

SOPHOS

Security made simple.

Sophos Enterprise Console

Guide de démarrage avancé

Pour installations distribuées

Version du produit : 5.5



Table des matières

1	À propos de ce guide.....	4
2	Planification de l'installation.....	5
2.1	Préparation de l'installation de l'Enterprise Console.....	5
2.2	Planification de la sécurité de la base de données.....	7
2.3	Préparation des groupes d'ordinateurs.....	7
2.4	Préparation des stratégies de sécurité.....	8
2.5	Préparation de la recherche d'ordinateurs en réseau.....	8
2.6	Préparation de la méthode de protection des ordinateurs.....	8
3	Configuration système requise.....	9
3.1	Matériel et système d'exploitation.....	9
3.2	Logiciels système Microsoft.....	9
3.3	Conditions applicables à l'accès aux ports.....	10
4	De quels comptes avez-vous besoin ?.....	11
4.1	Compte de base de données.....	11
4.2	Compte Update Manager.....	11
5	Sélection de l'emplacement d'installation des composants de l'Enterprise Console.....	13
5.1	Bases de données installées sur un serveur séparé.....	14
5.2	Gestionnaire de mise à jour supplémentaire installé sur un serveur séparé.....	14
6	Scénario 1 : bases de données installées sur un serveur séparé.....	16
6.1	Téléchargement du programme d'installation.....	16
6.2	Installation des bases de données SEC.....	16
6.3	Installation de SEC : console d'administration, serveur d'administration, gestionnaire de mise à jour.....	17
6.4	Installation d'une console d'administration SEC supplémentaire.....	18
6.5	Téléchargement du logiciel de sécurité.....	19
7	Scénario 2 : gestionnaire de mise à jour supplémentaire installé sur un serveur séparé.....	22
7.1	Téléchargement du programme d'installation.....	22
7.2	Installation de SEC : tous les composants.....	23
7.3	Installation d'une console d'administration SEC supplémentaire.....	24
7.4	Installation d'un gestionnaire de mise à jour supplémentaire.....	25
7.5	Téléchargement du logiciel de sécurité.....	25
8	Publication des logiciels de sécurité sur un serveur Web.....	33
9	Création de groupes d'ordinateurs.....	34
10	Configuration des stratégies de sécurité.....	35
10.1	Stratégies par défaut.....	35

10.2	Configuration d'une stratégie de pare-feu.....	35
10.3	Création ou modification d'une stratégie.....	36
10.4	Application d'une stratégie à un groupe.....	36
11	Recherche d'ordinateurs.....	37
12	Préparation de la protection des ordinateurs.....	38
12.1	Préparation de la suppression des logiciels tiers.....	38
12.2	Vérification que votre compte peut être utilisé pour l'installation du logiciel.....	38
12.3	Préparation de l'installation du logiciel antivirus.....	39
13	Protection des ordinateurs.....	40
13.1	Protection automatique des ordinateurs Windows.....	40
13.2	Protection manuelle des ordinateurs Windows ou Mac.....	41
13.3	Protection des ordinateurs Linux ou UNIX.....	41
14	Vérification du bon fonctionnement de votre réseau.....	42
15	Protection des ordinateurs autonomes.....	43
15.1	Envoi d'informations aux utilisateurs d'ordinateurs autonomes.....	43
16	Support technique.....	44
17	Mentions légales.....	45

1 À propos de ce guide

Ce guide vous explique comment installer le logiciel de sécurité de Sophos pour la première fois sur un réseau complexe ou sur un réseau avec plus de 1000 stations de travail. Il aborde l'installation sur les ordinateurs Windows et Mac.

Remarque : certaines fonctions seront indisponibles si elles ne font pas partie de votre contrat de licence.

Si vous procédez à l'installation sur un réseau simple comptant moins de 1000 postes de travail Windows et Mac, reportez-vous plutôt au *Guide de démarrage rapide* de *Sophos Enterprise Console*.

Retrouvez plus de renseignements sur l'installation sur des ordinateurs Linux ou UNIX dans le *Guide de démarrage de Sophos Enterprise Console pour Linux et UNIX* ainsi que dans ce guide.

Si vous procédez à la mise à niveau, reportez-vous plutôt au *Guide de mise à niveau* de *Sophos Enterprise Console*.

Retrouvez toute la documentation relative à Sophos Enterprise Console sur <http://www.sophos.com/fr-fr/support/documentation/enterprise-console.aspx>.

2 Planification de l'installation

Protégez vos ordinateurs en suivant les étapes principales ci-dessous :

1. Installez Sophos Enterprise Console.
2. Téléchargez le logiciel de sécurité dans un emplacement centralisé sur votre réseau.
3. Publiez le logiciel de sécurité sur un serveur Web, si nécessaire.
4. Créez des groupes pour les ordinateurs.
5. Configurez les stratégies de sécurité pour ces groupes.
6. Recherchez les ordinateurs sur le réseau et placez-les dans des groupes.
7. Protégez les ordinateurs.
8. Vérifiez le bon fonctionnement de votre réseau.
9. Protégez les ordinateurs autonomes.

Remarque : Si vous utilisez Active Directory, certaines de ces étapes seront effectuées automatiquement.

Cette section vous aide à déterminer quels choix vous allez faire à chaque étape.

2.1 Préparation de l'installation de l'Enterprise Console

Sophos Enterprise Console (SEC) vous permet d'installer et d'administrer les logiciels de sécurité sur vos ordinateurs.

L'Enterprise Console inclut quatre composants :

Console d'administration	Vous permet de protéger et d'administrer les ordinateurs.
Serveur d'administration	Gère les mises à jour et les communications.
Bases de données	Stocke les données concernant les ordinateurs du réseau.
Gestionnaire de mise à jour	Télécharge le logiciel Sophos et se met automatiquement à jour depuis Sophos dans un emplacement centralisé.

Console d'administration

Il se peut que vous souhaitiez installer une autre instance de la console d'administration sur un autre serveur afin de pouvoir mieux administrer les ordinateurs en réseau. Cette décision est liée à la manière dont vous souhaitez configurer l'administration déléguée pour la console d'administration et à la manière dont vous souhaitez diviser votre parc informatique en sous-parcs :

- Vous pouvez paramétrer l'*administration déléguée* pour la console d'administration en paramétrant des rôles, en ajoutant des droits, puis en attribuant des utilisateurs et des groupes Windows aux rôles. Par exemple, un ingénieur du support technique peut mettre à jour ou nettoyer des ordinateurs, mais ne peut pas configurer des stratégies, car il s'agit d'une opération relevant de la responsabilité d'un administrateur.

- Les *sous-parcs* peuvent être utilisés pour limiter le nombre d'ordinateurs et de groupes sur lesquels l'utilisateur peut effectuer des opérations. Vous pouvez diviser votre parc informatique en sous-parcs et attribuer des groupes d'ordinateurs de la console d'administration à ces sous-parcs. Vous pouvez ensuite contrôler l'accès aux sous-parcs en leur attribuant des utilisateurs et des groupes Windows. Le sous-parc par défaut contient tous les groupes de la console d'administration et le dossier **Non assignés**.

Ce guide vous explique comment installer une console d'administration supplémentaire. Retrouvez plus de renseignements sur le paramétrage de l'administration déléguée et sur la création de sous-parcs sur www.sophos.com/fr-fr/support/knowledgebase/63556.aspx.

Bases de données

Il se peut que vous ayez à installer les bases de données sur un autre serveur pour les raisons suivantes :

- Vous avez besoin de plus d'espace pour les bases de données.
- Vous avez un serveur SQL Server dédié.
- Vous voulez répartir la charge de traitement sur un certain nombre de serveurs.

Ce guide vous explique comment installer les bases de données soit sur le même serveur que les autres composants de l'Enterprise Console soit sur un serveur de bases de données dédié.

Remarque : si vous avez besoin d'installer les bases de données sur un serveur sécurisé à l'aide d'un script, ou dans un environnement SQL Server en cluster, rendez-vous sur www.sophos.com/fr-fr/support/knowledgebase/33980.aspx.

Important : la base de données d'audit de Sophos appelée **SophosSecurity** doit être présente et s'exécuter en même temps que les autres bases de données de l'Enterprise Console même si vous n'avez pas l'intention d'utiliser la fonction d'audit de Sophos. En effet, cette base de données est utilisée pour les événements de contrôle d'accès renforcé et de journalisation des audits.

Gestionnaire de mise à jour

Un gestionnaire de mise à jour vous permet de créer des partages qui contiennent le logiciel pour ordinateurs d'extrémité que vous souhaitez déployer. Les ordinateurs que vous souhaitez protéger se mettent automatiquement à jour depuis ces partages. Un gestionnaire de mise à jour est toujours installé comme composant de l'Enterprise Console. Par défaut, il place le logiciel de protection des ordinateurs d'extrémité et les mises à jour dans un partage UNC nommé SophosUpdate. Vous pouvez installer des gestionnaires de mise à jour supplémentaires sur d'autres serveurs et créer des partages supplémentaires pour télécharger et déployer le logiciel sur des réseaux plus étendus.

En règle générale, vous devez installer un gestionnaire de mise à jour supplémentaire tous les 25 000 ordinateurs clients connectés à votre réseau. Nous vous conseillons également d'installer un gestionnaire de mise à jour supplémentaire à un emplacement distant. Ceci vous permettra d'économiser de la bande passante lors de la mise à jour des partages réseau situés à cet emplacement. Vous serez également assuré que les partages ne sont pas incomplets en cas de panne de connexion.

Si vous utilisez un chemin UNC pour votre partage de mise à jour, il doit être utilisé par un nombre maximal de 1000 ordinateurs sauf s'il est sur un serveur de fichiers dédié. Si vous définissez un emplacement Web pour la mise à jour, celle-ci pourra être effectuée sur environ 10 000 ordinateurs.

2.2 Planification de la sécurité de la base de données

Audit de la base de données

En plus de la protection intégrée aux bases de données Enterprise Console, nous vous conseillons de paramétrer la protection supplémentaire au niveau de l'instance SQL Server (s'il n'est pas déjà en place) pour auditer les activités de l'utilisateur et les modifications qu'il a effectué sur votre SQL Server.

Par exemple, si vous utilisez une édition Enterprise de SQL Server 2008, vous pouvez utiliser la fonction SQL Server Audit. Des versions précédentes de SQL Server prennent en charge l'audit de connexion, l'audit par déclencheur externe et l'audit des événements à l'aide d'un utilitaire de suivi intégré.

Retrouvez plus de renseignements sur les fonctions que vous pouvez utiliser pour procéder à l'audit des activités et des modifications sur votre système SQL Server dans la documentation correspondant à votre version de SQL Server. Par exemple :

- [SQL Server Audit \(moteur de base de données\)](#)
- [Audit \(moteur de base de données\), SQL Server 2008 R2](#)
- [Audit dans SQL Server 2008](#)
- [Audit \(moteur de base de données\), SQL Server 2008](#)

Chiffrement des connexions à la base de données

Nous vous conseillons fortement de chiffrer les connexions entre tous les clients et la base de données Enterprise Console. Retrouvez plus de renseignements dans la documentation de SQL Server :

- [Activer les connexions chiffrées dans le moteur de base de données \(Gestionnaire de configuration SQL Server\)](#)
- [Chiffrement des connexions à SQL Server 2008 R2](#)
- [Comment faire pour activer le chiffrement SSL pour une instance de SQL Server à l'aide de la console MMC](#)

Contrôle de l'accès aux copies de sauvegardes de la base de données

Assurez-vous qu'un contrôle d'accès correct et restrictif aux copies de sauvegarde de la base de données est mis en place. Ceci permet de garantir que les utilisateurs non autorisés n'auront pas accès aux fichiers, ne pourront pas les altérer ou les supprimer accidentellement.

Remarque : les liens de cette section vous dirigent vers des informations mises à jour par des tiers et sont fournies pour vous aider. Même si nous vérifions régulièrement l'exactitude de ces liens, il se peut que ceux-ci soient modifiés sans que nous en ayons connaissance.

2.3 Préparation des groupes d'ordinateurs

Déterminez la manière dont vous allez regrouper les ordinateurs que vous souhaitez protéger. Retrouvez plus de renseignements sur www.sophos.com/fr-fr/support/knowledgebase/63556.aspx.

2.4 Préparation des stratégies de sécurité

Une *stratégie de sécurité* est un ensemble de paramètres applicables aux ordinateurs d'un ou de plusieurs groupes.

Lorsque vous créez des groupes, l'Enterprise Console leur applique les stratégies par défaut. Vous pouvez modifier ces stratégies ou en créer de nouvelles en suivant les explications de ce guide. Retrouvez plus de conseils sur les paramètres à utiliser dans le *Guide de configuration des stratégies de Sophos Enterprise Console*.

2.5 Préparation de la recherche d'ordinateurs en réseau

Avant de pouvoir installer un logiciel de sécurité sur vos ordinateurs en réseau, vous devez ajouter ces ordinateurs à la liste des ordinateurs dans l'Enterprise Console. Retrouvez plus de renseignements sur la recherche d'ordinateurs et sur leur ajout à la liste des ordinateurs dans l'Aide de l'Enterprise Console.

2.6 Préparation de la méthode de protection des ordinateurs

Vous pouvez installer le logiciel de sécurité automatiquement depuis l'Enterprise Console sur des ordinateurs Windows.

Remarque : vous ne pouvez pas installer Sophos Client Firewall sur des ordinateurs exécutant des systèmes d'exploitation serveur.

Si d'autres systèmes d'exploitation sont présents sur votre réseau, installez le logiciel manuellement ou à l'aide de scripts ou de toute autre méthode (par exemple, Active Directory). Ce guide aborde en détail l'installation manuelle pour les systèmes d'exploitation suivants :

- Windows
- Mac OS X

Le *Guide de démarrage de Sophos Enterprise Console pour Linux et UNIX* vous explique en détails comment procéder à l'installation manuelle pour d'autres systèmes d'exploitation.

3 Configuration système requise

Info : vous pouvez exécuter le programme d'installation de l'Enterprise Console pour vérifier si le serveur répond aux conditions requises pour l'installation de l'Enterprise Console, même si vous ne voulez pas passer à l'installation immédiatement. Vous pouvez voir les résultats de la vérification du système sur la page **Vérifications de la propriété du système** de l'assistant d'installation. Après avoir examiné les résultats, cliquez sur **Annuler** pour fermer l'assistant. Retrouvez plus de renseignements sur les résultats de la vérification du système sur <http://www.sophos.com/fr-fr/support/knowledgebase/113945.aspx>.

3.1 Matériel et système d'exploitation

Retrouvez plus de renseignements sur les configurations requises en matière de matériels et de systèmes d'exploitation sur le site Web de Sophos (www.sophos.com/fr-fr/products/all-system-requirements.aspx).

3.2 Logiciels système Microsoft

L'Enterprise Console requiert l'utilisation de certains logiciels système Microsoft (par exemple, des logiciels de base de données).

Le programme d'installation de l'Enterprise Console tente d'installer ce logiciel système s'il n'est pas déjà disponible sur votre serveur. Par contre, dans certains cas, le logiciel est incompatible avec votre serveur ou doit être installé manuellement.

Remarque : après avoir installé les logiciels système requis, redémarrez vos ordinateurs. Retrouvez plus de renseignements sur <https://www.sophos.com/fr-fr/support/knowledgebase/65190.aspx>.

Installation de SQL Server

Le programme d'installation tente d'installer SQL Server 2012 Express Edition avec Service Pack 2, sauf si vous choisissez d'utiliser une instance existante de SQL Server 2005 Express ou supérieur. Sachez que :

- Nous déconseillons l'installation de SQL Server sur un contrôleur de domaine.
- Si vous voulez installer les bases de données Enterprise Console sur un serveur séparé, assurez-vous que l'instance SQL Server est accessible à distance. Retrouvez plus de renseignements sur <https://www.sophos.com/fr-fr/support/knowledgebase/118473.aspx>.

Installation de .NET Framework

Le programme d'installation installe .NET Framework 4.5.2 sauf si la version 4.x est déjà installée.

Important : dans le cadre de l'installation de .NET Framework 4.5.2, certains services système (tel que le Service d'administration IIS) vont redémarrer.

Après l'installation de .NET Framework 4.5.2, un message vous demande de redémarrer votre ordinateur. Si vous acceptez, nous vous conseillons de redémarrer l'ordinateur immédiatement ou juste après l'installation.

Installation de Microsoft Message Queuing

Le programme d'installation tente d'installer Microsoft Message Queuing (MSMQ) sauf s'il est déjà installé.

Important : au cours de l'installation de MSMQ, les services suivants sont arrêtés : MSDTC, MSSQLServer, SQLSERVERAGENT. En conséquence, l'accès à la base de données SQL Server par défaut est interrompu. Assurez-vous que les services peuvent être arrêtés en toute sécurité au cours de l'installation. Vérifiez également que vous les avez bien redémarrés par la suite.

3.3 Conditions applicables à l'accès aux ports

Enterprise Console nécessite l'ouverture d'un certain nombre de ports. Retrouvez plus de renseignements sur www.sophos.com/fr-fr/support/knowledgebase/38385.aspx.

4 De quels comptes avez-vous besoin ?

Avant d'installer le logiciel Sophos, créez les comptes d'utilisateur dont vous avez besoin :

- **Compte de base de données.** Il s'agit d'un compte d'utilisateur Windows qui permet au service d'administration de l'Enterprise Console de se connecter à la base de données. Il est aussi utilisé par d'autres services Sophos.

Nous vous conseillons de nommer le compte de base de données **SophosManagement**.

- **Compte Update Manager.** Il s'agit d'un compte d'utilisateur Windows qui permet à vos ordinateurs d'extrémité d'accéder aux dossiers dans lesquels l'Enterprise Console place les mises à jour logicielles.

Nous vous conseillons de nommer le compte Update Manager **SophosUpdateMgr**.

4.1 Compte de base de données

Le compte de base de données doit :

- Pouvoir se connecter à l'ordinateur sur lequel vous allez installer Sophos Management Server (un composant de l'Enterprise Console).
- Pouvoir lire et écrire dans le répertoire temporaire du système, par exemple : « \windows\temp\ ». Par défaut, les membres du groupe « Utilisateurs » disposent de ce droit.
- Avoir un nom d'utilisateur principal (UPN, User Principal Name) associé au compte s'il s'agit d'un compte de domaine.

Tous les autres droits et abonnements de groupes dont il a besoin sont accordés automatiquement au cours de l'installation.

Le compte :

- Ne doit pas être paramétré pour expirer et ne doit avoir aucune limite de connexion.
- Ne doit pas être un compte administratif.
- Ne doit pas être modifié suite à l'installation.
- Doit être nommé **SophosManagement**.

Retrouvez plus de conseils et d'instructions sur

<https://www.sophos.com/fr-fr/support/knowledgebase/113954.aspx>.

4.2 Compte Update Manager

Le compte Update Manager doit avoir un accès en lecture au dossier dans lequel l'Enterprise Console place les mises à jour logicielles. Par défaut, il s'agit de : \\[nomserveur]\SophosUpdate

Sophos vous conseille d'utiliser un compte :

- N'est pas paramétré pour expirer et qui n'a aucune limite de connexion.
- N'est pas un compte administratif.

- A un nom d'utilisateur principal (UPN, User Principal Name) associé au compte s'il s'agit d'un compte de domaine.
- Est nommé **SophosUpdateMgr**.

Retrouvez plus de conseils et d'instructions sur

<https://www.sophos.com/fr-fr/support/knowledgebase/113954.aspx>.

5 Sélection de l'emplacement d'installation des composants de l'Enterprise Console

Sophos Enterprise Console (SEC) inclut quatre composants :

Console d'administration	Vous permet de protéger et d'administrer les ordinateurs.
Serveur d'administration	Gère les mises à jour et les communications.
Bases de données	Stocke les données concernant les ordinateurs du réseau.
Gestionnaire de mise à jour	Télécharge le logiciel Sophos et se met automatiquement à jour depuis Sophos dans un emplacement centralisé.

Si vous installez les composants SEC sur des serveurs différents, nous vous conseillons de joindre ces derniers au même domaine.

Nous vous conseillons de ne pas installer les bases de données SEC sur un contrôleur de domaine.

Ce guide aborde deux scénarios d'installation :

- Bases de données installées sur un serveur séparé
- Gestionnaire de mise à jour supplémentaire installé sur un serveur séparé

Pour chaque scénario, les composants de la SEC sont distribués sur le réseau de manière différente.

5.1 Bases de données installées sur un serveur séparé

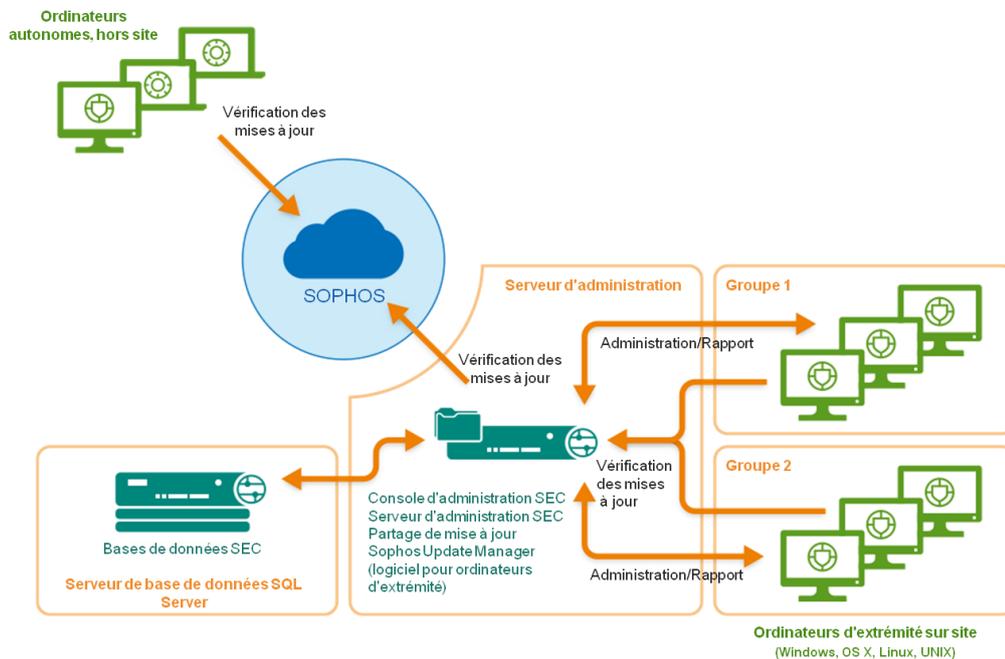


Figure 1 : Exemple d'un cas de figure de déploiement : bases de données installées sur un serveur séparé

Pour suivre ce cas de figure, rendez-vous à la section [Scénario 1 : bases de données installées sur un serveur séparé](#) à la page 16.

5.2 Gestionnaire de mise à jour supplémentaire installé sur un serveur séparé

Ce cas de figure inclut deux méthodes de configuration des sources de mise à jour sur les gestionnaires de mise à jour.

La première méthode consiste à :

- Configurer le gestionnaire de mise à jour principal que vous avez installé avec la console d'administration SEC pour qu'il se mette à jour directement depuis Sophos.
- Configurer le gestionnaire de mise à jour supplémentaire pour qu'il se mette à jour depuis le gestionnaire de mise à jour principal.

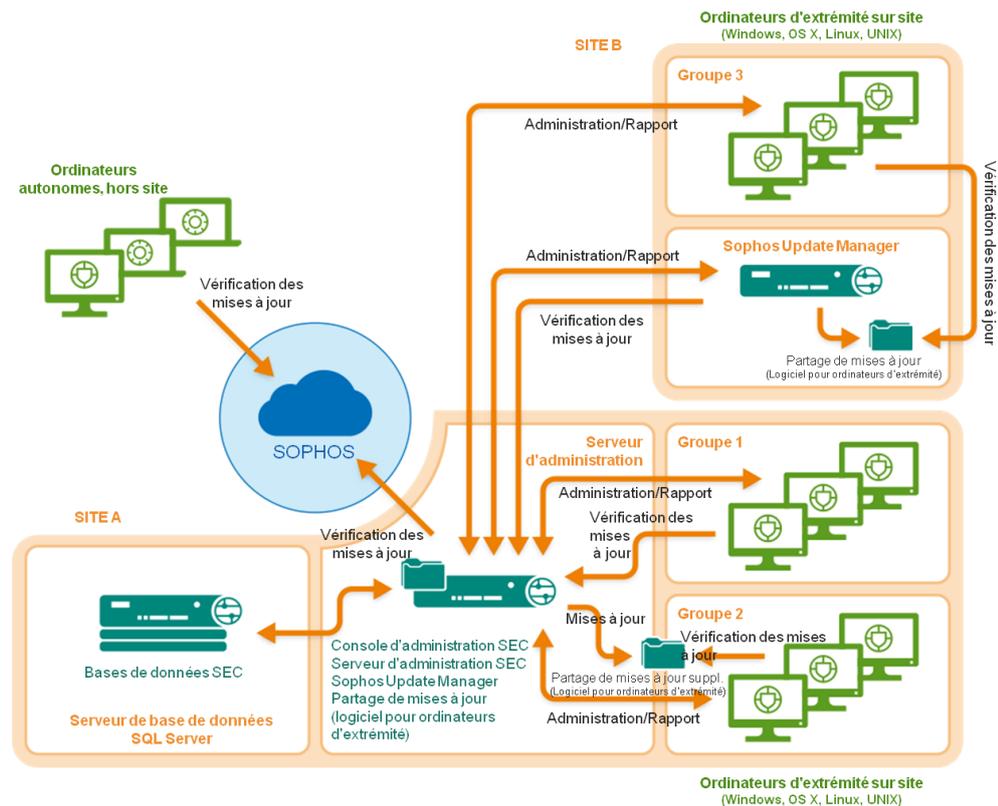


Figure 2 : Exemple de cas de figure de déploiement : mise à jour du gestionnaire de mise à jour supplémentaire à partir du gestionnaire de mise à jour principal

La seconde méthode consiste à :

- Configurer le gestionnaire de mise à jour supplémentaire pour qu'il se mette à jour directement depuis Sophos.
- Configurer le gestionnaire de mise à jour que vous avez installé avec la console d'administration SEC pour qu'il se mette à jour depuis le gestionnaire de mise à jour supplémentaire.

Quelle que soit la méthode que vous choisissiez pour ce cas de figure, retrouvez plus de renseignements à la section [Scénario 2 : gestionnaire de mise à jour supplémentaire installé sur un serveur séparé](#) à la page 22.

6 Scénario 1 : bases de données installées sur un serveur séparé

6.1 Téléchargement du programme d'installation

Remarque : vous pouvez télécharger les programmes d'installation sur tout ordinateur de votre choix, puis les copier sur l'ordinateur sur lequel vous les utiliserez.

1. Connectez-vous sur <https://www.sophos.com/fr-fr/support/downloads.aspx> à l'aide de votre Sophos ID.

Remarque : si vous avez besoin d'assistance pour utiliser votre Sophos ID, consultez l'article [111195 de la base de connaissances Sophos](#).

2. Si vous vous étiez déjà connecté pour procéder à des téléchargements auparavant, vous allez voir la page **Téléchargements et mises à jour des produits**.

Remarque : s'il s'agit de votre première connexion, vous allez voir la page de votre profil. Cliquez sur **Protection des systèmes et des serveurs** puis sur **Téléchargements et mises à jour**.

3. Sous **Console**, cliquez sur le lien **Sophos Enterprise Console** et téléchargez le programme d'installation.

6.2 Installation des bases de données SEC

Remarque : si vous avez besoin d'installer les bases de données sur un serveur sécurisé à l'aide d'un script, ou dans un environnement SQL Server en cluster, rendez-vous sur www.sophos.com/fr-fr/support/knowledgebase/33980.aspx.

Si le Contrôle de compte d'utilisateur (sur Windows Server 2008 ou supérieur) est activé sur le serveur, désactivez-le et redémarrez le serveur. Vous pouvez réactiver le Contrôle de compte d'utilisateur après avoir installé les bases de données.

Ouvrez une session en tant qu'administrateur.

- Si le serveur est dans un domaine, utilisez un compte de domaine disposant des droits d'administrateur local.
 - Si le serveur est dans un groupe de travail, utilisez un compte local disposant des droits d'administrateur local.
1. Recherchez le programme d'installation de l'Enterprise Console que vous avez téléchargé auparavant et cliquez deux fois dessus.
 2. Procédez à l'extraction des fichiers d'installation dans le dossier de destination suggéré ou dans un dossier de votre choix. Le dossier doit être sur ce serveur.

L'assistant d'installation vous guide tout au long de l'installation. Acceptez les options par défaut, à l'exception de celles ci-dessous :

- a) Sur la page **Sélection des composants**, assurez-vous que la case **Base de données** est sélectionnée et que les cases **Console d'administration** et **Serveur d'administration** ne sont pas sélectionnées.
- b) Sur la page **Détails de la base de données**, saisissez les détails d'un compte qui peut se connecter à la fois à ce serveur et au serveur sur lequel vous allez installer le serveur d'administration de l'Enterprise Console. Si les serveurs sont dans un *domaine*, vous pouvez utiliser un compte de domaine. Si les serveurs sont dans un *groupe de travail*, utilisez un compte local qui existe sur les deux serveurs. Il ne faut pas que ce soit un compte d'administrateur.

Remarque : vous avez créé le compte de base de données à la section [Compte de base de données](#) à la page 11.

Lorsque l'assistant de l'Enterprise Console a terminé, redémarrez le serveur si vous y êtes invité.

Si vous avez désactivé le Contrôle de compte d'utilisateur, vous pouvez le réactiver.

6.3 Installation de SEC : console d'administration, serveur d'administration, gestionnaire de mise à jour

Rendez-vous sur le serveur sur lequel vous voulez installer la console d'administration de l'Enterprise Console, le serveur d'administration et le gestionnaire de mise à jour. Assurez-vous qu'il est connecté à Internet.

Le nom d'hôte de ce serveur doit être différent de celui des autres serveurs sur lesquels vous installez un gestionnaire de mise à jour.

Si le Contrôle de compte d'utilisateur (sur Windows Server 2008 ou supérieur) est activé sur le serveur, désactivez-le et redémarrez le serveur. Après avoir installé l'Enterprise Console et vous être abonné aux mises à jour Sophos, vous pouvez réactiver UAC.

Ouvrez une session en tant qu'administrateur.

- Si le serveur est dans un domaine, utilisez un compte de domaine disposant des droits d'administrateur local.
 - Si le serveur est dans un groupe de travail, utilisez un compte local disposant des droits d'administrateur local.
1. Recherchez le programme d'installation de l'Enterprise Console que vous avez téléchargé auparavant et cliquez deux fois dessus.
 2. Procédez à l'extraction des fichiers d'installation dans le dossier de destination suggéré ou dans un dossier de votre choix. Le dossier doit être sur ce serveur.

L'assistant d'installation vous guide tout au long de l'installation. Acceptez les options par défaut, à l'exception de celles ci-dessous :

- a) Sur la page **Sélection des composants**, assurez-vous que les cases **Console d'administration** et **Serveur d'administration** sont sélectionnées et que la case **Bases de données** n'est pas sélectionnée.
- b) Sur la page **Détails de la base de données**, saisissez l'emplacement et le nom des bases de données de l'Enterprise Console que vous avez créées sur l'autre serveur. Saisissez les détails d'un compte qui peut se connecter à la fois à ce serveur et au serveur sur lequel vous avez installé les bases de données de l'Enterprise Console.

Si les serveurs sont dans un *domaine*, vous pouvez utiliser un compte de domaine. Si les serveurs sont dans un *groupe de travail*, utilisez un compte local qui existe sur les deux serveurs. Il ne faut pas que ce soit un compte d'administrateur.

Remarque : vous avez créé le compte de base de données à la section [Compte de base de données](#) à la page 11.

Lorsque l'installation est terminée, fermez la session ou redémarrez le serveur (la dernière page de l'assistant vous indique lequel). Lorsque vous rouvrez une session, l'Enterprise Console s'ouvre automatiquement et l'assistant de téléchargement des logiciels de sécurité est lancé. Annulez l'assistant et exécutez-le plus tard lorsque ce guide vous le demandera.

6.4 Installation d'une console d'administration SEC supplémentaire

Il se peut que vous souhaitiez installer une autre instance de la console d'administration Sophos Enterprise Console sur un autre ordinateur afin de pouvoir mieux administrer les ordinateurs en réseau. Dans le cas contraire, vous pouvez passer cette section.

Important : veuillez installer la même version que celle de l'Enterprise Console utilisée sur votre serveur d'administration.

Remarque : la nouvelle console va devoir accéder au serveur sur lequel vous avez installé le serveur d'administration de l'Enterprise Console. Si ce serveur exécute un pare-feu, vous allez devoir configurer ce pare-feu afin d'assurer que l'accès est possible. Retrouvez plus d'instructions sur l'ajout d'une règle de pare-feu afin d'autoriser le trafic DCOM à partir de la console distante vers le serveur d'administration dans l'[article 49028 de la base de connaissances](#).

Pour installer une console d'administration supplémentaire :

Si le Contrôle de compte d'utilisateur (sur Windows Server 2008 ou supérieur et sur Windows Vista ou supérieur) est activé sur le serveur, désactivez-le et redémarrez le serveur. Vous pouvez réactiver le Contrôle de compte d'utilisateur après avoir installé la console d'administration.

Ouvrez une session en tant qu'administrateur.

- Si l'ordinateur est dans un domaine, utilisez un compte de domaine disposant des droits d'administrateur local.
 - Si l'ordinateur est dans un groupe de travail, utilisez un compte local disposant des droits d'administrateur local.
1. Recherchez le programme d'installation de l'Enterprise Console que vous avez téléchargé auparavant et cliquez deux fois dessus.
 2. Procédez à l'extraction des fichiers d'installation dans le dossier de destination suggéré ou dans un dossier de votre choix. Le dossier doit être sur cet ordinateur.

L'assistant d'installation vous guide tout au long de l'installation. Acceptez les options par défaut, à l'exception de celles ci-dessous :

- a) Sur la page **Sélection des composants**, assurez-vous que la case **Console d'administration** est sélectionnée et que les cases **Serveur d'administration** et **Base de données** ne sont pas sélectionnées.
- b) Sur la page **Serveur d'administration**, saisissez le nom du serveur sur lequel vous avez installé le serveur d'administration de l'Enterprise Console.

Remarque : si vous changez le port au cours de l'installation du serveur d'administration, assurez-vous de spécifier le même port sur cette page.

- c) Si vous êtes dans un environnement de domaine, veuillez saisir le compte d'utilisateur qui est utilisé pour accéder aux bases de données Enterprise Console.

Il s'agit du compte que vous avez saisi lorsque vous avez installé les bases de données Enterprise Console. Il est aussi utilisé par le service Sophos Management Host sur le serveur sur lequel vous avez installé le serveur d'administration de l'Enterprise Console.

Lorsque l'assistant a terminé, fermez la session ou redémarrez l'ordinateur (la dernière page de l'assistant vous offre le choix). À votre prochaine ouverture de session, l'Enterprise Console s'ouvrira automatiquement. Si l'**Assistant de téléchargement des logiciels de sécurité** démarre, annulez-le.

Si vous avez désactivé le Contrôle de compte d'utilisateur avant l'installation, vous pouvez le réactiver.

Pour autoriser d'autres utilisateurs à utiliser la console d'administration supplémentaire :

- Ajoutez-les au groupe **Sophos Console Administrators** et au groupe **Distributed COM Users** sur le serveur sur lequel vous avez installé le serveur d'administration.
- Assignez-les à au moins un rôle et un sous-parc de l'Enterprise Console.

6.5 Téléchargement du logiciel de sécurité

Pour télécharger le logiciel de sécurité dans un emplacement centralisé pour qu'il soit prêt à être déployé sur les stations de travail, configurez le gestionnaire de mise à jour que vous avez installé. Vous pouvez utiliser les méthodes suivantes :

La section [Configuration automatique du gestionnaire de mise à jour](#) à la page 19 vous explique comment exécuter un assistant qui va vous permettre de télécharger :

- Le logiciel de sécurité de toutes les plates-formes prises en charge.
- La version actuellement conseillée uniquement.
- Uniquement dans les sous-dossiers du partage `\\nom_serveur\SophosUpdate`, où `nom_serveur` correspond au nom du serveur sur lequel le gestionnaire de mise à jour est installé.

La section [Configuration manuelle du gestionnaire de mise à jour](#) à la page 20 vous explique comment configurer directement le gestionnaire de mise à jour qui va vous permettre de télécharger :

- Le logiciel de sécurité de toutes les plates-formes prises en charge.
- Les versions « Preview » ou plus anciennes.
- Sur d'autres partages et peut-être sur d'autres serveurs.

6.5.1 Configuration automatique du gestionnaire de mise à jour

1. Dans l'Enterprise Console, sur le menu **Actions**, cliquez sur **Exécuter l'Assistant de téléchargement des logiciels de sécurité**.
2. Sur la page **Détails du compte de téléchargement Sophos**, saisissez le nom d'utilisateur et le mot de passe imprimés sur votre annexe de licence. Si vous accédez à Internet via un serveur proxy, sélectionnez la case à cocher **Accéder à Sophos via un serveur proxy**.

3. Sur la page **Sélection des plates-formes**, sélectionnez les plates-formes que vous souhaitez protéger.
Lorsque vous cliquez sur **Suivant**, l'Enterprise Console commence à télécharger vos logiciels.
4. Sur la page **Téléchargement des logiciels**, vous pouvez voir la progression du téléchargement. Cliquez sur **Suivant**.
5. Sur la page **Importation des ordinateurs depuis Active Directory**, sélectionnez la case **Définir des groupes pour vos ordinateurs** si vous voulez que l'Enterprise Console utilise vos groupes d'ordinateurs Active Directory existants.
Remarque : si un ordinateur est ajouté à plus d'un conteneur Active Directory, un problème d'échange continu de messages entre l'ordinateur et l'Enterprise Console va se poser.

Le logiciel que vous avez sélectionné est téléchargé dans le partage `\\nom_serveur\SophosUpdate`, où *nom_serveur* correspond au nom du serveur sur lequel le gestionnaire de mise à jour est installé.

Si vous avez désactivé le Contrôle de compte d'utilisateur avant l'installation de l'Enterprise Console, vous pouvez le réactiver.

À présent, vous pouvez configurer manuellement le gestionnaire de mise à jour si nécessaire. Passez à la section [Publication des logiciels de sécurité sur un serveur Web](#) à la page 33.

6.5.2 Configuration manuelle du gestionnaire de mise à jour

Si vous avez désactivé le Contrôle de compte d'utilisateur avant l'installation de l'Enterprise Console, vous pouvez le réactiver.

1. Dans l'Enterprise Console, sur le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**.
2. Si vous n'avez pas configuré le gestionnaire de mise à jour automatiquement, configurez-le pour qu'il utilise Sophos en tant que source de mise à jour :
 - a) Dans le volet **Gestionnaires de mise à jour**, sélectionnez le gestionnaire de mise à jour installé sur ce serveur. Cliquez avec le bouton droit de la souris et cliquez sur **Voir/Modifier la configuration**.
 - b) Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Sources**, cliquez sur **Ajouter**.
 - c) Dans la boîte de dialogue **Détails de la source**, dans la boîte **Adresse**, sélectionnez **Sophos**. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les codes d'accès de téléchargement fournis par Sophos.
 - d) Si vous accédez à la source de mise à jour via un serveur proxy, sélectionnez la case **Utiliser un serveur proxy pour se connecter**. Saisissez l'**Adresse** et le numéro du **Port** du serveur proxy. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les codes d'accès au serveur proxy. Si le nom d'utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme `domaine\nomutilisateur`.
 - e) Cliquez sur **OK** pour fermer la boîte de dialogue **Détails de la source**.
Sophos est répertorié sur l'onglet **Sources** de la boîte de dialogue **Configuration du gestionnaire de mise à jour**.
 - f) Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du gestionnaire de mise à jour**.

3. Abonnez-vous aux logiciels que vous souhaitez télécharger :
 - a) Dans le volet **Abonnements logiciels** :
 - Pour changer un abonnement existant, cliquez deux fois dessus.
 - Pour ajouter un nouvel abonnement, cliquez sur **Ajouter** en haut du volet.
 - b) Dans la boîte de dialogue **Abonnement logiciels**, si vous ajoutez un nouvel abonnement, saisissez un nom pour cet abonnement dans la boîte **Nom de l'abonnement**.
 - c) Dans la liste des plates-formes, sélectionnez la case à cocher près du logiciel que vous voulez et sélectionnez la version souhaitée dans la case version.
 Normalement, il convient de s'abonner à la version **Recommanded** (conseillée) pour s'assurer que votre logiciel est automatiquement maintenu à jour. Retrouvez plus de renseignements sur les autres types de version disponibles dans l'Aide de l'Enterprise Console à la section sur la configuration des abonnements logiciels.
 - d) Cliquez sur **OK** pour fermer la boîte de dialogue **Abonnement logiciels**.
 - e) Répétez ces étapes pour chaque abonnement que vous souhaitez modifier ou ajouter.
4. Configurez le gestionnaire de mise à jour pour qu'il utilise ces abonnements :
 - a) Dans le volet **Gestionnaires de mise à jour**, sélectionnez le gestionnaire de mise à jour installé sur ce serveur. Cliquez avec le bouton droit de la souris et cliquez sur **Voir/Modifier la configuration**.
 - b) Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Abonnements**, assurez-vous que les abonnements figurent dans la liste **Abonné à**. Autrement, sélectionnez les abonnements dans la liste **Disponible** et cliquez sur le bouton **>** pour les déplacer dans la liste **Abonné à**.
5. Si vous voulez télécharger dans d'autres partages que `\\nom serveur\SophosUpdate` :
 - a) Cliquez sur l'onglet **Distribution**.
 - b) Assurez-vous que l'abonnement que vous voulez utiliser est sélectionné dans la liste en haut de l'onglet.
 - c) Cliquez sur **Ajouter**.
 - d) Dans la boîte de dialogue **Rechercher un dossier**, naviguez jusqu'à l'un de ces partages. Cliquez sur **OK**.
 - e) Sélectionnez le partage dans la liste **Disponible** et cliquez sur le bouton **>** pour le déplacer dans la liste **Mettre à jour dans**.
 - f) Pour saisir une description pour le partage, ou les codes d'accès en écriture sur ce partage, sélectionnez le partage et cliquez sur **Configurer**. Dans la boîte de dialogue **Gestionnaire des partages**, saisissez la description et les codes d'accès.
 - g) Répétez ces étapes pour chaque partage.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du gestionnaire de mise à jour**.
 Le logiciel que vous avez sélectionné est téléchargé dans les partages que vous avez indiqués.

Vous avez maintenant terminé l'installation des outils d'administration. Passez maintenant à la section [Publication des logiciels de sécurité sur un serveur Web](#) à la page 33.

7 Scénario 2 : gestionnaire de mise à jour supplémentaire installé sur un serveur séparé

Ce scénario inclut deux méthodes de configuration des sources de mise à jour sur les gestionnaires de mise à jour.

La première méthode consiste à :

- Configurer le gestionnaire de mise à jour principal que vous avez installé simultanément avec la console d'administration pour qu'il se mette à jour directement depuis Sophos.
- Configurer le gestionnaire de mise à jour supplémentaire pour qu'il se mette à jour depuis le gestionnaire de mise à jour principal.

La seconde méthode consiste à :

- Configurer le gestionnaire de mise à jour supplémentaire pour qu'il se mette à jour directement depuis Sophos.
- Configurer le gestionnaire de mise à jour que vous avez installé simultanément avec la console d'administration pour qu'il se mette à jour depuis le gestionnaire de mise à jour supplémentaire.

La seconde méthode peut être utilisée si vous ne souhaitez pas connecter le serveur Enterprise Console principal à Internet.

La méthode que vous choisissez affecte :

- Le choix des serveurs devant être connectés à Internet. Dans les sections d'installation suivantes, vous êtes informé lorsque le serveur sur lequel vous effectuez l'installation nécessite une connexion à Internet.
- La méthode que vous choisissez pour télécharger le logiciel de sécurité dans un emplacement centralisé, prêt à être déployé sur les stations de travail. Choisissez la section qui vous convient lorsque vous arrivez à ce stade.
- Si vous pouvez utiliser la fonction d'évaluation des correctifs dans l'Enterprise Console. Pour utiliser cette fonction, choisissez la première méthode.

7.1 Téléchargement du programme d'installation

Remarque : vous pouvez télécharger les programmes d'installation sur tout ordinateur de votre choix, puis les copier sur l'ordinateur sur lequel vous les utiliserez.

1. Connectez-vous sur <https://www.sophos.com/fr-fr/support/downloads.aspx> à l'aide de votre Sophos ID.

Remarque : si vous avez besoin d'assistance pour utiliser votre Sophos ID, consultez l'[article 111195 de la base de connaissances Sophos](#).

2. Si vous vous étiez déjà connecté pour procéder à des téléchargements auparavant, vous allez voir la page **Téléchargements et mises à jour des produits**.

Remarque : s'il s'agit de votre première connexion, vous allez voir la page de votre profil. Cliquez sur **Protection des systèmes et des serveurs** puis sur **Téléchargements et mises à jour**.

3. Sous **Console**, cliquez sur le lien **Sophos Enterprise Console** et téléchargez le programme d'installation.

7.2 Installation de SEC : tous les composants

Rendez-vous sur le serveur sur lequel vous souhaitez installer tous les composants de l'Enterprise Console. Si vous voulez que le gestionnaire de mise à jour que vous avez installé sur ce serveur se mette directement à jour depuis Sophos, assurez-vous que le serveur est connecté à Internet.

Le nom d'hôte de ce serveur doit être différent de celui des autres serveurs sur lesquels vous installez un gestionnaire de mise à jour.

Si le Contrôle de compte d'utilisateur (sur Windows Server 2008 ou supérieur) est activé sur le serveur, désactivez-le et redémarrez le serveur. Après avoir installé l'Enterprise Console et vous être abonné aux mises à jour Sophos, vous pouvez réactiver UAC.

Ouvrez une session en tant qu'administrateur.

- Si le serveur est dans un domaine, utilisez un compte de domaine disposant des droits d'administrateur local.
 - Si le serveur est dans un groupe de travail, utilisez un compte local disposant des droits d'administrateur local.
1. Recherchez le programme d'installation de l'Enterprise Console que vous avez téléchargé auparavant et cliquez deux fois dessus.
 2. Procédez à l'extraction des fichiers d'installation dans le dossier de destination suggéré ou dans un dossier de votre choix. Le dossier doit être sur ce serveur.

L'assistant d'installation vous guide tout au long de l'installation. Acceptez les options par défaut, à l'exception de celles ci-dessous :

- a) Sur la page **Sélection des composants**, assurez-vous que *tous* les composants sont sélectionnés.
- b) Sur la page **Détails de la base de données**, saisissez les détails d'un compte pouvant se connecter à ce serveur. Si le serveur est dans un *domaine*, vous pouvez utiliser un compte de domaine. Si le serveur est dans un *groupe de travail*, utilisez un compte local qui existe sur le serveur. Il ne faut pas que ce soit un compte d'administrateur.

Remarque : vous avez créé le compte de base de données à la section [Compte de base de données](#) à la page 11.

Lorsque l'installation est terminée, fermez la session ou redémarrez le serveur (la dernière page de l'assistant vous indique lequel). Lorsque vous rouvrez une session, l'Enterprise Console s'ouvre automatiquement et l'assistant de téléchargement des logiciels de sécurité est lancé. Annulez l'assistant et exécutez-le plus tard lorsque ce guide vous le demandera.

7.3 Installation d'une console d'administration SEC supplémentaire

Il se peut que vous souhaitiez installer une autre instance de la console d'administration Sophos Enterprise Console sur un autre ordinateur afin de pouvoir mieux administrer les ordinateurs en réseau. Dans le cas contraire, vous pouvez passer cette section.

Important : veuillez installer la même version que celle de l'Enterprise Console utilisée sur votre serveur d'administration.

Remarque : la nouvelle console va devoir accéder au serveur sur lequel vous avez installé le serveur d'administration de l'Enterprise Console. Si ce serveur exécute un pare-feu, vous allez devoir configurer ce pare-feu afin d'assurer que l'accès est possible. Retrouvez plus d'instructions sur l'ajout d'une règle de pare-feu afin d'autoriser le trafic DCOM à partir de la console distante vers le serveur d'administration dans l'[article 49028 de la base de connaissances](#).

Pour installer une console d'administration supplémentaire :

Si le Contrôle de compte d'utilisateur (sur Windows Server 2008 ou supérieur et sur Windows Vista ou supérieur) est activé sur le serveur, désactivez-le et redémarrez le serveur. Vous pouvez réactiver le Contrôle de compte d'utilisateur après avoir installé la console d'administration.

Ouvrez une session en tant qu'administrateur.

- Si l'ordinateur est dans un domaine, utilisez un compte de domaine disposant des droits d'administrateur local.
 - Si l'ordinateur est dans un groupe de travail, utilisez un compte local disposant des droits d'administrateur local.
1. Recherchez le programme d'installation de l'Enterprise Console que vous avez téléchargé auparavant et cliquez deux fois dessus.
 2. Procédez à l'extraction des fichiers d'installation dans le dossier de destination suggéré ou dans un dossier de votre choix. Le dossier doit être sur cet ordinateur.

L'assistant d'installation vous guide tout au long de l'installation. Acceptez les options par défaut, à l'exception de celles ci-dessous :

- a) Sur la page **Sélection des composants**, assurez-vous que la case **Console d'administration** est sélectionnée et que les cases **Serveur d'administration** et **Base de données** ne sont pas sélectionnées.
- b) Sur la page **Serveur d'administration**, saisissez le nom du serveur sur lequel vous avez installé le serveur d'administration de l'Enterprise Console.
- c) Si vous êtes dans un environnement de domaine, veuillez saisir le compte d'utilisateur qui est utilisé pour accéder aux bases de données Enterprise Console.

Remarque : si vous changez le port au cours de l'installation du serveur d'administration, assurez-vous de spécifier le même port sur cette page.

Il s'agit du compte que vous avez saisi lorsque vous avez installé les bases de données Enterprise Console. Il est aussi utilisé par le service Sophos Management Host sur le serveur sur lequel vous avez installé le serveur d'administration de l'Enterprise Console.

Lorsque l'assistant a terminé, fermez la session ou redémarrez l'ordinateur (la dernière page de l'assistant vous offre le choix). À votre prochaine ouverture de session, l'Enterprise Console

s'ouvrira automatiquement. Si l'**Assistant de téléchargement des logiciels de sécurité** démarre, annulez-le.

Si vous avez désactivé le Contrôle de compte d'utilisateur avant l'installation, vous pouvez le réactiver.

Pour autoriser d'autres utilisateurs à utiliser la console d'administration supplémentaire :

- Ajoutez-les au groupe **Sophos Console Administrators** et au groupe **Distributed COM Users** sur le serveur sur lequel vous avez installé le serveur d'administration.
- Assignez-les à au moins un rôle et un sous-parc de l'Enterprise Console.

7.4 Installation d'un gestionnaire de mise à jour supplémentaire

Important : si vous voulez installer une console d'administration SEC supplémentaire sur le serveur sur lequel vous voulez installer un gestionnaire de mise à jour supplémentaire, installez tout d'abord la console supplémentaire, comme l'explique la section [Installation d'une console d'administration SEC supplémentaire](#) à la page 24.

Rendez-vous sur le serveur sur lequel vous souhaitez installer un gestionnaire de mise à jour supplémentaire. Si vous voulez que le gestionnaire de mise à jour que vous avez installé sur ce serveur se mette directement à jour depuis Sophos, assurez-vous que le serveur est connecté à Internet.

Le nom d'hôte de ce serveur doit être différent de celui des autres serveurs sur lesquels vous installez un gestionnaire de mise à jour.

Si la Découverte de réseau (sur Windows Server 2008 ou supérieur) est activée sur le serveur, désactivez-la et redémarrez le serveur.

Si le Contrôle de compte d'utilisateur (sur Windows Server 2008 ou supérieur) est activé sur le serveur, désactivez-le et redémarrez le serveur. Après avoir installé le gestionnaire de mise à jour et vous être abonné aux mises à jour Sophos, vous pouvez réactiver le Contrôle de compte d'utilisateur.

Ouvrez une session en tant qu'administrateur.

- Si le serveur est dans un domaine, utilisez un compte de domaine disposant des droits d'administrateur local.
 - Si le serveur est dans un groupe de travail, utilisez un compte local disposant des droits d'administrateur local.
1. Recherchez le dossier partagé `SUMInstallSet` sur le serveur sur lequel vous avez installé l'Enterprise Console.
 2. Cliquez deux fois sur `Setup.exe` pour exécuter le programme d'installation.
L'assistant d'installation vous guide tout au long de l'installation. Acceptez les options par défaut.

Vous venez d'installer un gestionnaire de mise à jour administré par l'Enterprise Console.

7.5 Téléchargement du logiciel de sécurité

Ce cas de figure inclut deux méthodes de configuration des sources de mise à jour sur les gestionnaires de mise à jour. Choisissez celle que vous semble la plus pratique :

- [Mise à jour du gestionnaire de mise à jour principal depuis Sophos](#) à la page 26

- [Mise à jour du gestionnaire de mise à jour supplémentaire depuis Sophos](#) à la page 29

7.5.1 Mise à jour du gestionnaire de mise à jour principal depuis Sophos

Configuration du gestionnaire de mise à jour principal pour qu'il se mette à jour depuis Sophos

Veillez configurer le gestionnaire de mise à jour principal que vous avez installé avec la console d'administration pour qu'il se mette à jour directement depuis Sophos. Vous pouvez utiliser les méthodes suivantes :

La section [Configuration automatique du gestionnaire de mise à jour principal](#) à la page 26 vous explique comment exécuter un assistant qui va vous permettre de télécharger :

- Le logiciel de sécurité de toutes les plates-formes prises en charge.
- Uniquement la version la plus récente.
- Uniquement dans les sous-dossiers du partage `\\nom_serveur\SophosUpdate`, où *nom_serveur* correspond au nom du serveur sur lequel le gestionnaire de mise à jour principal est installé.

La section [Configuration manuelle du gestionnaire de mise à jour principal](#) à la page 27 vous explique comment configurer directement le gestionnaire de mise à jour principal qui va vous permettre de télécharger :

- Le logiciel de sécurité de toutes les plates-formes prises en charge.
- Les versions antérieures.
- Sur d'autres partages et peut-être sur d'autres serveurs.

Retrouvez plus de renseignements sur les autres types de version disponibles à la section sur la configuration des abonnements de l'aide de l'Enterprise Console.

Configuration du gestionnaire de mise à jour supplémentaire pour qu'il se mette à jour depuis le gestionnaire de mise à jour principal

[Configuration du gestionnaire de mise à jour supplémentaire](#) à la page 28 explique comment configurer le gestionnaire de mise à jour supplémentaire pour qu'il se mette à jour depuis le gestionnaire de mise à jour principal

7.5.1.1 Configuration automatique du gestionnaire de mise à jour principal

1. Dans l'Enterprise Console, sur le menu **Actions**, cliquez sur **Exécuter l'Assistant de téléchargement des logiciels de sécurité**.
2. Sur la page **Détails du compte de téléchargement Sophos**, saisissez le nom d'utilisateur et le mot de passe imprimés sur votre annexe de licence. Si vous accédez à Internet via un serveur proxy, sélectionnez la case à cocher **Accéder à Sophos via un serveur proxy**.
3. Sur la page **Sélection des plates-formes**, sélectionnez les plates-formes que vous souhaitez protéger.

Lorsque vous cliquez sur **Suivant**, l'Enterprise Console commence à télécharger vos logiciels.

4. Sur la page **Téléchargement des logiciels**, vous pouvez voir la progression du téléchargement. Cliquez sur **Suivant**.

5. Sur la page **Importation des ordinateurs depuis Active Directory**, sélectionnez la case **Définir des groupes pour vos ordinateurs** si vous voulez que l'Enterprise Console utilise vos groupes d'ordinateurs Active Directory existants.

Remarque : si un ordinateur est ajouté à plus d'un conteneur Active Directory, un problème d'échange continu de messages entre l'ordinateur et l'Enterprise Console va se poser.

Le logiciel que vous avez sélectionné est téléchargé dans le partage `\\nom_serveur\SophosUpdate`, où *nom_serveur* correspond au nom du serveur sur lequel le gestionnaire de mise à jour est installé.

Si vous avez désactivé le Contrôle de compte d'utilisateur avant l'installation de l'Enterprise Console, vous pouvez le réactiver.

À présent, vous pouvez configurer manuellement le gestionnaire de mise à jour si nécessaire. Passez à la section [Configuration du gestionnaire de mise à jour supplémentaire](#) à la page 28.

7.5.1.2 Configuration manuelle du gestionnaire de mise à jour principal

Si vous avez désactivé le Contrôle de compte d'utilisateur avant l'installation de l'Enterprise Console, vous pouvez le réactiver.

1. Dans l'Enterprise Console, sur le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**.
2. Si vous n'avez pas configuré le gestionnaire de mise à jour automatiquement, configurez-le pour qu'il utilise Sophos en tant que source de mise à jour :
 - a) Dans le volet **Gestionnaires de mise à jour**, sélectionnez le gestionnaire de mise à jour installé sur ce serveur. Cliquez avec le bouton droit de la souris et cliquez sur **Voir/Modifier la configuration**.
 - b) Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Sources**, cliquez sur **Ajouter**.
 - c) Dans la boîte de dialogue **Détails de la source**, dans la boîte **Adresse**, sélectionnez **Sophos**. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les codes d'accès de téléchargement fournis par Sophos.
 - d) Si vous accédez à la source de mise à jour via un serveur proxy, sélectionnez la case **Utiliser un serveur proxy pour se connecter**. Saisissez l'**Adresse** et le numéro du **Port** du serveur proxy. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les codes d'accès au serveur proxy. Si le nom d'utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme `domaine\nomutilisateur`.
 - e) Cliquez sur **OK** pour fermer la boîte de dialogue **Détails de la source**.
Sophos est répertorié sur l'onglet **Sources** de la boîte de dialogue **Configuration du gestionnaire de mise à jour**.
 - f) Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du gestionnaire de mise à jour**.
3. Abonnez-vous aux logiciels que vous souhaitez télécharger :
 - a) Dans le volet **Abonnements logiciels** :
 - Pour changer un abonnement existant, cliquez deux fois dessus.

- Pour ajouter un nouvel abonnement, cliquez sur **Ajouter** en haut du volet.
 - b) Dans la boîte de dialogue **Abonnement logiciels**, si vous ajoutez un nouvel abonnement, saisissez un nom pour cet abonnement dans la boîte **Nom de l'abonnement**.
 - c) Dans la liste des plates-formes, sélectionnez la case à cocher près du logiciel que vous voulez et sélectionnez la version souhaitée dans la case version.
Normalement, il convient de s'abonner à la version **Recommended** (conseillée) pour s'assurer que votre logiciel est automatiquement maintenu à jour. Retrouvez plus de renseignements sur les autres types de version disponibles dans l'Aide de l'Enterprise Console à la section sur la configuration des abonnements logiciels.
 - d) Cliquez sur **OK** pour fermer la boîte de dialogue **Abonnement logiciels**.
 - e) Répétez ces étapes pour chaque abonnement que vous souhaitez modifier ou ajouter.
4. Configurez le gestionnaire de mise à jour pour qu'il utilise ces abonnements :
- a) Dans le volet **Gestionnaires de mise à jour**, sélectionnez le gestionnaire de mise à jour installé sur ce serveur. Cliquez avec le bouton droit de la souris et cliquez sur **Voir/Modifier la configuration**.
 - b) Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Abonnements**, assurez-vous que les abonnements figurent dans la liste **Abonné à**. Autrement, sélectionnez les abonnements dans la liste **Disponible** et cliquez sur le bouton **>** pour les déplacer dans la liste **Abonné à**.
5. Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du gestionnaire de mise à jour**.
- Le logiciel que vous avez sélectionné est téléchargé dans le gestionnaire de mise à jour installé sur ce serveur.

7.5.1.3 Configuration du gestionnaire de mise à jour supplémentaire

1. Dans l'Enterprise Console, sur le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**.
2. Configurez le gestionnaire de mise à jour supplémentaire pour qu'il utilise le gestionnaire de mise à jour principal comme source de mise à jour :
 - a) Dans le volet **Gestionnaire de mise à jour**, sélectionnez le gestionnaire de mise à jour supplémentaire. Cliquez avec le bouton droit de la souris et cliquez sur **Voir/Modifier la configuration**.
 - b) Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Sources**, cliquez sur **Ajouter**.
 - c) Dans la boîte de dialogue **Détails de la source**, dans la zone **Adresse**, sélectionnez le partage dans lequel le gestionnaire de mise à jour télécharge les logiciels.
Les boîtes **Nom d'utilisateur** et **Mot de passe** sont automatiquement chargées avec les codes d'accès nécessaires pour accéder à ce partage.
 - d) Si vous accédez à la source de mise à jour via un serveur proxy, sélectionnez la case **Utiliser un serveur proxy pour se connecter**. Saisissez l'**Adresse** et le numéro du **Port** du serveur proxy. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez

les codes d'accès au serveur proxy. Si le nom d'utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme domaine\nomutilisateur.

- e) Cliquez sur **OK** pour fermer la boîte de dialogue **Détails de la source**.

Le partage dans lequel le gestionnaire de mise à jour principal télécharge les logiciels est répertorié dans l'onglet **Sources** de la boîte de dialogue **Configuration du gestionnaire de mise à jour**.

3. Configurez le gestionnaire de mise à jour pour utiliser les abonnements que vous avez paramétrés auparavant :
 - Sur l'onglet **Abonnements**, assurez-vous que les abonnements figurent dans la liste **Abonné à**. Autrement, sélectionnez les abonnements dans la liste **Disponible** et cliquez sur le bouton > pour les déplacer dans la liste **Abonné à**.
4. Si vous voulez télécharger dans d'autres partages que \\nom_serveur\SophosUpdate :
 - a) Cliquez sur l'onglet **Distribution**.
 - b) Assurez-vous que l'abonnement que vous voulez utiliser est sélectionné dans la liste en haut de l'onglet.
 - c) Cliquez sur **Ajouter**.
 - d) Dans la boîte de dialogue **Rechercher un dossier**, naviguez jusqu'à l'un de ces partages. Cliquez sur **OK**.
 - e) Sélectionnez le partage dans la liste **Disponible** et cliquez sur le bouton > pour le déplacer dans la liste **Mettre à jour dans**.
 - f) Pour saisir une description pour le partage, ou les codes d'accès en écriture sur ce partage, sélectionnez le partage et cliquez sur **Configurer**. Dans la boîte de dialogue **Gestionnaire des partages**, saisissez la description et les codes d'accès.
 - g) Répétez ces étapes pour chaque partage.
5. Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du gestionnaire de mise à jour**.

Le logiciel que vous avez sélectionné sera téléchargé dans les partages que vous avez indiqués à la prochaine mise à jour planifiée.

Vous avez maintenant terminé l'installation des outils d'administration. Passez maintenant à la section [Publication des logiciels de sécurité sur un serveur Web](#) à la page 33.

7.5.2 Mise à jour du gestionnaire de mise à jour supplémentaire depuis Sophos

La section [Configuration du gestionnaire de mise à jour supplémentaire](#) à la page 30 vous explique comment configurer la mise à jour du gestionnaire de mise à jour supplémentaire directement à partir de Sophos.

La section [Configuration du gestionnaire de mise à jour principal](#) à la page 31 vous explique comment configurer le gestionnaire de mise à jour principal que vous avez installé avec la console d'administration SEC pour qu'il se mette à jour depuis le gestionnaire de mise à jour supplémentaire.

7.5.2.1 Configuration du gestionnaire de mise à jour supplémentaire

Si vous avez désactivé le Contrôle de compte d'utilisateur avant l'installation de l'Enterprise Console, vous pouvez le réactiver.

1. Dans l'Enterprise Console, sur le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**.
2. Configurez le gestionnaire de mise à jour supplémentaire pour qu'il utilise Sophos comme source de mise à jour :
 - a) Dans le volet **Gestionnaire de mise à jour**, sélectionnez le gestionnaire de mise à jour supplémentaire. Cliquez avec le bouton droit de la souris et cliquez sur **Voir/Modifier la configuration**.
 - b) Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Sources**, cliquez sur **Ajouter**.
 - c) Dans la boîte de dialogue **Détails de la source**, dans la boîte **Adresse**, sélectionnez **Sophos**. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les codes d'accès de téléchargement fournis par Sophos.
 - d) Si vous accédez à la source de mise à jour via un serveur proxy, sélectionnez la case **Utiliser un serveur proxy pour se connecter**. Saisissez l'**Adresse** et le numéro du **Port** du serveur proxy. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les codes d'accès au serveur proxy. Si le nom d'utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme domaine\nomutilisateur.
 - e) Cliquez sur **OK** pour fermer la boîte de dialogue **Détails de la source**.
Sophos est répertorié sur l'onglet **Sources** de la boîte de dialogue **Configuration du gestionnaire de mise à jour**.
 - f) Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du gestionnaire de mise à jour**.
3. Abonnez-vous aux logiciels que vous souhaitez télécharger :
 - a) Dans le volet **Abonnements logiciels** :
 - Pour changer un abonnement existant, cliquez deux fois dessus.
 - Pour ajouter un nouvel abonnement, cliquez sur **Ajouter** en haut du volet.
 - b) Dans la boîte de dialogue **Abonnement logiciels**, si vous ajoutez un nouvel abonnement, saisissez un nom pour cet abonnement dans la boîte **Nom de l'abonnement**.
 - c) Dans la liste des plates-formes, sélectionnez la case à cocher près du logiciel que vous voulez et sélectionnez la version souhaitée dans la case version.
Normalement, il convient de s'abonner à la version **Recommended** (conseillée) pour s'assurer que votre logiciel est automatiquement maintenu à jour. Retrouvez plus de renseignements sur les autres types de version disponibles dans l'Aide de l'Enterprise Console à la section sur la configuration des abonnements logiciels.
 - d) Cliquez sur **OK** pour fermer la boîte de dialogue **Abonnement logiciels**.
 - e) Répétez ces étapes pour chaque abonnement que vous souhaitez modifier ou ajouter.

4. Configurez le gestionnaire de mise à jour pour qu'il utilise ces abonnements :
 - a) Dans le volet **Gestionnaire de mise à jour**, sélectionnez le gestionnaire de mise à jour supplémentaire. Cliquez avec le bouton droit de la souris et cliquez sur **Voir/Modifier la configuration**.
 - b) Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Abonnements**, assurez-vous que les abonnements figurent dans la liste **Abonné à**. Autrement, sélectionnez les abonnements dans la liste **Disponible** et cliquez sur le bouton > pour les déplacer dans la liste **Abonné à**.
5. Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du gestionnaire de mise à jour**.
Le logiciel que vous avez sélectionné est téléchargé dans le gestionnaire de mise à jour supplémentaire.

7.5.2.2 Configuration du gestionnaire de mise à jour principal

1. Dans l'Enterprise Console, sur le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**.
2. Configurez le gestionnaire de mise à jour principal pour qu'il utilise le gestionnaire de mise à jour supplémentaire comme source de mise à jour :
 - a) Dans le volet **Gestionnaires de mise à jour**, sélectionnez le gestionnaire de mise à jour installé sur ce serveur. Cliquez avec le bouton droit de la souris et cliquez sur **Voir/Modifier la configuration**.
 - b) Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Sources**, cliquez sur **Ajouter**.
 - c) Dans la boîte de dialogue **Détails de la source**, dans la boîte **Adresse**, sélectionnez le partage dans lequel le gestionnaire de mise à jour supplémentaire télécharge les logiciels.
Les boîtes **Nom d'utilisateur** et **Mot de passe** sont automatiquement chargées avec les codes d'accès nécessaires pour accéder à ce partage.
 - d) Si vous accédez à la source de mise à jour via un serveur proxy, sélectionnez la case **Utiliser un serveur proxy pour se connecter**. Saisissez l'**Adresse** et le numéro du **Port** du serveur proxy. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les codes d'accès au serveur proxy. Si le nom d'utilisateur doit être qualifié pour indiquer le domaine, utilisez la forme domaine\nomutilisateur.
 - e) Cliquez sur **OK** pour fermer la boîte de dialogue **Détails de la source**.
Le partage dans lequel le gestionnaire de mise à jour supplémentaire télécharge les logiciels est répertorié dans l'onglet **Sources** de la boîte de dialogue **Configuration du gestionnaire de mise à jour**.
3. Configurez le gestionnaire de mise à jour pour utiliser les abonnements que vous avez paramétrés auparavant :
 - Sur l'onglet **Abonnements**, assurez-vous que les abonnements figurent dans la liste **Abonné à**. Autrement, sélectionnez les abonnements dans la liste **Disponible** et cliquez sur le bouton > pour les déplacer dans la liste **Abonné à**.

4. Si vous voulez télécharger dans d'autres partages que `\\nom_serveur\SophosUpdate` :
 - a) Cliquez sur l'onglet **Distribution**.
 - b) Assurez-vous que l'abonnement que vous voulez utiliser est sélectionné dans la liste en haut de l'onglet.
 - c) Cliquez sur **Ajouter**.
 - d) Dans la boîte de dialogue **Rechercher un dossier**, naviguez jusqu'à l'un de ces partages. Cliquez sur **OK**.
 - e) Sélectionnez le partage dans la liste **Disponible** et cliquez sur le bouton **>** pour le déplacer dans la liste **Mettre à jour dans**.
 - f) Pour saisir une description pour le partage, ou les codes d'accès en écriture sur ce partage, sélectionnez le partage et cliquez sur **Configurer**. Dans la boîte de dialogue **Gestionnaire des partages**, saisissez la description et les codes d'accès.
 - g) Répétez ces étapes pour chaque partage.
5. Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du gestionnaire de mise à jour**.

Le logiciel que vous avez sélectionné sera téléchargé dans les partages que vous avez indiqués à la prochaine mise à jour planifiée.

Vous avez maintenant terminé l'installation des outils d'administration. Passez maintenant à la section [Publication des logiciels de sécurité sur un serveur Web](#) à la page 33.

8 Publication des logiciels de sécurité sur un serveur Web

Vous pouvez, si vous le souhaitez, publier les logiciels de sécurité Sophos sur un serveur Web pour que les ordinateurs disposent d'un accès via HTTP. Ceci peut être utile en particulier pour les ordinateurs qui ne sont pas toujours connectés au réseau.

- Retrouvez plus de renseignements sur la publication des logiciels de sécurité sur un serveur Web sur www.sophos.com/fr-fr/support/knowledgebase/38238.aspx.

9 Création de groupes d'ordinateurs

Si vous avez utilisé l'Assistant de téléchargement des logiciels de sécurité pour paramétrer vos groupes d'ordinateurs (d'après vos groupes Active Directory), vous pouvez ignorer cette section. Passez à la section [Configuration des stratégies de sécurité](#) à la page 35.

Avant de pouvoir protéger et administrer les ordinateurs, vous devez leur créer des groupes.

1. Si le volet **Groupes** (à gauche de la fenêtre) n'apparaît pas, dans le menu **Affichage**, cliquez sur **Ordinateurs d'extrémité**.
2. Cliquez n'importe où dans le volet **Groupes**. Assurez-vous que le groupe **Non assigné** n'est pas sélectionné.
3. Dans le menu **Groupes**, cliquez sur **Créer un groupe**.
Un **Nouveau groupe** est ajouté dans le volet de gauche et son nom est mis en surbrillance.
4. Saisissez le nom que vous voulez utiliser pour le groupe.
5. Pour créer un autre groupe au niveau supérieur, sélectionnez le serveur qui apparaît en haut du volet **Groupes** et répétez les étapes 3 et 4.
Pour créer un sous-groupe dans un groupe existant, sélectionnez le groupe existant et répétez les étapes 3 et 4.

10 Configuration des stratégies de sécurité

Une *stratégie de sécurité* est un ensemble de paramètres applicables aux ordinateurs d'un ou de plusieurs groupes.

L'Enterprise Console applique les stratégies par défaut à vos groupes d'ordinateurs. Cette section vous explique :

- Quelles sont les stratégies par défaut et si vous devez les changer.
- La création ou la modification d'une stratégie.
- L'application d'une stratégie à vos groupes d'ordinateurs.

10.1 Stratégies par défaut

L'Enterprise Console applique les stratégies de sécurité « par défaut » à vos groupes d'ordinateurs. Sauf si vous le souhaitez, il n'est pas nécessaire de changer ces stratégies, sauf pour les exceptions suivantes :

- Vous devez immédiatement configurer une stratégie de pare-feu.
- Vous devez modifier les stratégies de contrôle des applications, de contrôle des données, de contrôle des périphériques, de protection antialtération, de correctifs, de prévention des Exploits ou de contrôle du Web si vous souhaitez utiliser ces fonctions. Vous pouvez effectuer cette opération à tout moment.

Retrouvez plus de renseignements sur les paramètres des stratégies conseillés dans le *Guide de configuration des stratégies de Sophos Enterprise Console*.

10.2 Configuration d'une stratégie de pare-feu

Par défaut, le pare-feu bloque toutes les connexions qui ne sont pas indispensables. Vous devez, par conséquent, configurer le pare-feu avant de protéger vos ordinateurs.

1. Dans le volet **Stratégies**, cliquez avec le bouton droit de la souris sur **Pare-feu** et cliquez sur **Créer une stratégie**.

Une **Nouvelle stratégie** est ajoutée à la liste et son nom est mis en surbrillance. Saisissez le nom que vous voulez utiliser pour la stratégie.

2. Cliquez deux fois sur la stratégie pour la modifier.

Un assistant se lance.

3. Dans l'**Assistant de stratégie de pare-feu**, nous vous conseillons d'effectuer les sélections suivantes.

- a) Sur la page **Configuration du pare-feu**, sélectionnez **Emplacement unique** sauf si vous voulez que le pare-feu utilise des paramètres différents en fonction de l'endroit où vous l'utilisez.
- b) Sur la page **Mode de fonctionnement**, sélectionnez **Bloquer le trafic entrant et autoriser le trafic sortant**.
- c) Sur la page **Partage de fichiers et d'imprimantes**, sélectionnez **Autoriser le partage de fichiers et d'imprimantes**.

10.3 Création ou modification d'une stratégie

1. Dans l'Enterprise Console, si le volet **Stratégies** (en bas à gauche de la fenêtre) n'apparaît pas, dans le menu **Affichage**, cliquez sur **Terminaux**.
2. Dans le volet **Stratégies**, effectuez l'une des opérations suivantes :

- Pour créer une nouvelle stratégie, cliquez avec le bouton droit de la souris sur la stratégie que vous souhaitez créer, par exemple, **Mise à jour**, et sélectionnez **Créer une stratégie**.
- Pour modifier une stratégie par défaut, cliquez deux fois sur le type de stratégie que vous souhaitez modifier. Puis, sélectionnez **Par défaut**.

Si vous avez créé une stratégie, une **Nouvelle stratégie** est ajoutée à la liste et son nom apparaît en surbrillance. Saisissez le nom que vous voulez utiliser pour la stratégie.

3. Cliquez deux fois sur la nouvelle stratégie. Saisissez les paramètres de votre choix.

Si vous avez créé une stratégie, vous devez l'appliquer à un groupe d'ordinateurs.

10.4 Application d'une stratégie à un groupe

- Dans le volet **Stratégies**, faites glisser la stratégie sur le groupe auquel vous souhaitez appliquer la stratégie.

Remarque : autrement, cliquez avec le bouton droit de la souris sur un groupe et sélectionnez **Voir/Modifier les détails de la stratégie du groupe**. Sélectionnez ensuite les stratégies de ce groupe dans les menus déroulants.

11 Recherche d'ordinateurs

Vous devez rechercher les ordinateurs sur le réseau avant que l'Enterprise Console ne puisse les protéger et les administrer.

1. Si le volet **Groupes** (à gauche de la fenêtre) n'apparaît pas, dans le menu **Affichage**, cliquez sur **Ordinateurs d'extrémité**.
2. Dans le menu **Actions**, cliquez sur **Détecter des ordinateurs**.
3. Sélectionnez la méthode que vous voulez utiliser pour rechercher les ordinateurs.
4. Saisissez les détails du compte, si nécessaire, et spécifiez où vous voulez effectuer la recherche.

Si vous utilisez une des options de **Détection**, les ordinateurs sont placés dans le groupe **Non assignés**.

12 Préparation de la protection des ordinateurs

12.1 Préparation de la suppression des logiciels tiers

Si vous voulez que le programme d'installation Sophos supprime tout logiciel de sécurité précédemment installé :

1. Sur les ordinateurs sur lesquels fonctionne le logiciel antivirus d'un autre éditeur, assurez-vous que l'interface utilisateur du logiciel antivirus est fermée.

Remarque : hitmanPro.Alert sera peut-être déjà installé en tant que produit autonome ou administré à partir de Sophos Central. Veuillez désinstaller HitmanPro.Alert avant d'appliquer l'administration locale à partir de Sophos Enterprise Console.

2. Sur les ordinateurs sur lesquels fonctionne le pare-feu ou le produit HIPS d'un autre éditeur, assurez-vous que ce pare-feu ou ce produit HIPS est désactivé ou configuré pour autoriser l'exécution du programme d'installation Sophos.

Si les ordinateurs utilisent l'outil de mise à jour d'un autre éditeur, vous pouvez le supprimer si vous le désirez. Retrouvez plus de renseignements dans l'Aide de l'Enterprise Console.

12.2 Vérification que votre compte peut être utilisé pour l'installation du logiciel

Il vous sera demandé de saisir les détails d'un compte d'utilisateur Windows qui peut être utilisé pour installer le logiciel de sécurité. Il doit impérativement :

- Posséder les droits d'administrateur local sur les ordinateurs que vous souhaitez protéger.
- Pouvoir se connecter à l'ordinateur sur lequel vous avez installé l'Enterprise Console.
- Avoir une autorisation de lecture de l'emplacement depuis lequel les ordinateurs se mettront à jour. Pour vérifier cet emplacement, dans le volet **Stratégies**, cliquez deux fois sur **Mise à jour**, puis cliquez deux fois sur **Par défaut**.

Remarque : si le volet **Stratégies** (en bas à gauche de la fenêtre) n'apparaît pas, dans le menu **Affichage**, cliquez sur **Ordinateurs d'extrémité**.

Nous vous conseillons d'utiliser un compte qui :

- N'est pas un compte d'administrateur de domaine et qui est configuré pour une délégation limitée.
- Ne dispose pas des droits administratifs ou de tout autre privilège élevé sur les ordinateurs sur les lesquels des gestionnaires de mise à jour supplémentaires de l'Enterprise Console ou des relais de message sont installés.
- Ne dispose pas de droit en écriture ou en modification sur l'emplacement depuis lequel les ordinateurs se mettront à jour.
- Est uniquement utilisé pour assurer la protection des ordinateurs et pas pour effectuer des tâches administratives générales.

- Change de mot de passe régulièrement.

12.3 Préparation de l'installation du logiciel antivirus

Vous pouvez avoir besoin de préparer les ordinateurs avant l'installation du logiciel antivirus. Retrouvez plus de conseils dans le guide de déploiement de Sophos Endpoint (https://docs.sophos.com/esg/enterprise-console/tools/deployment_guide/fr-fr/index.html) à la section sur la préparation des ordinateurs au déploiement.

Nous vous conseillons d'utiliser un pare-feu sur les ordinateurs protégés.

Remarque : une fois que les ordinateurs sont protégés et apparaissent comme étant administrés dans l'Enterprise Console, envisagez de désactiver toutes les exceptions de pare-feu créées spécialement pour autoriser le déploiement sur les ordinateurs.

13 Protection des ordinateurs

13.1 Protection automatique des ordinateurs Windows

Cette section vous décrit comment utiliser l'Enterprise Console pour protéger automatiquement les ordinateurs Windows.

Vous pouvez aussi utiliser vos propres outils ou scripts pour installer la protection sur les ordinateurs Windows. Retrouvez plus de renseignements sur www.sophos.com/fr-fr/support/knowledgebase/114191.aspx.

Remarque : lorsque vous installez Sophos Client Firewall, tous les adaptateurs réseau sont temporairement déconnectés. Ceci conduit à une indisponibilité pouvant aller jusqu'à 20 secondes des connexions réseau et à la déconnexion des applications en réseau comme le bureau à distance Microsoft.

1. Dans l'Enterprise Console, sélectionnez les ordinateurs que vous souhaitez protéger.
2. Procédez de l'une des manières suivantes :
 - Si les ordinateurs ont été placés dans des groupes, cliquez avec le bouton de la souris dessus et sélectionnez **Protéger les ordinateurs**.
 - Si les ordinateurs sont dans le dossier **Non assignés**, faites-les simplement glisser dans les groupes de votre choix.

Un assistant vous guide tout au long de l'installation des logiciels de sécurité Sophos. Acceptez les options par défaut, à l'exception de celles ci-dessous :

- a) Sur la page **Sélection des fonctions**, sélectionnez les fonctionnalités supplémentaires que vous souhaitez installer.
- b) Sur la page **Récapitulatif de la protection**, vous pouvez consulter tous les détails relatifs aux problèmes d'installation. Retrouvez plus d'aide à la section [Résolution des problèmes](#) à la page 40.
- c) Sur la page **Codes d'accès**, saisissez les détails d'un compte qui peut être utilisé pour installer le logiciel sur les ordinateurs.

Les ordinateurs que vous avez sélectionnés sont protégés par le logiciel de sécurité. L'installation s'effectue par étapes. Aussi, l'opération peut prendre un certain temps avant de se terminer sur tous les ordinateurs. Pour terminer l'installation, il se peut que certains ordinateurs doivent être redémarrés.

Une fois l'installation terminée, consultez de nouveau la liste des ordinateurs. Dans la colonne **Sur accès**, le mot **Actif** indique que l'ordinateur effectue un contrôle sur accès de l'ordinateur à la recherche de menaces.

13.1.1 Résolution des problèmes

Lorsque vous essayez de protéger les ordinateurs Windows automatiquement, l'installation du logiciel de sécurité peut échouer pour plusieurs raisons :

- L'installation automatique est impossible sur ce système d'exploitation. Effectuez une installation manuelle. Retrouvez plus de renseignements à la section [Protection manuelle des ordinateurs Windows ou Mac](#) à la page 41. Pour les autres systèmes d'exploitation, reportez-vous aux sections suivantes de ce guide.

- Le système d'exploitation n'a pas pu être déterminé. Vous n'avez peut-être pas saisi votre nom d'utilisateur au format domaine\nomutilisateur lors de la recherche des ordinateurs.
- Les règles de pare-feu bloquent l'accès nécessaire au déploiement du logiciel de sécurité.
- Sur les ordinateurs Windows XP, le Partage de fichiers simple n'a pas été désactivé.
- Sur les ordinateurs Windows Vista, l'Assistant Partage n'a pas été désactivé.
- Vous avez choisi d'installer une fonction qui n'est pas prise en charge sur ce système d'exploitation.

13.2 Protection manuelle des ordinateurs Windows ou Mac

Si vous avez des ordinateurs que vous ne pouvez pas protéger automatiquement, protégez-les en exécutant un programme d'installation depuis un dossier partagé dans lequel le logiciel de sécurité a été téléchargé. Ce dossier est plus connu sous le nom d'emplacement du fichier d'amorce.

Vous devez utiliser un compte administrateur sur les ordinateurs que vous souhaitez protéger.

Pour protéger manuellement les ordinateurs Windows ou Mac :

1. Dans le menu **Affichage** de l'Enterprise Console, cliquez sur **Emplacements des fichiers d'amorce**.

Une liste des emplacements apparaît. Notez l'emplacement de chaque système d'exploitation que vous souhaitez protéger.

2. Sur chaque ordinateur que vous voulez protéger, naviguez vers l'emplacement des fichiers d'amorce et procédez ainsi :
 - Pour les ordinateurs Windows, recherchez `setup.exe` et cliquez deux fois dessus.
 - Pour les Macs, copiez le fichier du programme d'installation `Sophos Installer.app` et le répertoire `Sophos Installer Components` à l'emplacement de votre choix (par exemple, le Bureau) et cliquez deux fois dessus.

Un assistant vous guide tout au long de l'installation. Acceptez les options par défaut, à l'exception de celles ci-dessous :

- Sur les ordinateurs Windows, sur la page **Détails du compte utilisateur**, saisissez les détails du compte que vous avez spécifié pour accéder au gestionnaire de mise à jour. Vous avez effectué cette opération lorsque vous avez installé l'Enterprise Console à la section [Compte Update Manager](#) à la page 11.

Info : si vous n'êtes pas sûr de quel compte il s'agit, utilisez tout compte ayant des droits peu élevés et pouvant accéder à l'emplacement du fichier d'amorce. L'Enterprise Console appliquera ultérieurement une stratégie de mise à jour qui inclut les bonnes informations du compte utilisateur.

13.3 Protection des ordinateurs Linux ou UNIX

Retrouvez plus de renseignements sur la protection des ordinateurs Linux ou UNIX dans le *Guide de démarrage de l'Enterprise Console pour Linux et UNIX*.

14 Vérification du bon fonctionnement de votre réseau

Pour vérifier le bon fonctionnement de votre réseau à partir de l'Enterprise Console:

1. Consultez le tableau de bord de l'Enterprise Console.

S'il n'est pas déjà affiché, dans le menu **Affichage**, cliquez sur **Tableau de bord**.

Le Tableau de bord vous montre combien d'ordinateurs :

- Ont détecté des menaces.
- Ne sont pas à jour.
- Ne sont pas conformes aux stratégies.

15 Protection des ordinateurs autonomes

Certains ordinateurs, par exemple les ordinateurs que le personnel utilise à domicile, ne sont jamais connectés au réseau et ne sont pas faciles d'accès. Pour les protéger, demandez à chaque utilisateur d'installer le logiciel de sécurité Sophos individuellement à l'aide d'un programme d'installation "autonome". Le logiciel sera ensuite maintenu à jour via Internet. Deux méthodes sont possibles :

- L'utilisateur peut télécharger le logiciel sur www.sophos.com/fr-fr/support/downloads/standalone-installers/esc-for-windows-2000-up.aspx. Il installe le logiciel et le configure pour qu'il se mette à jour depuis Sophos.
- Vous pouvez publier de nouveau le logiciel et toutes les mises à jour à venir sur votre propre site Web. L'utilisateur télécharge le logiciel depuis ce site Web, l'installe et le configure pour une mise à jour depuis ce site Web. Retrouvez plus de renseignements sur la manière de publier de nouveau les mises à jour de Sophos sur votre propre site sur www.sophos.com/fr-fr/support/knowledgebase/38238.aspx.

15.1 Envoi d'informations aux utilisateurs d'ordinateurs autonomes

Envoyez à tous les utilisateurs non présents sur votre réseau ce qui suit :

- L'emplacement depuis lequel ils peuvent télécharger le logiciel de sécurité (à moins que vous ne le fournissiez sur un CD-ROM).
- Le *Guide de démarrage autonome* de Sophos Endpoint Security and Control
- Leur nom d'utilisateur et leur mot de passe (pour un téléchargement direct depuis Sophos ou depuis votre propre site Web).

Lors de l'envoi du nom d'utilisateur et du mot de passe :

- Ne les envoyez pas par email sur un ordinateur infecté car ils pourraient être volés.
- Si nécessaire, envoyez-les par fax ou par la poste.

16 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum Sophos Community en anglais sur community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur www.sophos.com/fr-fr/support.aspx.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation.aspx.
- Ouvrez un incident support sur <https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx>.

17 Mentions légales

Copyright © 2009–2017 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos, Sophos Anti-Virus et SafeGuard sont des marques déposées de Sophos Limited, Sophos Group et de Utimaco Safeware AG, partout où ceci est applicable. Tous les autres noms de produits et d'entreprises mentionnés dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by [Douglas C. Schmidt](#) and his [research group](#) at [Washington University](#), [University of California, Irvine](#), and [Vanderbilt University](#), Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let [us](#) know so we can promote your project in the [DOC software success stories](#).

The [ACE](#), [TAO](#), [CIAO](#), [DAnCE](#), and [CoSMIC](#) web sites are maintained by the [DOC Group](#) at the [Institute for Software Integrated Systems \(ISIS\)](#) and the [Center for Distributed Object Computing](#) of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use,

correction, modification, or enhancement. A [number of companies](#) around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let [me](#) know.

[Douglas C. Schmidt](#)

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at <http://www.apache.org/licenses/LICENSE-2.0>

Boost Software License

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source

code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.fr or via the web at <https://www.sophos.com/fr-fr/support/contact-support.aspx>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Microsoft Public License (MS-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

A copy of the MS-PL terms can be found at <https://opensource.org/licenses/MS-PL>.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2016 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.

The use and distribution terms for this software are covered by the Common Public License. Source code for this component is available here: <https://sourceforge.net/projects/wtl/files/>

zlib data compression library

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu