Notes de mise à jour de Symantec™ Endpoint Protection 14.3 RU3 - French - France

Updated: September 17, 2021

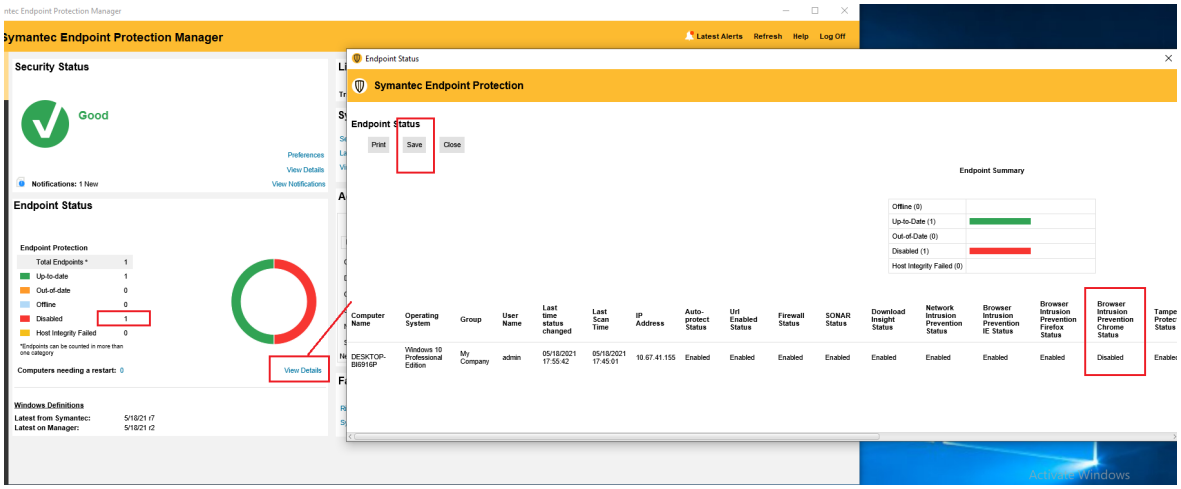
Table of Contents

Nouveautés dans Symantec Endpoint Protection 14.3 RU3

Cette section décrit les nouvelles fonctionnalités de cette version.

Fonctions de protection

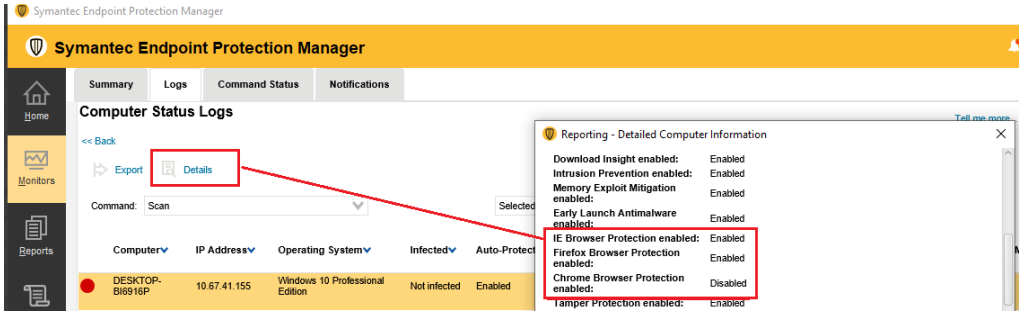
- Protection améliorée contre les outils Living off the Land. Pour plus d'informations, consultez la section Protection Symantec Endpoint Protection contre les ransomwares qui utilisent des techniques Living off the Land.
- Protection améliorée contre les ransomwares connus tels que REvil, avec des technologies d'inspection étendues pour les menaces émergentes. Détection des comportements suspects communs utilisés dans les attaques ciblées et verrouillage des fichiers et processus avant l'exécution du chiffrement
- Amélioration de la protection contre les menaces sous Linux à l'aide des fonctionnalités d'apprentissage automatique et d'analyse cloud. Pour exploiter ces fonctionnalités, dans la **Politique de protection contre les virus et les spywares**, cliquez sur **Paramètres Linux** > **Options d'analyse générales**.
- Symantec peut désormais libérer de nouvelles fonctions de détection beaucoup plus rapidement avec la fonction d'autoprotection.
- Amélioration des rapports d'extension de navigateur pour identifier les ordinateurs sur lesquels la protection est désactivée ou sur lesquels figure du contenu obsolète dans Symantec Endpoint Protection Manager :
  - La page **Clients** > onglet **Clients** > vue **Technologie de protection** indique si les extensions de navigateur sont activées ou désactivées.Sélectionnez le client et cliquez sur **Modifier les propriétés** > onglet **Clients**. Les champs **Etat d'activation du navigateur Internet Explorer**, **Etat d'activation du navigateur Firefox** et **Etat d'activation du navigateur Chrome** indiquent l'état **Activé(s)**, **Désactivé(s)** ou **Etat Rapports non créés**. Les **définitions d'extension de navigateur** indiquent le numéro de version des définitions.
  - Sur la page **Accueil**, sous **Etat des terminaux**, sélectionnez les clients dont l'état est **Désactivé(s)**, puis cliquez sur **Détails**. Dans le rapport, affichez les extensions de navigateur qui sont activées ou désactivées.



  - Rapports améliorés des clients avec désactivation de l'extension de navigateur. Sur la page **Accueil**, sous **Rapports sur les favoris**, le rapport **Symantec Endpoint Protection - Etat hebdo.** indique les clients pour lesquels les extensions sont activées ou désactivées.
  - Le rapport rapide **Versions du contenu de protection** indique la date et l'heure de la dernière mise à jour des définitions d'extension de navigateur Chrome. Cliquez sur **Rapports** > **Rapports rapides** > type de rapport **Etat de l'ordinateur** > rapport **Versions du contenu de protection**, puis sur **Créer un rapport**. Cliquez sur le rapport

Résumé de l'état de la sécurité pour identifier le nombre de clients pour lesquels une extension de navigateur est désactivée ou est défectueuse.

– Le journal Etat de l'ordinateur affiche des colonnes **Protection du navigateur IE activée**, **Protection du navigateur Firefox activée** et **Protection du navigateur Chrome activée**. Sur la page **Moniteurs**, cliquez sur **Journaux** > **Etat de l'ordinateur** > **Afficher le journal**. Dans l'onglet **Journaux**, cliquez sur **Détails** pour connaître le numéro de révision des **Définitions d'extension de navigateur**. Utilisez ces informations pour vous assurer que le contenu de l'extension de navigateur est téléchargé sur le client.



– Le journal système client affiche un événement chaque fois que l'extension de navigateur Chrome est activée, désactivée, installée, désinstallée ou supprimée.

Intégration des extensions de navigateur avec Symantec Endpoint Protection pour assurer la protection contre les sites Web malveillants

Mises à jour de Symantec Endpoint Protection Manager

- Symantec Endpoint Protection Manager prend désormais en charge Windows Server 2022.
- Flexibilité améliorée au niveau des mises à niveau client Windows à l'aide de la politique de mise à niveau client avec des paramètres d'identification d'emplacement. La politique permet également de réaliser la mise à niveau n'importe quel jour de la semaine, de la distribuer sur plusieurs jours et de la réessayer lorsqu'elle ne démarre pas comme prévu.

  Mise à niveau du logiciel client avec la politique de mise à niveau client

  Téléchargement du contenu de LiveUpdate vers Symantec Endpoint Protection Manager
- Si le client détecte la présence de contenu obsolète, les clients Windows assurent une protection continue en vérifiant les mises à jour à intervalles réguliers. Si les définitions sont manquantes, le client enregistre un événement toutes les 30 minutes. Les clients hérités effectuent plusieurs tentatives de remédiation avant de s'arrêter pour la journée et de consigner une erreur.Ce paramètre se contrôle au moyen de la politique de protection contre les virus et les spywares >**Divers** > onglet **Notifications** > option **Tentatives de remédiation avant apparition d'un avertissement dans Symantec Endpoint Protection**.
- Les composants tiers suivants ont été mis à niveau ou ajoutés : AjaxSwing, Apache HTTP Server, libcurl, libxml2, OpenJDK, OpenSSL et PHP.

Mises à jour de client et de plate-forme

Client Windows :

- Le client Windows est pris en charge sur Windows Server 2022 et Windows 10 Embedded. La version 14.3 RU3 a été testée et est compatible avec toutes les versions prépubliées de Windows 11 et de Windows 11 Embedded.
- Si un domaine Symantec Endpoint Protection Manager est inscrit dans le cloud, une page de dépannage apparaît avec le nom des politiques que la console cloud gère. Pour accéder à cette page, cliquez sur **Aide** > **Dépannage** > **Gestion hybride**.
- **Journal de débogage** : lorsque vous activez le fichier `debug.log` client dans le panneau **Aide** > **Dépannage** > **Journaux de débogage**, vous activez également le fichier `cve.log` .Vous n'avez pas besoin de redémarrer le client ou d'exécuter les commandes suivantes pour que les modifications apportées au journal de débogage prennent effet :

`smc -stop` ou `smc -start` .Les journaux de débogage client aident à dépanner les problèmes de communication du client à Symantec Endpoint Protection Manager ainsi que les problèmes de fonctionnalité client. Les journaux de communication `cve.log` et `cve-actions.log` se trouvent dans le répertoire **C:\ProgramData\Symantec \Symantec Endpoint Protection\CurrentVersion\Data\Logs**.

Advanced debug log options in SymDiag for Endpoint Protection clients (Options avancées du journal de débogage dans SymDiag pour les clients Endpoint Protection)

Configuration de la consignation du module de communication Endpoint Protection dans les versions 14.2 et ultérieures

Client Mac :

NOTE
La version 14.3 RU3 du client Symantec Endpoint Protection pour Mac est prévue pour octobre 2021.

- Ajout de la prise en charge de macOS 12.
- La taille du programme d'installation du client Mac a été réduite à 100 Mo.
- Le nombre d'alarmes **présentant un risque** a été réduit et optimisé.
- Dans un souci d'amélioration des performances, il n'est désormais plus possible d'exécuter plusieurs analyses simultanément. Si une analyse est en cours d'exécution, les autres analyses sont mises en attente.
- À partir de la version 14.3 RU3, le programme d'installation du client Mac ne permet pas d'installer une version antérieure du client.

Agent Linux :

- L'outil de ligne de commande de l'agent Linux (sav) a été amélioré avec l'ajout d'options permettant d'afficher les versions, d'exécuter LiveUpdate ou encore de démarrer et d'arrêter une analyse.Pour plus d'informations, consultez l'article :
  Gestion de l'agent Linux à l'aide de l'outil de ligne de commande (sav)
- Linux prend désormais en charge le protocole TCP pour les ordinateurs gérés par SEPM.
- Correction de plusieurs défaillances.
- Suppression de l'avertissement pour l'option **Utiliser les serveurs Symantec lorsque les serveurs privés ne sont pas disponibles** sur la page **Clients** > onglet **Clients** > **Communications externes**. Les clients 12.1.5 ne sont plus pris en charge.

Modifications de la documentation

- Les API Symantec Endpoint Protection Manager sont incluses dans un fichier PDF à l'emplacement suivant :
  DOCUMENTATION DE L'API REST ENDPOINT SECURITY

Pour plus d'informations, consultez l'article :

Nouveautés dans toutes les versions de Symantec Endpoint Protection

Problèmes connus et solutions de contournement dans Symantec Endpoint Protection (SEP)

Le contenu de cette section s'applique à cette version de Symantec Endpoint Protection.

NOTE

La colonne Problème affiche le numéro de version concerné par le problème. Par exemple, « [14.3 RU1] » signifie que le problème s'applique à la version 14.3 RU1 et aux versions ultérieures.Une fois ces problèmes résolus, ils apparaissent dans les notes de correction. Voir :

Versions, configuration système requise, dates de sortie, notes et correctifs pour Symantec Endpoint Protection et Endpoint Security

Problèmes de mise à niveau

Table 1: Problèmes de mise à niveau connus

Problème	Description et solution
Affichage du message d'erreur suivant : Symantec Endpoint Protection version 14.3 RU2 for Win64bit is the latest package. You cannot delete it (Symantec Endpoint Protection version 14.3 RU2 pour Win64bit est le dernier package. Vous ne pouvez pas le supprimer.) [14.3 RU2]	Vous ne pouvez pas supprimer le package d'installation client lorsque des packages de plusieurs builds apparaissent dans Symantec Endpoint Protection Manager. A compter de la version 14.3 RU2, LiveUpdate peut télécharger plusieurs packages d'installation client avec un numéro de build différent, qui apparaissent dans la page **Administration** > **Packages d'installation** > tableau **Packages d'installation client**. [SEP-72531]
Echec de la fonction Mise à niveau automatique lorsque l'option **Mettre à niveau vers l'anglais si la langue du client actuellement installé n'est pas prise en charge** de la version 14.3 RU2 est utilisée pour mettre à niveau les clients installés dans une langue non prise en compte vers l'anglais [14.3 RU2]	Ce problème se produit pour les clients que vous avez mis à niveau manuellement à partir d'une langue prise en charge vers une langue non prise en charge dans la version 14.3 RU1 MP1 ou antérieure. C'est le cas, par exemple, si vous avez mis à niveau un client tchèque vers un client japonais sur un système d'exploitation japonais, puis utilisé l'option **Mettre à niveau vers l'anglais si la langue du client actuellement installé n'est pas prise en charge** pour passer de la langue non prise en compte vers l'anglais dans la version 14.3 RU2. [SEP-72490] Ce problème est dû au fait que la langue du client est définie sur celle du système d'exploitation pris en charge (le japonais dans cet exemple). La fonction Mise à niveau automatique s'attend à utiliser la langue prise en charge et non l'anglais. Pour contourner ce problème, lancez à nouveau la fonction de mise à niveau automatique et désactivez l'option **Mettre à niveau vers l'anglais si la langue du client actuellement installé n'est pas prise en charge**.
Affichage du message d'avertissement suivant lors de l'exportation d'un package d'installation client à partir de Symantec Endpoint Protection Manager (SEPM) 14.3 RU2 : The client installation package does not have content (Le package d'installation client ne présente pas de contenu) [14.3 RU2]	Ce problème est dû au fait que la communication entre Symantec Endpoint Protection Manager et la console utilisée pour l'exportation du package a été interrompue.Voir : Affichage du message d'avertissement The client installation package does not have content (Le package d'installation client ne présente pas de contenu) lors de l'exportation d'un package d'installation client à partir de Symantec Endpoint Protection Manager

Problème	Description et solution
Un message d'erreur s'affiche lors de l'importation des derniers packages d'installation client dans une version plus ancienne de Symantec Endpoint Protection Manager. [14.3 RU2]	Les clients Symantec Endpoint Protection 14.3 RU2 ne peuvent pas être gérés par la version 14.3 RU1 MP1 ou antérieure de Symantec Endpoint Protection Manager. [SEP-72292]
Arrêt brutal de l'exécutable php-cgi.exe avec consignation d'une erreur dans l'observateur d'événements après la mise à niveau de Symantec Endpoint Protection Manager vers la version 14.3 RU2 [14.3 RU2]	Ce problème survient avec la version 17.4.1.1 du pilote Microsoft ODBC pour SQL Server. [SEP-70385] Pour contourner ce problème, téléchargez et installez la version 17.7.2 du pilote Microsoft ODBC pour SQL Server sous Windows : https://docs.microsoft.com/fr-fr/sql/connect/odbc/windows/release-notes-odbc-sql-server-windows?view=sql-server-ver15 Pour plus d'informations, consultez l'article : Arrêt brutal de l'exécutable php-cgi.exe sur Endpoint Protection Manager après la mise à niveau vers la version 14.3 RU2
Affichage possible de notifications « The client computer has been renamed » (L'ordinateur client a été renommé) après la mise à niveau vers Symantec Endpoint Protection Manager 14.3 RU2 [14.3 RU2]	Après la mise à niveau vers Symantec Endpoint Protection Manager 14.3 RU2, il se peut que les administrateurs reçoivent des notifications « The client computer has been renamed » (L'ordinateur client a été renommé). Ce problème s'applique uniquement aux clients Mac.Voir : Affichage possible de notifications « The client computer has been renamed » (L'ordinateur client a été renommé) après la mise à niveau vers Symantec Endpoint Protection Manager 14.3 RU2
Un instance de Symantec Endpoint Protection Manager dans un réseau invisible télécharge l'ancien contenu CIDS (Client Intrusion Detection System) sur de nouveaux clients, car LiveUpdate ne s'exécute pas pendant une mise à niveau [14.3 RU1]	Lorsqu'un Symantec Endpoint Protection Manager 14.3 RU1 ne peut pas accéder à Internet ou à un serveur LiveUpdate Administrator (LUA), il conserve l'ancien contenu incompatible dans son cache. Cet ancien contenu est normalement livré aux nouveaux clients.Pour mettre à jour le contenu dans le cache du serveur de gestion, téléchargez manuellement les définitions de virus certifiées et les fichiers .jdb CIDS.[SEP-69125] Pour vous assurer que les nouveaux clients n'obtiennent pas l'ancien contenu, installez manuellement un fichier .jdb CIDS sur SEPM avant d'installer de nouveaux clients ou de mettre à niveau les anciens clients.Voir : Download .jdb files to update definitions for Endpoint Protection Manager (Téléchargement de fichiers .jdb pour la mise à jour des définitions pour Endpoint Protection Manager)
Impossible de se connecter à Symantec Endpoint Protection Manager (SEPM) lorsque la carte d'interface réseau est désactivée [14.3 RU1]	Si après avoir installé Symantec Endpoint Protection Manager, vous ne pouvez pas vous connecter à la console et le message d'erreur suivant s'affiche : `Erreur de serveur inattendue.` Ce problème peut se produire si la carte d'interface réseau de l'ordinateur est désactivée lors de l'installation de SEPM, ce qui empêche la génération du certificat de serveur. [SEP-67040] Pour savoir si SEPM a été installé avec une carte d'interface réseau désactivée, examinez le certificat de serveur.Voir : Une erreur de serveur inattendue se produit lors de la connexion au logiciel SEPM lorsqu'il a été installé sur un serveur sur lequel aucune carte NIC n'a été activée
Lorsque vous désinstallez SEPM, que vous utilisez l'option de suppression de la base de données par défaut et que vous quittez l'instance SQL Server Express, l'erreur suivante s'affiche : `Une erreur s'est produite lors de la tentative de connexion au serveur de base de données.` [14.3 RU1]	Si vous désinstallez Symantec Endpoint Protection Manager et sélectionnez l'option **Supprimer uniquement la BdD et conserver l'instance SQL Server Express avec SEPM**, l'erreur suivante peut s'afficher : « `Une erreur s'est produite lors de la tentative de connexion au serveur de base de données.` »Ce problème se produit après l'ajout des informations d'authentification pour le DBA d'utilisateur par défaut et peut être lié aux privilèges d'utilisateur.[SEP-68670] Pour contourner ce problème, effectuez une désinstallation en exécutant le fichier setup.exe de SEPM et en cliquant sur **Supprimer uniquement la BdD et conserver l'instance SQL Server Express avec SEPM** pendant la désinstallation.

Problème	Description et solution
Echec de la mise à niveau de SQL Server de la version 2017 à la version 2019 lorsque le mode FIPS est activé [14.3]	Le message suivant s'affiche parfois : "The following error has occurred. An error occurred while installing extensibility feature with error message: AppContainer Creation Failed with error message NONE, state. This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms" (L'erreur suivante s'est produite. Une erreur s'est produite lors de l'installation de la fonctionnalité d'extensibilité avec le message d'erreur suivant : échec de la création du conteneur d'applications avec le message d'erreur Aucun, état. Cette implémentation ne fait pas partie des algorithmes de chiffrement validés FIPS pour les plates-formes Windows). Cette erreur se produit si vous disposez d'une version Symantec Endpoint Protection Manager 14.3 compatible FIPS et que vous effectuez une mise à niveau depuis Microsoft SQL Server 2017 vers Microsoft SQL Server 2019. [SEP-61473] Pour contourner ce problème, désactivez le mode FIPS au niveau du système d'exploitation : 1. Sous `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools`, cliquez sur **Stratégie de sécurité locale** > **Stratégies locales** > **Options de sécurité**, puis désactivez l'option **Chiffrement système : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature**. 2. Mise à niveau de SQL Server version 2017 vers la version 2019 3. Une fois la mise à niveau de SQL Server terminée, réactivez le mode FIPS. Pour plus d'informations, consultez l'article : SQL upgrade from 2017 to 2019 fails with FIPS mode enabled (Echec de la mise à niveau de SQL 2017 vers la version 2019 lorsque le mode FIPS est activé)
Des noms personnalisés peuvent empêcher la politique de pare-feu de procéder à une mise à jour lors d'une mise à niveau vers la version 14.2 ou version ultérieure	Pour une mise à niveau vers Symantec Endpoint Protection 14.2 ou version ultérieure, les politiques de pare-feu ne peuvent pas incorporer les changements liés à IPv6 si vous avez modifié certains noms par défaut. Les noms par défaut incluent les noms des politiques et des règles par défaut. Si les règles ne peuvent pas être mises à jour au cours de la mise à niveau, les options IPv6 ne s'affichent pas. Les nouvelles politiques ou règles que vous créez après la mise à niveau ne sont pas affectées. Si possible, réinitialisez les noms modifiés à leur valeur par défaut. Sinon, assurez-vous que les règles personnalisées que vous avez ajoutées à une politique par défaut ne bloquent pas la communication IPv6. Assurez-vous-en également pour les nouvelles politiques ou règles que vous ajoutez.

Problèmes liés à Symantec Endpoint Protection Manager

Table 2: Problèmes connus liés à Symantec Endpoint Protection Manager

Problème	Description et solution
Non-respect des paramètres de **planification de la mise à niveau** dans une politique de mise à niveau client par les clients Endpoint Protection (SEP) 14.2 RU1 MP1 et antérieurs [14.3 RU3]	Pour plus d'informations, consultez l'article : Non-respect de la politique de mise à niveau client par Endpoint Protection 14.3 RU1 MP1 et clients plus anciens [SEP-72814]
Certains événements EDR n'apparaissent pas sur le client [14.3 RU1]	Le client Symantec Endpoint Protection doit exécuter Windows 10 version 14393 ou une version ultérieure pour collecter les événements de suivi d'événements Symantec EDR pour Windows (ETW).[SEP-67175]

Problème	Description et solution
Limitations de la fonction Network Traffic Redirection (Protection Web et de l'accès au cloud) [14.3 RU1]	• Symantec Web Security Service est fourni avec IPv4 et non IPv6.[SEP-68700] • Méthode de redirection du tunnel : – S'exécute sur Windows 10 x64 version 1703 et ultérieure (canal de maintenance semi-annuel) uniquement. Cette méthode ne prend pas en charge les autres systèmes d'exploitation Windows ou le client Mac.[SEP-67927] – Ne prend pas en charge les unités Windows 10 64 bits activées par HVCI. [SEP-67648] – Redirige le trafic sortant du client Symantec Endpoint Protection vers WSS avant qu'il soit évalué par le pare-feu du client ou par les règles de réputation de l'URL. Au lieu de cela, le trafic est évalué par rapport au pare-feu WSS et aux règles d'URL. Par exemple, si une règle de pare-feu du client SEP bloque le site google.com et qu'une règle WSS l'autorise, le client autorise les utilisateurs à y accéder.Le trafic local entrant à destination du client continue d'être traité par le pare-feu Symantec Endpoint Protection. [SEP-67488] – Le portail captif WSS n'est pas disponible pour la méthode de tunnel et le client ignore les informations d'authentification de la demande d'accès.Dans une version ultérieure, l'authentification SAML dans WSS Agent remplacera le portail captif et sera disponible sur le client Symantec Endpoint Protection. – Si un ordinateur client se connecte au WSS à l'aide de la méthode de tunnel et héberge des machines virtuelles, chaque utilisateur invité doit installer le certificat SSL fourni dans le portail WSS. – Le trafic du réseau local comme votre répertoire de base ou l'authentification Active Directory n'est pas redirigé. – Incompatibilité avec le VPN Microsoft DirectAccess. La méthode de tunnel est actuellement considérée comme une fonctionnalité destinée aux utilisateurs précoces.
Duplication des entrées d'inscription de client après la mise à niveau depuis la version 14.2.x vers la version 14.3 MP1 ou ultérieure [14.3 RU1]	La mise à niveau des clients Symantec Endpoint Protection de la version 14.2.x à la version 14.3 MP1 et ultérieure crée des entrées d'inscription d'agent en double pour ces clients dans la page **Clients** de Symantec Endpoint Protection Manager. Il n'y a pas d'impact fonctionnel et vous pouvez continuer à utiliser les nouvelles entrées pour les clients 14.3 RU1. Symantec Endpoint Protection Manager supprime les entrées d'agent les plus anciennes.
Autoriser les URL dans Symantec Endpoint Security si vous utilisez l'option de gestion hybride, les serveurs proxy ou un pare-feu de périmètre [14.3]	Suite à l'acquisition de Symantec Enterprise Security par Broadcom, les URL des communications client-cloud ont été modifiées dans la version 14.2.2.1. [CDM-42467] Vous devez mettre à niveau vos clients vers la version 14.2.5569.2100 ou vers une version ultérieure dans la situation suivante : • Vous utilisez Symantec Endpoint Security pour gérer vos clients et vos politiques alors que vos domaines Symantec Endpoint Protection Manager sur site sont inscrits dans la console cloud. • Vous utilisez des serveurs proxy. Vous autorisez les URL dans des agents gérés en mode hybride ou entièrement cloud, et autorisez donc votre serveur proxy et/ou pare-feu de périmètre. Voir : • URL qui autorisent SEP et SES à se connecter aux serveurs Symantec • Mise à niveau des agents Symantec gérés dans le cloud vers la version 14.2 RU2 MP1 ou ultérieure

Problème	Description et solution
Fin de prise en charge de la plate-forme Windows 32 bits [14.3] par la console distante Symantec Endpoint Protection Manager	Dans la version 14.3 et versions ultérieures, vous ne pouvez pas vous connecter à la console distante Symantec Endpoint Protection Manager si vous exécutez une version 32 bits de Windows. L'environnement d'exécution Oracle Java SE ne prend plus en charge les versions 32 bits de Microsoft Windows.[SEP-61106] Si le message suivant s'affiche, connectez-vous à Symantec Endpoint Protection Manager en local : "This version of C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe is not compatible with the version of Windows you're running. Check your computer's system information and then contact the software publisher." (Cette version de C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin \javaw.exe n'est pas compatible avec la version de Windows que vous utilisez. Vérifiez les informations système de votre ordinateur, puis contactez l'éditeur de logiciels).
Affichage de l'erreur "Failed to install Microsoft Visual C++ Runtime" (Echec de l'installation de Microsoft Visual C ++ Runtime") lors de l'installation de Symantec Endpoint Protection Manager [14.3]	Le message d'erreur suivant s'affiche parfois lors de l'installation de Symantec Endpoint Protection Manager sous Windows 2012 R2 : "Failed to install Microsoft Visual C++ Runtime" (Echec de l'installation de Microsoft Visual C++ Runtime) [SEP-60396] Pour contourner ce problème, activez Windows et installez les mises à jour Windows. La mise à jour Windows installe le package redistribuable Visual C++ 2017, qui est un prérequis pour l'installation de Symantec Endpoint Protection Manager 14.3 sous Windows 2012 R2.
Mise à jour pour l'activation de TLS 1.1 et de TLS 1.2 comme protocoles sécurisés par défaut dans WinHTTP sous Windows [14.3]	Le serveur de gestion cesse de charger les journaux dans le cloud après la mise à niveau ou l'installation de Symantec Endpoint Protection Manager 14.3 (inscrit dans la console cloud). L'erreur suivante s'affiche parfois dans le fichier uploader.log : `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` Ce problème est dû à l'absence d'une mise à jour Microsoft qui assure la prise en charge de TLS 1.1 et 1.2. Pour résoudre ce problème, installez la mise à jour KB3140245 de Microsoft. Pour plus d'informations, consultez l'article : Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows (Mise à jour pour l'activation de TLS 1.1 et TLS 1.2 comme protocoles sécurisés par défaut dans WinHTTP sous Windows)
Affichage du message "Déploiement en cours" dans Symantec Endpoint Protection Manager, y compris après la réception d'une politique mise à jour pour Endpoint Threat Defense for Active Directory [14.2 RU1 MP1 et versions ultérieures] par le client	Ce comportement est tout à fait normal. Les politiques Endpoint Threat Defense for AD 3.3 sont prises en charge sur le client uniquement à partir de la version 14.2 RU1 MP1. Vous appliquez une politique Symantec Endpoint Threat Defense for Active Directory 3.3 à un groupe. Certains clients de ce groupe exécutent Symantec Endpoint Protection 14.2 RU1 ou version antérieure. Ces clients reçoivent et appliquent la politique comme prévu, mais l'état dans Symantec Endpoint Protection Manager continue à afficher le message Déploiement en cours.

Problèmes liés aux clients Windows, Mac et Linux

Table 3: Problèmes connus liés aux clients Windows, Mac et Linux

Problème	Description et solution
Affichage du message « Erreur de serveur inattendue » lors de la connexion à Endpoint Protection Manager et arrêt de la communication des clients après la modification de l'heure du système [14.3 RU3]	Si vous définissez l'horloge système sur une date et/ou une heure antérieures, l'erreur suivante peut se produire : • Une fois que vous vous êtes connecté à Symantec Endpoint Protection Manager, le message Erreur de serveur inattendue apparaît. • Les clients ne communiquent pas avec SEPM, qui signale une erreur 503. [SEP-74510] Pour contourner ce problème : • Redémarrez manuellement les services SEPM. • Patientez jusqu'à ce que la date et l'heure du système dépassent l'heure d'origine sur le système avant de les définir à nouveau.
Signalement du système d'exploitation Windows 10 sous Windows 11 dans le journal Protection Web et de l'accès au cloud d'Endpoint Protection 14.3 RU3 [14.3 RU3]	Lorsque l'utilisateur client affiche le journal Protection Web et de l'accès au cloud du client SEP, le journal indique que le système d'exploitation est de type Windows 10, alors que le client est installé sur un appareil Windows 11.Dans la console du client, cliquez sur **Protection Web et de l'accès au cloud** > **Options** > **Afficher les journaux**.
Impossibilité de lancer les navigateurs Microsoft Edge et Google Chrome après l'application de la technique de prévention **Valider l'intégrité des dépendances d'image** au système d'exploitation Windows 10 ou 11 [14.3 RU3]	La technique **Valider l'intégrité des dépendances d'image** est l'une des techniques de prévention que Microsoft Edge utilise pour protéger le système d'exploitation Windows.Les navigateurs Web Microsoft Edge et Google Chrome ne se lancent pas si cette option est activée sur les ordinateurs Windows 10 ou 11 qui exécutent la version 14.2 RU2 MP1 ou ultérieure des clients Symantec Endpoint Protection.[SEP-75086] Pour garantir le démarrage de Microsoft Edge, désactivez la technique **Valider l'intégrité des dépendances d'image**. Pour plus d'informations sur les techniques de prévention disponibles pour Microsoft Edge, consultez la section Customize exploit protection (Personnalisation de la protection contre les exploits). Voir également l'article Microsoft Edge and Google Chrome do not open if "Validate image dependence integrity" mitigation technique is applied and SEP 14.2 RU2 MP1 or later is installed (Impossible d'ouvrir Microsoft Edge et Google Chrome lorsque la technique de prévention « Valider l'intégrité des dépendances d'image » est appliquée et que SEP 14.2 RU2 MP1 ou version ultérieure est installé).
Relancement du client Windows sans redémarrage pour l'obtention des derniers événements EDR [14.3 RU3]	Vous devez redémarrer le client Symantec Endpoint Protection pour que les événements ETW supplémentaires soient disponibles dans la version 14.3 RU3. Vous devez redémarrer le client dans les situations suivantes : [SEP-73327] • EDR est activé et vous mettez à jour le client vers la version RU3. • La version 14.3 RU3 est déjà installée et vous activez ou désactivez EDR. Vous devez redémarrer le client pour activer ou désactiver les événements récemment ajoutés. Voir article A restart may be required to begin seeing some ETW events with EDR and SEP 14.3 RU3 (Redémarrage parfois requis pour afficher certains événements ETW avec EDR et SEP 14.3 RU3).
Impossibilité d'initialiser le moteur d'analyse après la mise à niveau du client Linux [14.3 RU3]	Le moteur d'analyse ne parvient pas à s'initialiser après la mise à niveau du client Symantec Endpoint Protection pour Linux vers la version 14.3 RU3. **Solution de contournement :** 1. Mettez à jour le serveur LiveUpdate avec le dernier contenu incluant SEF 1.7.6. 2. Désinstallez le client Linux 14.3 RU3 qui présente l'erreur Scan Engine initialization failure (Echec de l'initialisation du moteur d'analyse). 3. Réinstallez le client Linux 14.3 RU3.
Activation du démon `auditd` après l'installation du client Linux [14.3 RU3]	Le programme d'installation du client Symantec Endpoint Protection pour Linux active le démon `auditd` après l'installation de l'agent, y compris lorsque le démon `auditd` a été désactivé préalablement à l'installation.

Problème	Description et solution
Package `netstat` requis sur le client Linux pour la collecte des informations d'examen réseau (EDR) [14.3 RU3]	Si le package `netstat` ne figure pas sur le client Linux, les informations d'enquête sont collectées pour tous les autres types d'événements, excepté pour les événements réseau.
Problèmes de connexion possibles sur les appareils Mac [14.3 RU2]	• L'agent ne parvient parfois pas à se connecter au réseau après la mise à niveau de l'agent Mac à l'aide de la fonction de mise à niveau automatique et après le redémarrage de l'appareil. **Solution de contournement :** réexécutez le package d'installation de l'agent. • Après avoir été mis en veille, les appareils Mac peuvent perdre leur connexion réseau avec affichage de l'erreur suivante : Your connection was interrupted A network change was detected (Votre connexion a été interrompue. Une modification du réseau a été détectée). **Solutions de contournement :** – Si vous utilisez une station d'ancrage, renouvelez les adresses IP manuellement dans **Préférences système > Réseau**. – Débranchez la station d'ancrage de votre appareil Mac pendant quelques secondes, puis branchez-la à nouveau.
Blocage possible de l'installation de l'agent Mac par Rosetta sur les appareils Apple Silicon (M1) avec affichage de l'erreur suivante : This version of Symantec Agent for Mac is not supported on Apple M1 chip (Cette version de l'agent Symantec pour Mac n'est pas prise en charge par les puces Apple M1) [14.3 RU2]	Pour plus d'informations, consultez l'article : Article 222282 de la base de connaissances
Possibilité d'échec du téléchargement et de l'installation de l'agent Mac à l'aide du lien Web généré dans Symantec Endpoint Protection Manager [14.3 RU2]	L'installation de l'agent Mac échoue parfois avec affichage de l'erreur ci-après lorsqu'un administrateur invite des utilisateurs à installer l'agent Mac 14.3 RU2 à l'aide de l'option **Lien Web et adresse électronique** dans Symantec Endpoint Protection Manager et que les utilisateurs téléchargent le package à l'aide de ce lien dans le navigateur Safari : The application Symantec Endpoint Protection Installer can't be opened (Impossible d'ouvrir l'application Symantec Endpoint Protection Installer). **Solutions de contournement :** • Après avoir téléchargé le fichier, accédez au dossier **Downloads**, exécutez la commande suivante, puis exécutez l'installation à nouveau : `chmod +x ./Symantec\ Endpoint\ Protection/Symantec\ Endpoint\ Protection\ Installer.app/Contents/MacOS/Symantec\ Endpoint\ Protection\ Installer` • Ouvrez la section **Preferences** (Préférences) du navigateur Safari, puis, dans l'onglet **General** (Général), décochez l'option **Open "safe" files after downloading** (Ouvrir les fichiers sécurisés après les avoir téléchargés).Ensuite, téléchargez le package du programme d'installation et exécutez l'installation.
Affichage en anglais des paramètres de date des définitions dans le client en cas de mise à niveau automatique d'un client configuré dans une langue non prise en charge vers l'anglais [versions 14.3 RU1 et ultérieures]	Pour contourner ce problème, désinstallez le client hérité et installez manuellement un nouveau package d'installation client anglais. En outre, un correctif est prévu pour les clients qui sont mis à niveau automatiquement.[SEP-72481]

Problème	Description et solution
L'agent Symantec WSS Agent autonome bloque l'installation du client Symantec Endpoint Protection si vous installez SEP sur le même ordinateur que l'agent WSS.	Le composant Network Traffic Redirection (NTR) utilise les mêmes fichiers que l'agent Symantec WSS Agent (WSSA) autonome. NTR est installé par défaut dans Symantec Endpoint Protection et dans la console cloud Symantec Endpoint Security.WSSA ne peut pas être installé sur un terminal sur lequel la fonction NTR est installée. De même, la fonction NTR ne peut pas être installée si l'agent WSSA est installé. Vous pouvez supprimer la fonction Network Traffic Redirection des terminaux existants sans avoir à désinstaller la totalité du client à l'aide de l'une des méthodes suivantes : • Dans Symantec Endpoint Protection Manager, créez un ensemble de fonctionnalités d'installation client qui n'inclut pas la fonction NTR et appliquez-le aux terminaux.Voir : Ajout ou suppression de fonctions sur les clients Endpoint Protection existants • L'option de ligne de commande suivante utilise le fichier d'installation client pour supprimer la fonction NTR : `setup.exe /s /v" REMOVE=NTR /qn"`
Le package d'installation de mise à niveau utilisé pour nettoyer l'installation installe l'ensemble de fonctionnalités par défaut. [14.3 RU1 MP1 et versions antérieures]	Si vous créez un package d'installation de mise à niveau avec activation de l'option **Lors de la mise à jour, conserver les fonctionnalités existantes des clients** et que vous l'utilisez pour réaliser une nouvelle installation, l'ensemble de fonctionnalités par défaut est installé sur votre périphérique client. Pour installer un ensemble de fonctionnalités personnalisé, vous devez créer un package d'installation distinct pour la nouvelle installation.
Création de périphériques en double dans la console cloud en cas de séquence de mise à niveau non prise en charge [14.3 RU1]	La mise à niveau de macOS 10.15 vers la version 11.0 avant la mise à niveau de l'agent Symantec pour Mac à partir de la version 14.2/14.3 vers la version 14.3 RU1 crée des périphériques en double dans la console cloud. Pour éviter les doublons, vous devez mettre à niveau le client avant le système d'exploitation (c'est-à-dire mettre à niveau l'agent Symantec pour Mac de la version 14.2/14.3 vers la version 14.3 RU1, puis macOS de la version 10.15 vers la version 11.0).
Messages incorrects dans le journal du programme d'installation de l'agent Symantec pour Linux. [14.3 RU1]	Dans certains cas, le programme d'installation de l'agent consigne les messages incorrects liés à une version de pilote non correspondante ou à un redémarrage requis. Ces messages n'affectent pas la fonctionnalité de l'agent.
Sur une unité SuSe Linux, le décompresseur supprime les packages clients SEP Linux lors de la suppression du package 'at'. [14.3 RU1]	Sur une unité SuSe Linux, la commande 'zypper remove at' supprime les packages client Linux SEP, car le package 'at' est ajouté en tant que package dépendant requis et les commandes zypper tentent automatiquement de supprimer les packages client SEP 'sdcss-kmod' et 'sdcss-sepagent' en tant que packages avec dépendances inutilisées. **Solution :** pour supprimer le package 'at', exécutez la commande suivante : rpm-e--nodeps à
Problème de mise à niveau sur macOS 10.15 et versions ultérieures [14.3 MP1]	Sur macOS 10.15 et versions ultérieures, la fonction **Install Symantec Endpoint Protection to Remote Computers Installation de Symantec Endpoint Protection sur les ordinateurs distants** dans l'Assistant de déploiement de client ne parvient pas à mettre à niveau le client Symantec Endpoint Protection à partir de versions antérieures vers la version 14.3 MP1. **Solution :** utilisez **Symantec Endpoint Protection Manager Auto Upgrade (Mise à niveau automatique de Symantec Endpoint Protection Manager)** pour effectuer la mise à niveau de Symantec Endpoint Protection client sur macOS 10.15 et versions ultérieures.

Problème	Description et solution
Echec possible de l'installation du client Symantec Endpoint Protection 14.3 pour Windows, sauf en cas d'installation préalable de la prise en charge de SHA-2 [14.3]	Si vous exécutez des versions de système d'exploitation héritées (Windows 7 RTM ou SP1, Windows Server 2008 R2, R2 SP1 ou R2 SP2), vous devez installer la prise en charge de signature de code SHA-2 sur vos périphériques pour pouvoir installer les mises à jour Windows publiées en juillet 2019 ou à une date ultérieure. Sans la prise en charge de SHA-2, l'installation du client Windows échoue parfois. L'installation risque d'échouer si vous installez des clients pour la première fois ou si vous effectuez une mise à niveau automatique à partir d'une version antérieure.[SEP-61175/61403] Pour obtenir la prise en charge de signature de code SHA-2 appliquée par Microsoft, consultez les documents suivants : • Obligation de prise en charge de la signature du code SHA-2 2019 pour Windows et WSUS • Symantec Endpoint Protection 14.3 Windows client may fail to install unless SHA-2 support is installed (Echec de l'installation du client Symantec Endpoint Protection 14.3 pour Windows, sauf en cas d'installation de la prise en charge de SHA-2)
Non-exécution du client Windows de Symantec Endpoint Protection sous Windows 10 1803 lorsque l'UWF est activé [14.3]	Le client Symantec Endpoint Protection ne s'exécute pas correctement lorsqu'il est exécuté sur un système d'exploitation Windows 10 RS4 1803 32 bits et que le filtre d'écriture unifiée (UWF) est activé et qu'il protège le lecteur sur lequel le client Windows est installé. Ce système d'exploitation Windows inclut un défaut au niveau de l'UWF qui empêche le client Windows de s'exécuter. Pour contourner ce problème : • Effectuez une mise à niveau vers une autre version du système d'exploitation qui ne contient pas ce défaut. • Désactivez l'UWF.Voir : Endpoint Protection is malfunctioning when installed on Windows 10 1803 with UWF enabled (Problème de fonctionnement d'Endpoint Protection lorsqu'il est installé sous Windows 10 1803 et que l'UWF est activé)
Non-respect des paramètres de proxy personnalisés pour LiveUpdate [14.2 RU1 MP1 et versions ultérieures] par les clients Mac qui activent WSS Traffic Redirection	Vous avez configuré vos clients Mac gérés pour que Symantec Endpoint Protection 14.2 RU1 MP1 ou version ultérieure utilise des paramètres de proxy personnalisés pour LiveUpdate via les paramètres de communication externes. Cependant, après avoir activé WSS Traffic Redirection (WTR) pour vos clients Mac par le biais de la politique Symantec Endpoint Protection Manager, vous constatez que le trafic LiveUpdate ne respecte plus vos paramètres de proxy personnalisés. Au lieu de cela, LiveUpdate tente d'établir une connexion directe. Pour résoudre ce problème, n'utilisez les paramètres de proxy personnalisés pour LiveUpdate que lorsque WSS Traffic Redirection est désactivé.
Autorisation des téléchargements de fichiers PDF par Microsoft Edge lorsque le renforcement est activé (comportement inattendu)	Vous pouvez télécharger des fichiers PDF avec le navigateur Microsoft Edge bien que le renforcement d'application soit activé au niveau du client Symantec Endpoint Protection. Le blocage du téléchargement de fichiers PDF fonctionne comme prévu avec les autres navigateurs. Un correctif est prévu dans une version future pour ce problème.

Pour les problèmes résolus, consultez :

- Nouveaux correctifs et composants pour Symantec Endpoint Protection 14.3 RU3
- Nouveaux correctifs et composants pour Symantec Endpoint Protection 14.3 RU1 MP1
- Nouveaux correctifs et composants pour Symantec Endpoint Protection 14.3 RU1
- Nouveaux correctifs et composants pour Symantec Endpoint Protection 14.3 MP1
- Nouveaux correctifs et composants pour Symantec Endpoint Protection 14.3

Documentation

La documentation est disponible sur le portail Broadcom Symantec Security Tech Docs Portal.

Pour accéder à la documentation relative à Endpoint Protection, cliquez sur l'onglet **Symantec Security Software**, puis sur **Endpoint Security and Management** > **Endpoint Protection**.

Pour trouver un fichier PDF, des notes de mise à jour ou le schéma de base de données Symantec Endpoint Protection Manager, consultez la page Documents connexes. A l'avenir, Broadcom ajoutera les fichiers PDF hérités et les fichiers PDF traduits.

Configuration système requise pour Symantec Endpoint Protection (SEP) 14.3 RU3

De manière générale, la configuration requise pour les éléments suivants est la même que celle des systèmes d'exploitation sur lesquels ils sont pris en charge.

> **NOTE**
> Une version antérieure de Symantec Endpoint Protection Manager peut ne pas être capable de gérer correctement un client doté d'une version ultérieure. Des problèmes de mise à jour du contenu et de gestion des clients peuvent survenir.Par exemple, Symantec Endpoint Protection Manager 14.0.1 ou version antérieure ne peut pas fournir de client de la version 14.2 avec les monikers spécifiques à sa version. Symantec Endpoint Protection Manager pour les versions antérieures à la version 14 MP2 ne peut pas fournir les versions de client ultérieures à la version 14.0.1 avec les monikers spécifiques à leur version.

Les tableaux suivants décrivent la configuration matérielle et logicielle requise pour Symantec Endpoint Protection.

Table 4: Configuration logicielle requise pour instance de Symantec Endpoint Protection Manager (SEPM)

Composant	Configuration requise
Système d'exploitation	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 (à partir de la version 14.3 RU3) **Note:** Les systèmes d'exploitation pour ordinateurs de bureau ne sont pas pris en charge. **Note:** Windows Server Core Edition n'est pas pris en charge sur les versions 14.2x et antérieures.
Navigateur Web	Les navigateurs suivants sont pris en charge pour l'accès de la console web à instance de Symantec Endpoint Protection Manager et pour afficher l'aide de instance de Symantec Endpoint Protection Manager : • Navigateur basé sur Microsoft Edge Chromium (14.3 et versions ultérieures) • Microsoft Edge **Note:** La version 32 bits de Windows 10 ne prend pas en charge l'accès à la console Web sur le navigateur Edge. • Microsoft Internet Explorer 11 (14.2.x et versions antérieures) • Mozilla Firefox 5.x à 83 • Google Chrome 87

Composant	Configuration requise
Base de données	Symantec Endpoint Protection Manager inclut une base de données par défaut : • Microsoft SQL Server Express 2014 (pour Windows Server 2008 R2) • Microsoft SQL Server Express 2017 • Sybase Embedded Database (14.3 MP.x et versions antérieures uniquement) Vous pouvez également choisir d'utiliser une base de données d'une des versions suivantes de Microsoft SQL Server : • SQL Server 2008 SP4 • SQL Server 2008 R2, SP3 • SQL Server 2012 RTM - SP4 • SQL Server 2014 RTM - SP3 • SQL Server 2016 SP1, SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (14.3 et versions ultérieures) **Note:** Les bases de données SQL Server hébergées sur Amazon RDS sont prises en charge. (14.0.1 MP2 et versions ultérieures). **Note:** Si Symantec Endpoint Protection utilise une base de données SQL Server et que votre environnement utilise uniquement TLS 1.2, assurez-vous que SQL Server prend en charge TLS 1.2. Vous devrez peut-être appliquer un correctif à SQL Server. Ces recommandations s'appliquent à SQL Server 2008, 2012 et 2014.Voir : **Note:** Prise en charge de TLS 1.2 pour Microsoft SQL Server
Autres spécifications d'environnement	• Sur les réseaux uniquement IPv6, la pile IPv4 doit toujours être installée et désactivée. Si la pile IPv4 est désinstallée, instance de Symantec Endpoint Protection Manager ne fonctionne pas. • Package redistribuable Microsoft Visual C++ 2017 (x64/x86) **Note:** Notez que la version requise de Visual C++ est automatiquement installée pendant l'installation de instance de Symantec Endpoint Protection Manager

Table 5: Configuration matérielle requise pour instance de Symantec Endpoint Protection Manager

Composant	Configuration requise
Processeur	Intel Pentium Dual-Core ou équivalent minimum, 8 cœurs ou plus recommandé **Note:** Les processeurs Intel Itanium IA-64 ne sont pas pris en charge.
RAM physique	2 Go de RAM minimum, 8 Go ou plus recommandés. **Note:** Votre serveur instance de Symantec Endpoint Protection Manager peut nécessiter de la mémoire RAM supplémentaire en fonction de la configuration RAM requise pour les applications déjà installées.Par exemple, si Microsoft SQL Server est installé sur le serveur instance de Symantec Endpoint Protection Manager, celui-ci doit disposer d'un minimum de 8 Go d'espace disponible.
Affichage	1024 x 768 ou plus
Disque dur pour une installation sur le lecteur système	Avec une base de données SQL Server locale : • 40 Go minimum disponibles (200 Go recommandés) pour le serveur de gestion et une base de données Avec une base de données SQL Server distante : • 40 Go disponible minimum (100 Go recommandés) pour le serveur de gestion • Espace disque disponible supplémentaire sur le serveur distant pour la base de données

Composant	Configuration requise
Disque dur en cas d'installation sur un autre lecteur	Avec une base de données SQL Server locale : • Le lecteur système requiert un minimum de 15 Go d'espace disponible (100 Go recommandés) • Le lecteur d'installation requiert un minimum de 25 Go d'espace disponible (100 Go recommandés) Avec une base de données SQL Server distante : • Le lecteur système requiert un minimum de 15 Go d'espace disponible (100 Go recommandés) • Le lecteur d'installation requiert un minimum de 25 Go d'espace disponible (100 Go recommandés) • Espace disque disponible supplémentaire sur le serveur distant pour la base de données
Autres	Carte d'interface réseau activée

Si vous utilisez une base de données SQL Server, vous devrez peut-être libérer davantage d'espace disque. La quantité et l'emplacement de l'espace supplémentaire dépendent du lecteur utilisé par SQL Server, des exigences en maintenance de la base de données et d'autres paramètres de base de données.

Table 6: Configuration logicielle requise pour le client Symantec Endpoint Protection for Windows

Composant	Configuration requise
Système d'exploitation (ordinateur)	• Windows 7 (32 bits, 64 bits, RTM et SP1) • Windows Embedded 7 Standard, POSReady et Enterprise (32 bits et 64 bits) • Windows 8 (32 bits, 64 bits) • Windows Embedded Standard 8 (32 bits et 64 bits) • Windows 8.1 (32 bits, 64 bits), y compris Windows To Go • Mise à jour de Windows 8.1 pour avril 2014 (32 bits, 64 bits) • Mise à jour de Windows 8.1 pour août 2014 (32 bits, 64 bits) • Windows Embedded 8.1 Pro, Industry Pro et Industry Entreprise (32 bits et 64 bits) • Windows 10 (version 1507) (32 bits, 64 bits), y compris Windows 10 Entreprise 2015 LTSB • Windows 10 Mise à jour de novembre (version 1511) (32 bits, 64 bits) • Mise à jour anniversaire de Windows 10 (version 1607) (32 bits, 64 bits), y compris Windows 10 Entreprise 2016 LTSB • Windows 10 Creators Update (version 1703) (32 bits, 64 bits) • Windows 10 Fall Creators Update (version 1709) (32 bits, 64 bits) • Windows 10 Mise à jour d'avril 2018 (version 1803) (32 bits, 64 bits) • Windows 10 Mise à jour d'octobre 2018 (version 1809) (32 bits, 64 bits), y compris Windows 10 Entreprise 2019 • Windows 10 Mise à jour de mai 2019 (version 1903) (32 bits, 64 bits) • Windows 10 Mise à jour de novembre 2019 (version 1909) (32 bits et 64 bits) (versions 14.2 RU1 et ultérieures) • Windows 10 20H1 (Windows 10 version 2004) (version 14.3 et ultérieure) • Windows 10 20H2 (Windows 10 version 2009) (version 14.3 et ultérieure) • Windows 10 21H1 (à partir de la version 14.3 RU1) • La version 14.3 RU3 a été testée et est compatible avec toutes les versions précommerciales de Windows 11 (à partir de la version 14.3 RU3)
Système d'exploitation (serveur)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Mise à jour de Windows Server 2012 R2 pour avril 2014 • Mise à jour de Windows Server 2012 R2 pour août 2014 • Windows Server 2016 • Windows Server 2019 • Windows Server version 1803 (Server Core) (versions 14.2 et ultérieures) • Windows Server, version 1809 (Server Core) • Windows Server version 1903 (Server Core) (versions 14.2 RU1 et ultérieures) • Windows Server version 1909 (Server Core) (versions 14.2 RU1 et ultérieures) • Windows Server, version 2004 • Windows Server, version 20H2 (14.3 RU1) • Windows Server 2022 (à partir de la version 14.3 RU3) Pour obtenir la liste des systèmes d'exploitation pris en charge pour les versions précédentes, voir : • Compatibilité Windows avec le client Endpoint Protection • Prise en charge d'Endpoint Protection pour les mises à jour de Windows 10 et pour Windows Server 2016/Server 2019
Prévention d'intrusion du navigateur	La prise en charge de la fonction Prévention d'intrusion du navigateur dépend de la version du système de détection d'intrusion du client (CIDS).Voir : Voir Navigateurs pris en charge pour la prévention d'intrusion du navigateur dans Endpoint Protection

Table 7: Configuration matérielle requise pour le client Symantec Endpoint Protection pour Windows

Composant	Configuration requise
Processeur (pour les ordinateurs physiques)	• Processeur 32 bits : Intel Pentium 4 cadencé à 2 GHz ou équivalent minimum (Intel Pentium 4 ou équivalent recommandé) • Processeur 64 bits : Intel Pentium 4 cadencé à 2 GHz avec prise en charge x86-64 ou équivalent minimum **Note:** Les processeurs Itanium ne sont pas pris en charge.
Processeur (pour les ordinateurs virtuels)	Un socket virtuel et un cœur par socket à 1 GHz au minimum (un socket virtuel et deux cœurs par socket à 2 GHz sont recommandés) **Note:** La réservation de ressource de l'hyperviseur doit être activée.
RAM physique	1 Go (2 Go recommandé) ou plus si requis par le système d'exploitation
Affichage	800 x 600 ou plus
Disque dur	Les besoins en espace disque dépendent du type de client que vous installez, du lecteur sur lequel vous l'installez et de l'emplacement du fichier de données de programme. Le dossier de données de programme se trouve habituellement sur le lecteur système, à l'emplacement par défaut C:\ProgramData. De l'espace disque est toujours requis sur le lecteur système, quel que soit le lecteur d'installation que vous choisissez. **Note:** Les conditions d'espace requises sont basées sur les systèmes de fichiers NTFS. De l'espace supplémentaire est également requis pour les mises à jour et les journaux de contenu.

Table 8: Configuration requise sur le disque dur pour le client Symantec Endpoint Protection for Windows lorsqu'il est installé sur le lecteur système

Type de client	Configuration requise
Standard	Si le dossier de données de programme est situé sur le lecteur système : • 395 Mo* Si le dossier de données de programme est situé sur un autre lecteur : • Lecteur système : 180 Mo • Lecteur d'installation alternatif : 350 Mo
Client intégré/VDI	Si le dossier de données de programme est situé sur le lecteur système : • 245 Mo* Si le dossier de données de programme est situé sur un autre lecteur : • Lecteur système : 180 Mo • Lecteur d'installation alternatif : 200 Mo
Réseau invisible	Si le dossier de données de programme est situé sur le lecteur système : • 545 Mo* Si le dossier de données de programme est situé sur un autre lecteur : • Lecteur système : 180 Mo • Lecteur d'installation alternatif : 500 Mo

* 135 Mo supplémentaires sont requis pendant l'installation.

Table 9: Configuration requise sur le disque dur pour le client Symantec Endpoint Protection pour Windows lorsqu'il est installé sur un autre lecteur

Type de client	Configuration requise
Standard	Si le dossier de données de programme est situé sur le lecteur système : • Lecteur système : 380 Mo • Lecteur d'installation alternatif : 15 Mo* Si le dossier de données de programme est situé sur un autre lecteur :** • Lecteur système : 30 Mo • Lecteur de données de programme : 350 Mo • Lecteur d'installation alternatif : 150 Mo
Client intégré/VDI	Si le dossier de données de programme est situé sur le lecteur système : • Lecteur système : 230 Mo • Lecteur d'installation alternatif : 15 Mo* Si le dossier de données de programme est situé sur un autre lecteur :** • Lecteur système : 30 Mo • Lecteur de données de programme : 200 Mo • Lecteur d'installation alternatif : 150 Mo
Réseau invisible	Si le dossier de données de programme est situé sur le lecteur système : • Lecteur système : 530 Mo • Lecteur d'installation alternatif : 15 Mo* Si le dossier de données de programme est situé sur un autre lecteur :** • Lecteur système : 30 Mo • Lecteur de données de programme : 500 Mo • Lecteur d'installation alternatif : 150 Mo

* 135 Mo supplémentaires sont requis pendant l'installation.

** Si le dossier de données de programme est identique au lecteur d'installation alternatif, ajoutez 15 Mo au lecteur de données de programme. Cependant, le programme d'installation requiert toujours 150 Mo d'espace libre sur le lecteur d'installation alternatif pendant l'installation.

Table 10: Configuration requise pour le client Symantec Endpoint Protection for Windows Embedded

Composant	Configuration requise
Processeur	Intel Pentium cadencé à 1 GHz
RAM physique	256 MO **Note:** Ce chiffre illustre l'installation du client intégré Symantec Endpoint Protection. Si vous implémentez également d'autres fonctionnalités d'une solution intégrée, comme EDR, de la RAM physique supplémentaire est requise.
Disque dur	Le client Symantec Endpoint Protection intégré/VDI requiert l'espace minimum suivant sur le disque dur : • Installé sur le lecteur système : 245 Mo • Installé sur un autre lecteur : 230 Mo sur le lecteur système et 15 Mo sur le lecteur alternatif 135 Mo supplémentaires sont requis pendant l'installation. Ces chiffres supposent que le dossier de données de programme se trouve sur le lecteur système. Pour obtenir des informations plus détaillées ou pour connaître les conditions relatives aux autres types de clients, consultez la configuration requise pour le client Symantec Endpoint Protection pour Windows.

Composant	Configuration requise
Système d'exploitation Embedded	• Windows Embedded Standard 7 (32 et 64 bits) • Windows Embedded POSReady 7 (32 et 64 bits) • Windows Embedded Enterprise 7 (32 et 64 bits) • Windows Embedded Standard 8 (32 bits et 64 bits) • Windows Embedded Industry Pro 8.1 (32 et 64 bits) • Windows Embedded Industry Enterprise 8.1 (32 et 64 bits) • Windows Embedded Pro 8.1 (32 et 64 bits) • Windows Embedded 10 (à partir de la version 14.3 RU3) • La version 14.3 RU3 a été testée et est compatible avec toutes les versions précommerciales de Windows 11 Embedded (à partir de la version 14.3 RU3)
Composants requis au minimum	• Gestionnaire de filtres (FltMgr.sys) • Assistant de performance des données (pdh.dll) • Service Windows Installer
Modèles	• Compatibilité des applications (par défaut) • Signalisation numérique • Automatisation industrielle • IE, Media Player, RDP • Décodeur • Client léger Le modèle de configuration minimale n'est pas pris en charge. Le filtre d'écriture amélioré (EWF) et le filtre d'écriture unifié (UWF) ne sont pas pris en charge. Le filtre d'écriture recommandé est le filtre d'écriture basé sur le fichier installé avec le filtre du registre.

Table 11: Configuration requise pour le client Symantec Endpoint Protection pour Mac

Composant	Configuration requise
Processeur/puce	Intel Core 2 Duo 64 bits ou version ultérieure Puce Apple M1 (à partir de la version 14.3 RU2)
RAM physique	2 Go de RAM
Disque dur	1 Mo d'espace disponible sur le disque dur pour l'installation
Affichage	800 x 600
Système d'exploitation	• macOS 10.15 à 10.15.7 • macOS 11 (Big Sur) Pour obtenir la liste des systèmes d'exploitation pris en charge pour les versions précédentes, voir : Compatibilité Mac avec le client Endpoint Protection

Table 12: Configuration requise pour le client Symantec Endpoint Protection pour Linux

Composant	Configuration requise
Matériel	• Intel Pentium 4 (2 GHz) ou supérieur • 1 Go de RAM libre (4 Go de RAM recommandés) • 2 Go d'espace disque disponible si les répertoires `/var`, `/opt` et `/tmp` partagent le même système de fichiers/volume • 500 Mo d'espace disque disponible dans chaque répertoire `/var`, `/opt` et `/tmp` s'ils se trouvent sur des volumes différents
Systèmes d'exploitation	Systèmes d'exploitation pris en charge à partir de la version 14.3 RU1 : • Amazon Linux 2 • CentOS 6, 7, 8 • Debian 9, 10 (14.3 RU2 et versions ultérieures) • Oracle Enterprise Linux 6, 7, 8 • Red Hat Enterprise Linux 6, 7, 8 • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Pour plus d'informations et pour obtenir la liste des versions mineures du système d'exploitation Linux prises en charge, voir : Noyaux de l'agent Symantec Linux pris en charge Systèmes d'exploitation pris en charge pour la version 14.3 MP1 et les versions antérieures : • Amazon Linux • CentOS 6U3 - 6U9, 7 - 7U7, 8 ; 32 bits et 64 bits • Debian 6.0.5 Squeeze, Debian 8 Jessie ; 32 et 64 bits • Fedora 16, 17 ; 32 et 64 bits • Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8 ; 7, 7U1, 7U2, 7U3, 7U4 • Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2 • SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32 et 64 bits ; 12, 12 SP1 - 12 SP3, 64 bits • SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32 bits et 64 bits ; 12 SP3, 64 bits • Ubuntu 12.04, 14.04, 16.04, 18.04 (à compter de la version 14.3) ; 32 bits et 64 bits Pour obtenir la liste des noyaux système pris en charge pour les versions précédentes, voir : Liste des distributions et noyaux Linux avec pilotes/modules Auto-Protect précompilés pour Symantec Endpoint Protection for Linux 14.x
Autres exigences au niveau de l'environnement (14.3 RU1 et versions ultérieures)	• OpenSSL 1.0.2 k-FIPS ou version ultérieure

Composant	Configuration requise

Autres exigences liées à l'environnement (14.3 MP1 et versions précédentes)	• Glibc
	Les systèmes d'exploitation exécutant une version de glibc antérieure à 2.6 ne sont pas pris en charge.
	• net-tools ou iproute2
	Symantec Endpoint Protection utilise l'un de ces deux outils, selon celui qui est déjà installé sur l'ordinateur.
	• Outils de développement
	La compilation automatique et le processus de compilation manuelle pour le module de noyau Auto-Protect requièrent l'installation de certains outils de développement. Ces outils de développement incluent gcc et les fichiers d'en-tête et de source du noyau. Pour plus d'informations sur les éléments à installer et la procédure d'installation à suivre pour les versions spécifiques de Linux, consultez :
	Compilation manuelle des modules de noyau Auto-Protect pour Endpoint Protection pour Linux
	• Packages dépendants i686 sur les ordinateurs 64 bits
	Beaucoup de fichiers exécutables dans le client Linux sont des programmes 32 bits. Pour les ordinateurs 64 bits, vous devez installer les packages dépendants i686 avant d'installer le client Linux.
	Si vous n'avez pas encore installé les packages dépendants i686, vous pouvez les installer avec une ligne de commande. Cette installation requiert les privilèges de superutilisateur, comme l'illustrent les commandes suivantes, qui incluent `sudo` :
	– Pour les distributions basées sur Red Hat : `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Pour les distributions basées sur Debian : `sudo apt-get install ia32-libs`
	– Pour les distributions basées sur Ubuntu :
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`

Environnements de bureau graphique	Vous pouvez utiliser les environnements de bureau graphiques suivants pour afficher le client Symantec Endpoint Protection pour Linux : • KDE • Gnome • Unity Symantec Agent for Linux 14.3 RU1 ne dispose pas d'une interface utilisateur graphique.

Autres informations

Versions de mise à jour, notes, nouveaux correctifs et configuration système requise pour Endpoint Security et toutes les versions d'Endpoint Protection

Séquences de mise à niveau vers la dernière version de Symantec Endpoint Protection 14.x prise en charge et non prise en charge.

Généralement, pour les versions de Symantec Endpoint Protection antérieures à la version la plus récente, chaque version sur la liste avant sa prise en charge. Cependant, vous devez vérifier en vous reportant aux notes de mise à jour pour votre version spécifique.Voir :

Versions de mise à jour, notes, nouveaux correctifs et configuration système requise pour Endpoint Security et toutes les versions d'Endpoint Protection

Chemins de mise à niveau pris en charge

- Symantec Endpoint Protection Manager 12.1.6 MP10 et versions ultérieures avec la base de données imbriquée est mis à niveau de manière transparente vers la base de données Microsoft SQL Server Express, version 14.3 RU1 MP1. Les mises à niveau de la version 12.1.6 MP9 ou d'une version antérieure vers la version 14.3 RU1 MP1 sont bloquées.
- Symantec Endpoint Protection Manager 14.x est mis à niveau de manière transparente vers la version 12.1.x, à l'exception des systèmes d'exploitation suivants : Windows Server 2003, les systèmes d'exploitation de bureau et les systèmes d'exploitation 32 bits, ainsi que certaines versions de SQL Server.
- Le client Symantec Endpoint Protection 14.x est mis à niveau en toute transparence sur toutes les versions client 12.1 antérieures installées sur les systèmes d'exploitation pris en charge.Voir :

Remarques concernant la migration de Symantec Endpoint Protection 14

instance de Symantec Endpoint Protection Manager et client Windows

Les versions suivantes de instance de Symantec Endpoint Protection Manager et du client Windows Symantec Endpoint Protection peuvent être directement mises à niveau vers la version actuelle :

- 11.x et Small Business Edition 12.0 (clients Symantec Endpoint Protection uniquement, pour les systèmes d'exploitation pris en charge)
- 12.1.x, jusqu'à la version 12.1.6 MP10
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1, 14.3 RU2

Client Mac

Les versions suivantes du client Symantec Endpoint Protection pour Mac peuvent être directement mises à niveau vers la version actuelle :

- 12.1.4 - 12.1.6 MP9

Le client Mac n'a pas été mis à jour pour la version 12.1.6 MP10.
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
  Le client Symantec Endpoint Protection pour Mac n'a pas été mis à jour vers la version 14.0.1 MP2.
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1 (disponible depuis juin 2021), 14.3 RU2

Client Linux

> **NOTE**
> À partir de la version 14.3 RU1, le programme d'installation du client Linux détecte et désinstalle le client Linux hérité (antérieur à la version 14.3 RU1), puis effectue une nouvelle installation du nouveau client. Les anciennes configurations ne sont pas conservées.

Les versions suivantes du client Symantec Endpoint Protection pour Linux peuvent être directement mises à niveau vers la version actuelle :

- 12.1. x, jusqu'à la version 12.1.6 MP9
  Le client Linux n'a pas été mis à jour pour la version 12.1.6 MP10.
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1, 14.3 RU2

Symantec AntiVirus for Linux 1.0.14 est la seule version que vous pouvez migrer directement vers Symantec Endpoint Protection. Vous devez d'abord désinstaller toutes les autres versions de Symantec AntiVirus for Linux. Vous ne pouvez pas migrer un client géré vers un client non géré.

Séquences de mise à niveau non prises en charge

Vous ne pouvez pas migrer vers Symantec Endpoint Protection à partir de tous les produits Symantec. Vous devez désinstaller les produits suivants avant d'installer le client Symantec Endpoint Protection.

- Symantec AntiVirus et Symantec Client Security, qui ne sont pas pris en charge.
- Tous les produits Norton de Symantec
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Tout Symantec Endpoint Protection pour le client Mac de plus de 12.1.4.Vous pouvez également le mettre à niveau vers 12.1.4 ou une version ultérieure.

Informations supplémentaires

- Toute migration de client Symantec Endpoint Protection pour la version antérieure à la version 12.1.x n'est pas prise en charge.
- Vous ne pouvez pas mettre à niveau Symantec Endpoint Protection Manager 11.0.x ou Symantec Endpoint Protection Manager Small Business Edition 12.0.x directement vers n'importe quelle version de Symantec Endpoint Protection

Manager 14. Vous devez d'abord désinstaller ces versions ou effectuer une mise à niveau vers la version 12.1.x avant la mise à niveau vers la dernière version de 14.x.

- Vous ne pouvez pas mettre à niveau instance de Symantec Endpoint Protection Manager 12.1.6 MP7 vers la version 14 car la version de schéma de la base de données dans la version 12.1.6 MP7 est ultérieure à celle dans la version 14. À la place, vous devez mettre à niveau la version 12.1.6 MP7 vers la version 14 MP1 ou ultérieure.
- 14.0.x a supprimé la prise en charge de Windows XP, Server 2003 et de tout système d'exploitation Windows Embedded basé sur Windows XP. Symantec Endpoint Protection Manager 14.2 RU1 peut gérer ces ordinateurs comme des clients hérités 12.1.x, même si les clients 12.1.x sont en fin de vie. Pour ces clients, vous pouvez utiliser un produit Symantec qui prend toujours en charge ces systèmes d'exploitation hérités, tels que le Data Center Security (DCS).
- La mise à niveau de 14 MP1 (14.0.2332.0100) vers le build d'actualisation 14 MP1 (14.0.2349.0100) n'est pas prise en charge.
- Les chemins d'accès de mise à niveau vers une version antérieure ne sont pas pris en charge. Par exemple, si vous voulez effectuer la migration de Symantec Endpoint Protection 14.2.1.1 vers la version 12.1.6 MP10, vous devez d'abord désinstaller Symantec Endpoint Protection 14.2.1.
- Si vous disposez d'un numéro de build mais que vous ne savez pas comment le convertir en numéro de version, consultez :

  A propos des types et versions d'Endpoint Protection

Sites web à visiter pour obtenir des informations complémentaires

Le tableau suivant répertorie les sites Web où vous pouvez obtenir des pratiques d'excellence, des informations de dépannage et d'autres ressources pour vous aider à utiliser le produit.

Table 13: Informations disponibles sur le site Web d'Endpoint Protection

Types d'informations	Lien vers le site web
Versions d'évaluation	Contactez votre responsable de compte.
Mises à jour des manuels et de la documentation	Page Documents connexes Pour les autres langues, cliquez sur le menu déroulant **Anglais**.
Support technique	Support technique Endpoint Protection Inclut des articles de base de connaissances, des détails de version du produit, des mises à jour et des correctifs et des options de contact pour la prise en charge.
Informations et mises à jour sur les menaces	Symantec Security Center
Formation	Education Services Accédez aux cours de formation, eLibrary et bien plus.
Forums Symantec Connect	Endpoint Protection


Symantec
A Division of Broadcom