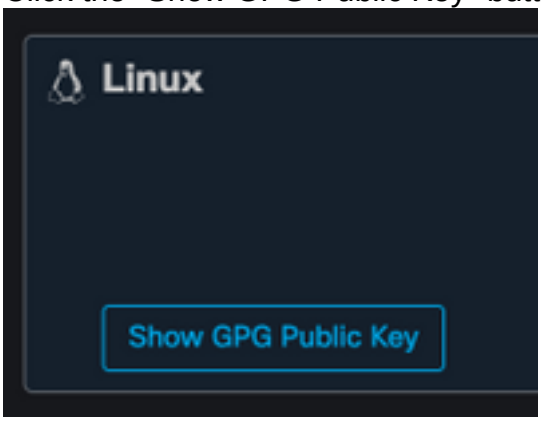
1. Access the AMP for Endpoints console.
2. Download the DEB package for a Debian-based system.




3. Transfer the DEB package to the Debian-based system. For example: amp_ciscoampconnector.deb.

## Retrieving the GPG Public Key

1. Click the "Show GPG Public Key" button, as shown in the image below.




2. If the connector version is earlier than 1.17.0, download and transfer, or copy the public key to the machine. For example: cisco.gpg. If the connector version is at least 1.17.0, the GPG key is available in /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp.

## Verifying the DEB package

The DEB package is signed using the debsigs tool and can be verified using debsig-verify.

1. Install the debsig-verify tool.
   ```
   sudo apt-get install debsig-verify
   ```
2. Import the Cisco GPG Public Key into the debsigs keyring. **Note:** As of version 1.17.0, the debsig.gpg file will be created automatically so step 2 can be skipped.
   ```
   sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output
   /usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg
   ```

3. Create policy directory.
   ```
   sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
   ```
4. Copy the policy contents below into a new file "/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol".
   ```
   <?xml version="1.0"?> <!DOCTYPE Policy SYSTEM
   "https://www.debian.org/debsig/1.0/policy.dtd"> <Policy
   xmlns="https://www.debian.org/debsig/1.0/"> <Origin Name="Debsig" id="914E5BE0F2FD178F"
   Description="Cisco AMP for Endpoints"/> <Selection> <Required Type="origin"
   File="debsig.gpg" id="914E5BE0F2FD178F"/> </Selection> <Verification MinOptional="0">
   <Required Type="origin" File="debsig.gpg" id="914E5BE0F2FD178F"/> </Verification> </Policy>
   ```
5. Verify the DEB signature with debsig-verify.
   ```
   debsig-verify amp_ciscoampconnector.deb
   ```
   The output should look as follows:
   ```
   debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
   ```

**Note**: Step 5 can be repeated for any Debian-based packages downloaded from the AMP for Endpoints console.

# Installation

To install the connector execute the following command where [deb package] is the name of the file, for example amp_test.deb:

```
sudo dpkg -i [deb package]
```

**IMPORTANT!** If you are running other security products in your environment, there is a possibility that they will detect the connector installer as a threat. In order to successfully install the connector, add Cisco Secure to an allowed list or exclude Cisco Secure in the other security products and try again.

**IMPORTANT!** During connector installation, a user and group named cisco-amp-scan-svc are created on the system. If this user or group already exists but is configured differently, then the installer will attempt to delete and then re-create them with the necessary configuration. The installer will fail if the user and group could not be created with the necessary configuration.

# Uninstallation

Please refer to the Secure Endpoint User Guidefor uninstall instructions

# Revision History

December 10, 2020

- Initial version

April 12, 2022

- Content is applicable to both Debian and Ubuntu.