# Notes de mise à jour de Symantec™ Endpoint Protection 14.3

**Dernière mise à jour : juin 2020**

# Table of Contents

# Déclaration de copyright

# Nouveautés dans Symantec Endpoint Protection 14.3

Cette section décrit les fonctionnalités nouvelles dans la version 14.3.

**Fonctions de protection**

- Les développeurs d'applications tierces peuvent protéger leurs clients contre les malwares basés sur un script dynamique et contre les sources de cyberattaques non traditionnelles. L'application tierce appelle l'interface AMSI de Windows pour demander une analyse du script fourni par l'utilisateur, qui est routé vers le client Symantec Endpoint Protection. Le client répond par un verdict afin d'indiquer si le comportement du script est malveillant ou non. Si le comportement n'est pas malveillant, le script est exécuté. S'il est malveillant, le script n'est pas exécuté.Sur l'ordinateur client, la boîte de dialogue Résultats de la détection affiche l'état Accès refusé.Windows PowerShell, JavaScript et VBScript sont quelques exemples de scripts tiers. La fonction Auto-Protect doit être activée. Cette fonctionnalité est disponible sur les ordinateurs tournant sous Windows 10 et versions ultérieures.
  How the Antimalware Scan Interface (AMSI) helps you defend against malware
  Antimalware Scan Interface (AMSI)

**Symantec Endpoint Protection Manager**

- La console distante de Symantec Endpoint Protection prend désormais en charge Java 11 et non Java 8.Pour accéder à la console distante, ouvrez un navigateur Web pris en charge, saisissez l'adresse `http://SEPMServer:9090/symantec.html` dans la zone d'adresse, puis téléchargez le package correspondant à la console distante. Suivez les instructions qui s'affichent. La version précédente de la console distante de Symantec Endpoint Protection Manager n'est plus prise en charge.
  Connexion à Symantec Endpoint Protection
- Vous pouvez configurer l'un des gestionnaires Symantec Endpoint Protection Manager sur le site en tant que serveur de journalisation principal pour transférer les journaux vers le serveur Syslog. Si le serveur de journalisation principal est hors ligne, un deuxième serveur de gestion prend le relais et transfère les journaux vers le serveur Syslog. Lorsque le serveur de journalisation principal est à nouveau en ligne, il reprend le contrôle du transfert des journaux.
  Configuration d'un serveur de basculement pour la journalisation externe
- La politique Intégrations inclut une nouvelle option **Activer le fichier PAC personnalisé LPS** pour WSS Traffic Redirection.Cette option permet de remplacer le fichier PAC par défaut hébergé sur le serveur LPS du client par un fichier PAC personnalisé. Le fichier PAC personnalisé résout les problèmes de compatibilité avec les applications tierces qui ne fonctionnent pas avec un serveur proxy local à l'écoute sur la carte de bouclage.
  Configuration de WSS Traffic Redirection
- Prise en charge de la base de données Microsoft SQL Server 2019.
- Le processus d'analyse antivirus utilise désormais un service distinct du service principal non sécurisé. Ce nouveau processus d'analyse offre une utilisation plus efficace de la mémoire, une protection continue et une dépendance moindre vis-à-vis des problèmes liés au service principal.
- Le schéma de base de données inclut de nouvelles colonnes pour une fonctionnalité devant être ajoutée dans une version future (tables AGENT_SECURITY_LOG_1, AGENT_SECURITY_LOG_2, SEM_AGENT).
- L'API REST inclut les champs suivants dans le fichier JSON de réponse d'API /sepm/api/v1/computers pour appeler et télécharger le rapport sur l'état de l'ordinateur : quarantineStatus, quarantineCode, wssStatus et pskVersion.
- Les composants tiers suivants ont été mis à niveau vers la version la plus récente : Apache Tomcat, Boost C++ Libraries, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, Microsoft JDBC Driver for SQL Server, OpenSC, OpenSSL, Spring Security, spring-framework et sqlite.
- Pour inscrire le domaine Symantec Endpoint Protection Manager dans la console cloud, vous devez d'abord obtenir le jeton d'inscription via la console Symantec Endpoint Security. Jusqu'à présent, le jeton d'inscription s'obtenait en cliquant sur **Get Started** (Démarrage) dans la page **Cloud**.

**Mises à jour de client et de plate-forme**

- Le client Windows prend en charge Windows 10 20H1 (Windows 10 version 2004)
- Le client Linux prend désormais en charge Ubuntu 18.04, RHEL 8 et CentOS 8.
- L'outil AppRemover a été mis à jour vers une version plus récente.Il se charge de supprimer les applications tierces pour que vous puissiez installer le client Windows.Pour plus d'informations sur les applications qu'il supprime, reportez-vous à l'article Third-party security software removal in Endpoint Protection 14.3 (Suppression de logiciels de sécurité tiers dans Symantec Endpoint Protection 14.3).

**Fonctionnalités supprimées**

- Les notifications suivantes n'affichent plus les champs **Gravité du risque** et **Type de risque** : Propagation de risque, Evénement de risque unique et Nouveau risque détecté.

Nouveautés dans toutes les versions de Symantec Endpoint Protection

# Problèmes connus et solutions

Les informations répertoriées dans cette section s'appliquent à cette version de Symantec Endpoint Protection.

**Table 1: Problèmes de mise à niveau**

| 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]<br>Pour contourner ce problème, désactivez le mode FIPS au niveau du système d'exploitation :<br>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**.<br>2. Mise à niveau de SQL Server version 2017 vers la version 2019<br>3. Une fois la mise à niveau de SQL Server terminée, réactivez le mode FIPS.<br>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.<br>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. |

### Table 2: Problèmes liés à Symantec Endpoint Protection Manager

| Problème | Description et solution |
|---|---|
| Présence d'URL supplémentaires dans la liste blanche de Symantec Endpoint Security lors de l'utilisation de l'option de gestion hybride et de serveurs proxy [14.2.2.1 ou version ultérieure] | Avec l'acquisition récente de Symantec Enterprise Security, les URL des communications client à cloud ont été modifiées dans la version 14.2.2.1. [CDM-42467]<br>Vous devez mettre à niveau vos clients vers la version 14.2.5569.2100 ou vers une version ultérieure dans la situation suivante :<br>• 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.<br>• Vous utilisez des serveurs proxy.<br>Pour ajouter des URL à la liste blanche dans des agents entièrement gérés dans le cloud ou gérés de manière hybride, vous devez utiliser Symantec Endpoint Security :<br>1. Dans Symantec Endpoint Security, sélectionnez **Endpoint > Policies > [policy name] Whitelist Policy** (Terminal > Politiques > Politique Liste blanche [nom de la politique]).<br>2. Dans la politique Liste blanche, en regard de **Excluded by Domain** (Exclu par domaine), sélectionnez **Add** (Ajouter), ajoutez les URL suivantes une par une, puis sélectionnez **Add** (Ajouter) :<br>`us.spoc.securitycloud.symantec.com`<br>`eu.spoc.securitycloud.symantec.com` (ajouter si vous possédez des périphériques en Europe).<br>Conservez spoc.norton.com si vous continuez à gérer les clients avec une version ultérieure.<br>3. Sélectionnez **Save Policy** (Enregistrer la politique), puis **Yes** (Oui) pour mettre à jour la politique et l'appliquer aux groupes existants.<br>Voir URL à ajouter à la liste blanche pour Symantec Endpoint Security.<br>Voir Mise à niveau des agents Symantec gérés dans le cloud vers la version 14.2 Ru2 MP1 ou vers une version ultérieure avant le 4 mai 2020. |
| Fin de prise en charge de la plate-forme Windows 32 bits [14.3] par la console distante Symantec Endpoint Protection Manager | A partir de la version 14.3, 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]<br>Si le message suivant s'affiche, connectez-vous à Symantec Endpoint Protection Manager en local :<br>"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).<br>Logging on to the Symantec Endpoint Protection Manager (Connexion à Symantec Endpoint Protection Manager) |
| 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]<br>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. |

| Problème | Description et solution |
|---|---|
| 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 :<br>`<SEVERE> WinHttpSendRequest: 12175: A security error occurred`<br>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.<br>Pour résoudre ce problème, installez la mise à jour KB3140245 de Microsoft. Pour plus d'informations, consultez l'article :<br>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.<br>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. |

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

| 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]<br>Pour obtenir la prise en charge de signature de code SHA-2 appliquée par Microsoft, consultez les documents suivants :<br>Obligation de prise en charge de la signature du code SHA-2 2019 pour Windows et WSUS<br>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.<br>Pour contourner ce problème :<br>• Effectuez une mise à niveau vers une autre version du système d'exploitation qui ne contient pas ce défaut.<br>• 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). |

| Problème | Description et solution |
|---|---|
| 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.<br>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.<br>Un correctif est prévu dans une version future pour ce problème. |

Avec l'annonce récente par Broadcom de l'intégration officielle de Symantec Enterprise Protection, Symantec a migré la documentation vers le portail Symantec Security Tech Docs Portal de Broadcom.

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

**Table 4: Problèmes liés à la documentation**

| Problème | Description et solution |
|---|---|
| Les articles de procédure HOWTO ont expiré. | Les articles de procédure HOWTO, qui étaient des doublons des rubriques de l'aide de Symantec Endpoint Protection Manager, ont été republiés sur le site d'Endpoint Protection et possèdent maintenant une URL différente.<br>Pour rechercher un article, utilisez le **champ de recherche**. |
| Fichiers PDF | Symantec a publié tous les fichiers PDF sur les articles DOC. Ces pages ont expiré.<br>Pour trouver la version la plus récente du fichier PDF, rendez-vous sur la page Documents connexes. A l'avenir, Broadcom ajoutera les fichiers PDF hérités et les fichiers PDF traduits. |

Pour connaître la liste des problèmes résolus, reportez-vous à l'article New fixes and components for Symantec Endpoint Protection 14.3 (Nouveaux correctifs et composants pour Symantec Endpoint Protection 14.3).

# Configuration système requise pour Symantec Endpoint Protection (SEP)

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 un 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 5: Configuration logicielle requise pour Symantec Endpoint Protection Manager (SEPM)**

| Composant | Configuration requise |
|---|---|
| Système d'exploitation | • Windows Server 2008 R2<br>• Windows Server 2012<br>• Windows Server 2012 R2<br>• Windows Server 2016<br>• Windows Server 2019<br>**Note:** Les systèmes d'exploitation pour ordinateurs de bureau ne sont pas pris en charge.<br>**Note:** L'édition Windows Server Core n'est pas prise en charge. Windows Server Core n'inclut pas Internet Explorer, requis par Symantec Endpoint Protection Manager pour fonctionner. |
| Navigateur Web | Les navigateurs suivants sont pris en charge pour l'accès de la console web à Symantec Endpoint Protection Manager et pour afficher l'aide de Symantec Endpoint Protection Manager :<br>• Microsoft Edge<br>Remarque : la version 32 bits de Windows 10 ne prend pas en charge l'accès à la console web sur le navigateur Edge.<br>• Microsoft Internet Explorer 11<br>• Mozilla Firefox 5.x à 68.x<br>• Google Chrome 75.x |

| Composant | Configuration requise |
|---|---|
| Base de données | **Symantec Endpoint Protection Manager comprend une base de données intégrée. Vous pouvez également choisir d'utiliser une base de données d'une des versions suivantes de Microsoft SQL Server :**<br>• SQL Server 2008, SP4<br>• SQL Server 2008 R2, SP3<br>• SQL Server 2012, RTM - SP4<br>• SQL Server 2014, RTM - SP3<br>• SQL Server 2016, RTM, SP1, SP2<br>• SQL Server 2017, RTM<br>• SQL Server 2019, RTM (à compter de la version 14.3)<br>**Note:** La base de données SQL Server Express Edition n'est pas prise en charge.Les bases de données SQL Server hébergées sur Amazon RDS sont prises en charge (à compter de la version 14.0.1 MP2).<br>**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.Sans le correctif SQL Server permettant de prendre en charge TLS 1.2, vous risquez de rencontrer des problèmes lors de la mise à niveau de Symantec Endpoint Protection 12.1 vers la version 14.<br>**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, Symantec Endpoint Protection Manager ne fonctionne pas. |

### Table 6: Configuration matérielle requise pour Symantec Endpoint Protection Manager

| Composant | Configuration requise |
|---|---|
| Processeur | Intel Pentium Dual-Core ou équivalent minimum, 8 cœurs ou plus recommandé<br>**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.<br>**Note:** Votre serveur 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 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 intégrée ou une base de données SQL Server locale :**<br>• 40 Go minimum disponibles (200 Go recommandés) pour le serveur de gestion et une base de données<br>**Avec une base de données SQL Server distante :**<br>• 40 Go disponible minimum (100 Go recommandés) pour le serveur de gestion<br>• 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 intégrée ou une base de données SQL Server locale :**<br>• Le lecteur système requiert un minimum de 15 Go d'espace disponible (100 Go recommandés)<br>• Le lecteur d'installation requiert un minimum de 25 Go d'espace disponible (100 Go recommandés)<br>**Avec une base de données SQL Server distante :**<br>• Le lecteur système requiert un minimum de 15 Go d'espace disponible (100 Go recommandés)<br>• Le lecteur d'installation requiert un minimum de 25 Go d'espace disponible (100 Go recommandés)<br>• Espace disque disponible supplémentaire sur le serveur distant pour la base de données |

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 7: 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)<br>• Windows Embedded 7 Standard, POSReady et Enterprise (32 bits et 64 bits)<br>• Windows 8 (32 bits, 64 bits)<br>• Windows Embedded Standard 8 (32 bits et 64 bits)<br>• Windows 8.1 (32 bits, 64 bits), y compris Windows To Go<br>• Mise à jour de Windows 8.1 pour avril 2014 (32 bits, 64 bits)<br>• Mise à jour de Windows 8.1 pour août 2014 (32 bits, 64 bits)<br>• Windows Embedded 8.1 Pro, Industry Pro et Industry Entreprise (32 bits et 64 bits)<br>• Windows 10 (version 1507) (32 bits, 64 bits), y compris Windows 10 Entreprise 2015 LTSB<br>• Windows 10 Mise à jour de novembre (version 1511) (32 bits, 64 bits)<br>• Mise à jour anniversaire de Windows 10 (version 1607) (32 bits, 64 bits), y compris Windows 10 Entreprise 2016 LTSB<br>• Windows 10 Creators Update (version 1703) (32 bits, 64 bits)<br>• Windows 10 Fall Creators Update (version 1709) (32 bits, 64 bits)<br>• Windows 10 Mise à jour d'avril 2018 (version 1803) (32 bits, 64 bits)<br>• Windows 10 Mise à jour d'octobre 2018 (version 1809) (32 bits, 64 bits), y compris Windows 10 Entreprise 2019<br>• Windows 10 Mise à jour de mai 2019 (version 1903) (32 bits, 64 bits)<br>• Windows 10 Mise à jour de novembre 2019 (version 1909) (32 bits et 64 bits) (versions 14.2 RU1 et ultérieures)<br>• Windows 10 20H1 (Windows 10 version 2004) (à compter de la version 14.3) |
| Système d'exploitation (serveur) | • Windows Server 2008 R2<br>• Windows Small Business Server 2011<br>• Windows Server 2012<br>• Windows Server 2012 R2<br>• Mise à jour de Windows Server 2012 R2 pour avril 2014<br>• Mise à jour de Windows Server 2012 R2 pour août 2014<br>• Windows Server 2016<br>• Windows Server 2019<br>• Windows Server version 1803 (Server Core) (versions 14.2 et ultérieures)<br>• Windows Server, version 1809 (Server Core)<br>• Windows Server version 1903 (Server Core) (versions 14.2 RU1 et ultérieures)<br>• Windows Server version 1909 (Server Core) (versions 14.2 RU1 et ultérieures) |
| Prévention d'intrusion du navigateur | La prise en charge de la prévention d'intrusion du navigateur dépend de la version du système de détection des intrusions du client (CIDS).<br>Reportez-vous à la section Navigateurs pris en charge pour la prévention d'intrusion du navigateur dans Endpoint Protection. |

### Table 8: Configuration matérielle requise pour le client Symantec Endpoint Protection for 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)<br>• Processeur 64 bits : Intel Pentium 4 cadencé à 2 GHz avec prise en charge x86-64 ou équivalent minimum<br>**Note:** Les processeurs Itanium ne sont pas pris en charge. |
| Processeur (pour les machines virtuelles) | 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)<br>**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.<br>De l'espace disque est toujours requis sur le lecteur système, quel que soit le lecteur d'installation que vous choisissez.<br>**Configuration requise du disque dur :**<br>• La section Configuration requise sur le disque dur pour le client Symantec Endpoint Protection for Windows lorsqu'il est installé sur le lecteur système décrit la configuration requise au niveau du disque dur quand Symantec Endpoint Protection est installé sur le lecteur système.<br>• Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to an alternate drive décrit la configuration requise au niveau du disque dur quand Symantec Endpoint Protection est installé sur un lecteur alternatif.<br>**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 9: 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 :**<br>• 395 Mo*<br>**Si le dossier de données de programme est situé sur un autre lecteur :**<br>• Lecteur système : 180 Mo<br>• Lecteur d'installation alternatif : 350 Mo |
| Embedded/VDI | **Si le dossier de données de programme est situé sur le lecteur système :**<br>• 245 Mo*<br>**Si le dossier de données de programme est situé sur un autre lecteur :**<br>• Lecteur système : 180 Mo<br>• Lecteur d'installation alternatif : 200 Mo |
| Réseau invisible | **Si le dossier de données de programme est situé sur le lecteur système :**<br>• 545 Mo*<br>**Si le dossier de données de programme est situé sur un autre lecteur :**<br>• Lecteur système : 180 Mo<br>• Lecteur d'installation alternatif : 500 Mo |

*135 Mo supplémentaires sont requis pendant l'installation.

**Table 10: Configuration requise sur le disque dur pour le client Symantec Endpoint Protection for 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 :**<br>• Lecteur système : 380 Mo<br>• Lecteur d'installation alternatif : 15 Mo*<br>**Si le dossier de données de programme est situé sur un autre lecteur :****<br>• Lecteur système : 30 Mo<br>• Lecteur de données de programme : 350 Mo<br>• Lecteur d'installation alternatif : 150 Mo |
| Embedded/VDI | **Si le dossier de données de programme est situé sur le lecteur système :**<br>• Lecteur système : 230 Mo<br>• Lecteur d'installation alternatif : 15 Mo*<br>**Si le dossier de données de programme est situé sur un autre lecteur :****<br>• Lecteur système : 30 Mo<br>• Lecteur de données de programme : 200 Mo<br>• Lecteur d'installation alternatif : 150 Mo |
| Réseau invisible | **Si le dossier de données de programme est situé sur le lecteur système :**<br>• Lecteur système : 530 Mo<br>• Lecteur d'installation alternatif : 15 Mo*<br>**Si le dossier de données de programme est situé sur un autre lecteur :****<br>• Lecteur système : 30 Mo<br>• Lecteur de données de programme : 500 Mo<br>• 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 11: 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<br>**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 Embedded/VDI requiert l'espace disque minimum suivant :<br>• Installé sur le lecteur système : 245 Mo<br>• Installé sur un autre lecteur : 230 Mo sur le lecteur système et 15 Mo sur le lecteur alternatif<br>135 Mo supplémentaires sont requis pendant l'installation.<br>Ces chiffres supposent que le dossier de données de programme se trouve sur le lecteur système. Pour des informations plus détaillées ou pour les conditions relatives aux autres types de clients, consultez la configuration requise pour le client Symantec Endpoint Protection for Windows. |

| Composant | Configuration requise |
|---|---|
| Système d'exploitation Embedded | • Windows Embedded Standard 7 (32 et 64 bits)<br>• Windows Embedded POSReady 7 (32 et 64 bits)<br>• Windows Embedded Enterprise 7 (32 et 64 bits)<br>• Windows Embedded Standard 8 (32 bits et 64 bits)<br>• Windows Embedded Industry Pro 8.1 (32 et 64 bits)<br>• Windows Embedded Industry Enterprise 8.1 (32 et 64 bits)<br>• Windows Embedded Pro 8.1 (32 et 64 bits) |
| Composants requis au minimum | • Gestionnaire de filtres (FltMgr.sys)<br>• Assistant de performance des données (pdh.dll)<br>• Service Windows Installer |
| Modèles | • Compatibilité des applications (par défaut)<br>• Signalisation numérique<br>• Automatisation industrielle<br>• IE, Media Player, RDP<br>• Décodeur<br>• Client léger<br>Le modèle de configuration minimale n'est pas pris en charge.<br>Enhanced Write Filter (EWF) et Unified Write Filter (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 12: Configuration requise pour le client Symantec Endpoint Protection for Mac**

| Composant | Configuration requise |
|---|---|
| Processeur | Intel Core 2 Duo 64 bits ou version ultérieure |
| RAM physique | 2 Go de RAM |
| Disque dur | 500 Mo d'espace disponible sur le disque dur pour l'installation |
| Affichage | 800 x 600 |
| Système d'exploitation | • macOS 10.13<br>• macOS 10.14<br>• macOS 10.15 à 10.15.5<br>macOS 10.14.5 et versions ultérieures prennent en charge les exigences de notarisation kext. Rendez-vous sur la page Endpoint Protection 14.2 RU1 and kext notarization for macOS 10.14.5 (Endpoint Protection 14.2 RU1 et notarisation kext pour macOS).<br>Pour obtenir la liste des systèmes d'exploitation pris en charge pour les versions précédentes, consultez le document Mac compatibility with the Endpoint Protection client. |

**Table 13: Configuration requise pour les clients Symantec Endpoint Protection pour Linux**

| Composant | Configuration requise |
|---|---|
| Matériel | • Intel Pentium 4 (2 GHz) ou supérieur<br>• 1 Go de RAM<br>• 7 Go d'espace disponible sur le disque dur |
| Systèmes d'exploitation | • Amazon Linux<br>• CentOS 6U3 - 6U9, 7 - 7U7, 8 ; 32 bits et 64 bits<br>• Debian 6.0.5 Squeeze, Debian 8 Jessie ; 32 et 64 bits<br>• Fedora 16, 17 ; 32 et 64 bits<br>• Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8 ; 7, 7U1, 7U2, 7U3, 7U4<br>• Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2<br>• SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32 et 64 bits ; 12, 12 SP1 - 12 SP3, 64 bits<br>• SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32 bits et 64 bits ; 12 SP3, 64 bits<br>• Ubuntu 12.04, 14.04, 16.04, 18.04 (à compter de la version 14.3) ; 32 bits et 64 bits<br>Pour obtenir la liste des noyaux de système d'exploitation pris en charge pour les versions précédentes, reportez-vous à l'article Supported Linux kernels for Symantec Endpoint Protection. |
| Environnements de bureau graphique | Vous pouvez utiliser les environnements de bureau graphiques suivants pour afficher le client Symantec Endpoint Protection pour Linux :<br>• KDE<br>• Gnome<br>• Unity |
| Autres spécifications d'environnement | • Glibc<br>Les systèmes d'exploitation exécutant une version de glibc antérieure à 2.6 ne sont pas pris en charge.<br>• Packages dépendants i686 sur les ordinateurs 64 bits<br>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.<br>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 le montrent les commandes suivantes avec `sudo` :<br>– Pour les distributions basées sur Red Hat : `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`<br>– Pour les distributions basées sur Debian : `sudo apt-get install ia32-libs`<br>– Pour les distributions basées sur Ubuntu :<br>`sudo dpkg --add-architecture i386`<br>`sudo apt-get update`<br>`sudo apt-get install gcc-multilib libx11-6:i386`<br>• net-tools ou iproute2<br>Symantec Endpoint Protection utilise l'un de ces deux outils, selon ce qui est déjà installé sur l'ordinateur.<br>• Outils de développement<br>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 :<br>Compilation manuelle des modules de noyau Auto-Protect pour Endpoint Protection pour Linux |

Notes de mise à jour et configuration système requise pour toutes les versions de Symantec Endpoint Protection

# Séquences de mise à niveau vers la dernière version de Symantec Endpoint Protection 14.x prises en charge

**NOTE**

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.

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

**Symantec Endpoint Protection Manager et client Windows**

Les versions suivantes 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

**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
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

**NOTE**

Le client Symantec Endpoint Protection pour Mac n'a pas été mis à jour vers la version 14.0.1 MP2.

**Client Linux**

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

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 :

- Produits Symantec non pris en charge Symantec AntiVirus et Symantec Client Security
- Tous les produits Norton™ de Symantec
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Versions de Symantec Endpoint Protection for Mac antérieures à 12.1.4

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 toute 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 version 14.x.

Vous ne pouvez pas mettre à niveau 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. A la place, vous devez mettre à niveau la version 12.1.6 MP7 vers la version 14 MP1 ou ultérieure.

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 14.2.1.1.

Si vous disposez d'un numéro de build mais que vous ne savez pas comment le convertir en numéro de version, consultez :

- Versions publiées de Symantec Endpoint Protection
- A propos des types et versions d'Endpoint Protection

# Sites web à visiter pour obtenir des informations complémentaires

La section Informations sur Endpoint Protection répertorie les sites Web sur lesquels vous pouvez vous rendre pour obtenir des pratiques d'excellence, informations de dépannage et autres ressources susceptibles de vous aider dans l'utilisation du produit.

**Table 14: 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 | • Guides disponibles pour la version la plus récente du produit (anglais)<br>• Guides disponibles pour la version la plus récente du produit (langues autres que l'anglais)<br>• Guides de produit pour toutes les versions de Symantec Endpoint Protection 14.x (anglais)<br>**Autres langues :** |
| Support technique | Support technique Endpoint Protection<br>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<br>Accédez aux cours de formation, eLibrary et bien plus. |
| Forums Symantec Connect | Endpoint Protection |


Symantec
A Division of Broadcom