Politique d'assistance logicielle Secure Endpoint

Table des matières

Introduction

Politique de support

- Politique de support standard
- Politique d'assistance à long terme (LTS)
  - Connecteur
  - Cloud privé
- Exceptions
  - Versions logicielles de point de terminaison sécurisé pré-version
  - Retrait unique

Utilisation du logiciel Secure Endpoint au-delà de la politique de support

Annexe A : Identifier les connecteurs de terminaux sécurisés non pris en charge

Annexe B : Tableau Historique des révisions de la politique de support logiciel Secure Endpoint

Introduction

Ce document décrit la politique de support pour le logiciel Cisco Secure Endpoint.

La présente politique d'assistance est en vigueur à compter du 7 juillet 2026.

Politique de support

La politique d'assistance de Cisco pour le logiciel Secure Endpoint s'applique aux éléments suivants :

- Logiciel Secure Endpoint Connector pour Windows, Linux et macOS.
- Logiciel de cloud privé Secure Endpoint.

La politique d'assistance de Cisco pour le logiciel Secure Endpoint ne s'applique PAS aux éléments suivants :

- Matériel d'appliance de cloud privé. Reportez-vous à la politique de fin de vie de Cisco pour la prise en charge matérielle des appliances de cloud privé.
- Connecteur de terminal sécurisé pour iOS et Android. L'App Store d'Apple et le Google Play Store ne proposent que les dernières versions disponibles du connecteur Secure Endpoint Connector pour iOS et Android, respectivement.

Politique de support standard

Cisco fournira une assistance technique par l'intermédiaire du centre d'assistance technique

(TAC) et des correctifs de bogues pour le logiciel Secure Endpoint, pendant au moins un an après la publication de chaque version logicielle. Après cette période, la version ne sera plus prise en charge pour les corrections de bogues futures, à l'exception des versions logicielles spécifiquement publiées pour la prise en charge des systèmes d'exploitation hérités. Si vous rencontrez un problème avec une version de logiciel non prise en charge, il peut vous être demandé de vérifier si une version de maintenance plus récente ou la version la plus récente résout votre problème.

La prise en charge du logiciel Secure Endpoint sur tous les systèmes d'exploitation sera alignée sur le calendrier de fin de prise en charge publié par le fournisseur. La politique d'assistance standard pour les terminaux sécurisés se termine et est remplacée par la politique d'assistance à long terme (LTS) lorsque la prise en charge étendue publiée par le fournisseur commence. LTS n'est pas disponible pour les systèmes d'exploitation dont les fournisseurs n'offrent pas de prise en charge étendue, tels que macOS.

Les versions du logiciel Secure Endpoint peuvent nécessiter un correctif du système d'exploitation ou une mise à niveau vers une version plus récente pour des raisons de compatibilité, d'accès à toutes les fonctionnalités ou de correction de bogues.

Les consoles Secure Endpoint affichent les versions du logiciel Secure Endpoint officiellement prises en charge. Les versions logicielles peuvent être supprimées de la console lorsque le logiciel n'est plus pris en charge.

Les connecteurs Secure Endpoint et Secure Endpoint Private Cloud sont disponibles selon des calendriers différents. Reportez-vous aux notes de version de chaque type de déploiement pour déterminer les dernières versions de connecteur Secure Endpoint prises en charge :

- Notes de version du cloud privé Secure Endpoint
- Notes de version de Secure Endpoint

Politique d'assistance à long terme (LTS)

La stratégie LTS de point de terminaison sécurisé commence au début de la période de prise en charge étendue publiée par le fournisseur. Cisco exige du client qu'il maintienne tous les contrats d'assistance étendus nécessaires pour garantir que le système d'exploitation du terminal bénéficie d'une assistance fournisseur active. Au cours de la période LTS, Cisco fournit une assistance technique via le centre d'assistance technique, des correctifs de bogues et des correctifs de sécurité pour le logiciel Secure Endpoint.

La prise en charge des versions logicielles de Secure Endpoint est limitée aux versions de maintenance critiques et aux correctifs de sécurité, car elles ne contiennent pas de nouvelles fonctionnalités.

Pour bénéficier d'une assistance technique, les clients doivent mettre à jour leur système d'exploitation existant avec les mises à jour les plus récentes et leur logiciel Secure Endpoint LTS avec la version la plus récente.

Connecteur

Pour plus d'informations sur les logiciels de connecteur Secure Endpoint pris en charge et non pris en charge pour des systèmes d'exploitation spécifiques, consultez les documents suivants.

Fenêtres

- Compatibilité du système d'exploitation Cisco Secure Endpoint Connector Windows

Linux

- Compatibilité du système d'exploitation avec Cisco Secure Endpoint Linux Connector
- Prise en charge à long terme du connecteur Linux Cisco Secure Endpoint

Mac

- Compatibilité du système d'exploitation avec Cisco Secure Endpoint Mac Connector

Cloud privé

Pour plus d'informations sur les logiciels de cloud privé pris en charge et non pris en charge, consultez le document suivant :

- Annonce de fin de prise en charge des versions AMP pour terminaux/cloud privé pour terminaux sécurisés

Exceptions

Versions logicielles de point de terminaison sécurisé pré-version

Les versions préliminaires telles que les bêtas et les premiers tests sur site ne respectent pas la politique de support standard. Le déploiement des logiciels de pré-version est pris en charge et régi par le contrat correspondant lors de la participation. L'assistance technique n'est pas fournie pour les versions précommerciales du logiciel, sauf si le contrat du programme le définit spécifiquement.

Toute assistance fournie pour les versions préliminaires prendra fin une fois que la version officielle associée sera disponible. Les clients qui souhaitent accéder aux nouvelles fonctionnalités après la fin de la version bêta devront passer à la version du logiciel Secure Endpoint, disponible publiquement et officiellement prise en charge.

Retrait unique

Bien que Cisco fasse tout son possible pour éviter le problème, il peut être nécessaire de supprimer une version logicielle Secure Endpoint en raison de la gravité ou de la fréquence des problèmes constatés sur le terrain ou pour résoudre les problèmes de sécurité. Dans ce cas, Cisco peut supprimer la version du logiciel Secure Endpoint et effectuer l'une des opérations suivantes :

1. Mettre à disposition une nouvelle version qui résout les problèmes.
2. Fournir une recommandation sur la version vers laquelle les clients doivent effectuer la mise à niveau.

Si une version du logiciel Secure Endpoint est supprimée, elle ne pourra pas être téléchargée. Pour le logiciel du connecteur, la version supprimée ne sera pas configurable pour une mise à niveau via les paramètres de stratégie. Ces modifications peuvent nécessiter une version programmée du logiciel Private Endpoint Console ou Public Secure Endpoint Console ou Private Cloud et seront disponibles dès que possible.

Utilisation du logiciel Secure Endpoint au-delà de la politique de support

Cisco recommande aux clients de mettre à niveau leur logiciel Secure Endpoint vers la dernière version afin de garantir l'accès aux dernières fonctionnalités et correctifs de sécurité. Cisco ne peut pas garantir que le logiciel Secure Endpoint continuera à fonctionner et à se connecter au cloud Secure Endpoint ou au cloud privé Secure Endpoint une fois qu'ils ne seront plus pris en charge par la politique d'assistance, car ils peuvent ne plus être compatibles avec la technologie cloud la plus récente.

Les versions non prises en charge des connecteurs Secure Endpoint seront supprimées des consoles Secure Endpoint et ne seront plus disponibles pour le déploiement via les paramètres de stratégie de connecteur. Les stratégies de connecteur Secure Endpoint configurées pour une mise à niveau vers une version de connecteur non prise en charge seront automatiquement mises à jour pour supprimer la configuration.

Les logiciels Secure Endpoint non pris en charge encore utilisés peuvent fonctionner à une capacité réduite en raison du manque de fonctionnalités disponibles dans les versions plus récentes et peuvent également contenir des problèmes de sécurité non résolus. Les packages d'installation de Secure Endpoint qui ont été téléchargés avant la fin de la prise en charge ne doivent pas être installés une fois la prise en charge terminée.

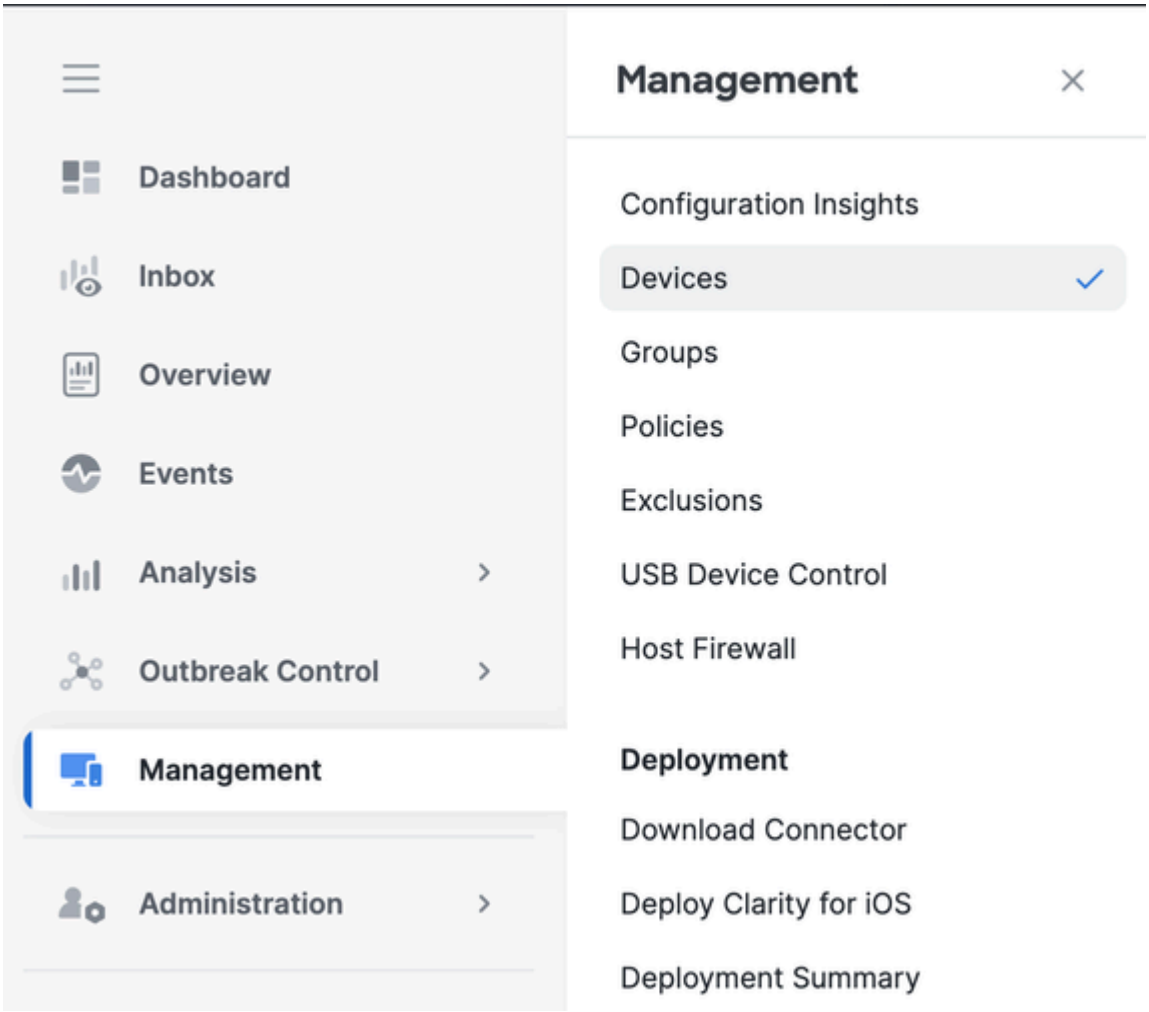
Reportez-vous aux articles sur la compatibilité du système d'exploitation de chaque connecteur Secure Endpoint pour plus de détails sur les distributions actuellement prises en charge :

- Compatibilité du système d'exploitation Cisco Secure Endpoint Connector Windows
- Compatibilité du système d'exploitation avec Cisco Secure Endpoint Linux Connector
- Compatibilité du système d'exploitation avec Cisco Secure Endpoint Mac Connector

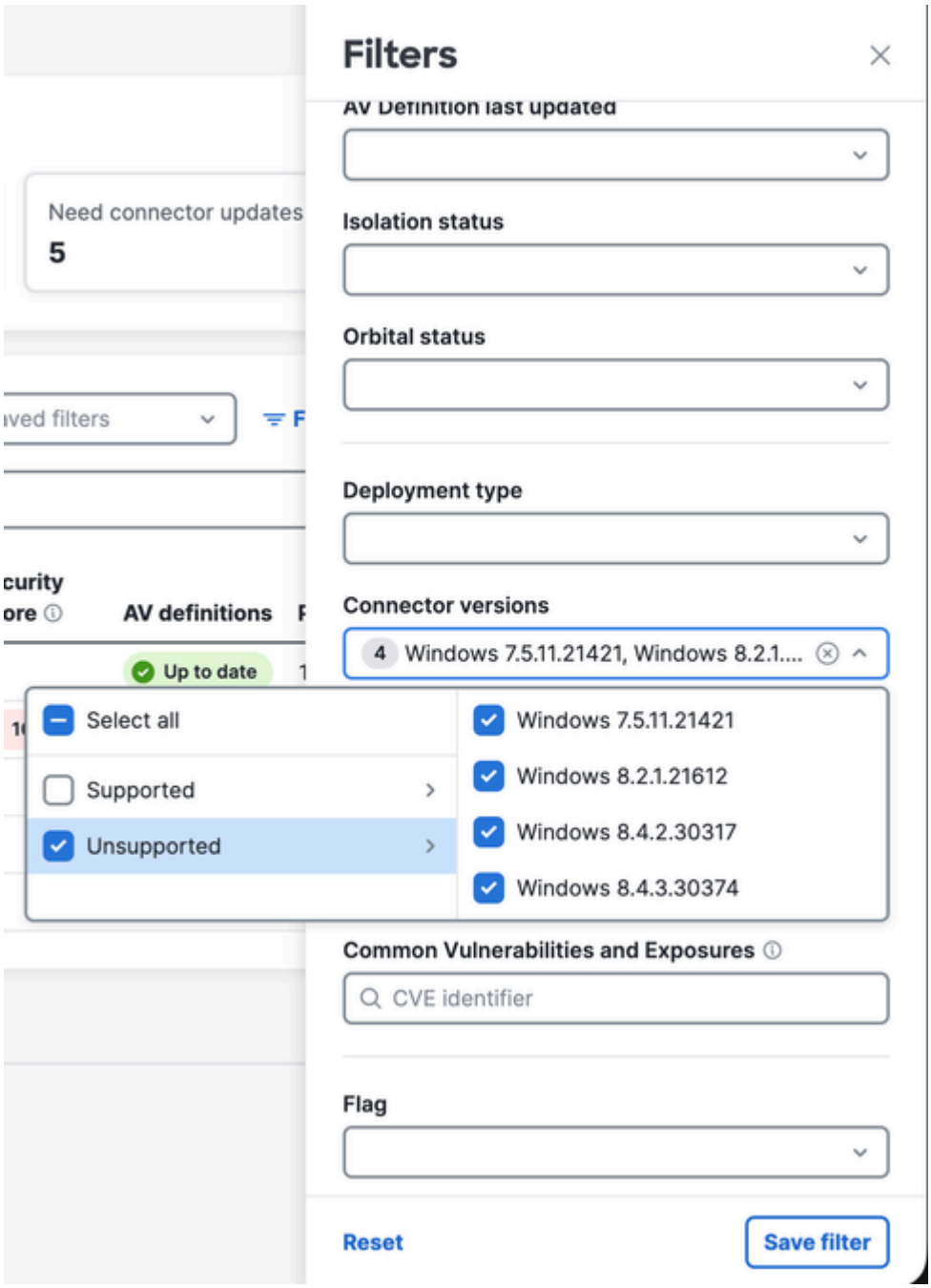
Annexe A : Identifier les connecteurs de terminaux sécurisés non pris en charge

Les connecteurs Secure Endpoint actuellement déployés, qui ne sont pas pris en charge, peuvent être identifiés dans la console Secure Endpoint :

1. Accédez à la page Device Management en sélectionnant `Management` -> `Devices`.



2. Développez `Filters`, puis sélectionnez `Unsupported` dans le menu déroulant Connector Versions. Cliquez sur `Enregistrer le filtre`.



Tous les périphériques exécutant actuellement une version de connecteur non prise en charge s'affichent.

Annexe B : Tableau Historique des révisions de la politique de support logiciel Secure Endpoint

Révision	Date de publication	Commentaires
4.0	30-juin-2026	Liens mis à jour vers les notes de version et les tableaux de compatibilité des systèmes d'exploitation. Captures d'écran mises à jour pour refléter les modifications apportées à la console.

3.0	21-février-2024	Réorganisation de la politique en sections : Politique de support standard et politique de support LTS. Section FAQ supprimée. La stratégie d'assistance a été rendue plus générique pour s'appliquer au cloud privé et aux connecteurs.
2.0	01-août-2022	Mise à jour du processus de détermination de la fin de la prise en charge du logiciel de connexion d'une politique de prise en charge basée sur la version à une politique de prise en charge basée sur le temps. Cette politique s'applique désormais aux logiciels de cloud privé, à l'appliance de cloud privé virtuel et à tous les systèmes d'exploitation Connector. Ajout d'un langage pour indiquer la prise en charge des systèmes d'exploitation hérités. FAQ mises à jour.
1.0	07-avr-2020	Publication initiale

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.