Deploying the Cisco Secure Endpoint Linux Connector

Contents

Introduction

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

Requirements

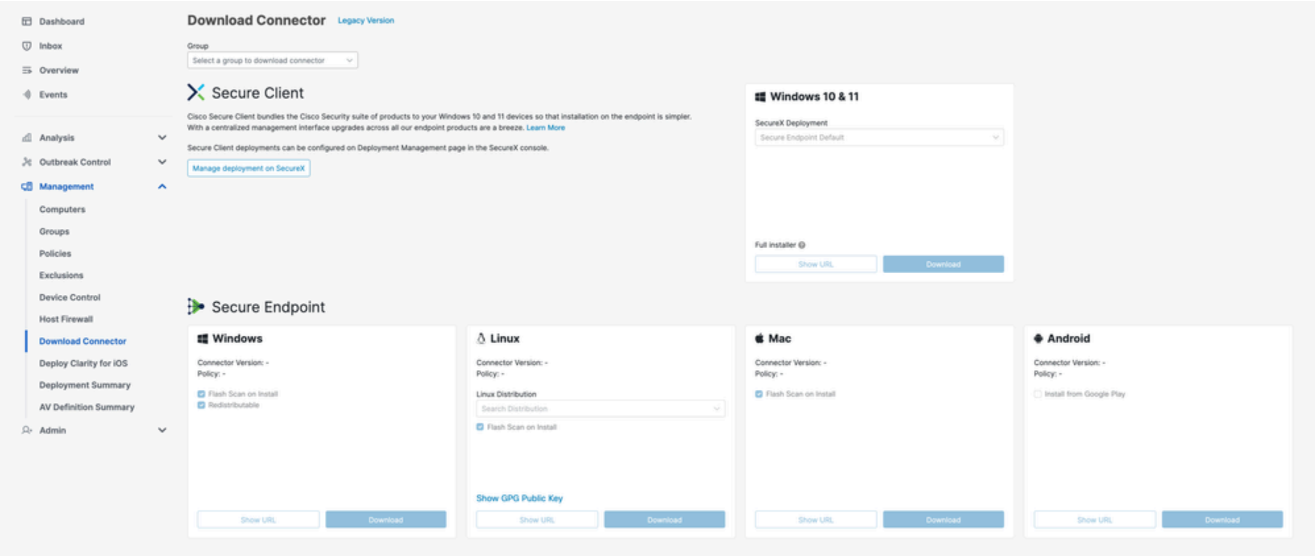
Consult the Cisco Secure Endpoint Linux Connector OS Compatibility article for OS Compatibility.

Consult the Secure Endpoint User Guide for the recommended Linux system requirements.

Deploy the Linux Connector

Download the Linux Connector Package

1. In the Secure Endpoint Console, navigate to the `Download Connector` page.



Download Connector

Group: Select a group to download connector

Secure Client

Cisco Secure Client bundles the Cisco Security suite of products to your Windows 10 and 11 devices so that installation on the endpoint is simpler. With a centralized management interface upgrades across all our endpoint products are a breeze. Learn More

Secure Client deployments can be configured on Deployment Management page in the SecureX console.

Windows 10 & 11

SecureX Deployment: Secure Endpoint Default

Full installer

Secure Endpoint

Windows

Connector Version: -
Policy: -

☑ Flash Scan on Install
☑ Redistributable

Linux

Connector Version: -
Policy: -

Linux Distribution: Search Distribution

☑ Flash Scan on Install

Mac

Connector Version: -
Policy: -

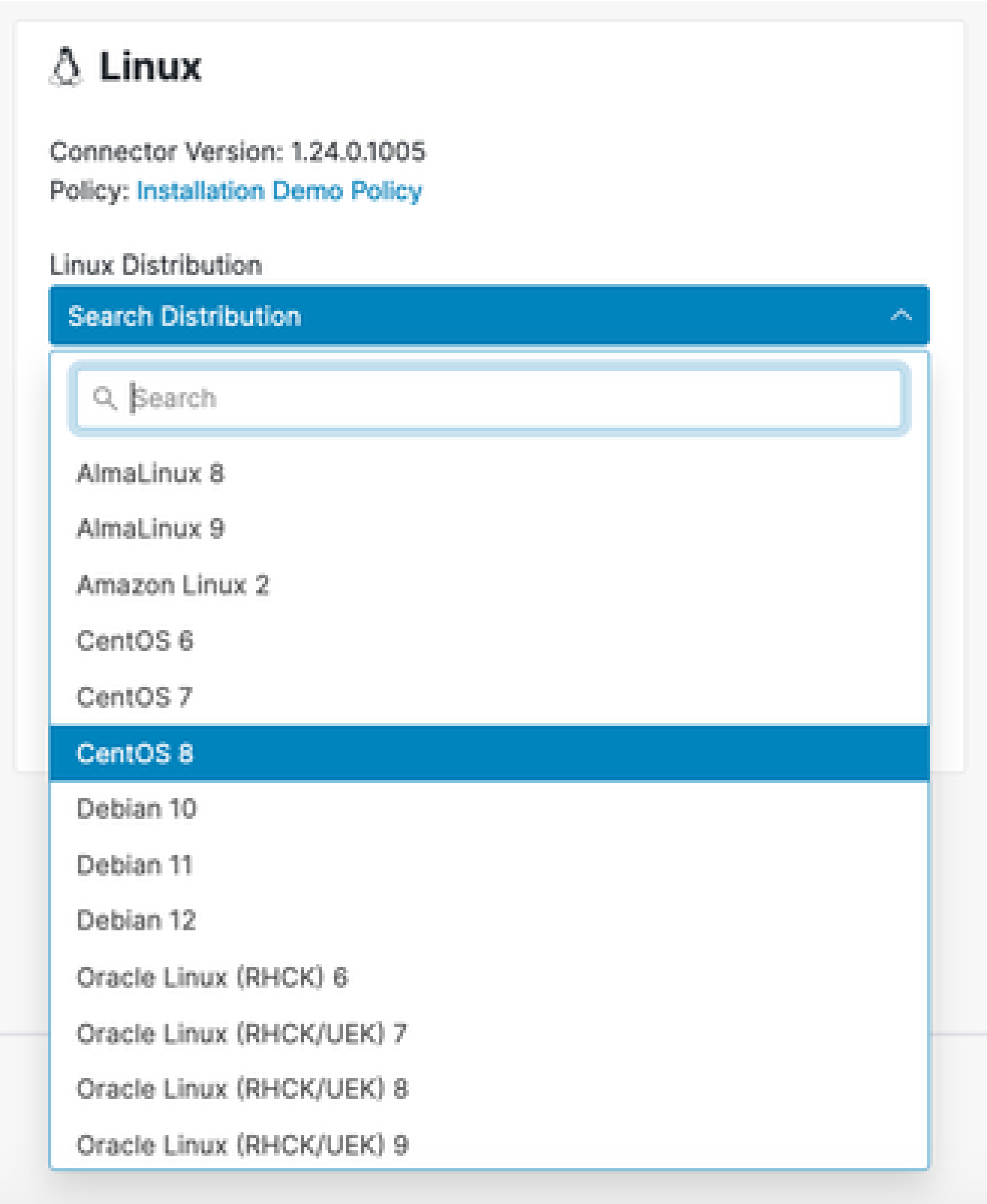
☑ Flash Scan on Install

Android

Connector Version: -
Policy: -

□ Install from Google Play

2. Select the appropriate Linux connector package by using the "Linux Distribution" dropdown to choose a distribution.



Linux

Connector Version: 1.24.0.1005

Policy: Installation Demo Policy

Linux Distribution

Search Distribution

Search

AlmaLinux 8

AlmaLinux 9

Amazon Linux 2

CentOS 6

CentOS 7

CentOS 8

Debian 10

Debian 11

Debian 12

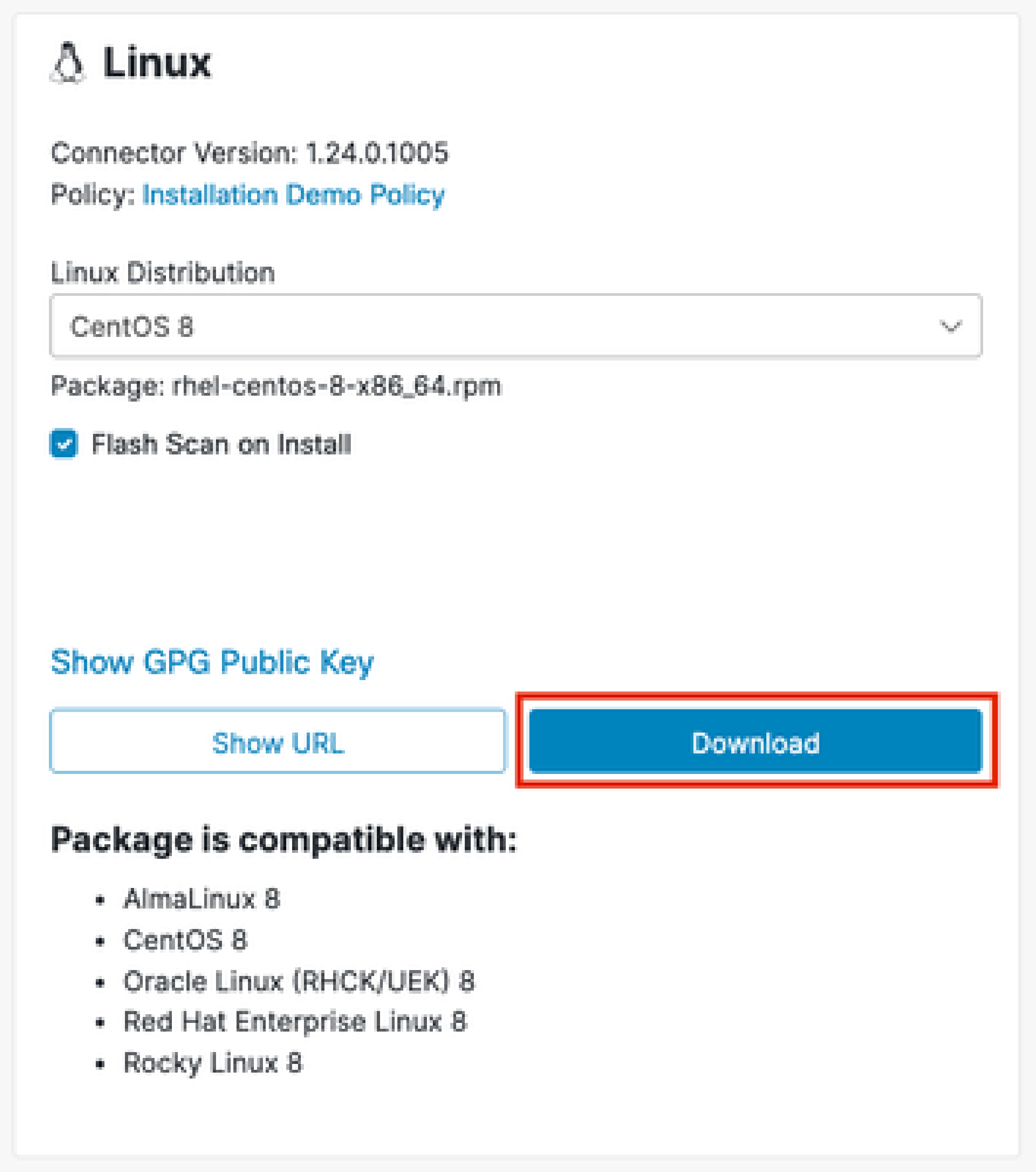
Oracle Linux (RHCK) 6

Oracle Linux (RHCK/UEK) 7

Oracle Linux (RHCK/UEK) 8

Oracle Linux (RHCK/UEK) 9

3. Click the `Download` button to begin downloading the selected package.



Linux

Connector Version: 1.24.0.1005
Policy: Installation Demo Policy

Linux Distribution
CentOS 8
Package: rhel-centos-8-x86_64.rpm

☑ Flash Scan on Install

Package is compatible with:

- AlmaLinux 8
- CentOS 8
- Oracle Linux (RHCK/UEK) 8
- Red Hat Enterprise Linux 8
- Rocky Linux 8

4. Transfer the downloaded package to the endpoint.

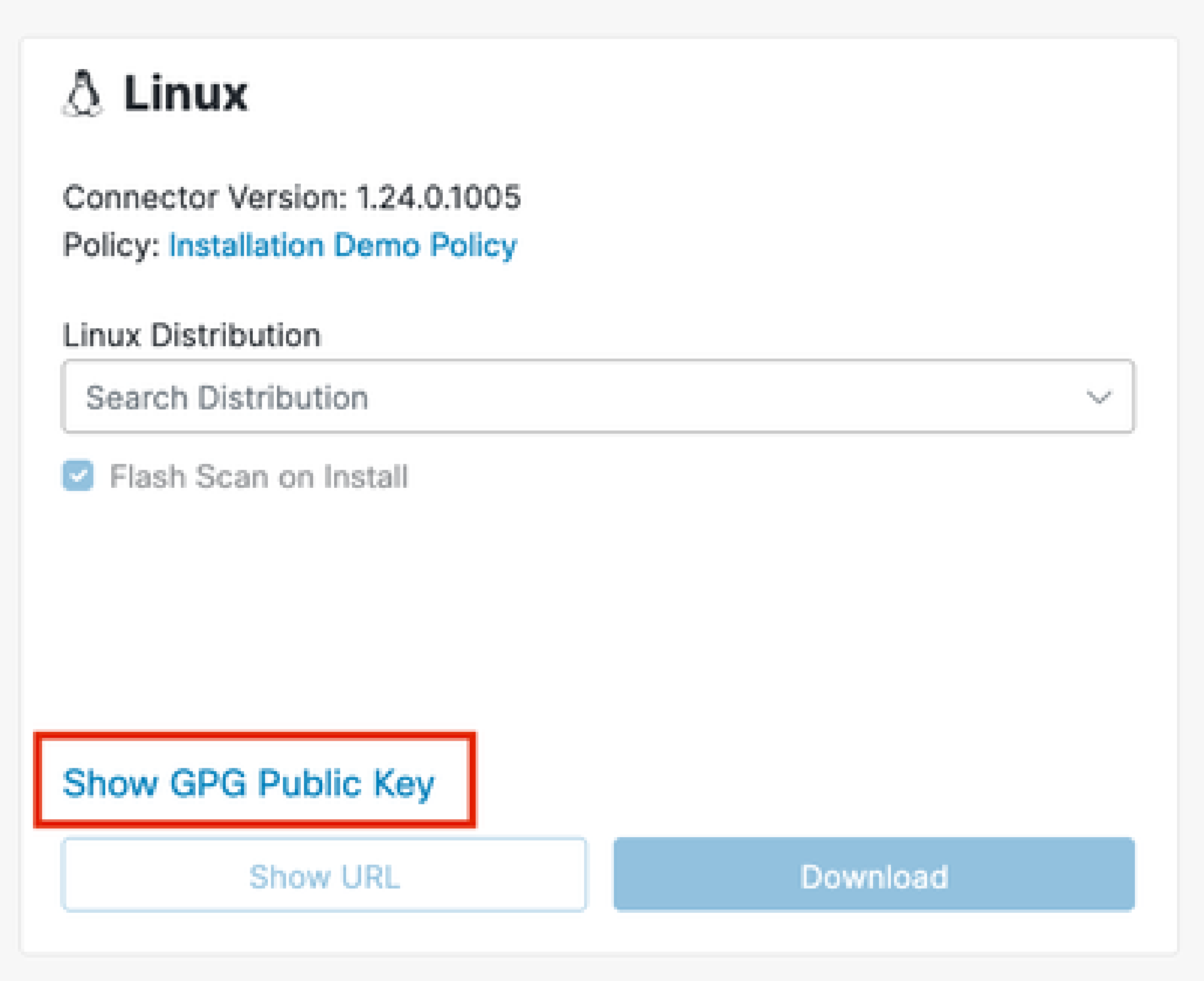
Verify the Linux Connector Package

The Linux connector can be installed without the Cisco GPG public key. However, if you plan on pushing connector updates via policy, then you will need to install the public key on the endpoint. For RPM-based distributions import the key into the RPM database. For Debian-based distributions import the key into the debsig keyring.

This section outlines how to import the Cisco GPG public key onto your system and how verify the downloaded connector package using the imported key.

Retrieve the Cisco GPG Public Key

1. On the Secure Endpoint Console `Download Connector` page, select the `Show GPG Public Key` link from the Linux section.



Linux

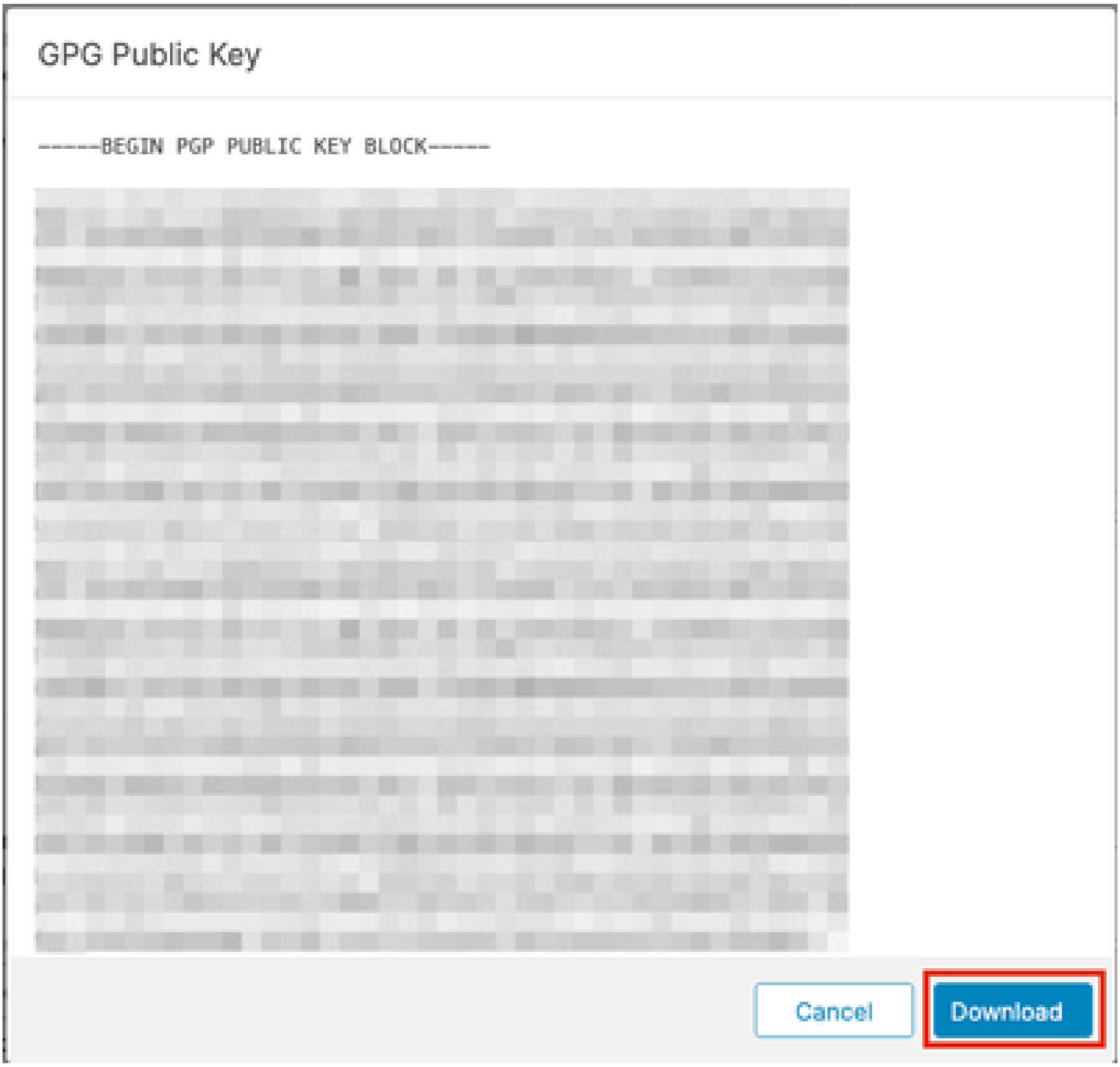
Connector Version: 1.24.0.1005

Policy: Installation Demo Policy

Linux Distribution: Search Distribution

☑ Flash Scan on Install

2. The Cisco GPG public key will appear in a pop-up window. Select `Download` in this pop-up to download the key to your system. The key will appear as `cisco.gpg` in your Downloads folder.



GPG Public Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
[redacted]
```

3. Transfer the downloaded key to the endpoint.

RPM-based

The RPM package is signed and can be verified using the RPM package manager.

1. Import the Cisco GPG public key into the RPM database.

   ```
   sudo rpm --import cisco.gpg
   ```

2. Verify the Cisco GPG public key was installed.

   ```
   rpm -q gpg-pubkey --qf ‘%{name}-%{version}-%{release} --> %{summary}\n’
   ```

   You should see the following public key listed:

   ```
   gpg-pubkey-34532611-6477a906 --> Cisco, Inc. <support@cisco.com> public key
   ```

3. Verify the Linux connector package using RPM. Example:

```
rpm -K amp_Installation_Demo_rhel-centos-8-x86_64.rpm
```

The following output should be displayed:

```
amp_Installation_Demo_rhel-centos-8-x86_64.rpm: digests signatures OK
```

Debian-based

The Debian package is signed using the Debian package signature verification (debsig) 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 debsig 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 the 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 signature with `debsig-verify`. Example:

   ```
   debsig-verify ubuntu-20-04-amd64.deb
   ```

   The following output should be displayed:

   ```
   debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
   ```

Install the Linux Connector Package

Install the Kernel Headers

Most modern Linux distributions use kernel versions that support eBPF, which the connector uses to monitor the system. To determine the kernel version of your endpoint, run the following command:

```
uname -r
```

If your distribution version matches any of the following then the connector will use eBPF for system monitoring:

- RPM-based distributions with a kernel version of 3.10.0-940 or later (EL7 / Enterprise Linux 7.9 is the earliest distribution with this kernel version).
- Debian-based distributions with a kernel version of 4.18 or later.

More details on mapping between distribution and kernel version can be found here.

If eBPF is supported on your endpoint, then the correct kernel headers must be installed in order for the connector to monitor the system. If your endpoint does not have the correct kernel headers installed, then the connector will raise fault 11 (Missing System Dependency) and it will run in a degraded state without file, process, or network monitoring.

Refer to the Linux Kernel-Devel Fault article for guidance on how install the correct kernel headers.

Install the Connector

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.

RPM-based

To install the connector execute one of the following commands where [rpm package] is the name of the file, for example `amp_Installation_Demo_rhel-centos-8-x86_64.rpm`:

- Via YUM:

  ```
  sudo yum localinstall -y [rpm package]
  ```

- Via Zypper:

  ```
  sudo zypper install -y [rpm package]
  ```

Note: Installing via yum or zypper will handle the installation of any required dependencies.

Debian-based

To install the connector execute the following command where [deb package] is the name of the file, for example `amp_Installation_Demo_ubuntu-20-04-amd64.deb`:

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

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.
```

Where <package_name> is the name of the missing dependency. Use the following command to install any missing dependencies required by the Linux connector:

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

You can re-attempt to install the connector once all missing dependencies have been installed.

Compare Cisco GPG Public Key

If the Linux connector version is at least 1.17.0, then the Cisco GPG public key used to verify upgrade packages during connector updates is installed automatically to the following locations:

- RPM-based: `/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp`
- Debian-based: `/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp`

Compare the key installed by the connector to the one retrieved from the Secure Endpoint Console.

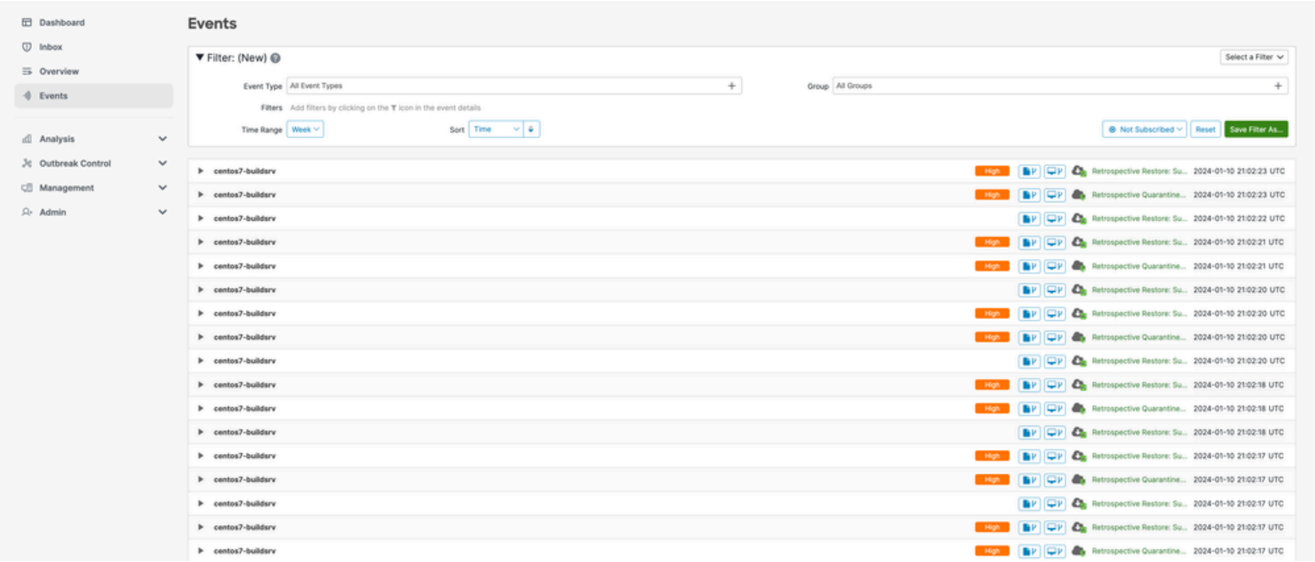
Verify Installation

The Linux connector command line interface can be used to verify the successful installation on the Linux connector. Run `/opt/cisco/amp/bin/ampcli status`. If your connector was successfully installed then you should see that it is `Connected` and has no faults listed when running the `/opt/cisco/amp/bin/ampcli/ampcli status` command:

```
$ /opt/cisco/amp/bin/ampcli status
Trying to connect...
Connected.
Status:                    Connected
Mode:                    Normal
Scan:                    Ready for scan
Last Scan:                2024-01-09 01:45:49 PM
Policy:                    Installation Demo Policy (#9606)
Command-line:           Enabled
Orbital:                Enabled (Running)
Behavioural Protection: Protect
Faults:                    None
```

To verify that the connector is connected, you can confirm the existence of the installation event in the Secure Endpoint Console:

1. Navigate to the `Events` page.



Events

▼ Filter: (New)

Select a Filter

Event Type: All Event Types

Group: All Groups

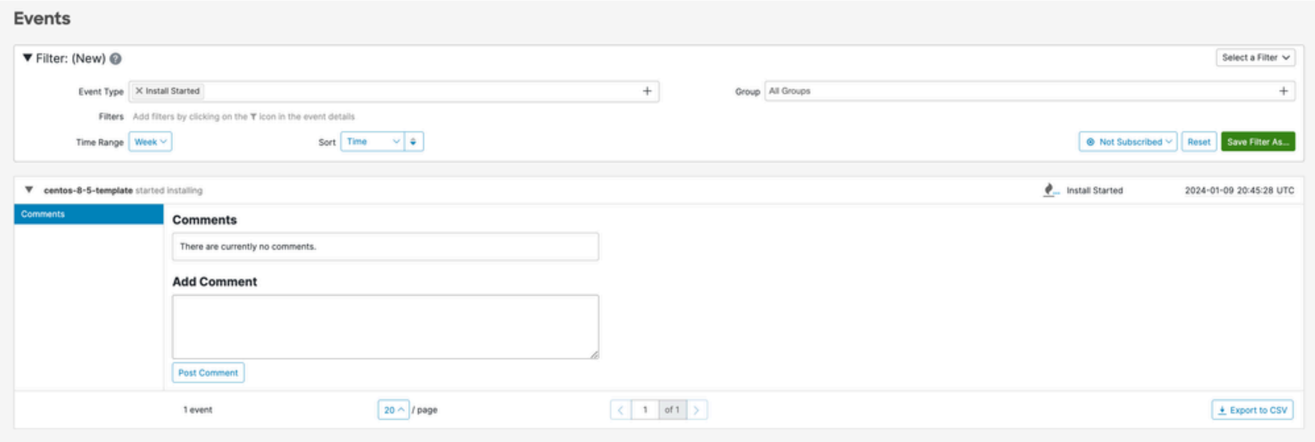
Filters: Add filters by clicking on the ▼ icon in the event details

Time Range: Week

Sort: Time

▸ centos7-buildsrv	High	Retrospective Restore: Su...	2024-01-10 21:02:23 UTC
▸ centos7-buildsrv	High	Retrospective Quarantine...	2024-01-10 21:02:23 UTC
▸ centos7-buildsrv		Retrospective Restore: Su...	2024-01-10 21:02:22 UTC
▸ centos7-buildsrv	High	Retrospective Restore: Su...	2024-01-10 21:02:21 UTC
▸ centos7-buildsrv	High	Retrospective Quarantine...	2024-01-10 21:02:21 UTC
▸ centos7-buildsrv		Retrospective Restore: Su...	2024-01-10 21:02:20 UTC
▸ centos7-buildsrv	High	Retrospective Restore: Su...	2024-01-10 21:02:20 UTC
▸ centos7-buildsrv	High	Retrospective Quarantine...	2024-01-10 21:02:20 UTC
▸ centos7-buildsrv		Retrospective Restore: Su...	2024-01-10 21:02:20 UTC
▸ centos7-buildsrv	High	Retrospective Restore: Su...	2024-01-10 21:02:18 UTC
▸ centos7-buildsrv	High	Retrospective Quarantine...	2024-01-10 21:02:18 UTC
▸ centos7-buildsrv		Retrospective Restore: Su...	2024-01-10 21:02:18 UTC
▸ centos7-buildsrv	High	Retrospective Restore: Su...	2024-01-10 21:02:17 UTC
▸ centos7-buildsrv	High	Retrospective Quarantine...	2024-01-10 21:02:17 UTC
▸ centos7-buildsrv		Retrospective Restore: Su...	2024-01-10 21:02:17 UTC
▸ centos7-buildsrv	High	Retrospective Restore: Su...	2024-01-10 21:02:17 UTC
▸ centos7-buildsrv	High	Retrospective Quarantine...	2024-01-10 21:02:17 UTC

2. Locate the installation event for your connector. It should be categorized under the `Install Started` event type.


Events

▼ Filter: (New)

Select a Filter

Event Type: ✕ Install Started

Group: All Groups

Filters: Add filters by clicking on the ▼ icon in the event details

Time Range: Week

Sort: Time

▼ **centos-8-5-template** started installing — Install Started — 2024-01-09 20:45:28 UTC

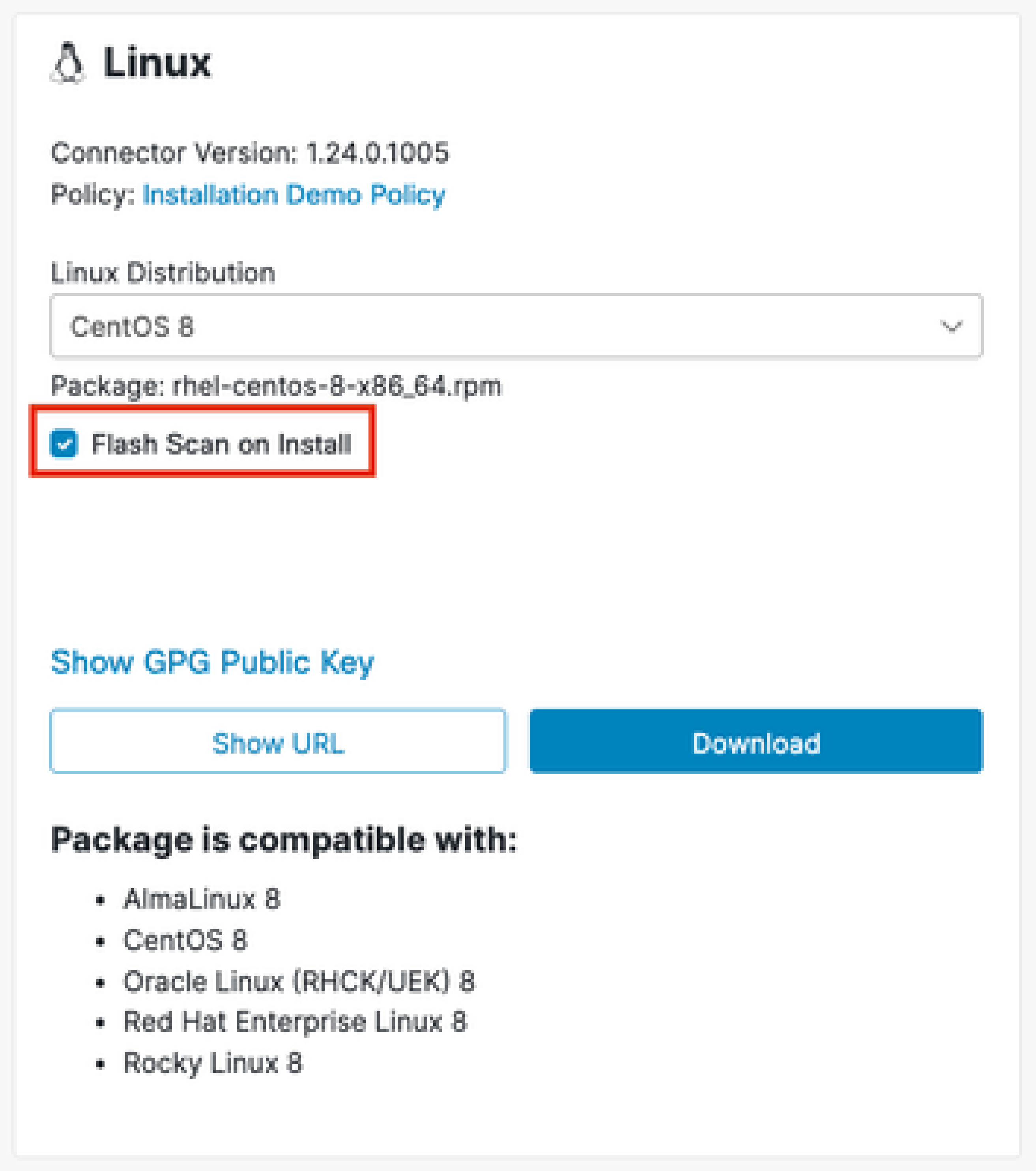
Comments

There are currently no comments.

Add Comment

1 event — 20 / page — 1 of 1

3. If you selected the checkbox to `Flash Scan on Install` when downloading the connector, then you can also confirm that the existence of two scan events.



Linux

Connector Version: 1.24.0.1005

Policy: Installation Demo Policy

Linux Distribution

CentOS 8

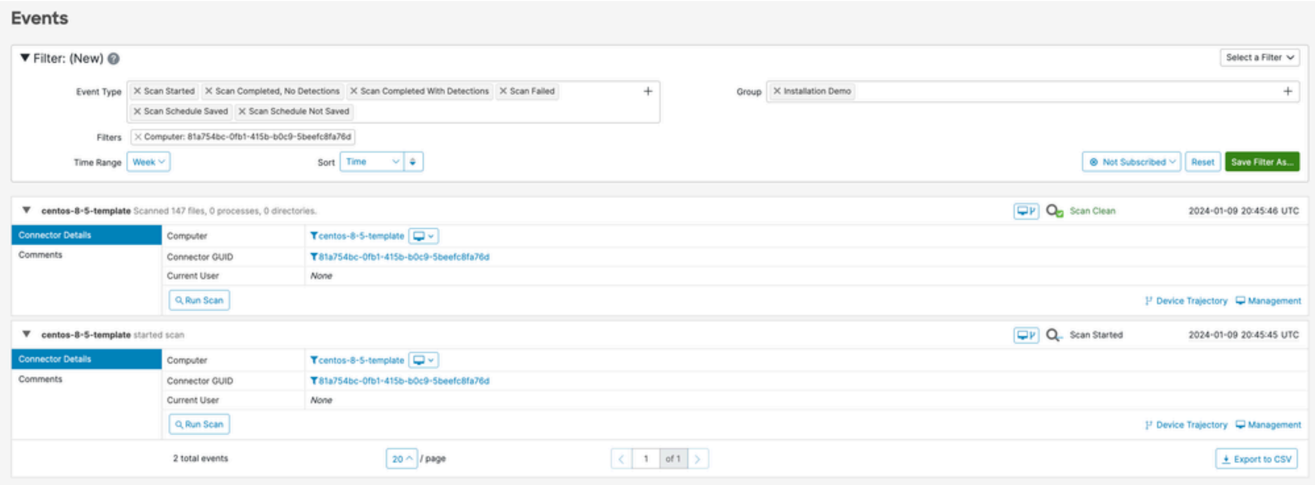
Package: rhel-centos-8-x86_64.rpm

☑ Flash Scan on Install

Package is compatible with:

- AlmaLinux 8
- CentOS 8
- Oracle Linux (RHCK/UEK) 8
- Red Hat Enterprise Linux 8
- Rocky Linux 8

4. Locate the scan events for you connector by filtering by the `Scan` event types. Note: you can also narrow down your search by adding filters for Group and Connector GUID. You should see two events corresponding to the start and end of the scan.



Events

Filter: (New)

Event Type: Scan Started, Scan Completed, No Detections, Scan Completed With Detections, Scan Failed, Scan Schedule Saved, Scan Schedule Not Saved

Group: Installation Demo

Filters: Computer: 81a754bc-0fb1-415b-b0c9-5beefc8fa76d

Time Range: Week

Sort: Time

centos-8-5-template Scanned 147 files, 0 processes, 0 directories. — Scan Clean — 2024-01-09 20:45:46 UTC

Connector Details		
Comments	Computer	centos-8-5-template
	Connector GUID	81a754bc-0fb1-415b-b0c9-5beefc8fa76d
	Current User	*None*

centos-8-5-template started scan — Scan Started — 2024-01-09 20:45:45 UTC

Connector Details		
Comments	Computer	centos-8-5-template
	Connector GUID	81a754bc-0fb1-415b-b0c9-5beefc8fa76d
	Current User	*None*

2 total events — 20 / page — 1 of 1

Uninstall the Linux Connector

RPM-based

1. Uninstall the Linux connector using the systems package manager.
   - Via YUM:

     ```
     sudo yum remove ciscoampconnector -y
     ```

   - Via Zypper:

     ```
     sudo zypper remove -y ciscoampconnector
     ```

2. Purge the Linux connector by running the provided purge script.

   ```
   /opt/cisco/amp/bin/purge_amp_local_data
   ```

Debian-based

1. Uninstall the Linux connector using the systems package manager.

   ```
   sudo dpkg --remove cisco-orbital ciscoampconnector
   ```

2. Purge the Linux connector by running the provided purge script.

   ```
   sudo dpkg --purge cisco-orbital ciscoampconnector
   ```

Please refer to the Secure Endpoint User Guide for more detailed uninstall instructions.

See Also

- Install Cisco Secure Endpoint Connector on RHEL video
- Linux Kernel-Devel Fault
  - Resolve Cisco Secure Endpoint Linux Kernel-Devel Fault video
- Secure Endpoint User Guide

- Technical Support & Documentation - Cisco Systems
- Troubleshoot Secure Endpoint Linux Faults
- Verify Secure Endpoint Linux Connector OS Compatibility