

Politique de prise en charge du connecteur Secure Endpoint

Contenu

[Introduction](#)

[Policy \(politique\)](#)

[Exceptions](#)

[Références supplémentaires](#)

[Forum aux questions](#)

Introduction

Ce document décrit la politique de prise en charge du logiciel Secure Endpoint Connector.

Policy (politique)

Cisco publie la présente Politique de support pour les logiciels d'administration de cloud privé, les appareils virtuels de cloud privé et les logiciels Secure Endpoints Connector hébergés sur le cloud de terminal sécurisé ou le cloud privé.

Cisco fournira une assistance technique (TAC), des correctifs de bogues et des améliorations de produits pour le logiciel Private Cloud Administration, Private Cloud Virtual Appliance ou Secure Endpoint Connector pendant au moins un an après la sortie de chaque version logicielle. La date de sortie du connecteur Secure Endpoint pour le cloud public Secure Endpoints et le cloud privé peut varier en fonction de la date de sortie de la même version de connecteur pour chaque type de déploiement. Au bout d'un an, la version ne sera plus prise en charge pour les correctifs de bogues et les améliorations de produits ultérieurs, à l'exception des versions de connecteur 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 connecteur Secure Endpoint sur tous les systèmes d'exploitation sera conforme au calendrier de fin de prise en charge publié par le fournisseur. La prise en charge par Cisco des systèmes d'exploitation existants, tels que ceux de la prise en charge étendue, exige du client qu'il maintienne tous les contrats de prise en charge étendue nécessaires pour s'assurer que le système d'exploitation du terminal bénéficie d'une prise en charge fournisseur active.

Les versions antérieures d'un système d'exploitation peuvent nécessiter l'exécution d'une version spécifique du logiciel du connecteur Secure Endpoint pour bénéficier d'une assistance technique. La version spécifique conservera la compatibilité du système d'exploitation, mais ne recevra peut-être pas toutes les nouvelles fonctionnalités et mises à jour du produit uniquement pour les corrections de bogues critiques. Le test des logiciels Secure Endpoint et des chemins de mise à niveau sera limité aux versions prises en charge, comme indiqué dans cette stratégie.

Les prochaines versions de Secure Endpoint Cloud et de la console Private Cloud seront limitées

à l'affichage et au téléchargement des versions du connecteur Secure Endpoint officiellement prises en charge. Le site Web Secure Endpoint Private Cloud sera mis à jour pour afficher uniquement et permettre le téléchargement des versions prises en charge du logiciel Private Cloud. Les versions de console Secure Endpoint Cloud ou Private Cloud peuvent supprimer les versions non prises en charge une fois que le logiciel n'est plus pris en charge.

Jalon

Politique de support publiée

Date d'effet

Date

4 août 2022

5 septembre 2022

Tableau 1. Calendrier des politiques

Ce tableau présente les étapes de la politique d'assistance annoncée.

À la date de publication de la présente politique de support, l'[annonce de fin de support pour les versions de connecteur de terminal sécurisé](#) a été faite pour détailler les versions spécifiques de connecteur de terminal sécurisé immédiatement affectées par cette politique de support.

Exceptions

- Versions précommerciales

Les versions pré-commercialisation telles que les versions bêta et les premiers tests sur site ne respectent pas la politique d'assistance standard et sont régies par l'assistance fournie pendant la période bêta.

- Retrait unique

Bien que Cisco fasse tout son possible pour éviter le problème, il peut être nécessaire de supprimer une version du connecteur Secure Endpoints 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, nous pouvons supprimer et soit 1) rendre disponible une nouvelle version qui résout les problèmes ou 2) fournir une recommandation sur la version vers laquelle les clients doivent effectuer la mise à niveau. Si un connecteur est retiré, sa version peut ne pas être téléchargeable et ne pas être configurable pour une mise à niveau via les paramètres de stratégie de connecteur. Ces modifications peuvent nécessiter une version planifiée de la console Secure Endpoint ou du logiciel de cloud privé et seront disponibles dès que possible.

- Compatibilité du système d'exploitation

Certaines fonctionnalités du connecteur peuvent nécessiter une mise à niveau vers le système d'exploitation ou le niveau de correctif le plus récent, car elles peuvent dépendre de la compatibilité ou des capacités du système d'exploitation installé. Par conséquent, toutes les fonctionnalités Secure Endpoint ne sont pas disponibles sur toutes les versions d'un système d'exploitation et peuvent nécessiter une mise à niveau pour que toutes les fonctionnalités soient disponibles pour le connecteur.

- Versions plus anciennes du connecteur

Les versions du connecteur Secure Endpoint pour les systèmes d'exploitation anciens ou anciens peuvent ne pas avoir toutes les fonctionnalités et fonctionnalités rétroportées en raison de limitations techniques. La prise en charge des versions de connecteur sur ces systèmes d'exploitation sera limitée aux versions de maintenance et aux correctifs critiques et ne garantit pas la prise en charge des nouvelles fonctionnalités.

Références supplémentaires

[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](#)

[Notes de version de Secure Endpoint](#)

[Notes de version du cloud privé Secure Endpoint](#)

Forum aux questions

Q : Quand la politique d'assistance entrera-t-elle en vigueur ?

A : Cette politique d'assistance a été annoncée le 1er août 2022 et entrera en vigueur le 1er septembre 2022. La version originale de la politique de support est remplacée par la version actuelle.

Q : Les connecteurs de terminaux sécurisés continueront-ils à fonctionner une fois qu'ils ne seront plus pris en charge par la politique de support ?

A : Oui, les connecteurs de terminaux sécurisés continueront à fonctionner et à se connecter au cloud de terminaux sécurisés ou au cloud privé pour les services de destruction, mais ils 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. Dans certains cas, les versions plus anciennes des connecteurs risquent de ne plus fonctionner ou de ne plus pouvoir communiquer avec le nuage de points d'extrémité sécurisés et nécessiteront une mise à niveau en raison de modifications techniques au fur et à mesure du développement du nuage de points d'extrémité sécurisés. Référez-vous la [Notes de version de Secure Endpoints](#) qui contient des détails sur les dernières fonctionnalités et mises à jour de sécurité pour chaque version. Nous vous recommandons d'effectuer une mise à niveau vers la dernière version du connecteur pour vous assurer que vous pouvez accéder aux dernières fonctionnalités et disposer des correctifs de sécurité les plus récents.

Q : Ai-je accès aux versions des connecteurs qui ont été étendues au-delà de la politique de support ?

A : Les connecteurs activement déployés dans votre environnement continueront à fonctionner et à se connecter au cloud de terminaux sécurisés. Toutefois, ils ne pourront pas bénéficier d'une assistance technique et ne disposeront peut-être pas de toutes les fonctionnalités du produit et mises à jour de sécurité. Les connecteurs qui ne sont plus pris en charge comme défini dans la politique de support seront supprimés pour téléchargement et ne seront plus disponibles pour déploiement via les paramètres de la politique de connecteur dans les versions futures de la console Secure Endpoint Cloud et Private Cloud. Les stratégies déjà configurées pour la mise à niveau vers une version de connecteur non prise en charge seront automatiquement mises à jour pour supprimer la configuration. Pour les systèmes d'exploitation pris en charge par le passé, des versions spécifiques du logiciel Secure Endpoint Connector devront être compatibles avec un système d'exploitation existant et continuer à bénéficier d'une assistance technique.

Q : Puis-je toujours déployer une ancienne version de connecteur que j'ai téléchargée précédemment ?

A : Oui, il est possible que d'anciennes versions de connecteur déjà téléchargées soient toujours déployées, mais vous ne pourrez pas télécharger une version de connecteur déjà supprimée de la console Secure Endpoint. Le déploiement de versions non prises en charge n'est pas recommandé car il peut manquer de nouvelles fonctionnalités de produit, d'importants correctifs de sécurité ou ne plus être compatible avec la technologie cloud la plus récente. En outre, aucune assistance technique ne sera fournie et vous devrez peut-être effectuer une mise à niveau vers une version actuellement prise en charge avant de bénéficier de l'assistance technique pour ces connecteurs.

Q : Comment puis-je savoir quelles versions non prises en charge des connecteurs Secure Endpoint sont déployées dans mon environnement ?

A : La console Secure Endpoint offre plusieurs moyens de rechercher et d'afficher les connecteurs non pris en charge. La page Gestion de l'ordinateur (Gestion -> Ordinateurs) permet de filtrer manuellement la liste des connecteurs déployés pour afficher les connecteurs non pris en charge. Sur la page Ordinateurs, développez Filtres et sélectionnez « Non pris en charge » dans le menu déroulant Version du connecteur. Tous les périphériques exécutant une version de connecteur non prise en charge s'affichent. Le panneau Ordinateur de l'onglet Vue d'ensemble du tableau de bord affiche également un graphique indiquant le pourcentage de connecteurs non pris en charge dans votre environnement. Cliquez sur « Fin de vie » pour accéder automatiquement à la page de gestion de l'ordinateur préfiltrée et afficher les périphériques concernés.

Q : Comment les versions bêta ou les premières versions de connecteur d'essai sur site sont-elles prises en charge avec la politique de support ?

A : Le déploiement du logiciel Secure Endpoint pre-release est pris en charge par chaque équipe et est régi par le contrat respectif lors de la participation. Les clients qui souhaitent accéder aux nouvelles fonctionnalités après la fin de la version bêta devront suivre les instructions pour passer à la version de connecteur disponible publiquement et officiellement prise en charge. Il n'existe aucune assistance technique pour les versions précommerciales des logiciels, sauf si l'équipe chargée de la gestion du programme le définit spécifiquement.

Q : Comment les versions du connecteur de cloud privé Secure Endpoint seront-elles affectées ?

A : Cette politique de support s'applique au cloud de terminaux sécurisés et au cloud privé de terminaux sécurisés. En raison de la cadence de publication différente pour le cloud privé Secure Endpoint, les dates de publication des versions de connecteur disponibles sur chaque modèle de déploiement peuvent différer de celles du cloud Secure Endpoint, mais le même calendrier de prise en charge des connecteurs s'applique toujours en fonction de la version du logiciel de connecteur sur la console de cloud privé.

Q : Quelles versions de connecteur sont affectées par cette politique de support ?

A : La politique de support s'applique à tous les connecteurs de terminaux sécurisés, y compris les systèmes d'exploitation Windows, Mac, Linux et les appareils mobiles disponibles sur le cloud de terminaux sécurisés ou le cloud privé de terminaux sécurisés. Les versions des connecteurs qui sont immédiatement affectées par cette politique d'assistance sont disponibles sur le [Annonce de fin de prise en charge des versions Secure Endpoint Connector et Private Cloud](#).

Q : Une version plus ancienne est toujours disponible sur la console. Puis-je encore la télécharger

et l'installer ?

A : Une version peut supprimer une version de connecteur de la console quelque temps après que le connecteur est devenu officiellement non pris en charge. Nous vous recommandons de sélectionner une version plus récente du logiciel afin d'éviter les problèmes de compatibilité et de disposer des derniers correctifs de sécurité, de protection et d'ensemble de fonctionnalités du produit.

Q : Dois-je exécuter la dernière version d'un système d'exploitation pour continuer à utiliser mes connecteurs Secure Endpoint ?

A : Les versions du connecteur peuvent nécessiter un correctif du système d'exploitation ou une mise à niveau vers une version ultérieure, si nécessaire pour des raisons de compatibilité, d'accès à toutes les fonctionnalités ou de correction de bogues. Ceci est courant pour les appareils Android et Apple iOS qui ont des cycles de mise à jour et de mise à jour fréquents, mais s'applique à tous les systèmes d'exploitation. Les [Notes de version de Secure Endpoint](#) Le contient des détails spécifiques sur la configuration système requise pour des versions de connecteur spécifiques.

Les sites Web suivants contiennent des informations supplémentaires spécifiques à la compatibilité de chaque système d'exploitation :

[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

Q : Quel est l'impact du logiciel de cloud privé Secure Endpoint ou de l'appliance virtuel de cloud privé ?

A : Le calendrier d'assistance pour le logiciel de cloud privé Secure Endpoint et l'appliance virtuel de cloud privé est aligné pour fournir une assistance d'un an à compter de la date de publication. Si vous exécutez une version du logiciel de cloud privé ou de l'appliance virtuel de cloud privé plus ancienne qu'un an, nous vous recommandons de mettre à jour vers la version la plus récente pour les derniers correctifs de sécurité, les dernières fonctionnalités du produit et l'assistance technique. Vous devrez peut-être effectuer une mise à niveau vers une version prise en charge de votre logiciel de cloud privé ou de votre appliance virtuel de cloud privé si vous avez besoin d'une assistance technique et rencontrez des problèmes avec une version antérieure. Les connecteurs du cloud privé sont également affectés et ne sont plus pris en charge depuis un an. Reportez-vous à la section : [Notes de version du cloud privé Secure Endpoint](#) pour plus d'informations sur les fonctionnalités mises à jour.

Q : Quel est l'impact sur le matériel de l'appliance de cloud privé Secure Endpoint ?

A : Le matériel de l'appliance de cloud privé n'est pas couvert ou affecté par cette politique et sera pris en charge comme indiqué dans la [Politique de fin de vie](#). Seul le logiciel de cloud privé exécuté sur l'appliance matérielle est affecté par le calendrier spécifié dans cette stratégie.

Historique de révision

| Révision | Date de publication | Commentaires |
|----------|---------------------|--------------|
|----------|---------------------|--------------|

| | | |
|-----|--------------|--|
| 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, aux appareils virtuels de cloud privé 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 |