# Installation des Cisco Secure Endpoint Linux Connectors

## Inhalt



## Einleitung

Dieses Dokument beschreibt, wie der Cisco Secure Endpoint Linux Connector für Red Hat Enterprise Linux (RHEL) und Debian-basierte Systeme installiert und verifiziert wird.

Verfasst von Juan Carlos Castillero und herausgegeben von Yeraldin Sanchez, Cisco TAC Engineers.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Linux-Computer auf einem Linux-Anschluss unterstützen Betriebssystem (OS)

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Ein Secure Endpoint Linux Connector Installer Red Hat Package Manager (RPM)
- Ein Secure Endpoint Linux Connector Installer Debian Package Manager (dpkg)
- Ein GNU Privacy Guard (GPG)-Schlüssel zum Überprüfen von Updates (optional)

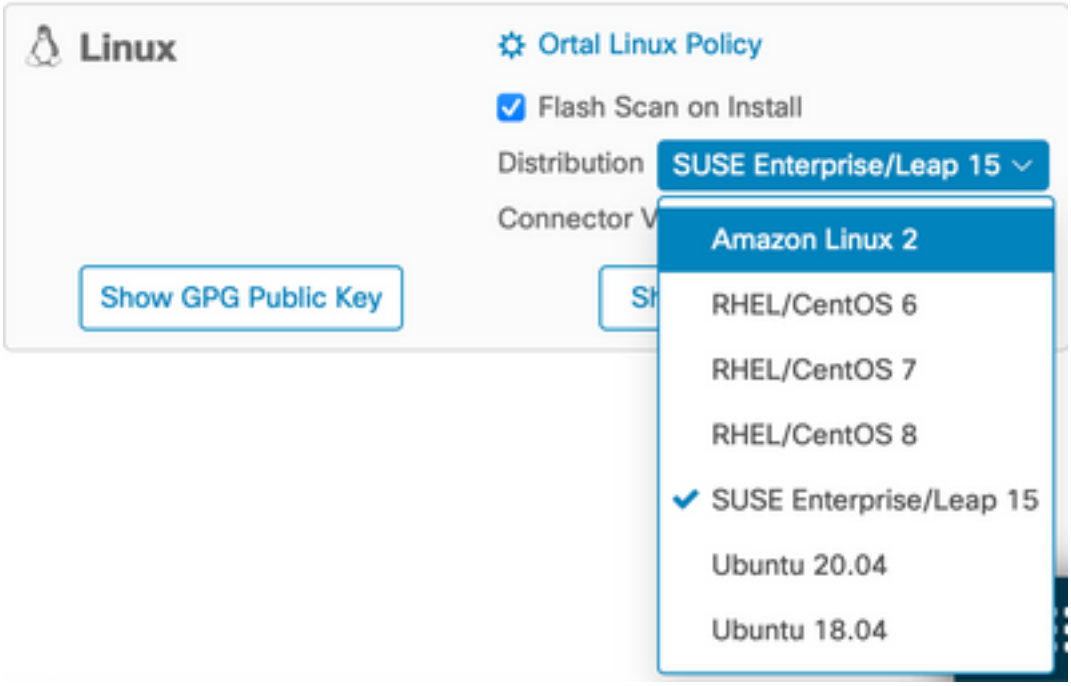
- Ein Linux Connector Installer DPKG (Debian Package Management System)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# RHEL/CentOS/Amazon Linux 2/SUSE 15

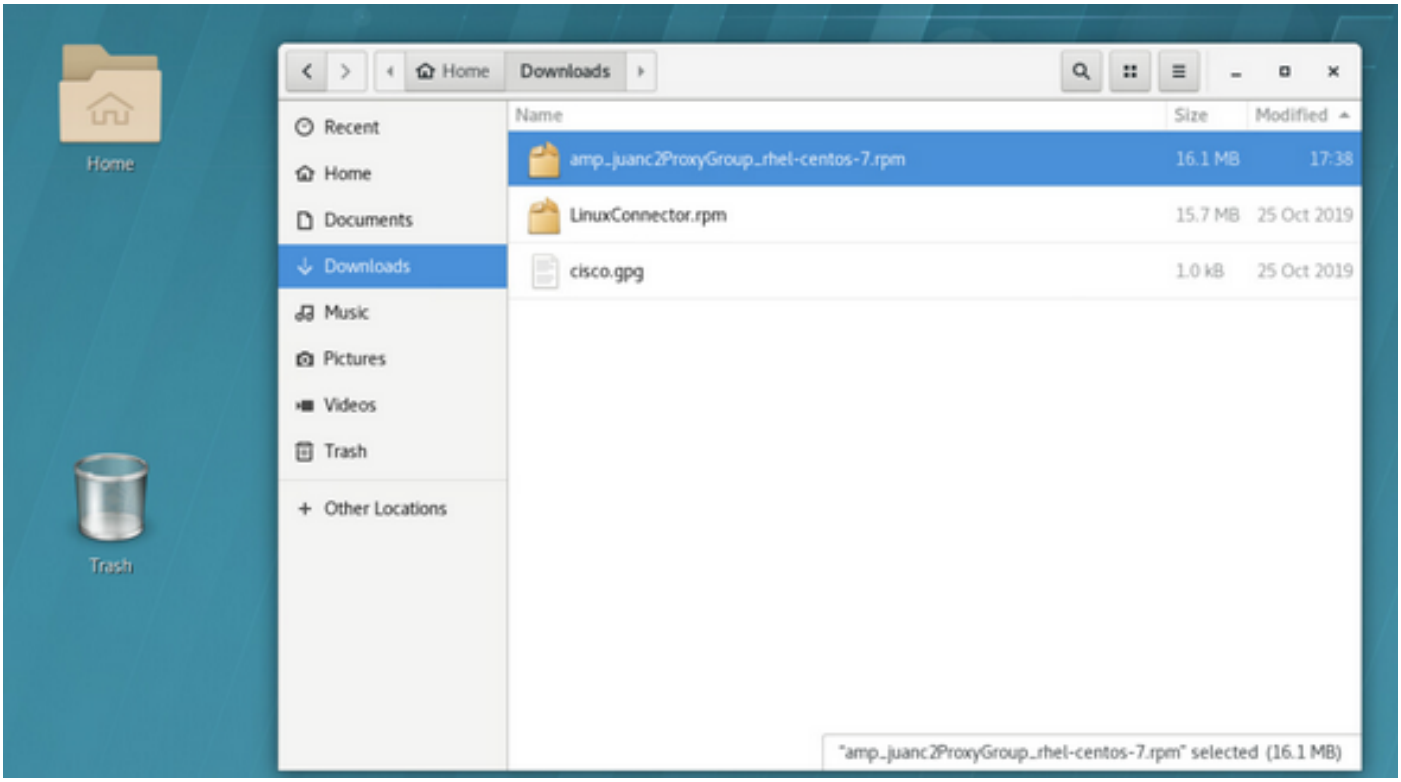
## Konfigurationen

Schritt 1: Laden Sie das Linux RPM-Paket vom Cisco Secure Endpoint Portal herunter, wie im Bild gezeigt.




> **Anmerkung:** Beachten Sie, dass die Verteilung des Betriebssystems wichtig ist, da beide Connectors äußerst unterschiedliche Architekturen haben.

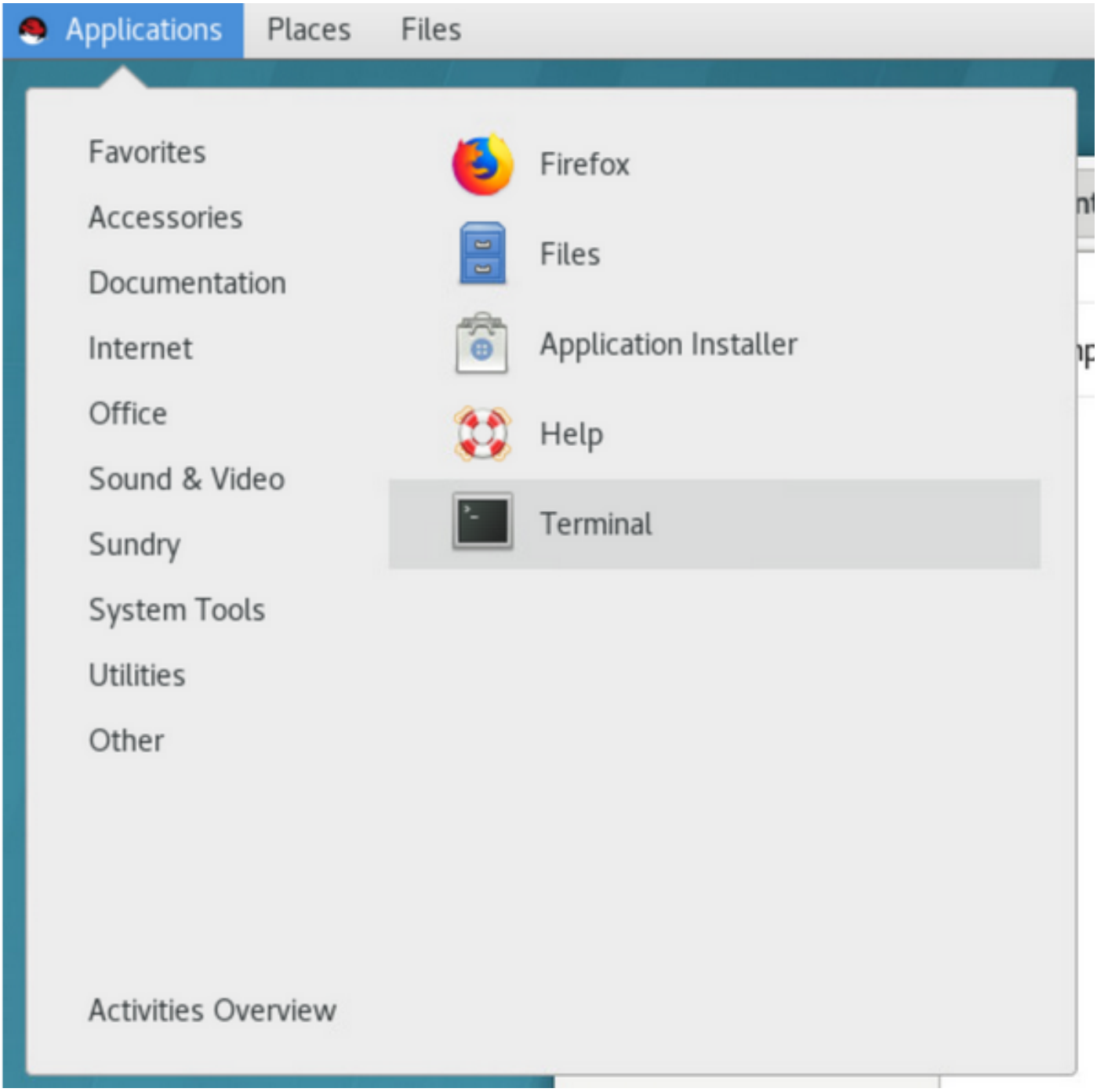
Schritt 2: Verschieben Sie das RPM-Paket an den betreffenden Endpunkt, indem Sie es entweder direkt vom Dashboard herunterladen oder manuell auf die Endpunkte verschieben. In diesem Beispiel wird eine grafische Benutzeroberfläche (Graphic User Interface, UI) verwendet, obwohl es möglich und häufig üblich ist, mit einer Minimalinstallation zu arbeiten. In diesem Fall muss man wissen, wie man das Linux-Terminal handhabt und das RPM-Paket findet.




Schritt 3: Um den Linux-Anschluss zu installieren, führen Sie den folgenden Befehl aus: **sudo yum localinstall [rpm-Paket] -y** (oder **sudo zypper install -y [rpm-Paket]** auf SUSE 15)

wobei [rpm-Paket] der Name der Datei ist, zum Beispiel "amp_Audit.rpm". Das RPM-Paket muss installiert werden, während der ATD-Dienst ausgeführt wird.

Wenn die Benutzeroberfläche verwendet wird, öffnen Sie das Terminal, wie im Bild gezeigt.



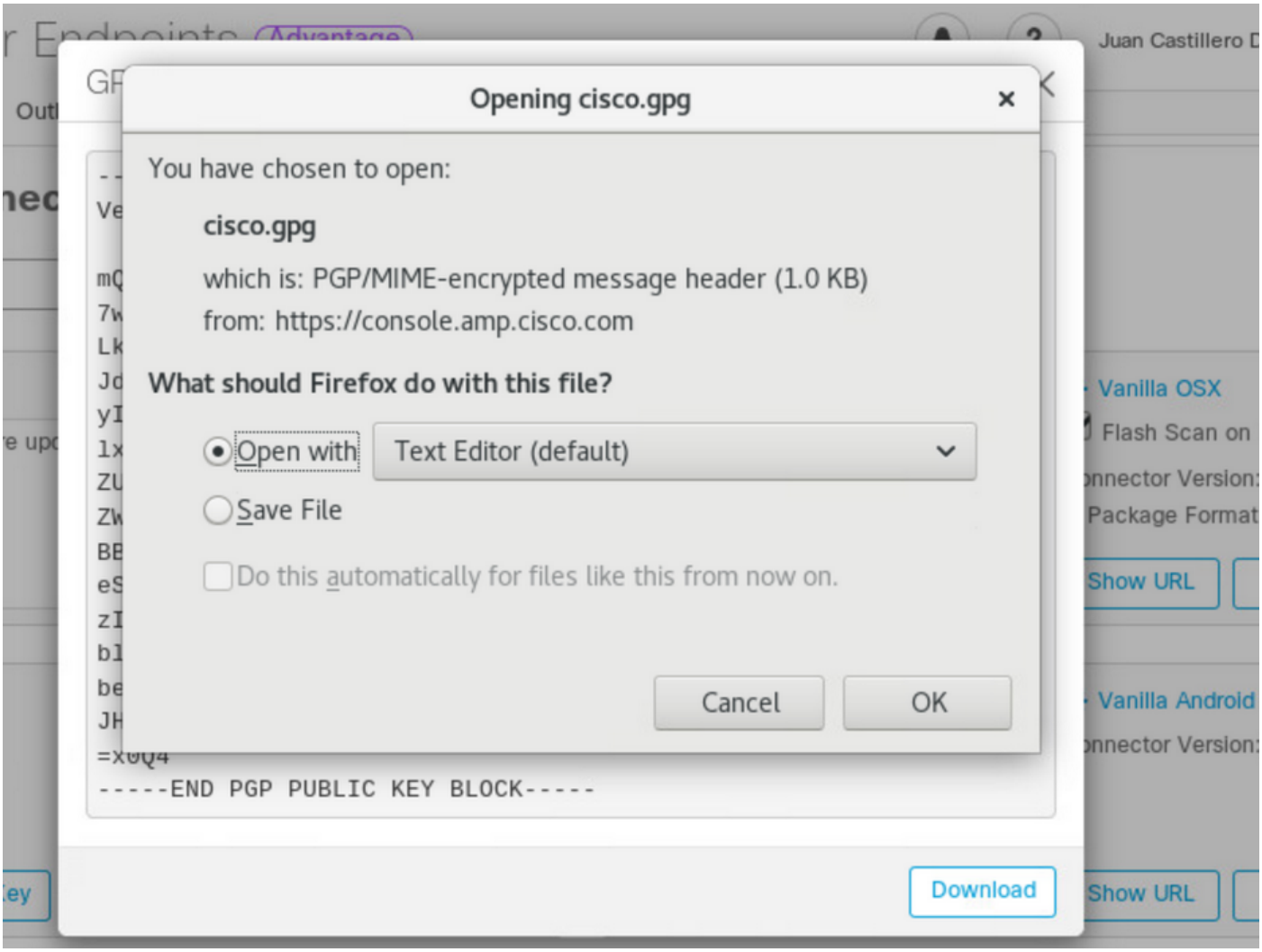

Nach Beginn der Installation ist keine Benutzereingabe erforderlich, sondern ein automatischer Prozess, wie im Bild gezeigt.

## Importieren des GPG-Schlüssels

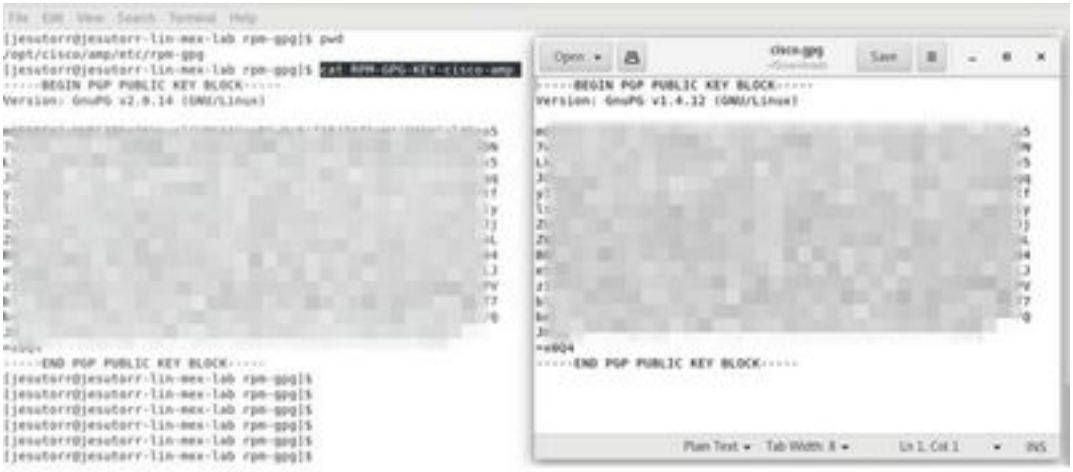
Der öffentliche GPG-Schlüssel kann von der Seite Download Connector kopiert werden, um die Signierung des RPM-Pakets zu überprüfen. Der Anschluss kann ohne GPG-Schlüssel installiert werden.; Allerdings Benutzer Muss den GPG-Schlüssel in die RPM-DB importieren, wenn er plant, Anschlussaktualisierungen über RHEL-Richtlinien zu übertragen..

**Anmerkung:** Ab der Connector-Version 1.17.0 wird der GPG-Schlüssel, der zur Verifizierung von Upgrade-Paketen während der Connector-Updates verwendet wird, automatisch installiert.

Schritt 1: Überprüfen Sie den GPG-Schlüssel, und klicken Sie auf der Seite "Download Connector" auf den Link GPG Public Key. Vergleichen Sie den Schlüssel mit dem Schlüssel bei **/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp**.




Schritt 2: Führen Sie den Befehl von einem Terminal aus, um den Schlüssel zu importieren: **sudo rpm —import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp**.



Schritt 3: Überprüfen Sie, ob der Schlüssel installiert wurde, führen Sie den Befehl vom Terminal aus: **rpm -q gpg-pubkey —qf '%{name}-%{version}-%{release} -> %{summary}\n**.

Schritt 4: Suchen Sie in der Ausgabe nach einem GPG-Schlüssel von Sourcefire. Der Updater

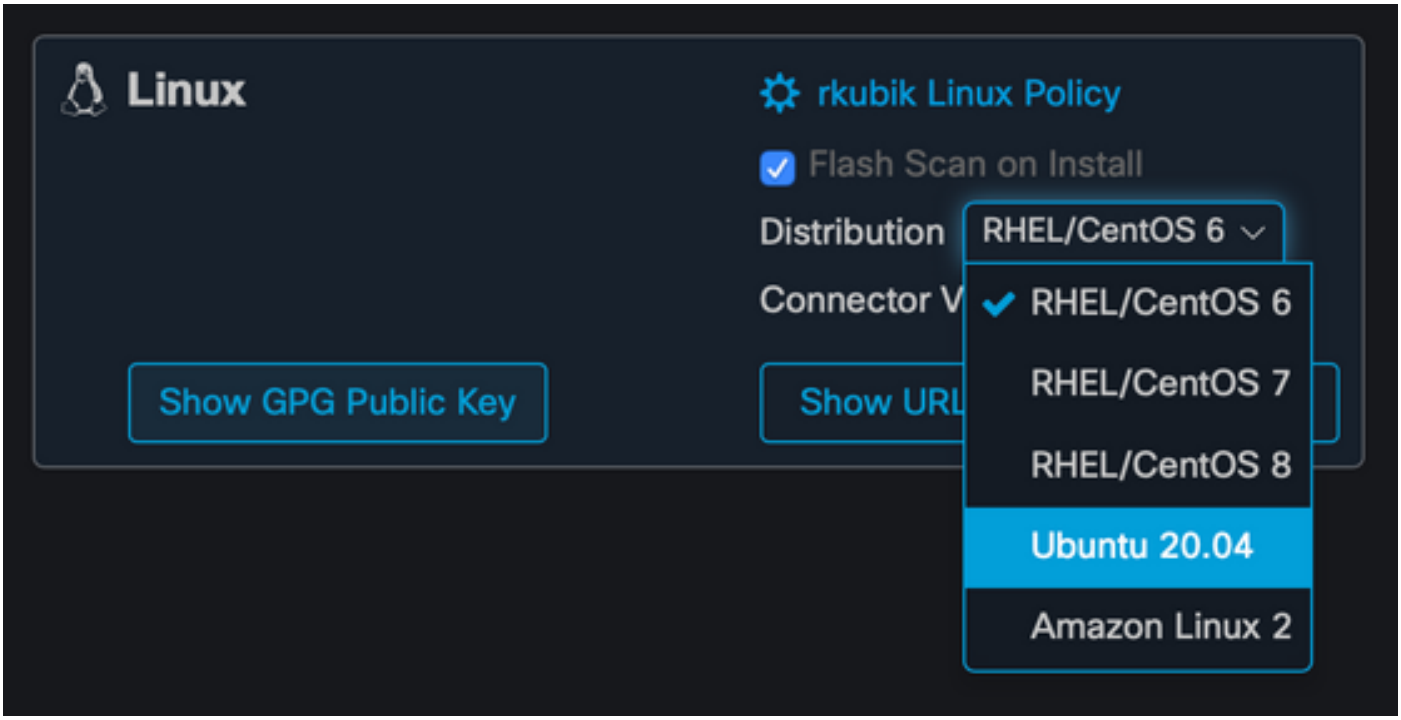
wird über den init-Daemon des Systems ausgeführt, und wenn ein Update verfügbar ist, wird automatisch der RPM-Upgrade-Prozess ausgelöst. Einige SELinux-Konfigurationen verbieten dieses Verhalten und führen zum Ausfall des Updaters.

Wenn Sie vermuten, dass dies der Fall ist, überprüfen Sie das Überwachungsprotokoll des Systems (z. B. **/var/log/audit/audit.log**) und suchen Sie nach Denial-Ereignissen im Zusammenhang mit Ampupdater. Sie müssen möglicherweise SELinux-Regeln anpassen, damit Updater funktioniert.

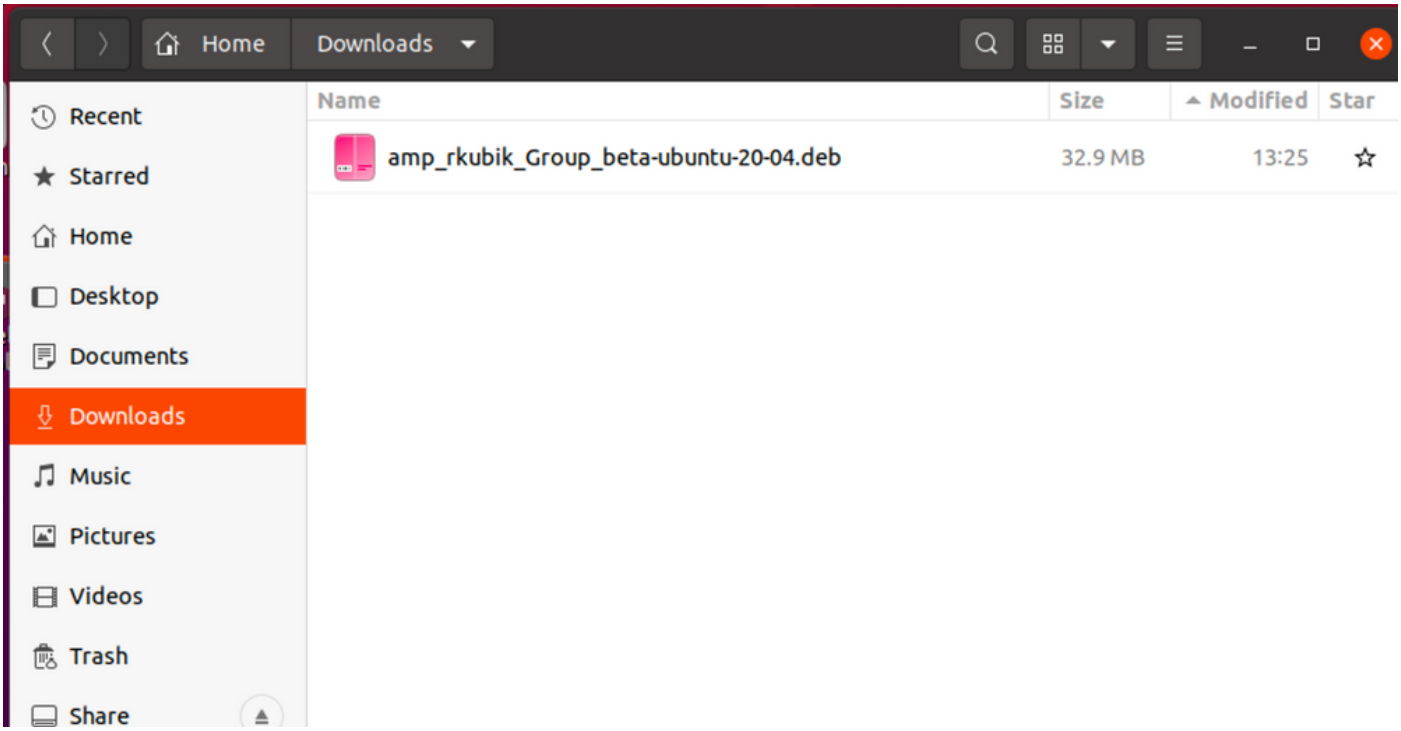
# Ubuntu

## Konfigurationen

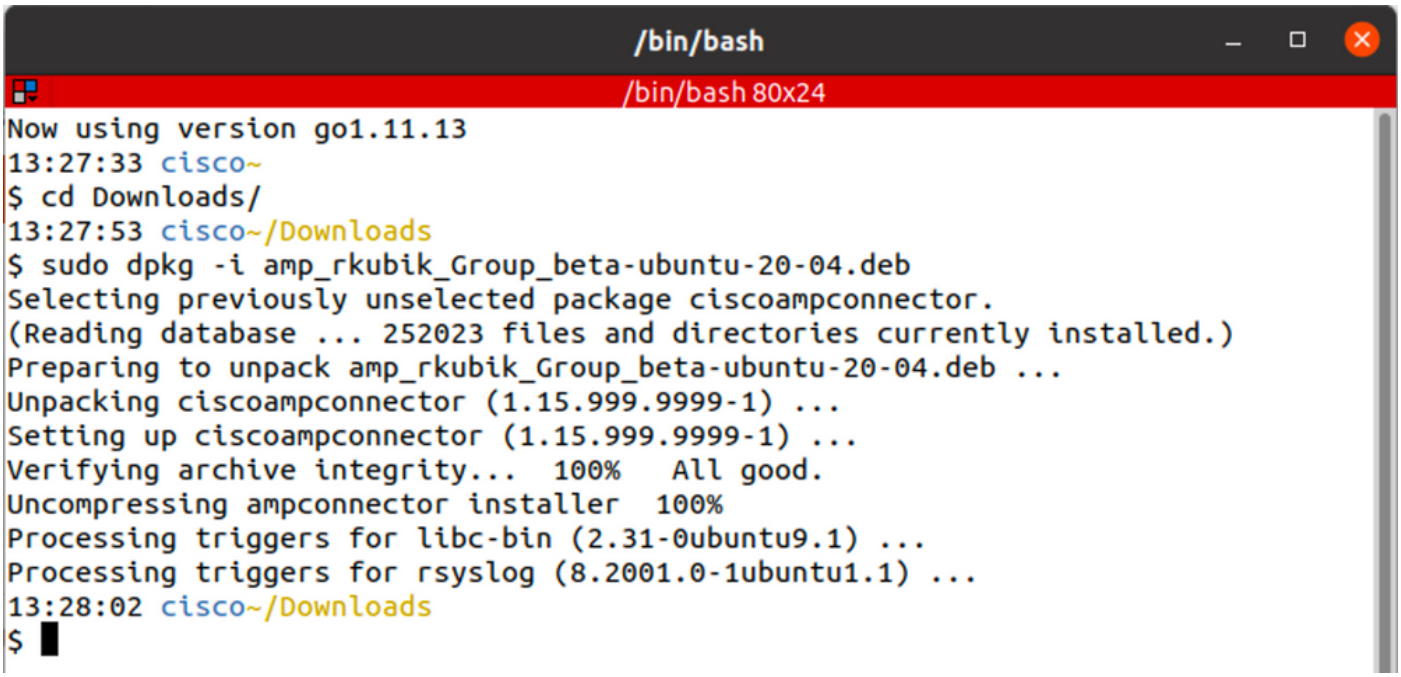
Schritt 1: Laden Sie das Linux DEB-Paket vom Cisco Secure Endpoint Portal herunter, wie im Bild gezeigt.




Schritt 2: Verschieben Sie das DEB-Paket an den betreffenden Endpunkt, indem Sie es entweder direkt vom Dashboard herunterladen oder manuell auf die Endpunkte verschieben. In diesem Beispiel wird eine grafische Benutzeroberfläche (Graphic User Interface, UI) verwendet, obwohl es möglich und häufig üblich ist, mit einer Minimalinstallation zu arbeiten. In diesem Fall muss man wissen, wie man das Linux-Terminal behandelt und das DEB-Paket findet.




Schritt 3: Um den Linux-Anschluss zu installieren, führen Sie den folgenden Befehl aus: **sudo dpkg -i [deb-Paket]**, wobei [deb-Paket] der Name der Datei ist, zum Beispiel "amp_Audit.deb". Nach Beginn der Installation ist keine Benutzereingabe erforderlich, sondern ein automatischer Prozess, wie im Bild gezeigt.




## Importieren des GPG-Schlüssels

Der öffentliche GPG-Schlüssel kann von der Seite Download Connector kopiert werden, um die Signierung des DEB-Pakets zu überprüfen. Der Anschluss kann ohne GPG-Schlüssel installiert werden. Ein Benutzer müsste jedoch den GPG-Schlüssel in seinen Debsig-Keyring importieren, wenn er die Verbindungsupdates mithilfe der Ubuntu-Richtlinie weiterleiten möchte. Weitere Informationen zum Importieren des GPG-Schlüssels und zum Überprüfen, dass der Anschluss unter Ubuntu nicht modifiziert wurde, finden Sie unter https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6

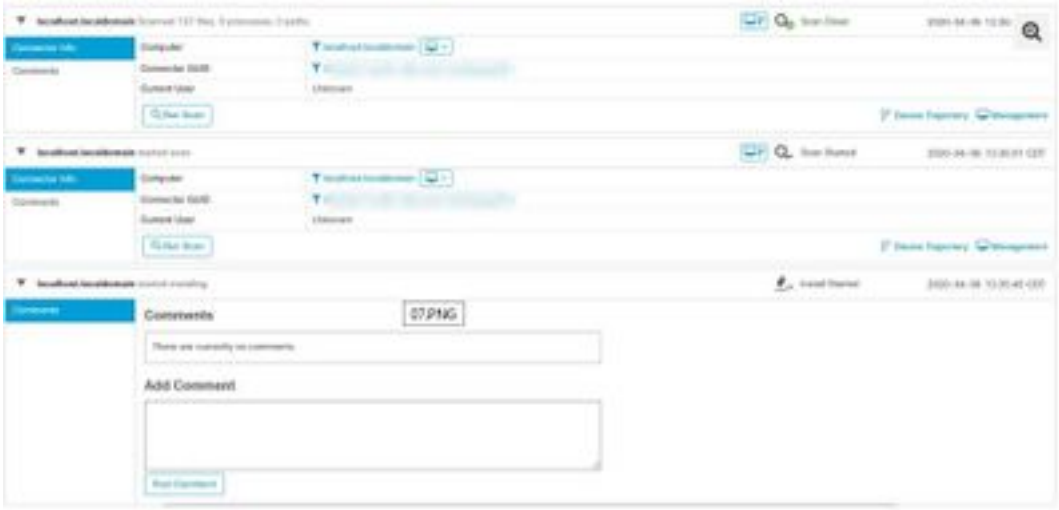
**Anmerkung:** Ab der Connector-Version 1.17.0 wird der GPG-Schlüssel, der zur Verifizierung von Upgrade-Paketen während der Connector-Updates verwendet wird, automatisch installiert. Um diesen GPG-Schlüssel zu überprüfen, klicken Sie auf der Seite Download Connector auf den Link GPG Public Key (GPG-Schlüssel), und vergleichen Sie ihn mit dem Schlüssel, der unter **/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp** installiert wurde.

# Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um die erfolgreiche Installation zu überprüfen, führen Sie die **AMP-CLI aus**. Die Befehlszeilenschnittstelle für den Linux-Anschluss finden Sie unter **/opt/cisco/amp/bin/ampcli**. Es kann im interaktiven Modus ausgeführt werden oder es kann ein einzelner Befehl ausgeführt und dann beendet werden. Führen Sie den Befehl **./ampcli —help aus**, um eine vollständige Liste der verfügbaren Optionen und Befehle anzuzeigen. Alle vom Connector generierten Protokolldateien sind in **/var/log/cisco** zu finden.


Auf der Cisco Secure Console wird auch eine Installationsveranstaltung angezeigt. Wenn beim Herunterladen des RPM-Pakets Flash-Scans angefordert wurden, werden diese ebenfalls angezeigt.




# Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

## Zugehörige Informationen

- Installation des AMP für Endpoints-Anschlusses in Linux-Video
- Technischer Support und Dokumentation für Cisco Systeme