

Prise en charge à long terme du connecteur Linux Cisco Secure Endpoint

Table des matières

[Introduction](#)

[Prise en charge à long terme de Cisco Secure Endpoint Connector](#)

[Annonces LTS](#)

[Légende](#)

[Enterprise Linux](#)

[Amazon Linux](#)

[SUSE Linux Enterprise et openSUSE Leap](#)

[Ubuntu LTS](#)

[Debian](#)

[Configurer une stratégie de prise en charge à long terme des connecteurs](#)

[Voir également](#)

Introduction

Ce document décrit les engagements de prise en charge à long terme du connecteur Cisco Secure Endpoint Linux (LTS).

Prise en charge à long terme de Cisco Secure Endpoint Connector

Cisco Secure Endpoint connector LTS est la période au cours de laquelle une distribution Linux ne reçoit que des correctifs de bogues et de sécurité et ne reçoit plus de nouvelles fonctionnalités.

Le connecteur LTS ne prendra en charge que le dernier noyau officiellement pris en charge sur la distribution Linux. Si une distribution est entrée dans le connecteur LTS, elle arrive en fin de vie, comme défini par le fournisseur de distribution. Les clients devront mettre à jour leur point de terminaison avec la dernière version officiellement prise en charge de la distribution et du noyau disponible. Les clients doivent également se préparer à mettre à niveau leurs terminaux vers une distribution plus récente avant la fin du LTS de connecteur.

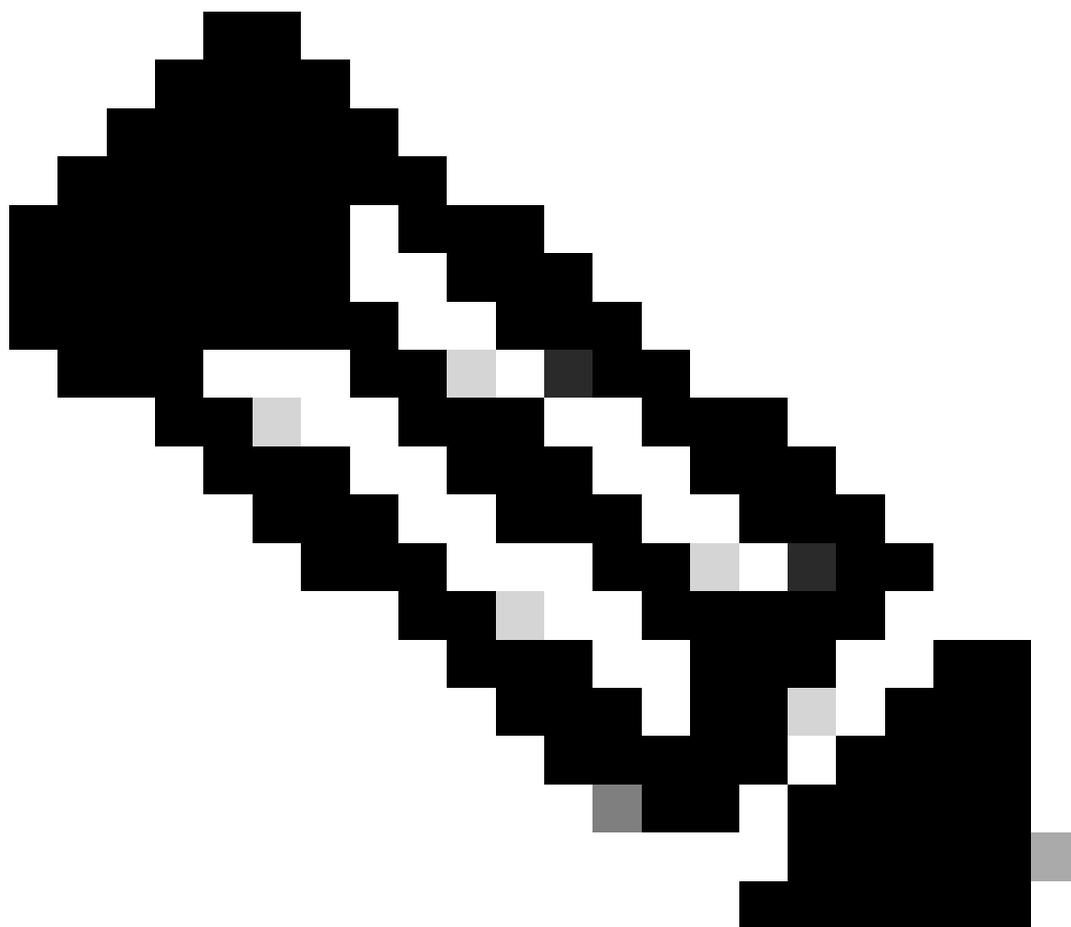
Le connecteur LTS s'aligne sur la politique du fournisseur de distribution pour prendre en charge uniquement la dernière version de la version de distribution en fin de vie ; par exemple, la version 7.9, dernière version mineure d'Enterprise Linux 7, est prise en charge à long terme par le connecteur. Ceci est conforme à la [Politique d'assistance logicielle Secure Endpoint](#) :

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.

Le LTS de connecteur prend uniquement en charge la dernière version de patch disponible dans la famille de versions LTS de connecteur spécifiée pour une distribution héritée. Par exemple, si la famille de versions LTS du connecteur est 1.20.X, X doit être la version de correctif disponible la plus importante. Les clients doivent conserver la version LTS de leur connecteur à jour avec la dernière version de correctif pour continuer à bénéficier de l'assistance.

Une distribution Linux utilisée au-delà de la période LTS du connecteur perdra la prise en charge de Cisco Secure Endpoint. Ceci est vrai pour une distribution Linux qui n'est plus prise en charge :

- Cisco Engineering ne développera, ne réparera, ne maintiendra ni ne testera le connecteur Secure Endpoint sur ces distributions.
- Le centre d'assistance technique de Cisco (TAC) ne prend pas en charge le connecteur Secure Endpoint sur ces distributions.
- Tous les services d'assistance du produit ne sont pas disponibles et le produit devient obsolète.



Remarque : L'assistance continue selon les termes et conditions du contrat de service du client sur les systèmes d'exploitation et les distributions pris en charge pour les clients

disposant de contrats de service et d'assistance actifs.

Voir la [configuration système requise](#) et les tableaux pour la compatibilité [basée sur RPM](#) et [basée sur Debian](#).

Annonces LTS

Distribution	Version	Annonce LTS
Enterprise Linux (EL)	7	Se termine le 30 juin 2028
	8	Débute le 31 mai 2029
	9	Débute le 31 mai 2032
SUSE Enterprise / openSUSE Leap	15 SP3 / 15,3	Se termine le 31 décembre 2025
	15 SP4 / 15,4	Se termine le 31 décembre 2026
	15 SP5 / 15,5	Débute le 31 décembre 2024
Debian	11	Se termine le 30 juin 2026
	12	Débute le 10 juin 2026
Ubuntu LTS	18.04	Se termine le 1er avril 2028
	20.04	Débute le 2 avril 2025.
	22.04	Débute le 1er avril 2027
	24.04	Débute le 25 avril 2029
Amazon Linux	2	Se termine le 30 juin 2026
	2023	Débute le 30 juin 2027

Légende

	Pris en charge
	Pris en charge sur la version de la famille LTS ; Actuellement dans le connecteur Cisco Secure Endpoint LTS
	Non pris en charge ; Passé la fin du connecteur Cisco Secure Endpoint LTS

Enterprise Linux

Le connecteur Cisco Secure Endpoint LTS pour Enterprise Linux (EL) englobe les distributions suivantes :

- Rocky Linux
- Alma Linux
- Red Hat Enterprise Linux (RHEL)
- Oracle Linux (RHCK)
- Linux CentOS
- Oracle Linux

La fin de la maintenance et la fin du cycle de vie étendu de RHEL sont utilisées pour déterminer les périodes LTS des connecteurs pour les distributions basées sur EL.

Distributeur	Fournisseur de distribution		Connecteur Cisco Secure Endpoint	
	Fin du support de maintenance	Fin du support de cycle de vie étendu	Fin du LTS	Famille de versions LTS
EL9	31 mai 2032	31 mai 2035	31 mai 2035	À DÉTERMINER
EL8	31 mai 2029	31 mai 2032	31 mai 2032	À DÉTERMINER
EL7	30 juin 2024	30 juin 2028	30 juin 2028	1,24.X
EL6	30 novembre 2020	30 juin 2024	7 novembre 2024	1.20.X

Amazon Linux

Veillez noter que la fin de l'assistance standard et de l'assistance de fin de sécurité pour Amazon Linux 2 sont prévues pour se terminer à la même date. Par conséquent, l'assistance à long terme (LTS) pour Cisco Secure Endpoint Connector prendra également fin à cette date.

Distributeur	Fournisseur de distribution		Connecteur Cisco Secure Endpoint	
	Fin du support standard	Fin du support de sécurité	Fin du LTS	Famille de versions LTS
Amazon Linux 2023	30 juin 2027	30 juin 2029	30 juin 2029	À DÉTERMINER
Amazon Linux 2	30 juin 2026	30 juin 2026	30 juin 2026	S/O

SUSE Linux Enterprise et openSUSE Leap

Distributeur	Version	Fournisseur de distribution		Connecteur Cisco Secure Endpoint	
		Fin de l'assistance générale	Fin de la prise en charge du Service Pack à long terme	Fin du LTS	Famille de versions LTS
SUSE	15 SP6 / À	À	À DÉTERMINER	À	À

Enterprise / Leap	15,6	DÉTERMINER		DÉTERMINER	DÉTERMINER
	15 SP5 / 15,5	31 décembre 2024	31 décembre 2026	31 décembre 2026	1,25.X
	15 SP4 / 15,4	31 décembre 2023	31 décembre 2026	31 décembre 2026	1,24.X
	15 SP3 / 15,3	31 décembre 2022	31 décembre 2025	31 décembre 2025	1,24.X
	15 SP2 / 15,2	31 décembre 2021	31 décembre 2024	31 décembre 2024	1,24.X
	15 SP1 / 15,1	31 janvier 2021	31 janvier 2024	31 janvier 2024	1,24.X
	15 SP0 / 15,0	31 décembre 2019	31 décembre 2022	31 janvier 2024	1,24.X

Ubuntu LTS

Distributeur	Fournisseur de distribution		Connecteur Cisco Secure Endpoint	
	Fin de la maintenance et du support de sécurité	Fin de la maintenance de sécurité étendue	Fin du LTS	Famille de versions LTS
Ubuntu LTS 24.04	25 avril 2029	25 avril 2036	25 avril 2036	À DÉTERMINER
Ubuntu LTS 22.04	1er avril 2027	9 avril 2032	9 avril 2032	À DÉTERMINER
Ubuntu LTS 20.04	2 avril 2025	2 avril 2030	2 avril 2030	À DÉTERMINER
Ubuntu LTS 18.04	31 mai 2023	1er avril 2028	1er avril 2028	1,24.X

Debian

Distribution	Fournisseur de distribution		Connecteur Cisco Secure Endpoint	
	Fin du support de sécurité	Fin du LTS	Fin du LTS	Famille de versions LTS
Debian 12	10 juin 2026	10 juin 2028	30 juin 2028	À DÉTERMINER
Debian 11	1er juillet 2024	30 juin 2026	30 juin 2026	1,24.X
Debian 10	10 sept. 2022	30 juin 2024	30 juin 2024	1,24.X

Configurer une stratégie de prise en charge à long terme des

connecteurs

Le connecteur télécharge une valeur initiale de mise à jour (xml) avec chaque synchronisation de stratégie si la stratégie de ce connecteur est pour une version supérieure, mais le connecteur ne se met pas à jour si la valeur initiale de mise à jour est pour une version supérieure à la famille LTS du connecteur. Les clients qui souhaitent éviter les téléchargements inutiles de semences de mise à jour peuvent placer leurs distributions héritées actuellement dans le LTS de connecteur dans une stratégie distincte dont la version est la plus récente de la famille LTS pour cette distribution héritée.

Si vous souhaitez continuer à utiliser une distribution héritée tout au long de la période LTS de son connecteur, il est recommandé de créer une stratégie distincte pour la distribution héritée. Reportez-vous à la section « Enable Debug Mode Using the Secure Endpoint Console » de l'article [Cisco Secure Endpoint Connector for Linux Diagnostic Data Collection](#) pour obtenir des instructions détaillées sur la façon de dupliquer une stratégie avec de nouveaux paramètres. Lors de la modification de votre stratégie, vous allez effectuer les étapes suivantes :

1. Sur la page Modifier la stratégie, sélectionnez l'onglet Mises à jour du produit.
2. Dans la liste déroulante Version du produit, sélectionnez la dernière version du produit dans la famille de versions LTS du connecteur qui correspond à votre distribution héritée.

The screenshot shows the 'Edit Policy' interface for a Linux connector. The 'Product Updates' tab is selected. The 'Product Version' dropdown is highlighted with a red box and shows '1.20.7.982'. Other fields include 'Name: Legacy EL6 Policy', 'Update Server', and 'Date Range'.

← Policies
Edit Policy
Linux

Name: Legacy EL6 Policy
Description:

Modes and Engines

Exclusions
No exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Product Version: 1.20.7.982
Update Server: [Redacted]
Date Range: 2024-01-27 18:08 - 2024-02-19 18:08

Cancel Save

Voir également

- [Cisco Secure Endpoint Connector pour la collecte de données de diagnostic Linux](#)
- [Politique d'assistance logicielle Secure Endpoint](#)
- [Vérifier la compatibilité du système d'exploitation du connecteur Linux Secure Endpoint](#)

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.