Secure Endpoint Software Support Policy

Contents

Introduction

This document describes the Support Policy for Cisco Secure Endpoint software.

This Support Policy is effective as of September 5th, 2022.

Support Policy

Cisco's Support Policy for Secure Endpoint software applies to:

- Secure Endpoint Connector software for Windows, Linux, and macOS.
- Secure Endpoint Private Cloud software.

Cisco's Support Policy for Secure Endpoint software does **NOT** apply to:

- Private Cloud appliance hardware. Refer to Cisco’s End-of-Life Policy for Private Cloud appliance hardware support.
- Secure Endpoint Connector for iOS and Android. The Apple App Store and Google Play store provide only the latest available Secure Endpoint Connector versions for iOS and Android, respectively.

Standard Support Policy

Cisco will provide technical support through the Technical Assistance Center (TAC) and bug fixes for Secure Endpoint software, for a minimum of one year after the release of each software version. After one year, the version will no longer be supported for future bug fixes, except for software versions specifically published for legacy operating system support. If you experience a problem with an unsupported software version, you may be asked to validate whether a newer maintenance release or most current release resolves your issue.

Secure Endpoint software support on all operating systems will align with the vendor’s published end-of-support schedule. The Secure Endpoint Standard Support Policy ends and is replaced by the Long Term

Support (LTS) Policy when the vendor's published extended support begins. LTS is not available for operating systems whose vendors do not offer extended support, such as macOS.

Secure Endpoint software versions may require an operating system patch or upgrade to a newer version as necessary for compatibility, access to all features, or bug fixes.

The Secure Endpoint Consoles display Secure Endpoint software versions that are officially supported. Software versions may be removed from the console when the software is no longer supported.

Secure Endpoint and Secure Endpoint Private Cloud connectors release on different schedules. Refer to the release notes for each deployment type to determine the most recently supported Secure Endpoint connector versions:

- Secure Endpoint Private Cloud Release Notes
- Secure Endpoint Release Notes

Long Term Support (LTS) Policy

Secure Endpoint software support on all operating systems aligns with the vendor’s published end-of-support schedule.

The Secure Endpoint LTS Policy begins when the vendor's published extended support period starts. Cisco requires the customer to maintain all necessary extended support contracts to ensure the endpoint operating system has active vendor support. During the LTS period, Cisco provides technical support through TAC, bug fixes, and security patches for the Secure Endpoint software.

Support for Secure Endpoint software versions is limited to critical maintenance releases and security patches, they do not contain new features.

Customers are required keep their legacy operating systems patched with the latest updates and their Secure Endpoint LTS software updated to the most recent version to receive technical support.

Connector

See the following documents for details on supported and unsupported Secure Endpoint connector software for specific operating systems.

Windows

- Cisco Secure Endpoint Windows Connector OS Compatibility

Linux

- Cisco Secure Endpoint Linux Connector OS Compatibility
- Cisco Secure Endpoint Linux Connector Long Term Support

Mac

- Cisco Secure Endpoint Mac Connector OS Compatibility

Private Cloud

See the following document for details on supported and unsupported Private Cloud software:

- End-of-Support Announcement for AMP for Endpoints/Secure Endpoint Private Cloud Versions

Exceptions

Pre-release Secure Endpoint Software Versions

Pre-release versions such as betas and early field tests do not follow the Standard Support Policy. The deployment of pre-release software is supported and governed by the respective agreement during participation. Technical support is not provided for pre-release versions of software unless specifically defined by the agreement for the program.

Any support provided for pre-release versions will end once the associated official release version is made available. Customers who wish to access the new features after the beta ends will need to move to the publicly available and officially supported Secure Endpoint software version.

One-off Removal

While Cisco will make every attempt to avoid the case, it may be necessary to remove a released Secure Endpoint software version due to the severity or frequency of issues seen in-field or to address security concerns. In that event, Cisco may remove the Secure Endpoint software version and do one of the following:

1. Make available a new version that addresses the issues.
2. Provide a recommendation on which version customers should upgrade to.

If a Secure Endpoint software version is removed, it will be unavailable for download. For connector software, the removed version will not be configurable for upgrade through policy settings. These changes may require a scheduled release of the Private or Public Secure Endpoint Console or Private Cloud software and will be made available at the earliest opportunity.

Use of Secure Endpoint Software Beyond the Support Policy

Cisco recommends that customers upgrade their Secure Endpoint software to the latest version to ensure access to the latest features and security patches. Cisco cannot guarantee that Secure Endpoint software will continue to function and connect to the Secure Endpoint Cloud or Secure Endpoint Private Cloud after they are no longer supported by the Support Policy, as they may no longer be compatible with the most current cloud technology.

Unsupported Secure Endpoint connector versions will be removed from the Secure Endpoint Consoles and will no longer be available for deployment via connector policy settings. Secure Endpoint connector policies that are configured to upgrade to an unsupported connector version will be automatically updated to remove the configuration.

Unsupported Secure Endpoint software still in use may run at a reduced capacity due to lack of features available in newer releases and may also contain unaddressed security concerns. Any Secure Endpoint software installation packages that were downloaded prior to the end of support should not be installed once support has ended.

Refer to each Secure Endpoint connector software OS compatibility articles for details on currently supported distributions:

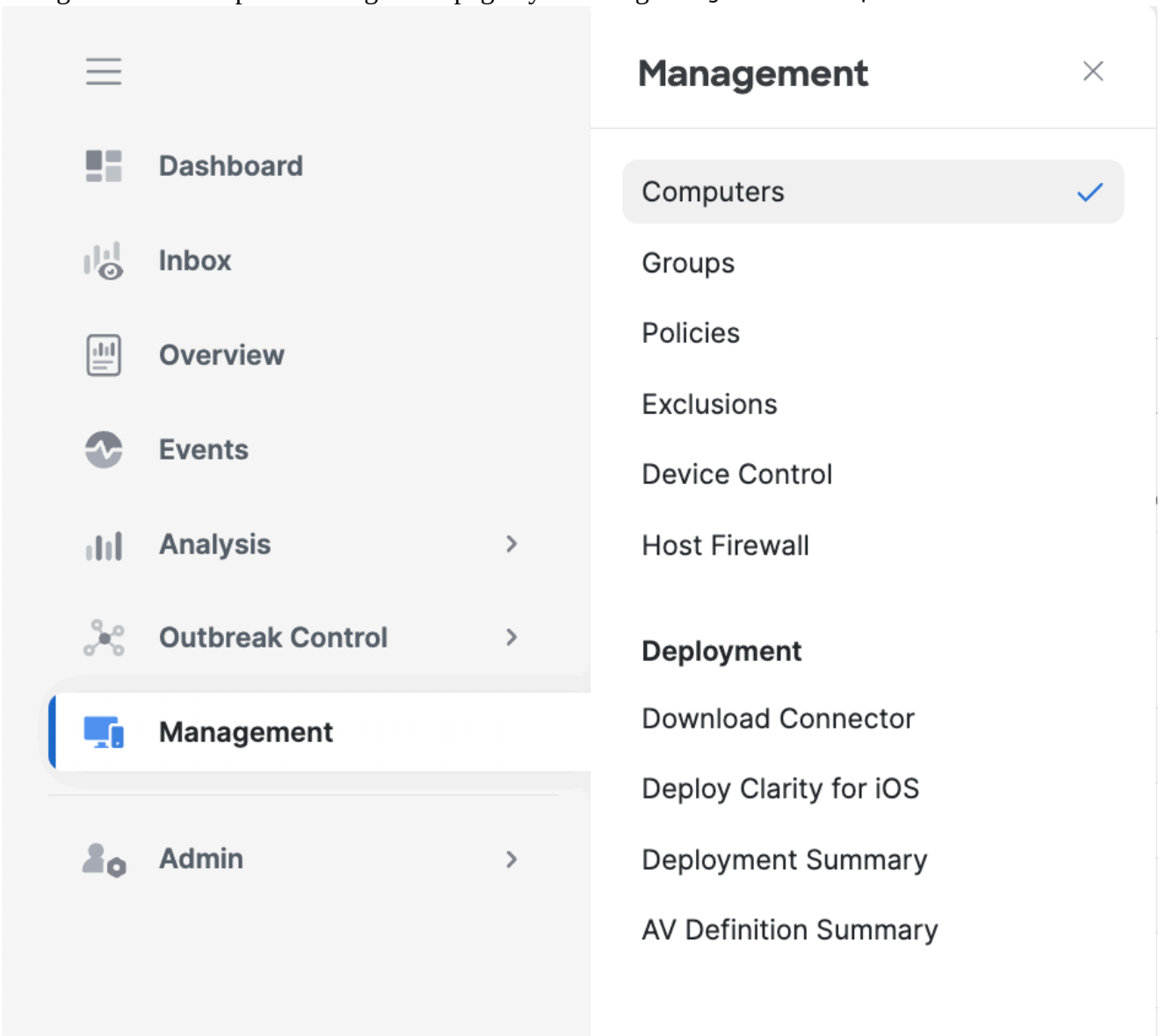
- Cisco Secure Endpoint Windows Connector OS Compatibility
- Cisco Secure Endpoint Linux Connector OS Compatibility

- Cisco Secure Endpoint Mac Connector OS Compatibility

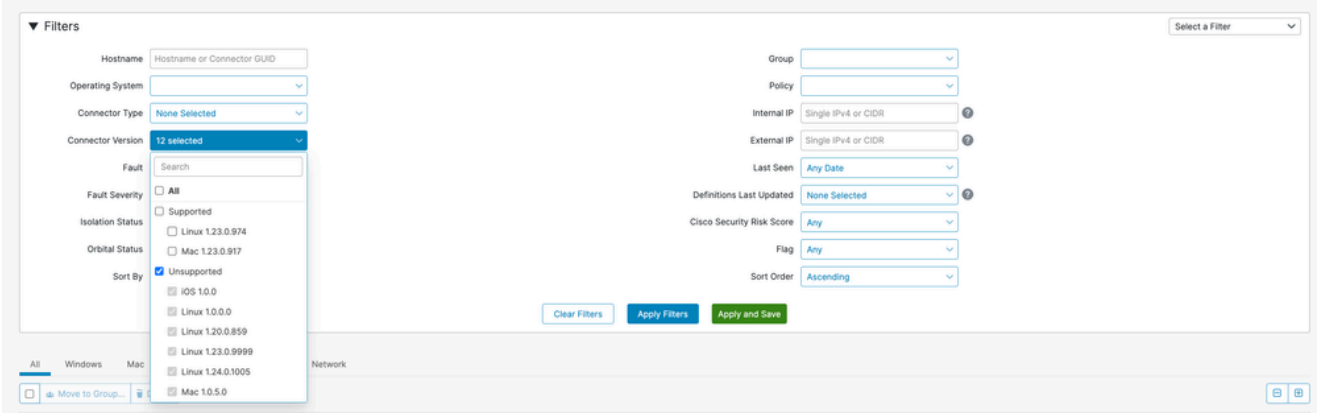
Appendix A: Identify Deployed Unsupported Secure Endpoint Connectors

Unsupported Secure Endpoint connectors that are currently deployed can be identified in the Secure Endpoint Console:

1. Navigate to the Computer Management page by selecting `Management` -> `Computers`.



2. Expand `Filters`, and select `Unsupported` from the Connector Version drop-down menu. Click `Apply Filters`.



This will show all devices currently running an unsupported connector version.

Appendix B: Secure Endpoint Software Support Policy Revision History Table

Revision	Publish Date	Comments
3.0	21-February-2024	Reorganized the policy into sections: Standard Support Policy and LTS Support Policy. Removed FAQ section. Made support policy more generic to apply to Private Cloud and Connectors.
2.0	01-August-2022	Updated the process to determine the end of support for connector software from a version-based to a time-based support policy. This policy is now applicable to Private Cloud software, Private Cloud Virtual appliance, and all Connector operating systems. Added language to call out support for legacy operating systems. Updated FAQs.
1.0	07-Apr-2020	Initial Publish