

# Notes de mise à jour de Symantec™ Endpoint Protection 12.1.6 MP10

# Notes de mise à jour de Symantec Endpoint Protection

Version du produit : 12.1.6 MP10

Version de la documentation : 1

Ce document à été mis à jour pour la dernière fois le : avril 06, 2018

## Mentions légales

Copyright © 2018 Symantec Corporation. Tous droits réservés.

Symantec, le logo Symantec, le logo Checkmark, LiveUpdate et Norton sont des marques commerciales ou des marques déposées de Symantec Corporation ou ses filiales aux États-Unis et dans d'autres pays. Les autres noms sont des marques commerciales de leurs détenteurs respectifs.

Le produit décrit dans ce document est distribué aux termes d'une licence limitant son utilisation, sa copie, sa distribution et sa décompilation/ingénierie inverse. Ce document ne peut, en tout ou partie, être reproduit sous aucune forme et par aucun moyen sans l'autorisation préalable écrite de Symantec Corporation et de ses détenteurs de licence éventuels.

LA DOCUMENTATION EST FOURNIE « EN L'ÉTAT » ET TOUTE GARANTIE OU CONDITION D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, Y COMPRIS, SANS QUE CELA SOIT LIMITATIF, LES GARANTIES OU CONDITIONS IMPLICITES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER OU DE RESPECT DES DROITS DE PROPRIÉTÉ INTELLECTUELLE EST RÉFUTÉE, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT TENUES POUR LÉGALEMENT NON VALIDES. SYMANTEC CORPORATION NE PEUT ÊTRE TENUE POUR RESPONSABLE DES DOMMAGES DIRECTS OU INDIRECTS RELATIFS AU CONTENU OU À L'UTILISATION DE LA PRÉSENTE DOCUMENTATION. LES INFORMATIONS PRÉSENTÉES DANS CETTE DOCUMENTATION SONT SUJETTES À MODIFICATION SANS PRÉAVIS.

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043 - ÉTATS-UNIS

<http://www.symantec.fr>

# Support technique

Le support technique de Symantec met à jour des centres de support globalement. Le rôle primaire du support technique est de réagir aux requêtes spécifiques au sujet des fonctions et de la fonctionnalité d'un produit. Le groupe de support technique crée également le contenu pour notre base de données en ligne. Le groupe de support technique travaille en collaboration avec les autres domaines fonctionnels de Symantec pour répondre à vos questions en temps utile, par exemple avec l'ingénierie de produit et Symantec Security Response pour fournir des services d'alerte et des mises à jour de définitions de virus.

Les offres de support de Symantec englobent :

- Un intervalle des options de support qui vous donnent la flexibilité de sélectionner la bonne quantité de service pour les sociétés de toutes tailles
- Support téléphonique et/ou par le Web pour des réponses rapides et des informations actuelles ;
- garantie de mise à niveau par des mises à niveau logicielles ;
- prise en charge achetée sur une base des heures ouvrables régionales ou 24 heures sur 24 et 7 jours sur 7 ;
- offres de la meilleure qualité de service qui incluent des services de gestion des comptes.

Pour plus d'informations concernant les offres de support de Symantec, consultez notre site Web à l'adresse suivante :

[http://www.symantec.com/business/support/index?page=home&locale=fr\\_FR](http://www.symantec.com/business/support/index?page=home&locale=fr_FR)

Des services d'assistance vous seront fournis selon votre contrat de support et la politique de support technique d'entreprise en cours.

## Contactez le support technique

Les clients avec un contrat de support en cours peuvent accéder aux informations de support technique sur l'URL suivante :

[http://www.symantec.com/business/support/index?page=home&locale=fr\\_FR](http://www.symantec.com/business/support/index?page=home&locale=fr_FR)

Avant de contacter le support technique, vérifiez que votre système répond à la configuration requise indiquée dans la documentation du produit. En outre, nous vous conseillons être devant l'ordinateur sur lequel le problème se pose, au cas où il serait nécessaire de répliquer le problème.

Quand vous entrez en contact avec le support technique, ayez les informations disponibles suivantes en votre possession :

- Niveau de version du produit
- Les informations sur l'équipement

- Mémoire disponible, espace disque et informations NIC
- Système d'exploitation
- Version et niveau de correctif
- Topologie réseau
- Routeur, passerelle et informations d'Adresse IP
- Description du problème :
  - Messages d'erreur et fichiers journaux
  - Dépannage effectué avant de contacter Symantec
  - Les modifications récentes de la configuration logicielle et les modifications réseau

## Programme de licences et d'enregistrement

Si votre produit Symantec requiert un enregistrement ou une clé de licence, accédez à notre page Web de support technique à l'URL suivante :

[http://www.symantec.com/business/support/index?page=home&locale=fr\\_FR](http://www.symantec.com/business/support/index?page=home&locale=fr_FR)

## Service client

Les informations du service client sont disponibles sur l'URL suivante :

[http://www.symantec.com/business/support/index?page=home&locale=fr\\_FR](http://www.symantec.com/business/support/index?page=home&locale=fr_FR)

Le service client est fournit son aide pour les questions non techniques, telles que les types suivants de problèmes :

- Questions concernant le programme de licences ou la numérotation de produit
- Mises à jour d'enregistrement de produit, telles que l'adresse ou les changements de nom
- Les informations générales sur le produit (fonctions, disponibilité de langue, distributeurs locaux)
- Les dernières informations sur les mises à jour et les mises à niveau du produit
- Informations sur l'assurance et les contrats de support de mise à niveau
- Informations sur les Programmes d'achats Symantec
- Conseil sur les options du support technique Symantec
- Questions non techniques d'avant-vente
- Problèmes liés aux CD-ROM, DVD ou manuels

## Ressources de contrat de support

Si vous voulez entrer en contact avec Symantec concernant un contrat de support existant, veuillez contactez l'équipe administrative de contrat de support pour votre région comme suit :

Asie Pacifique et Japon [customercare\\_apj@symantec.com](mailto:customercare_apj@symantec.com)

Europe, Moyen-Orient et Afrique [semea@symantec.com](mailto:semea@symantec.com)

Amérique du Nord et Amérique latine [supportsolutions@symantec.com](mailto:supportsolutions@symantec.com)

# Notes de mise à jour

Ce document traite des sujets suivants:

- [A propos de ce document](#)
- [Nouveautés de Symantec Endpoint Protection 12.1.6 MP10](#)
- [Problèmes connus et solutions](#)
- [Configuration requise pour Symantec Endpoint Protection](#)
- [Chemins de mise à niveau pris en charge pour Symantec Endpoint Protection](#)
- [Où obtenir plus d'informations](#)

## A propos de ce document

Ce document contient les informations relatives à Symantec Endpoint Protection.

Lisez ce document attentivement avant d'installer ce produit ou de contacter le support technique. Les notes de mise à jour décrivent les problèmes connus et leurs solutions de contournement non incluses dans la documentation standard ou l'aide en ligne.

Se reporter à "[Problèmes connus et solutions](#)" à la page 7.

Se reporter à "[Configuration requise pour Symantec Endpoint Protection](#)" à la page 10.

## Nouveautés de Symantec Endpoint Protection 12.1.6 MP10

Cette version de Symantec Endpoint Protection inclut de nouvelles fonctions, des modifications et des améliorations dans les domaines suivants :

- Défauts client

- Mises à jour de composants tiers

[Nouveautés de toutes les versions de Symantec Endpoint Protection 12.1.x](#)

Se reporter à "[Problèmes connus et solutions](#)" à la page 7.

## Problèmes connus et solutions

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

- Se reporter à "[Informations d'installation](#)" à la page 7.
- Se reporter à "[Informations sur Symantec Endpoint Protection Manager](#)" à la page 7.
- Se reporter à "[Documentation et informations d'aide](#)" à la page 9.

Vous pouvez afficher une liste des problèmes résolus pour cette version à l'emplacement suivant :

[Nouveaux correctifs et nouvelles versions de composant dans Symantec Endpoint Protection 12.1.6 MP10](#)

## Informations d'installation

Cette section décrit la procédure d'installation du produit.

### **L'installation ou la mise à niveau vers Symantec Endpoint Protection Manager 12.1.6 MP10 est bloquée sur Windows XP/Server 2003**

En raison de la mise à niveau de la version de PHP, Symantec Endpoint Protection Manager n'est plus pris en charge sur Windows XP/Server 2003. PHP 5.6.27 apporte des améliorations de sécurité par rapport aux versions précédentes. Aucune solution n'est disponible. Au lieu de cela, vous devez mettre à niveau l'ordinateur ou déplacer Symantec Endpoint Protection Manager sur un nouvel ordinateur qui exécute un système d'exploitation Windows pris en charge.

Pour plus d'informations sur le déplacement de Symantec Endpoint Protection Manager 12.1.x vers un nouveau serveur, consultez [Transfert d'Endpoint Protection Manager sur un autre serveur sans rompre les communications client ni perdre de données](#).

## Informations sur Symantec Endpoint Protection Manager

Cette section contient des informations relatives à Symantec Endpoint Protection Manager.

## Les communications HTTPS échouent sur les clients Symantec Endpoint Protection installés sur Windows XP/Server 2003

Les communications client vers les ordinateurs Windows XP/Server 2003 échouent lorsque les communications HTTPS sont activées dans Symantec Endpoint Protection 12.1.6 MP10. Cette défaillance se produit en raison d'une non-correspondance de chiffrement.

Utilisez la procédure de la page suivante pour résoudre ce problème :

[Les communications HTTPS échouent sur les clients Endpoint Protection installés sur Windows XP/Server 2003](#)

## L'accès à la console web ne fonctionne pas avec Internet Explorer 8-10

En raison d'une mise à niveau de la version de JRE, Symantec Endpoint Protection Manager ne prend plus en charge Internet Explorer 8, 9 ou 10 à partir de 12.1.6 MP9. L'accès de la console web à Symantec Endpoint Protection Manager 12.1.6 MP10 échoue quand vous utilisez ces versions d'Internet Explorer. Utilisez plutôt Internet Explorer 11 ou un autre navigateur pris en charge.

Se reporter à "[Configuration requise pour Symantec Endpoint Protection Manager](#)" à la page 11.

## L'accès distant de la console Java à Symantec Endpoint Protection Manager échoue lorsque FIPS est activé

Dans un environnement compatible FIPS, l'accès à Symantec Endpoint Protection Manager 12.1.6 MP10 échoue avec l'erreur « Échec de validation du certificat. L'application ne sera pas exécutée. » Cette erreur résulte d'une incompatibilité entre Crypto-J et JRE 8. Pour contourner ce problème, accédez à Symantec Endpoint Protection Manager à l'aide de la console web.

[L'accès distant de la console Java à Endpoint Protection Manager échoue lorsque FIPS est activé](#)

## Pare-feu s'affiche dans la console web Symantec Endpoint Protection Manager comme Fire...

Quand vous vous connectez à Symantec Endpoint Protection Manager via la console web, dans l'onglet **Politiques**, **Pare-feu** s'affiche de manière erronée comme **Fire....** Ce problème est d'ordre esthétique. Cette correction est prévue pour une future version.

## Windows LiveUpdate affiche le texte en anglais pour les versions localisées de Symantec Endpoint Protection Manager

Symantec Endpoint Protection Manager inclut Windows LiveUpdate, qui télécharge le contenu pour le rendre disponible aux clients gérés. Dans les versions localisées de Symantec Endpoint Protection Manager, Windows LiveUpdate affiche des boîtes de dialogue en anglais seulement.



Ce comportement est connu. Windows LiveUpdate sera localisé dans les versions futures de Symantec Endpoint Protection.

## Documentation et informations d'aide

Cette section contient des modifications ou des ajouts à la documentation et à l'aide contextuelle.

### L'aide indique à tort que les alertes ne se produisent pas pour tous les types d'action SONAR

La rubrique d'aide SONAR : SONAR suggère à tort que pour **En cas de détection**, aucune alerte n'apparaît quand l'action est Consigner seulement. Une alerte apparaît pour tous les types d'action quand une détection SONAR a lieu, pas simplement pour Mettre en quarantaine ou Supprimer. Le texte corrigé pour **En cas de détection** est le suivant :

Configure des notifications pour alerter l'utilisateur lorsque SONAR détecte un élément.

### L'aide n'inclut pas les informations concernant la bande passante maximale pour les téléchargements de clients à partir d'un fournisseur de mises à jour groupées

Dans Symantec Endpoint Protection Manager, la rubrique d'aide contextuelle **Fournisseur de mises à jour groupées** n'inclut pas les informations de description du paramètre **Bande passante maximale autorisée pour les téléchargements de clients à partir du fournisseur de mises à jour groupées**. La description est la suivante :

**Bande passante maximale autorisée pour les téléchargements de clients à partir du fournisseur de mises à jour groupées** : cette option permet de configurer un fournisseur de mises à jour groupées (GUP) pour servir plusieurs sites qui n'ont que quelques clients. Cette fonction vous aide à réduire la bande passante pour les sites qui ont une connectivité faible et sur lesquels vous souhaitez éviter les surcharges de contenu lorsque vous fournissez un ensemble complet de définitions de contenu.

### Corrections et ajouts à la référence de schéma de bases de données pour 12.1.6

Les articles suivants sont soit introuvables dans la référence de schéma de bases de données pour Symantec Endpoint Protection 12.1.6, soit incorrects.

**Tableau 1-1** Mises à jour de référence de schéma de bases de données pour 12.1.6

Élément	Mise à jour
Les entrées des journaux de comportement des agents indiquent une unité de mesure incorrecte	<p>Les entrées de schéma des journaux de comportement des agents qui sont associées aux violations de contrôle d'application répertorient les tailles de fichiers en mégaoctets (Mo). Cette taille de fichier devrait être en octets, à la fois dans la base de données et dans les journaux client.</p> <p>Les éléments suivants sont affectés :</p> <ul style="list-style-type: none"> <li>■ AGENT_BEHAVIOR_LOG_1</li> <li>■ AGENT_BEHAVIOR_LOG_2</li> <li>■ BEHAVIOR_REPORT</li> </ul>
Valeurs manquantes pour le tableau d'ACTUALACTION	<p>Le tableau d'ACTUALACTION omet à tort les valeurs suivantes :</p> <ul style="list-style-type: none"> <li>■ 24 - RepairFailedPowerEraser Une analyse Power Eraser est recommandée. Symantec Endpoint Protection ne peut pas supprimer ou nettoyer la menace. Symantec Endpoint Protection peut seulement bloquer la menace.</li> <li>■ 25 - RepairFailedPowerEraser2 Une analyse Power Eraser est recommandée. Symantec Endpoint Protection ne peut pas supprimer ou nettoyer la menace. Symantec Endpoint Protection ne peut pas confirmer qu'il a bloqué la menace.</li> <li>■ 100 - Bloc IDS</li> <li>■ 101 - Violation de pare-feu</li> <li>■ 102 - Autorisé par l'utilisateur</li> <li>■ 200 - Pièce jointe éliminée</li> </ul>
Valeurs pour les journaux de comportement des agents pour la colonne DESCRIPTION	<p>Pour le tableau AGENT_BEHAVIOR_LOG_1, la colonne DESCRIPTION a une limite de 256 caractères. Par conséquent, les valeurs réelles du client peuvent être plus longues que celles qui sont affichées dans les journaux ou rapports Symantec Endpoint Protection Manager. Vérifiez sur le client pour confirmer.</p>

Pour la référence de schémas de base de données 12.1.6, consultez : [Schéma de base de données Symantec Endpoint Protection 12.1.6](#).

## Configuration requise pour Symantec Endpoint Protection

Généralement, la configuration requise pour les clients Symantec Endpoint Protection Manager et Symantec Endpoint Protection est la même que celle des systèmes d'exploitation sur lesquels ils sont pris en charge.

Pour la configuration système requise la plus récente, consultez :

### Configuration requise pour Symantec Endpoint Protection 12.1.6 MP10

- Se reporter à "Configuration requise pour Symantec Endpoint Protection Manager" à la page 11.
- Se reporter à "Configuration requise pour le client Symantec Endpoint Protection for Windows" à la page 13.
- Se reporter à "Configuration requise pour le client Symantec Endpoint Protection for Windows Embedded" à la page 15.
- Se reporter à "Configuration requise pour le client Symantec Endpoint Protection for Mac" à la page 16.
- Se reporter à "Configuration requise pour les clients Symantec Endpoint Protection for Linux" à la page 17.

Se reporter à "Installations virtuelles et produits de virtualisation pris en charge" à la page 18.

## Configuration requise pour Symantec Endpoint Protection Manager

---

**Remarque :** Cette version de Symantec Endpoint Protection Manager gère les clients 11.0.x et 12.0.x, indépendamment du système d'exploitation client. Cependant, la prise en charge de Symantec Endpoint Protection 11.0.x et 12.0.x a pris fin le 5 janvier 2015.

---

**Tableau 1-2** Configuration requise pour Symantec Endpoint Protection Manager

Composant	Configuration requise
Processeur	Intel Pentium Dual-Core ou équivalent minimum <b>Remarque :</b> Les processeurs Intel Itanium IA-64 ne sont pas pris en charge.
RAM physique	2 Go de RAM minimum, 4 Go ou plus recommandés <b>Remarque :</b> Votre serveur Symantec Endpoint Protection Manager peut nécessiter de la mémoire RAM supplémentaire selon les besoins en RAM des applications déjà installées.
Disque dur	16 Go minimum disponibles (100 Go recommandés) pour le serveur de gestion 40 Go minimum disponibles (200 Go recommandés) pour le serveur de gestion et une base de données installée en local
Affichage	1024 x 768 minimum

Composant	Configuration requise
Système d'exploitation (ordinateur)	<ul style="list-style-type: none"><li>■ Windows 7 (32 bits, 64 bits, RTM et SP1 ; toutes les éditions sauf Édition Starter et Édition familiale)</li><li>■ Windows 8 (32 bits, 64 bits)</li><li>■ Windows 8.1 (32 bits, 64 bits)</li><li>■ Mise à jour de Windows 8.1 pour avril 2014 (32 bits, 64 bits)</li><li>■ Mise à jour de Windows 8.1 pour août 2014 (32 bits, 64 bits)</li></ul> <p><b>Remarque :</b> Windows 7 autorise seulement 20 connexions simultanées. L'installation de Symantec Endpoint Protection Manager sous Windows 7 est recommandée pour les environnements moins volumineux uniquement. Consultez <a href="#">Pratiques d'excellence pour l'installation d'Endpoint Protection Manager sur Windows 7 ou XP</a> pour obtenir des recommandations pour la configuration.</p>
Système d'exploitation (serveur)	<ul style="list-style-type: none"><li>■ Windows Server 2008 (32 bits, 64 bits, R2, RTM, SP1 et SP2)</li><li>■ Windows Small Business Server 2008 (64 bits)</li><li>■ Windows Essential Business Server 2008 (64 bits)</li><li>■ Windows Small Business Server 2011 (64 bits)</li><li>■ Windows Server 2012</li><li>■ Windows Server 2012 R2</li><li>■ Mise à jour de Windows Server 2012 R2 pour avril 2014</li><li>■ Mise à jour de Windows Server 2012 R2 pour août 2014</li><li>■ Windows Server 2016</li></ul> <p><b>Remarque :</b> 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.</p>
Navigateur Web	<p>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 :</p> <ul style="list-style-type: none"><li>■ Microsoft Internet Explorer 11 Se reporter à "<a href="#">L'accès à la console web ne fonctionne pas avec Internet Explorer 8-10</a>" à la page 8.</li><li>■ Mozilla Firefox 5.x à 59.x</li><li>■ Google Chrome 65.x</li></ul>

Composant	Configuration requise
Base de données	<p>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 :</p> <ul style="list-style-type: none"> <li>■ SQL Server 2005, SP4</li> <li>■ SQL Server 2008, RTM - SP4</li> <li>■ SQL Server 2008 R2, RTM - SP3</li> <li>■ SQL Server 2012, RTM - SP3</li> <li>■ SQL Server 2014, RTM - SP2</li> <li>■ SQL Server 2016</li> </ul> <p><b>Remarque :</b> La base de données SQL Server Express Edition n'est pas prise en charge.</p> <p><b>Remarque :</b> 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.</p> <p>Pour plus d'informations :</p> <p><a href="#">Prise en charge de TLS 1.2 pour Microsoft SQL Server</a></p>

**Remarque :** 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.

Se reporter à "[Installations virtuelles et produits de virtualisation pris en charge](#)" à la page 18.

## Configuration requise pour le client Symantec Endpoint Protection for Windows

**Tableau 1-3** Configuration requise pour le client Symantec Endpoint Protection for Windows

Composant	Configuration requise
Processeur	<ul style="list-style-type: none"> <li>■ Processeur 32 bits : Intel Pentium III 1 GHz ou équivalent minimum (Intel Pentium 4 ou équivalent recommandé)</li> <li>■ Processeur 64 bits : Pentium 4 2 GHz avec prise en charge x86-64 ou équivalent minimum</li> </ul> <p><b>Remarque :</b> Les processeurs Itanium ne sont pas pris en charge.</p>
RAM physique	512 Mo (1 Go recommandé) ou plus si requis par le système d'exploitation

Composant	Configuration requise
Disque dur	<p>1,8 Mo d'espace disque disponible pour l'installation ; de l'espace supplémentaire est nécessaire pour le contenu et les journaux</p> <p><b>Remarque :</b> Les conditions d'espace requises sont basées sur les systèmes de fichiers NTFS.</p>
Affichage	800 x 600 minimum
Système d'exploitation (ordinateur)	<ul style="list-style-type: none"> <li>■ Windows XP Édition familiale ou Professionnel (32 bits, SP3 ; 64 bits, SP2)</li> <li>■ Windows XP Embedded (SP3)</li> <li>■ Windows Vista (32 bits, 64 bits)</li> <li>■ Windows 7 (32 bits, 64 bits, RTM et SP1)</li> <li>■ Windows Embedded 7 Standard, POSReady et Enterprise (32 bits et 64 bits)</li> <li>■ Windows 8 (32 bits, 64 bits)</li> <li>■ Windows Embedded Standard 8 (32 bits et 64 bits)</li> <li>■ Windows 8.1 (32 bits, 64 bits), y compris Windows To Go</li> <li>■ Mise à jour de Windows 8.1 pour avril 2014 (32 bits, 64 bits)</li> <li>■ Mise à jour de Windows 8.1 pour août 2014 (32 bits, 64 bits)</li> <li>■ Windows Embedded 8.1 Pro, Industry Pro, Industry Enterprise (32 bits et 64 bits)</li> <li>■ Windows 10 (32 bits, 64 bits)</li> <li>■ Windows 10 Mise à jour de novembre (2015) (32 bits, 64 bits)</li> <li>■ Windows 10 Mise à jour anniversaire (2016) (32 bits, 64 bits) (compatibilité de base)</li> <li>■ Windows 10 Creators Update (2017) (32 bits, 64 bits) (compatibilité de base)</li> <li>■ Windows 10 Fall Creators Update (2017) (32 bits, 64 bits) (compatibilité de base)</li> </ul> <p>Consultez <a href="#">Prise en charge d'Endpoint Protection pour les mises à jour de Windows 10 et Windows Server 2016</a> pour obtenir des détails importants sur la compatibilité de base.</p> <p>Se reporter à "<a href="#">Configuration requise pour le client Symantec Endpoint Protection for Windows Embedded</a>" à la page 15.</p>

Composant	Configuration requise
Système d'exploitation (serveur)	<ul style="list-style-type: none"> <li>■ Windows Server 2003 (32 bits, 64 bits, R2, SP1 ou ultérieur)</li> <li>■ Windows Small Business Server 2003 (32 bits)</li> <li>■ Windows Server 2008 (32 bits, 64 bits ; R2, SP1 et SP2)</li> <li>■ Windows Small Business Server 2008 (64 bits)</li> <li>■ Windows Essential Business Server 2008 (64 bits)</li> <li>■ Windows Small Business Server 2011 (64 bits)</li> <li>■ Windows Server 2012</li> <li>■ Windows Server 2012 R2</li> <li>■ Mise à jour de Windows Server 2012 R2 pour avril 2014</li> <li>■ Mise à jour de Windows Server 2012 R2 pour août 2014</li> <li>■ Windows Server 2016 (compatibilité de base)</li> </ul> <p>Consultez l'article <a href="#">Prise en charge d'Endpoint Protection pour les mises à jour de Windows 10 et Windows Server 2016</a> pour obtenir des détails importants sur la compatibilité de base.</p>
Prévention d'intrusion du navigateur	<p>La prise en charge de la prévention d'intrusion du navigateur dépend de la version du système de détection des intrusions du client (CIDS).</p> <p>Voir <a href="#">Navigateurs pris en charge pour la prévention d'intrusion du navigateur dans Endpoint Protection</a>.</p>

Se reporter à "[Installations virtuelles et produits de virtualisation pris en charge](#)" à la page 18.

## Configuration requise pour le client Symantec Endpoint Protection for Windows Embedded

**Tableau 1-4** Configuration requise pour le client Symantec Endpoint Protection for Windows Embedded

Composant	Configuration requise
Processeur	Intel Pentium 1 GHz
RAM physique	256 Mo
Disque dur	450 Mo d'espace disponible sur le disque dur

Composant	Configuration requise
Système d'exploitation Embedded	<ul style="list-style-type: none"> <li>■ Windows Embedded Standard (WES) 2009 (32 bits, SP3)</li> <li>■ Windows Embedded POSReady 2009 (32 bits, SP3)</li> <li>■ Windows Embedded Point of Service (WEPOS) (32 bits, SP3)</li> <li>■ Windows Embedded Standard 7 (32 et 64 bits)</li> <li>■ Windows Embedded POSReady 7 (32 et 64 bits)</li> <li>■ Windows Embedded Enterprise 7 (32 et 64 bits)</li> <li>■ Windows Embedded Standard 8 (32 bits et 64 bits)</li> <li>■ Windows Embedded Industry Pro 8.1 (32 et 64 bits)</li> <li>■ Windows Embedded Industry Enterprise 8.1 (32 et 64 bits)</li> <li>■ Windows Embedded Pro 8.1 (32 et 64 bits)</li> </ul>
Composants requis au minimum	<ul style="list-style-type: none"> <li>■ Gestionnaire de filtres (FltMgr.sys)</li> <li>■ Assistant de performance des données (pdh.dll)</li> <li>■ Service Windows Installer</li> <li>■ Authentification par formulaire (FBA) : signature du pilote (s'applique seulement à Embedded basé sur XP)</li> <li>■ WinLogon (s'applique seulement à Embedded basé sur XP)</li> </ul>
Modèles	<ul style="list-style-type: none"> <li>■ Compatibilité des applications (par défaut)</li> <li>■ Signalisation numérique</li> <li>■ Automatisation industrielle</li> <li>■ IE, Media Player, RDP</li> <li>■ Décodeur</li> <li>■ Client léger</li> </ul> <p>Le modèle de configuration minimale n'est pas pris en charge.</p> <p>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.</p>

Voir [Prise en charge de Windows Embedded par Symantec Endpoint Protection](#).

Se reporter à "[Installations virtuelles et produits de virtualisation pris en charge](#)" à la page 18.

## Configuration requise pour le client Symantec Endpoint Protection for Mac

**Tableau 1-5** Configuration requise pour le client Symantec Endpoint Protection for Mac

Composant	Configuration requise
Processeur	Intel Core 2 Duo 64 bits ou version ultérieure



Composant	Configuration requise
RAM physique	2 Go de RAM
Disque dur	500 Mo d'espace disque disponible pour l'installation
Affichage	800 x 600
Système d'exploitation	Mac OS X 10.8, 10.9, 10.10, 10.11 et macOS 10.12 <b>Remarque :</b> La version 12.1.6 MP10 n'est pas prise en charge sur macOS 10.13.

## Configuration requise pour les clients Symantec Endpoint Protection for Linux

**Tableau 1-6** Configuration requise pour les clients Symantec Endpoint Protection for Linux

Composant	Configuration requise
Matériel	<ul style="list-style-type: none"> <li>■ Intel Pentium 4 (2 GHz) ou supérieur</li> <li>■ 1 Go de RAM</li> <li>■ 7 Go d'espace disque disponible</li> </ul>
Systèmes d'exploitation	<ul style="list-style-type: none"> <li>■ Amazon Linux</li> <li>■ CentOS 6U4, 6U5, 6U6, 6U9, 7, 7U1, 7U2, 7U3 ; 32 bits et 64 bits</li> <li>■ Debian 6.0.5 Squeeze, Debian 8 Jessie ; 32 bits et 64 bits</li> <li>■ Fedora 16, 17 ; 32 et 64 bits</li> <li>■ Novell Open Enterprise Server (OES) 2 SP2 et 2 SP3 exécutant SUSE Linux Enterprise Server (SLES) 10 SP3 ; 32 bits et 64 bits</li> <li>■ Novell Open Enterprise Server (OES) 11 et 11 SP1 exécutant SUSE Linux Enterprise Server (SLES) 11 SP1 et SP2 ; 64 bits</li> <li>■ Oracle Linux (OEL) 5U8, 5U9, 6U2, 6U4, 6U5 ; 64 bits</li> <li>■ Red Hat Enterprise Linux Server (RHEL) 5U7 - 5U11, 6U2 - 6U9, 7 - 7U3 ; 32 bits et 64 bits</li> <li>■ SUSE Linux Enterprise Server (SLES) 10 SP3, 10 SP4, 11 SP1 - 11 SP3 ; 32 bits et 64 bits</li> <li>■ SUSE Linux Enterprise Desktop (SLED) 10 SP3, 10 SP4, 11 SP1 - 11 SP3 ; 32 bits et 64 bits</li> <li>■ Ubuntu 11.10, 12.04, 12.04.02, 14.04, 16.04 ; 32 bits et 64 bits</li> </ul> <p>Pour une liste des noyaux de système d'exploitation pris en charge, consultez l'article <a href="#">Noyaux Linux pris en charge par Symantec Endpoint Protection</a>.</p>

Composant	Configuration requise
Environnements de bureau graphiques	<p>Vous pouvez utiliser les environnements de bureau graphiques suivants pour afficher le client Symantec Endpoint Protection pour Linux :</p> <ul style="list-style-type: none"><li>■ KDE</li><li>■ Gnome</li><li>■ Unity</li></ul>
Autres spécifications d'environnement	<ul style="list-style-type: none"><li>■ Oracle Java 1.5 ou version ultérieure ; Java 7 ou version ultérieure recommandé L'installation requiert des privilèges de superutilisateur.</li><li>■ Unlimited Strength Java Cryptography Extension (JCE) Vous devez installer les fichiers de politiques Unlimited Strength Java Cryptography Extension pour faire correspondre votre version de Java. L'installation requiert des privilèges de superutilisateur. Vous pouvez télécharger les fichiers d'installation sous la section <b>Additional Resources</b> du site Web d'Oracle : <a href="http://www.oracle.com/technetwork/java/javase/downloads/">http://www.oracle.com/technetwork/java/javase/downloads/</a></li><li>■ 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 le montrent les commandes <code>sudo</code> suivantes : Pour les distributions basées sur Red Hat : <code>sudo yum install glibc.i686 libgcc.i686 libX11.i686</code> Pour les distributions basées sur Debian : <code>sudo apt-get install ia32-libs</code> Pour les distributions basées sur Ubuntu : <code>sudo apt-get install libx11-6:i386 libgcc1:i386 libc6:i386</code></li><li>■ net-tools Pour installer Symantec Endpoint Protection sur Red Hat Enterprise Linux Server (RHEL) 7.1 ou version antérieure, vous devez d'abord installer net-tools.</li><li>■ Les systèmes de fichiers XFS qui contiennent des attributs inode64 ne sont pas pris en charge.</li></ul>

Se reporter à "[Installations virtuelles et produits de virtualisation pris en charge](#)" à la page 18.

## Installations virtuelles et produits de virtualisation pris en charge

Vous pouvez installer Symantec Endpoint Protection sur les systèmes d'exploitation pris en charge qui s'exécutent dans des environnements virtuels. Installez Symantec Endpoint Protection sur le système d'exploitation invité, et non sur l'hôte.

Les produits de virtualisation suivants prennent en charge Symantec Endpoint Protection Manager, la console et les composants de base de données intégrés, ainsi que le logiciel client Symantec Endpoint Protection pour Windows et Linux :

- Windows Azure
- Amazon WorkSpaces
- VMware WS 5.0 (workstation) ou version ultérieure
- VMware GSX 3.2 (entreprise) ou version ultérieure
- VMware ESX 2.5 (workstation) ou version ultérieure
- VMware ESXi version 4.1 à 5.5
- VMware ESXi version 6.0
- VMware ESXi 6.0 mise à jour 1
- VMware ESXi 6.0 mise à jour 2
- Microsoft Virtual Server 2005
- Microsoft Enterprise Desktop Virtualization (MED-V), qui inclut le mode Windows XP
- Windows Server 2008 Hyper-V
- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V
- Citrix XenServer 5.6 ou version ultérieure
- Virtual Box, fourni par Oracle

## Chemins de mise à niveau pris en charge pour Symantec 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 12.1.6 MP10 :

- 11.0.x et Small Business Edition 12.0.x  
Pour obtenir plus de détails, consultez l'article [Chemins de mise à niveau et de migration vers Symantec Endpoint Protection 12.1.x pris en charge](#).
- 12.1 RTM (12.1.671.4971)
- 12.1.1 (12.1.1000.157)

- 12.1.1 MP1 (12.1.1101.401)
- 12.1.2 (12.1.2015.2015)
- 12.1.2 MP1 (12.1.2100.2093)
- 12.1.3 (12.1.3001.165)
- 12.1.4 (12.1.4013.4013)
- 12.1.4a (12.1.4023.4080)
- 12.1.4 MP1 (12.1.4100.4126)
- 12.1.4 MP1a (12.1.4104.4130)
- 12.1.4 MP1b (12.1.4112.4156b)
- 12.1.5 (12.1.5337.5000)
- 12.1.6 (12.1.6168.6000)
- 12.1.6 MP1 (12.1.6306.6100)
- 12.1.6 MP1a (12.1.6318.6100)
- 12.1.6 MP2 (12.1.6465.6200)
- 12.1.6 MP3 (12.1.6608.6300)
- 12.1.6 MP4 (12.1.6867.6400)
- 12.1.6 MP5 (12.1.7004.6500)
- 12.1.6 MP6 (12.1.7061.6600)
- 12.1.6 MP7 (12.1.7166.6700)
- 12.1.6 MP8 (12.1.7266.6800)
- 12.1.6 MP9a (12.1.7385.6900)

## Client Mac

Les versions suivantes du client Symantec Endpoint Protection pour Mac peuvent être directement mises à niveau vers la version 12.1.6 MP10 :

- 12.1 RTM (12.1.671.4971)
- 12.1.1 (12.1.1000.157)
- 12.1.2 (12.1.2015.2015)
- 12.1.4 (12.1.4013.4013)
- 12.1.5 (12.1.5337.5000)
- 12.1.6 (12.1.6168.6000)

- 12.1.6 MP2 (12.1.6465.6200)
- 12.1.6 MP4 (12.1.6867.6400)
- 12.1.6 MP6 (12.1.7061.6600)
- 12.1.6 MP8 (12.1.7266.6800)
- 12.1.6 MP9 (12.1.7369.6900)

---

**Remarque :** Le client Symantec Endpoint Protection pour Mac n'a pas été mis à jour pour les versions 12.1.3, 12.1.6 MP1/MP1a, 12.1.6 MP3, 12.1.6 MP5 et 12.1.6 MP7.

---

## Client Linux

Les versions suivantes du client Symantec Endpoint Protection pour Linux peuvent être directement mises à niveau vers la version 12.1.6 MP10 :

- 12.1.5 (12.1.5337.5000)
- 12.1.6 (12.1.6168.6000)
- 12.1.6 MP3 (12.1.6608.6300)
- 12.1.6 MP4 (12.1.6867.6400)
- 12.1.6 MP5 (12.1.7004.6500)
- 12.1.6 MP6 (12.1.7061.6600)
- 12.1.6 MP7 (12.1.7166.6700)
- 12.1.6 MP8 (12.1.7266.6800)
- 12.1.6 MP9 (12.1.7369.6900)

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.

## Chemins d'accès de mise à niveau non pris 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 12.1.6 MP10 :

- 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

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 14.0.1 MP1 vers la version 12.1.6 MP10, vous devez d'abord désinstaller Symantec Endpoint Protection 14.0.1 MP1.

## Mises à niveau vers Windows 10 prises en charge avec le client Symantec Endpoint Protection installé

Vous pouvez effectuer une mise à niveau vers Windows 10 avec le client Symantec Endpoint Protection installé, comme suit :

- Mise à niveau vers Windows 10 avec 12.1.6 MP1 ou versions ultérieures installées.
- Mise à niveau vers Mise à jour anniversaire Windows 10 ou Windows 10 Creators Update avec 12.1.6 MP5 ou versions ultérieures installées.
- Mise à niveau vers Windows 10 Fall Creators Update avec 12.1.6 MP9 ou versions ultérieures installées.

Avant d'effectuer la mise à niveau de Windows, vous devez vous assurer que les définitions de la Protection contre les virus et les spywares existent date du 27 juillet 2015 ou d'une date ultérieure. Les définitions créées à partir de cette date incluent une mise à jour vers le moteur Eraser (115.1.1.10) requise pour la compatibilité avec Windows 10.

Vous devez désinstaller toute version du client Symantec Endpoint Protection antérieure aux versions déjà spécifiées. La mise à niveau du système d'exploitation s'arrête si elle détecte une version précédente de Symantec Endpoint Protection.

Les chemins d'accès de mise à niveau du système d'exploitation suivants sont pris en charge avec la version client compatible appropriée installée :

- Windows 8.1 à Windows 10
- Windows 8 à Windows 10
- Windows 7 à Windows 10

---

**Remarque :** Windows 7 n'inclut pas le logiciel anti-programme malveillant (ELAM). Par conséquent, le composant Symantec Endpoint Protection ELAM n'est pas activé et ne s'active pas après que vous mettiez à niveau vers Windows 10 si Symantec Endpoint Protection est installé. Votre niveau de protection est le même qu'avec Windows 7.

Pour permettre au client Symantec Endpoint Protection d'identifier ELAM et d'activer le composant ELAM Symantec Endpoint Protection, vous devez désinstaller et réinstaller Symantec Endpoint Protection. Vous pouvez également effectuer la mise à niveau à partir de la version 12.1.6 MP1 vers la version la plus récente de Symantec Endpoint Protection pour identifier le composant ELAM. La réparation de l'installation client n'active pas le composant ELAM.

---

# Où obtenir plus d'informations

[Tableau 1-7](#) 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.

**Tableau 1-7** Informations sur le site Web de Symantec

Types d'informations	Lien vers le site web
Versions d'évaluation	<a href="#">Version d'évaluation</a> (14.x)
Mise à jour des manuels et de la documentation	<p><b>Anglais :</b></p> <ul style="list-style-type: none"> <li>■ <a href="#">Documentation produit Symantec</a></li> <li>■ <a href="#">Guides produit de toutes les versions de Symantec Endpoint Protection 12.1.x</a></li> <li>■ <a href="#">Guides produit de toutes les versions de Symantec Endpoint Protection 14</a></li> </ul> <p><b>Autres langues :</b></p> <ul style="list-style-type: none"> <li>■ <a href="#">Portugais (Brésil)</a></li> <li>■ <a href="#">Chinois (simplifié)</a></li> <li>■ <a href="#">Chinois (traditionnel)</a></li> <li>■ <a href="#">Français</a></li> <li>■ <a href="#">Allemand</a></li> <li>■ <a href="#">Italien</a></li> <li>■ <a href="#">Japonais</a></li> <li>■ <a href="#">Coréen</a></li> <li>■ <a href="#">Espagnol</a></li> </ul> <p>*Les fichiers tchèques, polonais et russes se trouvent sur la page Anglais.</p>
Support technique	<p><a href="#">Support technique Endpoint Protection</a></p> <p>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.</p>
Informations et mises à jour sur les menaces	<a href="#">Symantec Security Center</a>
Formation	<ul style="list-style-type: none"> <li>■ <a href="#">Symantec Education Services</a> Accédez aux cours de formation, eLibrary et bien plus.</li> </ul>
Forums Symantec Connect	<a href="#">Endpoint Protection</a>