ESET Remote Administrator

Console d'administration à distance

Manuel d'installation
& Guide Utilisateur

ESET Remote Administrator

Remote Administrator a été développé par ESET, spol. s.r.o. Pour plus d'informations, visitez www.eset.com ou le site de votre distributeur local.

ESET NOD32 France

Tél. : 01 55 89 08 85

http://www.eset-nod32.fr

Support Technique

Tél. : 0826 02 02 82 (0.15 € TTC/min)

par e-mail support@eset-nod32.fr

Version 110208

Sommaire

Table des matières

1.Introduction

ESET Remote Administrator (version 2.0.33) est une application qui vous permet de gérer les produits d'ESET dans un environnement réseau. ESET Remote Administrator (ERA) est une solution autorisant l'administration des produits d'ESET - y compris les stations de travail et les serveurs – à partir d'un emplacement central. Grâce au système de gestion de tâches prédéfinies d'ESET Remote Administrator, vous pouvez répondre rapidement à tout nouveau problème de menaces, et – bien sûr – installer les solutions d'ESET sur les ordinateurs distants.
ESET Remote Administrator ne fournit aucune forme de protection directe contre les codes malveillants, tels que virus et vers. ERA est relié à la présence d'une solution ESET sur les stations de travail et serveurs, comme ESET NOD32 Antivirus pour Windows, ou ESET Smart Security.

Pour effectuer un déploiement complet des solutions de sécurité d'ESET, les étapes suivantes doivent être suivies :

- Installation du Serveur ERA (ERAS),
- Installation de la Console ERA (ERAC),
- Installation du serveur Miroir,
- Installation des ordinateurs clients (ESET NOD32 Antivirus, ESET Smart Security, ESET Server Edition, etc...).

NOTE: Certaines parties de ce document utiliseront des variables système, faisant référence à un emplacement exact de dossiers et de fichiers : %ProgramFiles% = généralement C:\Program Files %ALLUSERSPROFILE% = généralement C:\Documents and Settings\All Users

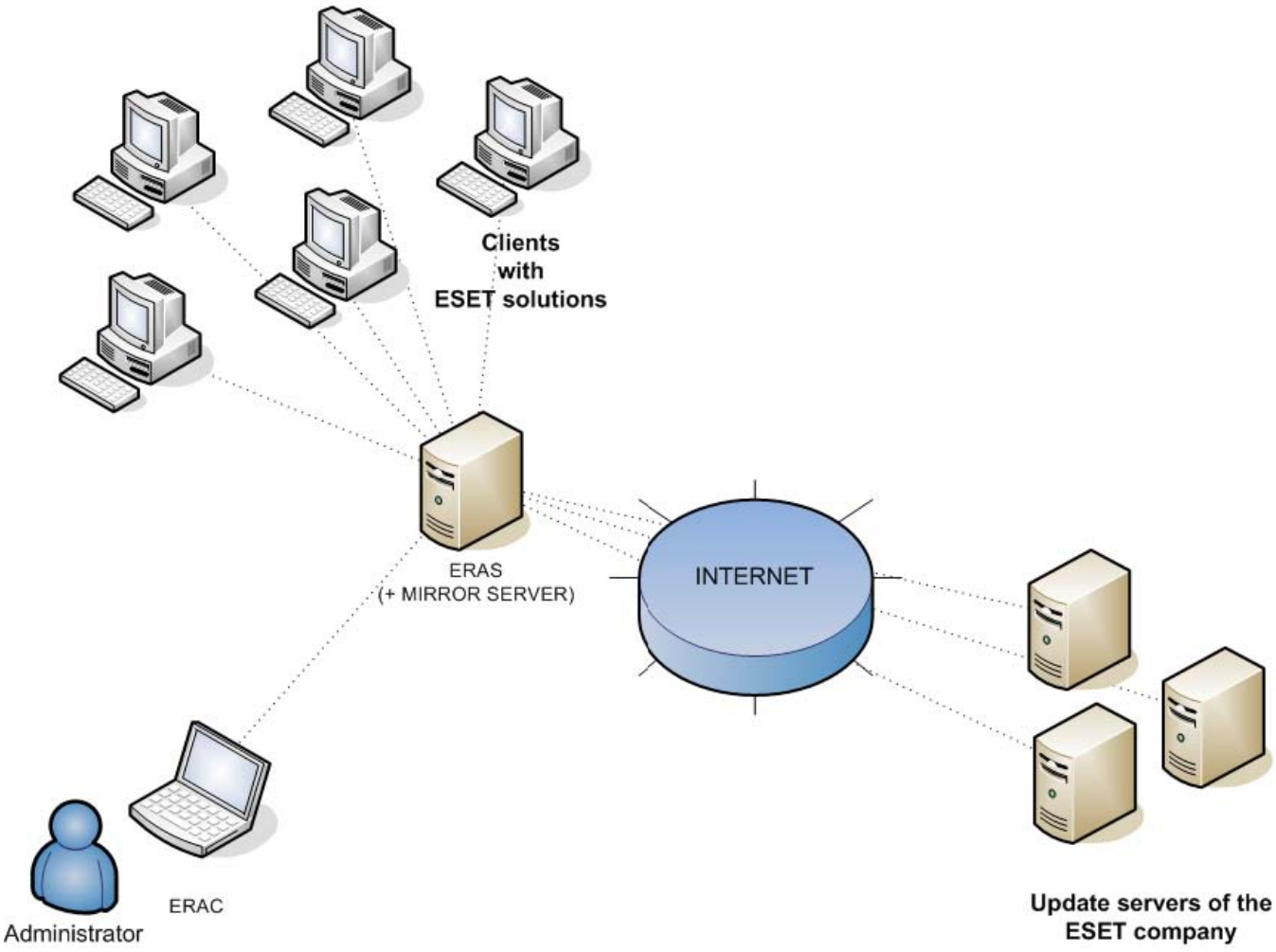


Figure 1
Modèle simplifié de déploiement : ESET pour les clients Windows, ESET Remote Administrator. Le Serveur ERA (ERAS) et le Serveur Miroir peuvent - mais n'ont pas à - être installés sur le même système.

2. ERA – architecture client/serveur

Techniquement, ESET Remote Administrator est constitué de 2 composants séparés: le Serveur ERA (ERAS) et la Console ERA (ERAC). Vous pouvez utiliser un nombre illimité de Serveurs ERA et de clients sur votre réseau, puisqu'il n'existe pas de limitations dans le Contrat de licence pour leurs utilisations. La seule limitation est liée au nombre total de clients que votre installation d'ERA peut administrer (voir section 2.1.6, “Clés de licence”).

2.1 Serveur ERA (ERAS)

Le composant serveur d'ESET Remote Administrator s'exécute comme un service sous les systèmes d'exploitation suivants, basés sur Microsoft Windows© NT : NT4, 2000, XP, et 2003. La principale tâche de ce service est de collecter les informations des clients et de leur envoyer diverses requêtes. Les requêtes, y compris les tâches de configuration, les requêtes d'installation à distance, etc., sont créées via la Console ERA (ERAC).

Le Serveur ERA est un point de rencontre entre la Console ERA et les ordinateurs clients – un endroit où toutes les informations sont traitées, maintenues ou modifiées avant d'être transférées aux clients ou à la Console ERA.

2.1.1 Configuration requise

Le Serveur ERA fonctionne comme un service, et requiert donc un système d'exploitation basé sur Microsoft Windows NT (NT4, 2000, XP, 2003). Microsoft Windows Server Edition n'est pas nécessaire pour faire fonctionner le Serveur ERA. Un ordinateur ERAS doit être en ligne 24h/24 - 7j/7 et accessible via le réseau informatique par :

- Les autres instances du Serveur ERAS (si répliqué)
- Le PC avec la Console ERA
- Les clients (généralement les stations de travail)

Le tableau ci-dessous illustre une liste de communications réseau possibles qui prennent place lorsque le Serveur ERA est installé. Le processus era.exe écoute sur les ports TCP : 2222, 2223, 2224 et 2846. Les autres instances de communication sont également liées aux processus natifs du système d'exploitation (par ex : “NetBIOS sur TCP/IP”).

Protocole	Port	Description
TCP	2222 (ERAS écoute)	Communication entre les clients et ERAS
TCP	2223 (ERAS écoute)	Communication entre ERAC et ERAS
TCP	2221 (ERAS écoute)	Par défaut, ce port propose des "packages" de mises à jour utilisant la fonction Miroir intégrée dans ERAS (communication HTTP)

Si vous utilisez toutes les fonctionnalités du programme, les ports de communication réseau suivant doivent également être ouverts :

Protocole	Port	Description
TCP	2224 (ERAS écoute)	Communication entre l’agent einstaller.exe et ERAS lors de l’installation à distance
TCP	2846 (ERAS écoute)	Réplication ERAS
TCP	139 (Port cible du point de vue de ERAS)	Copie de l’agent einstaller.exe depuis ERAS vers un client en utilisant le partage admin$ lors de l’installation par la méthode "push"
UDP	137 (Port cible du point de vue de ERAS)	“Résolution du nom” lors de l’installation à distance
UDP	138 (Port cible du point de vue de ERAS)	“Navigation réseau“ lors de l’installation à distance
TCP	445 (Port cible du point de vue de ERAS	Accès direct aux ressources partagées en utilisant TCP/IP lors de l’installation (une alternative à TCP 139)

La configuration matérielle minimum pour le déploiement de ERAS est la même que celle recommandée pour le système d’exploitation Windows utilisé sur la machine.

2.1.2 Réplication de serveurs ESET dans un réseau multi sites.

Dans des réseaux importants, il est possible d'installer des Serveurs ERA additionnels et ainsi de réaliser de futures installations sur des ordinateurs clients depuis des serveurs qui sont plus facilement accessibles. Pour cela, le Serveur ERA dispose de la "réplication", qui permet aux informations d'être transmises à un Serveur ERA supérieur ("upper server"). La réplication est configurée en utilisant ERAC.

La fonctionnalité de réplication est très utile pour les entreprises possédant de multiples branches ou bureaux distants. Le scénario de déploiement typique pourrait être le suivant : installation de ERAS dans chaque branche, et réplication de ceux-ci vers un Serveur ERA central situé au siège de l'entreprise. L'avantage de cette configuration est particulièrement visible avec des réseaux privés connectés entre eux par VPN, qui sont généralement plus lent – l'administrateur n'aura besoin de se connecter qu'à un ERAS central (la communication indiquée par la lettre A dans le schéma ci-dessus). Il n'aura pas à utiliser de tunnel VPN pour accéder à chaque branche (les communications B, C, D et E), lui permettant ainsi de contourner une voie de communication plus lente par l'utilisation de la réplication des Serveurs ERA.

La configuration de la réplication permet à l'administrateur de définir quelles informations seront automatiquement et régulièrement transmises aux serveurs supérieurs, et quelles seront celles envoyées sur demande de l'administrateur. La réplication permet une utilisation plus souple de ERA et allège également le trafic réseau.

Un autre avantage de la réplication est que de multiples utilisateurs disposant de niveaux d'accès différents peuvent se connecter. L'administrateur ayant accès à ERAS london1.company.com avec la console (communication E) sera capable d'administrer uniquement les clients connectés à london1.company.com, london.company.com, paris.company.com. Si vous êtes connecté au point central company.com (A), vous serez capable de contrôler tous les clients situés au siège et dans les différents départements / branches de l'entreprise.

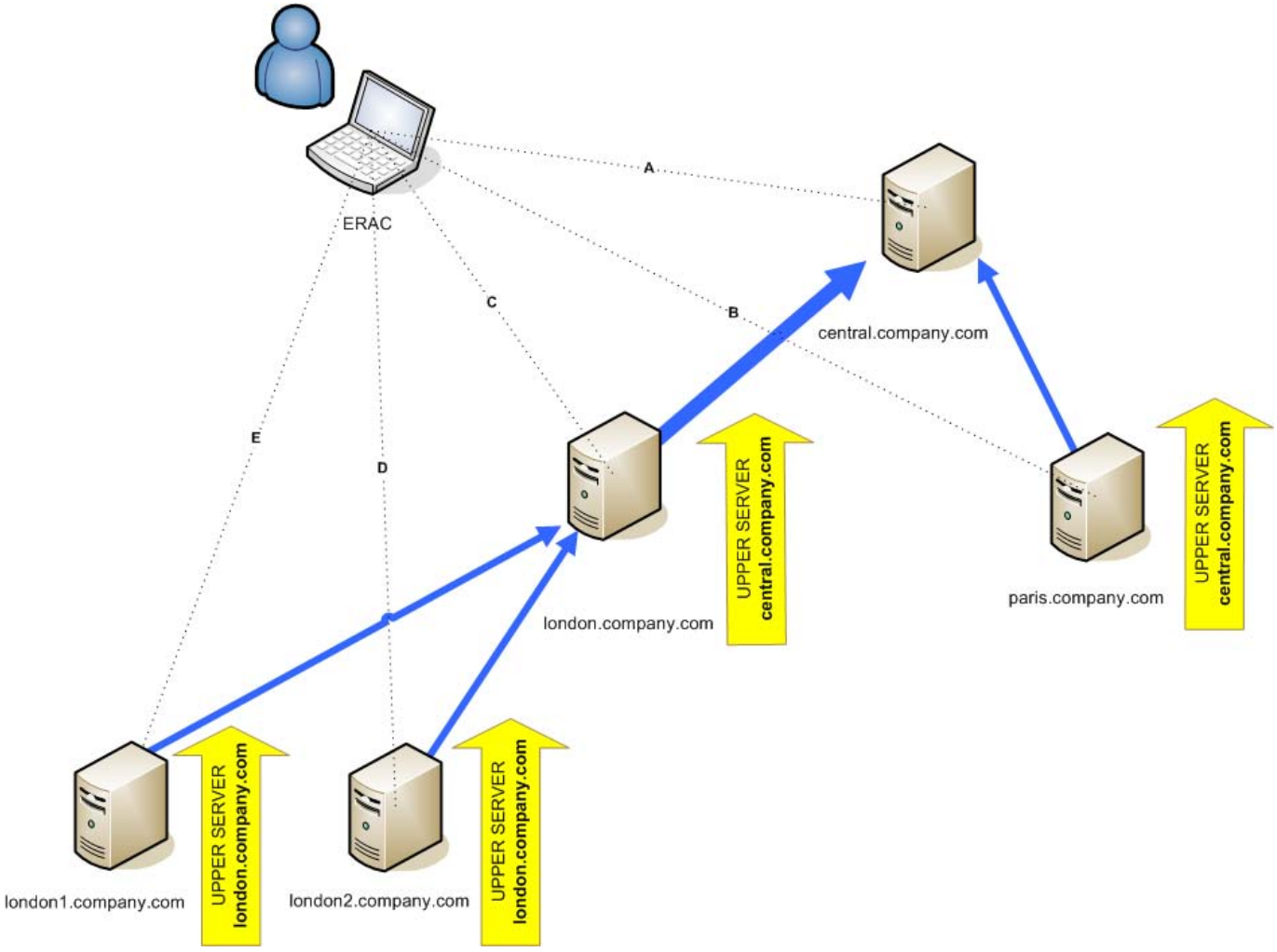


Figure 2
Réplication dans un réseau constitué d'un siège et de départements/filiales.

2.1.3 Installation

Le processus d'installation est initié par l'exécution du package d'installation. Lors de cette phase, le fichier de licence, qui est un fichier avec l'extension .lic, vous sera demandé. Si le mode d'installation Expert est sélectionné, plusieurs autres paramètres peuvent être définis. Ils pourront être modifiés ultérieurement dans ERAC, mais dans la plupart du temps, ceci n'est pas nécessaire. La seule exception est le nom du serveur. Ce nom doit être le même que dans le DNS, ou le nom de l'ordinateur dans votre système d'exploitation (Mon ordinateur > Propriétés > onglet Nom de l'ordinateur). L'adresse IP de l'ordinateur peut également être utilisée. Ceci est l'information la plus importante pour pouvoir faire une installation a distance. Si le nom n'est pas spécifié lors de l'installation, le programme affectera automatiquement la valeur %COMPUTERNAME%, ce qui est suffisant dans la plupart des cas.

Par défaut, les composants du programme ERAS sont installés dans le répertoire suivant :
%ProgramFiles%\Eset\Eset Remote Administrator\Server

Et les données (logs, packages d'installation, configurations, etc.) sont situés dans le répertoire :
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server

NOTE: Sur les serveurs avec ERAS, la partie cliente devrait également être installée. ERAS adopte le numéro de version de base de virus actuelle et l'utilise comme valeur de référence. L'installation d'une solution avec le miroir de mise à jour local (LAN Update Server) est recommandée.

2.1.4 Rapports (journaux)

ERAS génère un fichier journal (log) au format texte. Ce fichier est situé dans le répertoire :
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\logs

Le fichier le log, nommé "era.log" enregistre tous les évènements survenant lors du fonctionnement de ERAS, y compris les messages d'erreur relatifs au démarrage du service de ERAS tels qu'une erreur de corruption de la base de données ou une erreur de clé de licence. Le fichier de log vous permet de déterminer rapidement la cause d'un problème de démarrage de ERAS.

NOTE: Dans les paramètres de ERAS (accessibles avec ERAC) vous pouvez définir plusieurs niveaux de journalisation, incluant la rotation du log – permettant de réduire significativement la taille de celui-ci. L'enregistrement dans le système de log du système d'exploitation peut également être configuré.

2.1.5 Configuration

Dans une certaine mesure, ERAS peut être configuré lors de l'installation (surtout avec le mode expert) ou ultérieurement en utilisant la Console ERA connectée au Serveur ERA. Si besoins est, les fichiers de configuration .xml sur le serveur peuvent être modifiés. Ces fichiers sont situés dans le répertoire suivant :
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\configuration

NOTE: Pour des raisons de sécurité, le paramètre définissant le mot de passe est séparé (dans un fichier xml individuel) des autres options de configuration. La perte du mot de passe (pour accéder au serveur ERA) peut être résolue en supprimant le fichier era_private.xml situé dans le répertoire de configuration.

2.1.6 Clés de licence

La clé de licence est un fichier avec l'extension .lic, ayant une structure similaire au format xml, mais protégé par une signature électronique. Ce fichier est nécessaire pour une installation complète de ERAS. Il contient les informations suivantes :

- Propriétaire de la licence
- Nombre de machines clientes (nombre de licences)
- Date d'expiration de la licence

Ci-dessous quatre scenarii communs relatifs aux fichiers de licence :

- Le fichier .lic n'est pas présent
  ERAS se lancera en mode d'évaluation – il sera possible d'administrer uniquement 2 clients, sans limitation dans le temps.

- Le fichier .lic file est corrompu
  Le service ERA Server ne démarrera pas du tout. L'évènement sera inscrit dans le fichier era.log.

- Le fichier .lic a expiré
  Si la date d'expiration définie dans le fichier .lic est plus ancienne que la date actuelle, il ne sera pas possible d'établir la connexion entre ERAC et ERAS. ERAS continuera à accepter les informations des clients, mais il ne sera pas possible de les administrer.

- Le nombre de clients définis dans le fichier .lic est dépassé
  Ceci sera annoncé par un message d'erreur affiché par ERAC. Il ne sera pas possible d'administrer les clients supplémentaires communiquant avec le serveur ERA.

Les clés de licence doivent être placées dans le répertoire :

%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\license
Durant l'installation de ERAS, la clé de licence est automatiquement copiée dans le répertoire mentionné ci-dessus. Si la licence est mise à jour, la clé de licence doit être mise à jour manuellement. Le répertoire peut contenir plusieurs fichiers de licence, mais ERAS choisira toujours le fichier avec l'extension .lic le plus approprié. A chaque fois qu'une nouvelle licence est installée, le service ERAS doit être redémarré.

Il y a plusieurs possibilités pour envoyer le fichier de licence vers ERAS :

- Copier le fichier dans le répertoire indiqué précédemment, puis redémarrer le service ERAS.
- Utiliser l'éditeur de configuration de ERAC et importer le fichier de licence.
- Utiliser la gestion de licence dans ESET Smart Security/ESET NOD32 Antivirus pour importer le fichier de licence.

2.1.7 Base de données & stockage des informations

ERAS utilise le composant de base de données MDAC (Microsoft Data Access Components), tandis que les données plus volumineuses sont sauvegardées dans des fichiers individuels (dans le répertoire de stockage).
Les outils de ERAS permettent aux administrateurs de réaliser une maintenance automatique de la base de données et des informations stockées. Ceci peut être configuré lors de l'installation (niveau expert) ou alors ultérieurement avec ERAC. La maintenance de la base de données permet des réponses plus rapides aux requêtes et permettent également de minimiser l'espace disque utilisé.

Nous recommandons d'utiliser les paramètres par défaut, qui suppriment automatiquement toute entrée de plus de 6 mois. Diminuez cette valeur uniquement si le système est surchargé par des évènements en provenance de très nombreux clients.

La base de données est située dans le répertoire suivant :
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\database

Les fichiers relatifs aux enregistrements de la base de données sont situé dans:
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\storage

Les informations relatives aux communications des clients avec ERAS sont enregistrées dans des fichiers individuels. Ces fichiers se situent dans le répertoire de stockage et contiennent les informations suivantes :

- Détails du client (configuration .xml, Statut de la Protection, Eléments de Protection, Informations Système),
- Détails des journaux (journaux des menaces et d'analyses),
- Détails des tâches,
- Détails des rapports planifiée (ceci n'est pas directement en rapport avec les communications client / ERAS).

NOTE: Si le répertoire de stockage se trouve sur un ordinateur avec le système de fichier NTFS, vous pouvez utiliser la fonctionnalité de compression NTFS afin de réduire significativement l'espace disque utilisé tout en conservant un grand nombre d'informations.

2.2 Console ERA (ERAC)

ERAC est la partie cliente de ERA et est généralement installée sur une station de travail. Cette station de travail est utilisée par l'administrateur afin de contrôler à distance les produits ESET sur chacun des différents clients. En utilisant ERAC, l'administrateur peut se connecter au composant serveur de ERA – sur le port TCP 2223. La communication est contrôlée par le programme console.exe, qui se situe généralement dans le répertoire :
%ProgramFiles%\Eset\Eset Remote Administrator\Console

Vous pouvez également démarrer ERA Console en cliquant sur Démarrer > Tous les Programmes > ESET > ESET Remote Administrator Console

Lors de l'installation de ERAC, vous pouvez être amené à saisir le nom d'un Serveur ERA. Lors du démarrage, la console va alors automatiquement se connecter à ce serveur. La Console ERA peut également être configurée après l'installation.

ERAC génère des rapports graphiques au format HTML, qui sont sauvegardés localement. Toutes les autres informations sont envoyées à ERAS par le port TCP 2223.

3. Autres composants ESET dans un environnement réseau

3.1 Solutions client ESET

Les solutions clientes sont les produits de sécurité permettant de détecter et bloquer les codes malicieux sur les stations de travail et les serveurs. Les solutions clientes principales sont ESET NOD32 Antivirus 3.0 et ESET Smart Security.
Les clients communiquent par deux canaux principaux:

- Serveur ERA sur le port TCP 2222 pour soumettre les informations telles que les logs, configuration actuelle, alertes de menaces, etc., et pour exécuter toutes les tâches et requêtes en provenance de ERAS et qui sont en attente pour le client (modification de configuration, exécution d'une analyse, etc.).

- Le serveur de mise à jour sur un port prédéfini (en utilisant les protocoles HTTP ou SMB). Nous aborderons plus loin dans ce manuel les méthodes permettant de créer un serveur local de mise à jour (ou "miroir") des serveurs ESET de mise à jour.

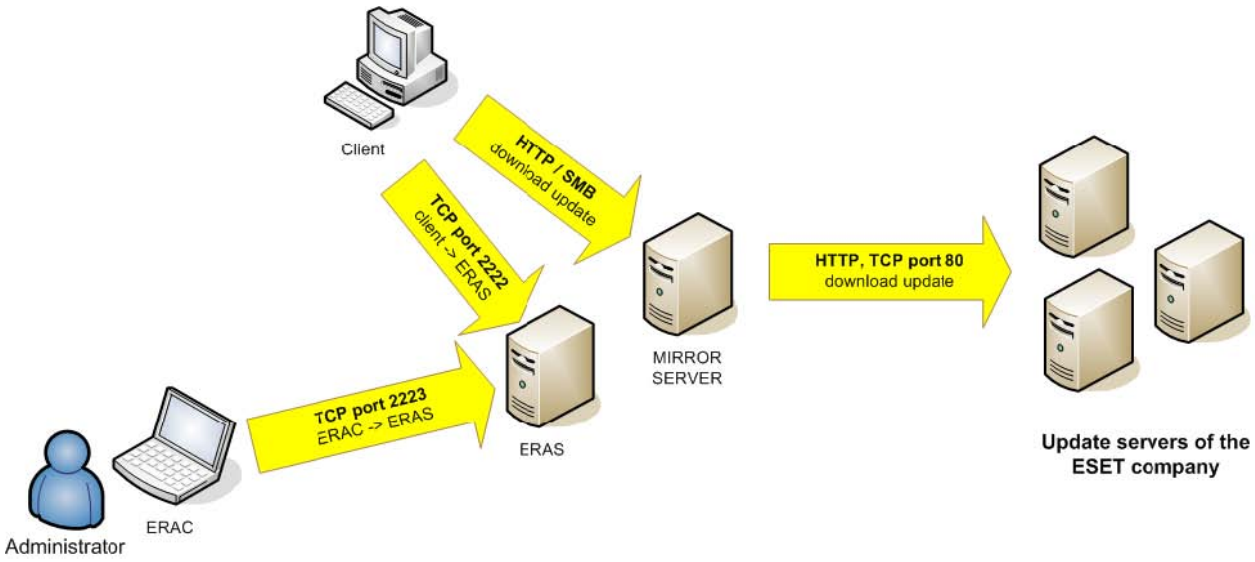


Figure 3
Les principaux canaux de communication entre ERAS, ERAC et serveurs de mise à jour.
ERAS et le serveur miroir peuvent fonctionner sur la même machine

3.2 Editeur de configuration ESET

L'éditeur de configuration ESET est un composant important de ERAC et est utilise dans de multiples buts. Les plus importants sont la création des éléments suivants :

- Configurations prédéfinies pour les packages d'installation
- Configurations envoyées comme tâche aux clients
- Un fichier (.xml) de configuration générale

L'éditeur de configuration permet à un administrateur de configurer à distance la plupart des paramètres disponibles dans les solutions de sécurité ESET. Il permet également d'exporter les configurations vers des fichiers .xml, pouvant être utilisés ultérieurement pour dans de nombreux buts (ex : création de tâches dans ERAC, importation de la configuration localement dans ESET Smart Security, etc.).
La structure de l'éditeur de configuration est essentiellement un formulaire contenant les informations dans une structure arborescente. Le modèle est situé dans le fichier cfgedit.exe.

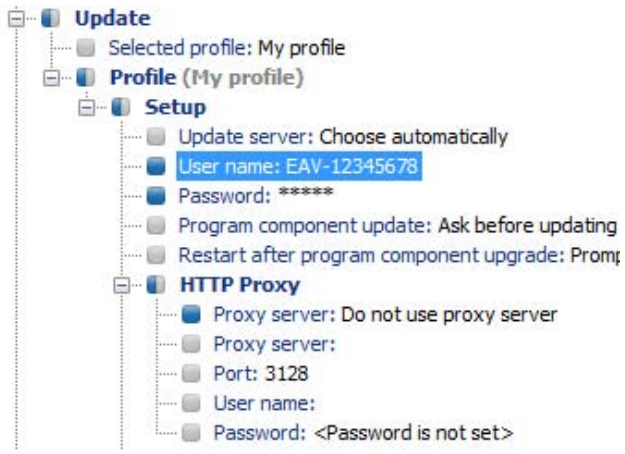
L'éditeur de configuration vous permet de modifier n'importe quel fichier .xml. Evitez cependant de modifier le fichier source cfgedit.xml ! Pour que l'éditeur de configuration fonctionne, il faut également que les fichiers suivants soient présents : eguiEpfw.dll, cfgeditLang.dll et eguiEpfwLang.dll.

Pour accéder à l'éditeur de configuration, démarrez la Console ERA et cliquez sur Tools > ESET Configuration Editor.

3.2.1 Configuration layering

Si une valeur est modifiée dans l'éditeur de configuration, alors ce changement est indiqué par un symbole bleu.

Toutes les lignes avec le symbole gris n'ont pas été modifiées et ne seront pas inscrites dans le fichier de configuration .xml généré. Lorsque l'on applique une configuration aux clients, seules les modifications enregistrées dans le fichier .xml seront appliquées. Dans l'exemple ci-dessous, le nom d'utilisateur et le mot de passe sont inscrits, et l'utilisation d'un serveur proxy est empêchée.



La seconde configuration (ci-dessous) permet de s'assurer que les modifications précédents seront préservées (y compris le nom d'utilisateur AV-12345678 et le mot de passe), mais permet également l'utilisation d'un serveur proxy et définit son adresse ainsi son port.

3.2.2 Principaux éléments de configuration

Dans cette section nous allons expliquer certaines clés de configuration pour ESET Smart Security, disponibles dans l'éditeur de configuration ESET (Tools > ESET Configuration Editor) Pour changer un paramètre spécifique, sélectionnez l'option à gauche dans l'arborescence et changez la valeur correspondante dans la partie de droite.

- **Kernel > Setup > Remote administrator**
  Vous pouvez ici activer la communication entre l'ordinateur client et le Serveur ERA (Connect to Remote Administrator server). Saisissez le nom ou l'adresse IP du Serveur ERA (Server address). L'intervalle de temps entre les connexions devrait être laissé à la valeur par défaut qui est de 5 minutes. Pour des raisons de test, cette valeur peut être réduite à 0 (ce qui établira une connexion toutes les 10 secondes). Si un mot de passe a été paramétré (password), alors saisissez celui spécifié dans le Serveur ERA (voir le chapitre à propos de la configuration de ERAS – Option pour le mot de passe pour les clients). Si un mot de passe est utilisé, alors la communication entre les clients et ERAS sera encryptée.

- **Kernel > Setup > License keys**
  Les ordinateurs clients ne nécessitent pas de clé de licence pour pouvoir être ajoutés ou gérés. Les clés de licence sont utilisées uniquement pour certaines solutions serveur.

- **Kernel > Setup > ThreatSense.Net**
  Cette branche définit le comportement de ThreatSense.Net Early Warning System, qui permet la soumission de fichiers suspects aux laboratoires d'ESET pour analyse. Lorsque vous déployez les solutions ESET dans un grand réseau, les options "Submit suspicious files" et "Enable submission of anonymous statistical information" sont particulièrement importantes.

  Si celles-ci sont paramétrées respectivement à "Do not submit" et "No", le système ThreatSense.Net sera complètement désactivé. Pour soumettre automatiquement les fichiers sans que l'utilisateur n'ait à intervenir, sélectionnez respectivement "select Submit without asking" et "Yes". Si un serveur proxy est nécessaire pour pouvoir effectuer une connexion Internet, spécifiez ses paramètres dans la partie Kernel > Setup > Proxy server.

- **Kernel > Setup > Protect setup parameters**
  Permet de protéger par mot de passé l'accès aux paramètres de configuration. Si un mot de passe est spécifié, il sera demandé afin d'accéder aux paramètres sur les ordinateurs clients. Cependant, ce mot de passe n'affecte pas les changements faits depuis ERAC.

- **Kernel > Setup > Scheduler/Planner**
  Cette clé contient les options de planification qui permettent par exemple de réaliser des analyses régulières, les mises à jour, etc.

  NOTE : Par défaut, toutes les solutions de sécurité de ESET comportent plusieurs tâches planifiées prédéfinies, et il ne devrait pas être nécessaire de les modifier ou d'en ajouter de nouvelles.

- **Update**
  Cette branche de l'éditeur de configuration vous permet de définir la façon dont les mises à jour des bases virales et des programmes sont gérées sur les ordinateurs clients. Dans la plupart des cas il est nécessaire que de modifier le profile My profile et de bien vérifier les paramètres pour les serveurs de mise à jour, le nom d'utilisateur et le mot de passe. Si le serveur de mise à jour est paramétré à "Choose Automatically", toutes les mises à jour seront téléchargées depuis les serveurs ESET. Dans ce cas, il faut alors spécifier les paramètres pour le nom d'utilisateur et le mot de passe, qui vous ont été donnés lors de l'achat de votre licence. Pour plus d'information sur la configuration des clients pour recevoir les mises à jour par l'intermédiaire d'un serveur local (miroir), référez-vous à la partie 3.3, "Serveur de mise à jour LAN - Miroir".

  NOTE : Sur les ordinateurs itinérants, 2 profiles peuvent être configurés – un pour effectuer les mises à jour à partir d'un miroir local, et l'autre pour télécharger celle-ci directement depuis les serveurs ESET. Pour plus d'informations, voir la section 8.2 "Mise à jour combinée pour les ordinateurs portables ".

3.3 Serveur de mise à jour LAN -Miroir

La fonctionnalité de miroir permet de créer un serveur local de mises à jour. Les ordinateurs clients ne vont pas télécharger les mises à jour des bases virales sur Internet depuis les serveurs ESET, mais vont se connecter sur un serveur miroir dans votre réseau. Les principaux avantages de cette solution sont de ne pas encombrer le trafic réseau et de ne pas utiliser inutilement la liaison internet. Seul le serveur miroir va se connecter sur Internet pour les mises à jour, au lieu de centaines de machines. Le seul inconvénient est une défaillance potentielle du serveur miroir, ce qui empêcherait la mise à jour des stations clientes (au cas où il est le seul serveur à fournir les mises à jour).

Attention! Un serveur miroir qui a effectué une mise à jour de composants et qui n'a pas redémarré pourrait poser un problème. Dans ce scénario, le serveur ne pourrait télécharger AUCUNE mise à jour, ou ne pourrait pas les mettre à disposition pour les stations clientes. IL NE FAUT PAS PARAMETRER LA MISE À JOUR DES COMPOSANTS 'AUTOMATQUE' SUR LES SERVEURS! (Voir la section 3.3.1 pour de plus amples informations concernant la mise à jour des composants)

La fonctionnalité de miroir est disponible en deux endroits :

- ESET Remote Administrator (miroir fonctionnant physiquement dans ERAS, et administrable par ERAC)
- ESET Smart Security Business Edition ou ESET NOD32 Antivirus Business Edition (sous réserve que la Business Edition ait été activée par une clé de licence)

Le choix est laissé à l'administrateur quant à la méthode utilisée pour le miroir (Attention cependant car si les 2 méthodes sont utilisées simultanément, ceci pourrait engendrer un conflit sur le port TCP 2221).

Dans des réseaux importants, il est possible de créer plusieurs serveurs miroirs (ex : pour chaque branche de l'entreprise), et de définir l'un d'entre eux comme miroir central (au siège le l'entreprise) dans un mode cascadé – similaire à une configuration de ERAS avec des clients multiples.

3.3.1 Opérations du serveur miroir

L'ordinateur hébergeant le miroir doit être opérationnel 24/7, et doit également être connecté à Internet ou à un autre serveur miroir (réplication). Les éléments de mise à jour peuvent être téléchargés du miroir de deux façons :

1. En utilisant le protocole HTTP (recommandé)
2. En utilisant un partage de répertoire sur le réseau (SMB)

Les serveurs de mise à jour ESET utilisent le protocole HTTP avec authentification. Un miroir central doit accéder à ces serveurs avec un nom d'utilisateur (généralement de la forme EAV-XXXXXXX) et un mot de passe.
Le serveur miroir faisant partie de ESET Smart Security/ESET NOD32 Antivirus possède un serveur web HTTP intégré ne requérant aucune authentification. Ceci signifie qu'un client se connectant sur ce serveur HTTP n'a pas besoin de s'authentifier avec un nom d'utilisateur et un mot de passe.

NOTE : Si vous décidez d'utiliser ce serveur web HTTP, soyez certain qu'il ne sera pas accessible depuis l'extérieur de votre réseau (c'est à dire depuis des clients non inclus dans votre licence). Le serveur ne doit pas être accessible depuis internet. Par défaut, le serveur web HTTP écoute sur le port TCP 2221. Soyez certain que ce port n'est pas utilisé par une autre application !

Tout autre type de serveur HTTP peut également être utilisé. ESET supporte également des méthodes additionnelles d'authentification (accès par nom d'utilisateur/mot de passe – sur les serveurs web Apache la méthode .htaccess est utilisée).

La seconde méthode (partage de répertoire) nécessite un droit d'accès en lecture sur répertoire contenant les mises à jour. Dans ce scénario, le nom d'utilisateur et le mot de passe d'un utilisateur ayant un droit d'accès en écriture à ce répertoire doivent être saisis sur la station cliente.

NOTE: Les solutions ESET utilisent le compte SYSTEM et donc ont des droits d'accès sur le réseau différents que ceux de l'utilisateur actuellement connecté sur l'ordinateur. L'authentification est requise même si le partage réseau est accessible pour 'tout le monde' et que l'utilisateur courant peut y accéder. Par ailleurs, utilisez le nom UNC pour le répertoire réseau sur le serveur local. Nous recommandons de ne pas utiliser le format DISK:\

Si vous décidez d'utiliser la méthode de partage de répertoire, nous vous recommandons de créer un compte utilisateur spécifique (ex : NODUSER). Ce compte sera utilisé sur tous les clients dans le seul but de télécharger les mises à jour. Le compte NODUSER devra avoir les droits d'accès en lecture sur le répertoire partagé qui contient les mises à jour.

NOTE: Pour l'authentification sur le répertoire partagé, veuillez saisir les informations de façon complète : *WORKGROUP\User, ou DOMAIN\User.*

En plus de l'authentification, vous devez également définir la source des mises à jour pour les solutions de sécurité ESET. La source est doit une adresse URL vers un serveur local :

http://Mirror_server_name:port
Où alors un chemin UNC vers un partage réseau :
\\Mirror_server_name\share_name

3.3.2 Types de mises à jour

En plus des mises à jour des bases de signatures virales, qui incluent également les mises à jour du noyau des programmes ESET, des mises à jour de composants du programme peuvent également être régulièrement téléchargées. Les mises à jour du programme ajoutent généralement de nouvelles fonctionnalités aux solutions de sécurité ESET et nécessitent un redémarrage de la machine. Si il y un serveur miroir installé dans le réseau, les mises à jour du programme sont également téléchargées depuis celui-ci.

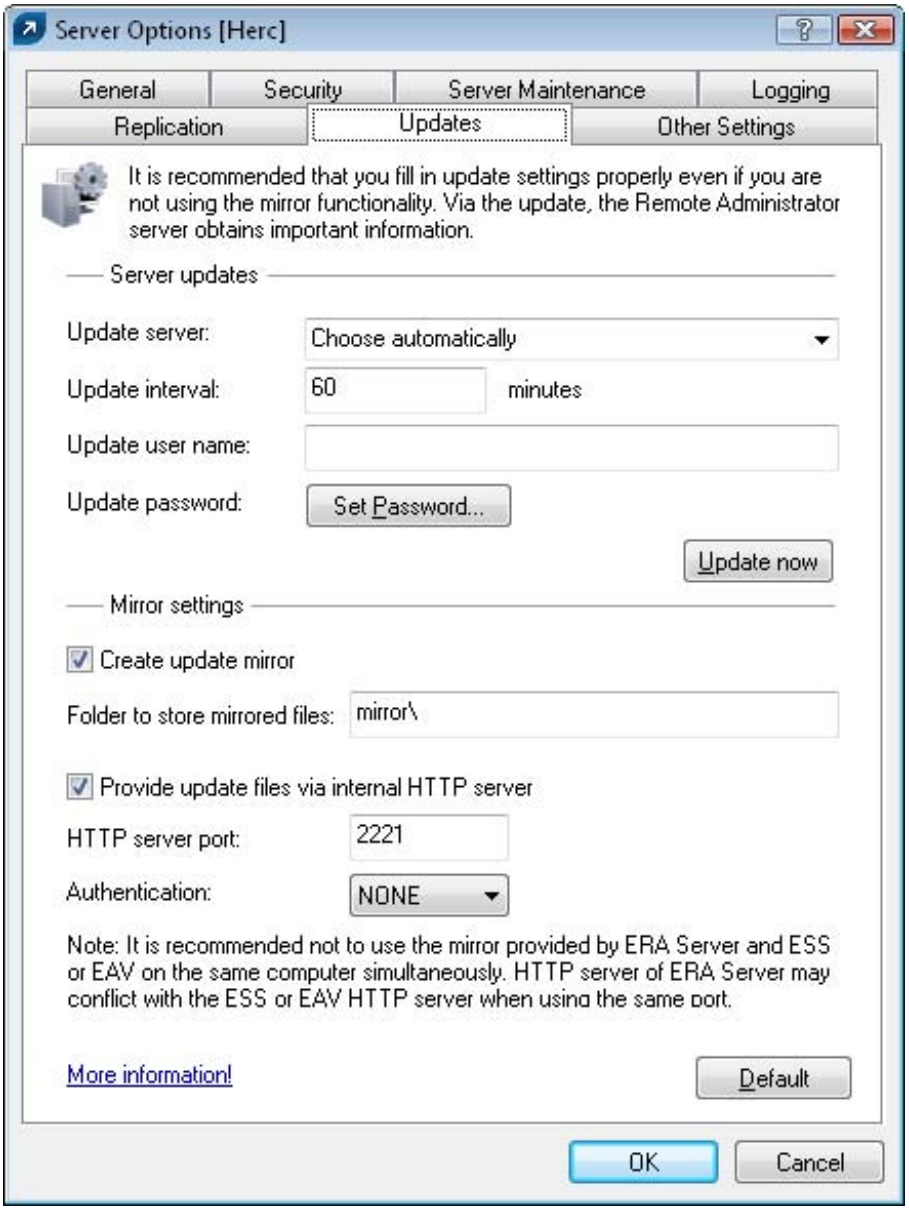
Le serveur miroir permet également de désactiver le téléchargement automatique des mises à jour de composants de programme depuis les serveurs ESET (ou d'un serveur miroir supérieur), désactivant ainsi sa distribution vers les clients. La distribution peut être déclenchée manuellement ultérieurement (ex : quand il est certain qu'il n'y aura pas de conflit entre la nouvelle version et d'autres applications).

Cette fonctionnalité est particulièrement intéressante si l'administrateur souhaite télécharger et utiliser les nouvelles bases virales bien qu'il y ait également une nouvelle version du programme disponible en téléchargement. Dans ce cas, la nouvelle version du programme peut être testée dans un environnement hors production avant son déploiement. Si une ancienne version du programme est utilisée avec la dernière version des bases virales, le programme continuera à fournir la meilleure protection possible. Nous recommandons cependant de télécharger et installer la nouvelle version sans trop de délai.

3.3.3 Comment activer et configurer le Miroir

Si le serveur miroir intégré dans ERAS est utilisé, connectez-vous sur la Console ERA et procédez comme suit :

- Dans la Console ERA, cliquez sur Tools > Server Options... et cliquez sur l'onglet Updates.
- Dans la liste déroulante des serveurs, sélectionnez Choose Automatically (Les mises à jour seront téléchargées depuis les serveurs de ESET), ou sélectionnez le chemin vers un serveur miroir (URL/UNC).
- Sélectionnez l'intervalle (Update interval) entre deux mises à jour (nous recommandons 60 minutes).
- Si vous avez sélectionné 'Choose Automatically' dans l'étape précédente, inscrivez le nom d'utilisateur et le mot de passe pour pouvoir faire les mises à jour (ils vous ont été envoyée lors de l'achat de votre licence).
- Sélectionnez l'option de création de miroir (Create update mirror) et saisissez le répertoire dans lequel seront placées les fichiers de mise à jour. Par défaut, celui-ci est un chemin relatif ver le répertoire miroir, si l'option 'Provide update files via internal HTTP server' est sélectionnée (et disponible sur le port HTTP défini dans le serveur HTTP – par défaut 2221).
- Mettez l'authentification à 'NONE'.
- Dans la partie 'Advanced Setup', sélectionnez les composants qui seront téléchargés (les composants pour toutes les versions et langues utilisées dans le réseau devraient être sélectionnées).



La fonctionnalité de miroir est également disponible directement depuis l'interface de ESET Smart Security Business Edition et ESET NOD32 Antivirus Business Edition. L'activation de cette option est laissée au libre choix de l'administrateur.

Pour activer le miroir dans ESET Smart Security Business Edition ou ESET NOD32 Antivirus Business Edition, procédez comme suit :

- Installez ESET Smart Security Business Edition ou ESET NOD32 Antivirus Business Edition
- Dans la fenêtre de paramètres avancés (F5), cliquez sur Avancé > clés de licence. Cliquez sur le bouton 'Ajouter…', et recherchez le fichier nod32.lic et cliquez sur 'Ouvrir'. Ceci installera la licence et permettra de faire apparaître l'onglet miroir pour effectuer sa configuration du miroir.
- Dans la partie 'Mise à jour', cliquez sur le bouton 'Paramètres' et sélectionnez l'onglet Miroir.
- Cochez la case activant la création d'un miroir et l'option d'utilisation du serveur HTTP interne.
- Inscrivez le chemin complet du répertoire où seront placés les fichiers de mise à jour. (Ne pas y inscrire de répertoire connecté en tant que lecteur réseau).
- Le nom d'utilisateur et le mot de passe sont utilisés pour authentifier le client lors de l'accès au répertoire Miroir. Dans la plupart des cas, il n'est pas nécessaire de remplir ces champs, vu que les données d'authentification seront saisies au niveau du client.
- Cliquez sur le bouton 'Configuration avancée' et mettez l'authentification à 'NONE'[1].
- Dans les paramètres avancés, sélectionnez les composants qui seront téléchargés (les composants pour toutes les versions et langues qui seront utilisées sur le réseau devraient être sélectionnés).

Pour avoir les fonctionnalités optimales, nous recommandons d'activer le téléchargement et la mise en miroir des composants de programme. Si cette option est désactivée, seules les bases de signatures virales seront mises à jour, et non les composants de programme. Si le miroir est celui de ESET Remote Administrator, cette option peut être configurée dans ERAC par le menu Tools > Server Options... > onglet Other Settings > bouton Edit Advanced Settings... > ESET Remote Administrator > ERA Server > Setup > Mirror. Activez toutes les versions de langue présentes dans votre réseau.

1. Pour plus d'informations, voir la section 2.1.5, "Configuration" du Serveur ERA.

4. Console d'administration à distance en détail

4.1 Connexion au serveur ERA

La plupart des fonctionnalités de la Console ERA sont disponibles uniquement après s'être connecté sur le Serveur ERA. Avant de se connecter pour la première fois, il faut définir le serveur sur lequel ont veux se connecter, soit par son nom, soit par son adresse IP :
Ouvrez la Console ERA, cliquez sur File > Edit Connections... et cliquez sur l'onglet Connexion.

Cliquez sur le bouton Add/Remove... pour ajouter un nouveau Serveur ERA, ou pour modifier les serveurs déjà présent dans la liste. Cliquez sur OK après avoir ajouté ou modifié les serveurs, et sélectionnez le serveur désiré dans la liste déroulante. Ensuite cliquez sur le bouton Connect.

Les autres options de cette fenêtre sont :

- **Connect to selected server on the console startup**
  Si cette option est cochée, la console se connectera automatiquement au Serveur ERA sélectionné lorsqu'on la démarrera.

- **Show message when connection fails**
  Si une erreur de communication survient entre ERAC et ERAS, un message d'avertissement sera affiché.

Les connexions peuvent être protégées par un mot de passe. Par défaut, il n'y a pas de mot de passe pour se connecter sur un Serveur ERA, mais nous recommandons fortement d'en définir un. Pour cela, procédez comme suit :
Cliquez sur File > Change Password... puis sur le bouton 'Change...' à la droite de 'Password for Console'

Quand vous saisissez un mot de passe, il y a une option pour que le système se souvienne de celui-ci (considérez cependant le risque de sécurité possible). Pour supprimer tous les mots de passe qui ont été ainsi mémorisés, cliquez sur File > Clear Cached Passwords...

Lorsque la connexion est établie, le titre de la fenêtre du programme change et passe à Connected [nom du serveur].

4.2 Console ERA – écran principal

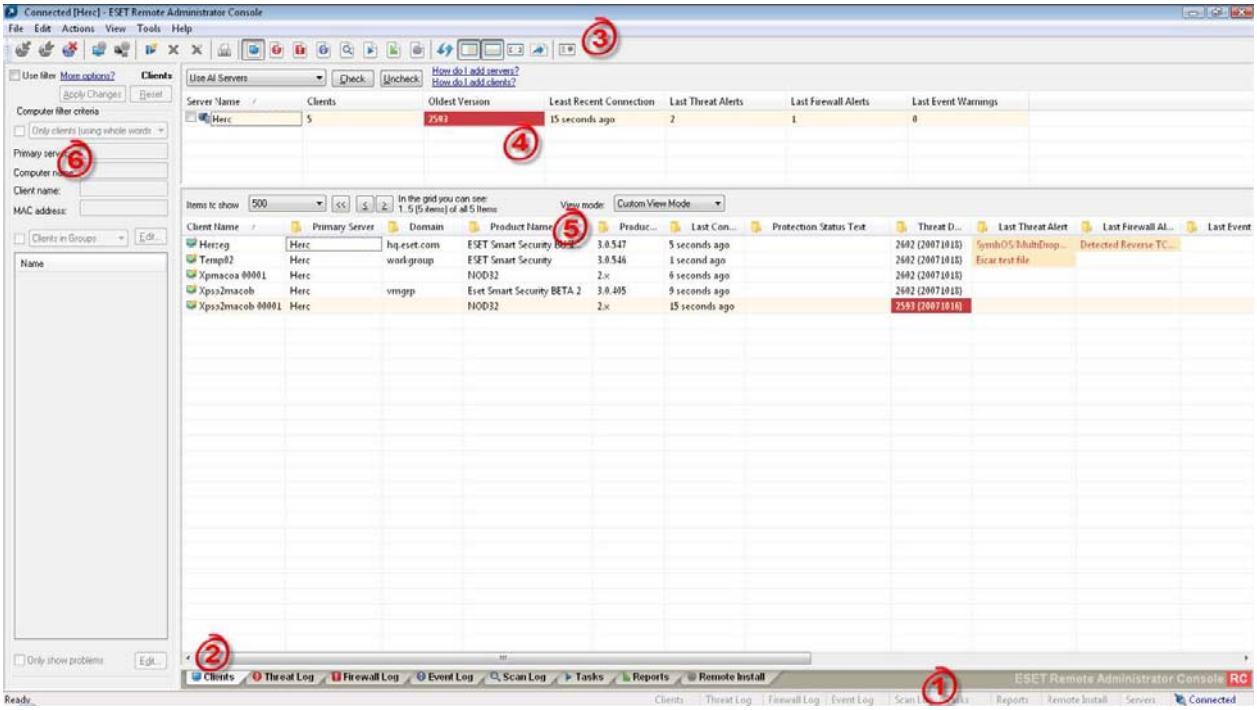


Figure 4
Ecran principal d'ESET Remote Administrator Console

Le statut actuel des communications entre ERAC et ERAS est affiché dans la barre de statuts (1). Toutes les données nécessaires du serveur sont actualisées régulièrement (par défaut toutes les minutes. Voir Tools > Console Options...). La progression de l'actualisation peut également être visualisée dans la barre de statuts.

NOTE : Appuyez sur F5 pour réactualiser les données affichées.

Les informations sont divisées en plusieurs onglets (2) par ordre d'importance. Dans la plupart des cas les données peuvent être triées (5) par ordre croissant ou décroissant en cliquant sur l'entête de colonne. Vous pouvez glisser/déplacer les colonnes afin de les réorganiser. Si de nombreuses lignes de données doivent être visualisées, vous pouvez en limiter le nombre en sélectionnant la valeur appropriée dans la liste déroulante 'Items to show' et passer d'une page à l'autre avec les boutons de sélection de page. Sélectionnez le mode de visualisation (View mode) selon vos besoins. Pour plus d'information, voir la section 4.3, "Filtrage des informations ".
La section 'Server' (4) est importante dans le cas ou vous faites de la réplication de Serveurs ERA. Vous pouvez visualiser ici les informations à propos du serveur sur lequel votre console est connectée, mais également a propos des Serveurs ERA parents ou enfants. La liste de serveurs (4) a une influence sur les informations affichées dans la section 5.
Les options sont :

- **Use All Servers**
  Affiche les informations de tous les Serveurs ERA
- **Use Only Checked Servers**
  Affiche uniquement les informations des serveurs sélectionnés
- **Exclude Checked Servers**
  N'affiche pas les informations des serveurs sélectionnés

Les colonnes de la section 4 sont :

- **Server Name**
  Affiche le nom du serveur
- **Clients**
  Nombre total de clients se connectant sur ce Serveur ERA
- **Oldest Version**
  Base de signatures virales la plus ancienne parmi les clients de ce Serveur ERA
- **Least Recent Connection**
  Donne la plus longue période d'inactivité (temps depuis la dernière connexion) parmi les clients du Serveur ERA
- **Last Threat Alerts**
  Nombre total d'alertes virales (voir la colonne Last Threat Alert dans la section 5 de l'image 4)
- **Last Firewall Alerts**
  Nombre total d'alertes du pare-feu (voir la colonne Last Firewall Alert dans la section 5 de l'image 4)
- **Last Event Warnings**
  Nombre total d'évènements système (voir la colonne Last Event Warning dans la section 5 de l'image 4)

Si vous n'êtes pas connecté, vous pouvez cliquer droit sur un serveur (4), et sélectionner 'Connect to This Server' dans le menu contextuel pour vous connecter à celui-ci.

NOTE: Si la réplication est active, les serveurs enfants seront automatiquement affichés dans la section 'Server' (4).

Les fonctionnalités principales de ERAC sont accessibles depuis le menu ou depuis la barre d'outils (3).

La dernière section est 'Computer filter criteria'(6) (critères de filtres d'ordinateurs) – voir ci-après.

4.3 Filtrage des informations

ERAC propose plusieurs outils et fonctionnalités afin de fournir une administration aisée des différents clients et évènements.

4.3.1 Groupes

Les différents clients peuvent être divisés en groupes en cliquant sur Edit > Groups... dans la console ERA. Les groupes peuvent ensuite être utilisés lors de l'application de filtres ou la création de tâches, car ces éléments peuvent être appliqués sur l'ensemble du groupe simultanément. Les groupes sont indépendants sur chaque ERAS et ne sont pas répliqués. La fonctionnalité de synchronisation avec Active Directory permet à l'administrateur de trier les clients en groupes, si le nom du client est le même que l'objet "computer" dans l'Active Directory (AD) et fait partie du groupe dans AD.

4.3.2 Filtres

Les filtres permettent d'afficher uniquement les informations relatives à des serveurs ou clients spécifiques. Pour visualiser les options de filtre, cliquez sur View > Show/Hide Filter Pane dans le menu de ERAC.
Pour activer le filtrage, cochez la case 'Use Filter' et cliquez sur le bouton 'Apply Changes'. Toute modification future des critères de filtres affichera automatiquement les données correspondantes, sauf si cela a été paramétré autrement dans la partie Tools > Console Options... > onglet Other Settings.

Dans cette section, il est également possible de filtrer les Serveurs ERA / clients en utilisant les critères suivants :

- **Only clients (using whole word)**
  Affiche uniquement les clients dont le nom est identique à la chaîne de caractères spécifiée.
- **Only clients beginning like**
  Affiche uniquement les clients dont le nom commence par la chaîne de caractères spécifiée.
- **Only clients like**
  Affiche uniquement les clients dont le nom contient la chaîne de caractères spécifiée
- **Exclude clients (using whole word), Exclude clients beginning like, Exclude clients like**
  Ces options vont générer le résultat opposé aux précédentes

Les champs Primary server, Computer name, Client name et MAC Address acceptent toute chaîne de caractères. Si l'un de ces champs est rempli, alors une requête sera générée dans la base de données et les résultats seront affichés en fonction des éléments saisis.

La section suivante permet de filtrer les clients en se basant sur les groupes :

- **Clients in Groups**
  Affiche uniquement les clients appartenant au(x) groupe(s) spécifié(s)
- **Clients in other Groups or N/A**
  Affiche uniquement les clients appartenant à un autre groupe, ou les clients n'appartenant à aucun groupe. Si un client appartient à la fois à des groupes spécifiés et non spécifiés, alors il sera inclus dans les éléments affichés.
- **Clients in no Groups**
  Affiche uniquement les clients n'appartenant à aucun groupe

Les options de filtrage changent légèrement en fonction de l'onglet sélectionné (Clients, Threat Log, etc.).

4.3.3 Menu contextuel

Cliquez sur le bouton droit de la souris pour faire apparaître le menu contextuel et ainsi ajuster les éléments affichés dans les différentes colonnes.

- **Select by '...'**
  Celle option vous permet de sélectionner une caractéristique et ainsi de sélectionner tous les autres clients ayant cette même caractéristique.
- **Inverse selection**
  Fait une sélection inverse des éléments
- **Hide selected**
  Cache les éléments sélectionnés
- **Hide unselected**
  Cache les éléments non sélectionnés de la liste

Les deux dernières options sont utiles si une organisation supplémentaire est nécessaire après l'utilisation de la méthode précédente de filtres. Pour désactiver tous les filtres mis en place par le menu contextuel, cliquez sur View > Cropped View, ou cliquez sur l'icône 'Refresh' dans la barre d'outils de ERAC. Vous pouvez également appuyer sur F5 pour rafraîchir les informations affichées et désactiver les filtres.

Exemple :

- **Pour afficher uniquement les clients avec des alertes de menaces :**
  Dans l'onglet Clients, cliquez droit sur une ligne vide dans la colonne 'Last Virus Alert' et choisissez Select by '...' dans le menu contextuel. Puis à nouveau dans le menu contextuel, cliquez sur 'Hide selected'.

- **Pour afficher les alertes de menaces pour les clients "Joseph" et "Charles" :**
  Cliquez sur l'onglet 'Threat Log' et effectuer un cliquez droit sur n'importe quelle ligne ayant la valeur 'Joseph' dans la colonne 'Client Name'. Dans le menu contextuel, sélectionnez Select by 'Joseph'. Ensuite, appuyez sur la touche CTRL et maintenez-là enfoncée. Cliquez droit sur une ligne correspondant au client 'Charles' et choisissez dans le menu contextuel Select by 'Charles'. Enfin, cliquez droit et sélectionnez 'Hide unselected' dans le menu contextuel. Vous pouvez à présent relâcher la touche CTRL.

  La touche CTRL peut être utilisée pour sélectionner/désélectionner des éléments spécifiques et la touché SHIFT pour marquer/démarquer un groupe d'éléments.

NOTE : Le filtrage peut également être utilisé pour faciliter la création de nouvelles tâches pour des clients spécifiques (mis en surbrillance). Il y a de nombreuses possibilités pour faire un filtrage efficace, faites des essais afin de trouver ce qui vous convient le mieux.

4.3.4 Vues

Dans l'onglet 'Clients', le nombre de colonnes affichées peut être ajusté par le biais de la liste déroulante du mode de visualisation ('View mode'). Si 'Full View Mode' est sélectionné, toutes les colonnes sont affichées, tandis 'Minimal View Mode' n'affiche que les plus importantes. Ces modes sont prédéfinis et ne peuvent pas être modifiés. Pour afficher le mode personnalisé, sélectionnez 'Custom View Mode' dans la liste. Le mode d'affichage personnalisé peut être configuré dans Tools > Console Options... > onglet Columns – Show/Hide tab.

4.4 Onglets de la console ERA

4.4.1 Description générale des onglets et clients

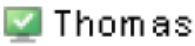
La plupart des informations des différents onglets est liée aux clients connectés. Chacun des clients connectés à ERAS est identifié par les éléments suivants :

Computer Name (client name) + *MAC Address* + *Primary Server* [2]
(Nom de l'ordinateur + Adresse MAC + Serveur primaire)

Le comportement de ERAS par rapport à certaines opérations sur le réseau (telle que renommer un PC) peut être défini dans les fonctionnalités avancées de ERAS (ERAS Advanced Setup) (Pour plus de détails, voir la section "Other Settings" dans le chapitre 4). Par exemple, si l'un des ordinateurs du réseau à été renommé mais que son adresse MAC est inchangée, vous pouvez éviter qu'une nouvelle entrée soit crée dans l'onglet 'Clients'.

Les clients (stations de travail et serveurs ayant une solution de sécurité ESET installée) se connectant pour la première fois sur ERAS sont repérés par la valeur 'Yes' dans la colonne 'New User' et sont marquées par un petit astérisque sur l'icône du client. Ceci permet à l'administrateur de repérer facilement tout nouvel ordinateur se connectant à ERAS. Cette caractéristique peut avoir différentes significations en fonction des choix de l'administrateur.

Si un client a été configuré (et déplacé dans un groupe), le statut 'New' peut être désactivé en cliquant droit sur ce client et en sélectionnant 'Reset "New" Flag'. L'icône de ce client changera comme celle ci-dessous (et la caractéristique 'New User' sera mise à 'No').



NOTE: Le commentaire est optionnel. L'administrateur peut y insérer une description (ex: "Office No. 129").

NOTE: Les valeurs de temps peuvent être configures dans ERAS soit de façon relative ("2 days ago"), ou alors de façon absolue (20. 5. 2007).

Dans la plupart des cas, les données peuvent être triées en ordre croissant ou décroissant en cliquant sur le nom de la colonne. La méthode glisser/déplacer peut être utilisée pour réorganiser les colonnes.

En double-cliquant sur certaines valeurs vous pouvez afficher des informations plus détaillées. Par exemple, si vous cliquez sur une valeur de la colonne 'Last Threat Alert', le programme va alors se mettre sur l'onglet 'Threat Log' et afficher les éléments relatifs au client donné. Si vous cliquez sur un élément contenant trop d'informations pour être affichées sous une forme de tableau, alors une fenêtre s'ouvrira affichant les informations détaillées à propos de ce client.

4.4.2 Réplication & information dans les onglets individuels

Si une Console ERA est connectée à un Serveur ERA qui fonctionne en tant que serveur supérieur, alors toutes les informations en provenance des serveurs inférieurs seront affichées automatiquement, à moins que le serveur inférieur ne soit pas configuré pour permettre ceci.
Dans un tel cas, les informations suivantes pourraient manquer :

- Rapports d'alerte détaillés (onglet Threat Log)
- Rapports détaillés d'analyse à la demande (onglet Scan Log)
- Configurations détaillées des clients dans le format .xml (onglet Clients tab, colonnes Configuration, Protection Status, Protection Features, System Information)

Dans les fenêtres de dialogue où ces informations devraient être présentes, le bouton ''Request' est disponible. En cliquant sur ce bouton, vous pouvez télécharger les données manquantes depuis le serveur inférieur. Vu que les communications sont toujours initiées par le serveur inférieur, les informations seront délivrées lors de la prochaine réplication.
Computer Name (client name) + MAC Address + Primary Server2
(Nom de l'ordinateur + Adresse MAC + Serveur primaire)

2. Dans les anciennes versions des ESET Remote Administrator, l'identification était basée uniquement sur les éléments Computer Name + Primary Server.

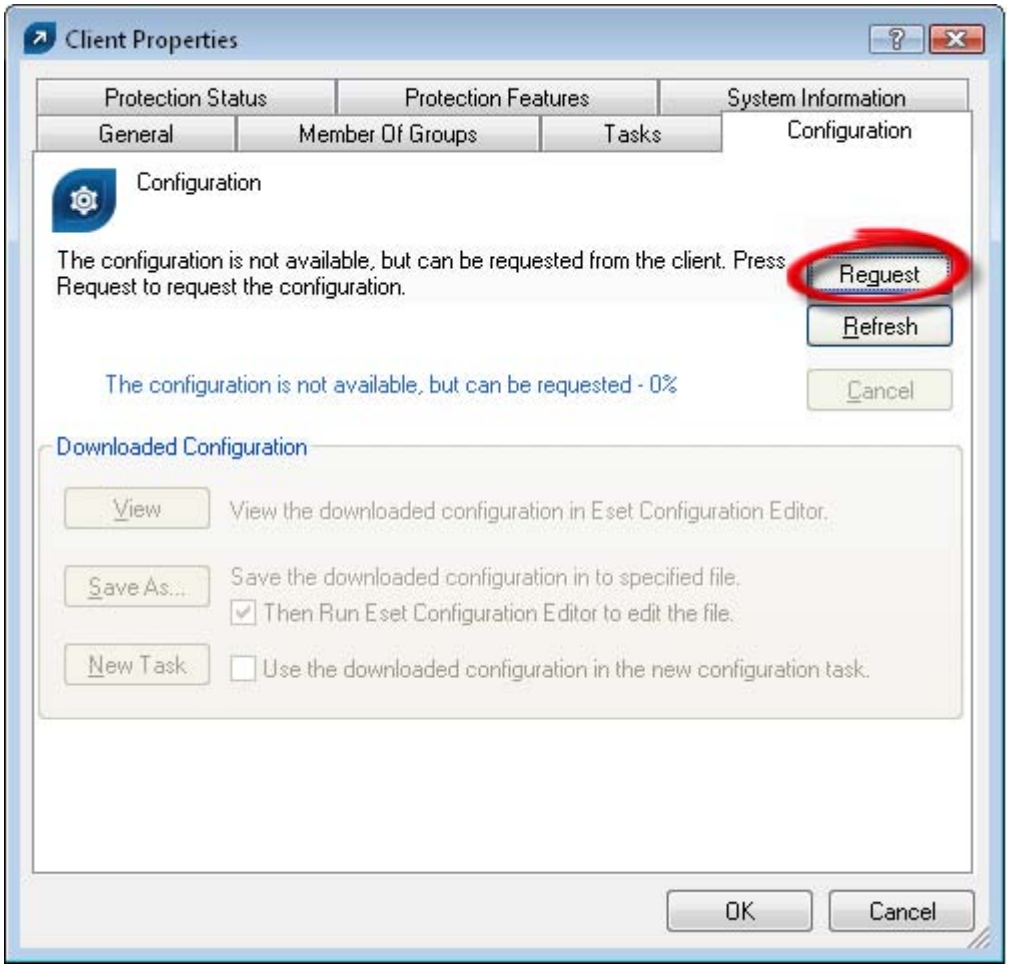


Figure 5
Cliquez sur ‘Request’ pour demander les informations manquantes depuis les Serveurs ERA inférieurs.

4.4.3 Onglet Clients

Ce panneau affiche les informations générales à propos des différents clients.

Attribut	Description
Client Name	Nom identifiant un client dans. Les nouveaux clients prennent la valeur “Computer Name” (nom de l’ordinateur). Le nom du client peut être modifié sans qu’il y ait d’effet secondaire.
Computer Name	Nom de l’ordinateur (station de travail / serveur)
MAC Address	Adresse MAC (interface réseau)
Primary Server	Non du Serveur ERA avec lequel le client communique
Domain	Nom de domaine / groupe dans lequel se trouve le client (ce ne sont pas les groupes crées dans ERAS)
IP	Adresse IP
Product Name	Nom du produit ESET installé
Product Version	Version du produit mentionné ci-dessus.
Last Connected	Dernière connexion d’un client sur son Serveur ERA. Toutes les autres données en provenance du client ont été actualisées à cette date, à l’exception de certaines données obtenues par réplication
Protection Status Text	Statut actuel de la solution de sécurité ESET installée sur le client
Threat DB Version	Version de la base de signature virale
Last Threat Alert	Dernière menace détectée
Last Firewall Alert	Dernier évènement détecté par le pare-feu
Last Event Warning	Dernier message d’erreur
Last Files Scanned	Nombre de fichiers scannés lors de la dernière analyse à la demande
Last Files Infected	Nombre de fichiers infectés lors de la dernière analyse à la demande
Last Files Cleaned	Nombre de fichiers nettoyés (ou supprimés) lors de la dernière analyse à la demande
Last Scan Date	Date et heure de la dernière analyse à la demande
Restart Request	Un redémarrage est requis (ex: après une mise à jour du programme)
Restart Request Date	Date de la première demande de redémarrage
Product Last Started	Affiche quand le programme a été démarré sur le client pour la dernière fois
Product Install Date	Date d’installation du programme
Mobile User	Les clients avec cet attribut effectueront une tâche “update now” (mise à jour immédiate) à chaque fois qu’ils établiront une connexion avec ERAS (approprié pour les ordinateurs portables)
New User	Voir dans la description générale des clients pour plus de détails
OS Name	Nom du système d’exploitation sur l’ordinateur
OS Platform	Type de système d’exploitation (Windows / Linux…)
HW Platform	32-bit / 64-bit
Configuration	Le client soumet également sa configuration courante au format .xml. L’heure de la dernière configuration est affichée (Si il n’y a pas de réplication, celle-ci est égale à l’heure de la dernière modification)
Protection Status	Etat de la protection. Similaire à la partie ‘Configuration’
Protection Features	Etat différents éléments de Similaire à la partie ‘Configuration’
System Information	Information à propos des versions des différents composants du programme. Similaire à la partie ‘Configuration’

NOTE: Certaines valeurs sont uniquement de nature informative et peuvent ne plus être d'actualité lorsque l'administrateur va les voir dans la console. Par exemple, une erreur a pu survenir lors de la mise à jour à 7:00 heures, mais à 8:00 heures, la mise à jour s'est passée correctement. Si l'administrateur sait que cette information est obsolète, alors il peut effectuer un clic droit sur cette valeur et sélectionner 'Clear "Last Threat Alert" Info', ou 'Clear "Last Event" Info'. Les informations a propos de ces éléments seront alors supprimées. Ceci ne s'applique que sur les éléments des colonnes Last Threat Alert et Last Event.

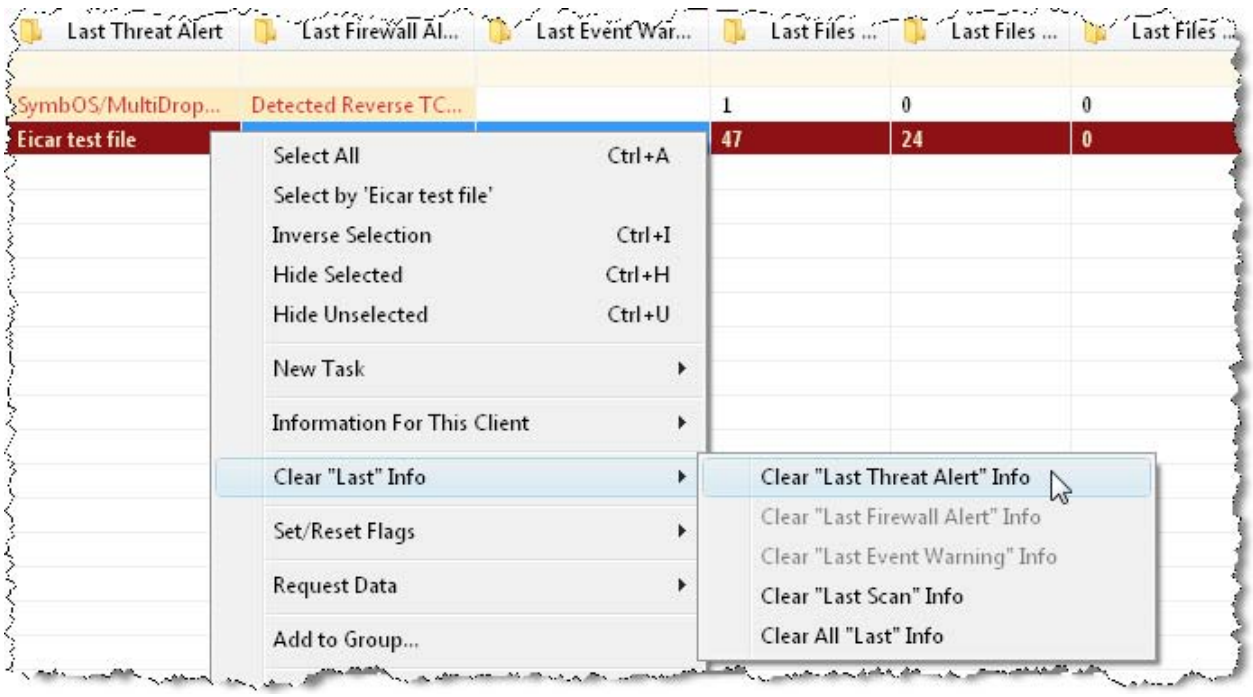


Figure 6
Les informations obsolètes des colonnes Last Threat Alert et Last Event Warning peuvent être aisément supprimés.

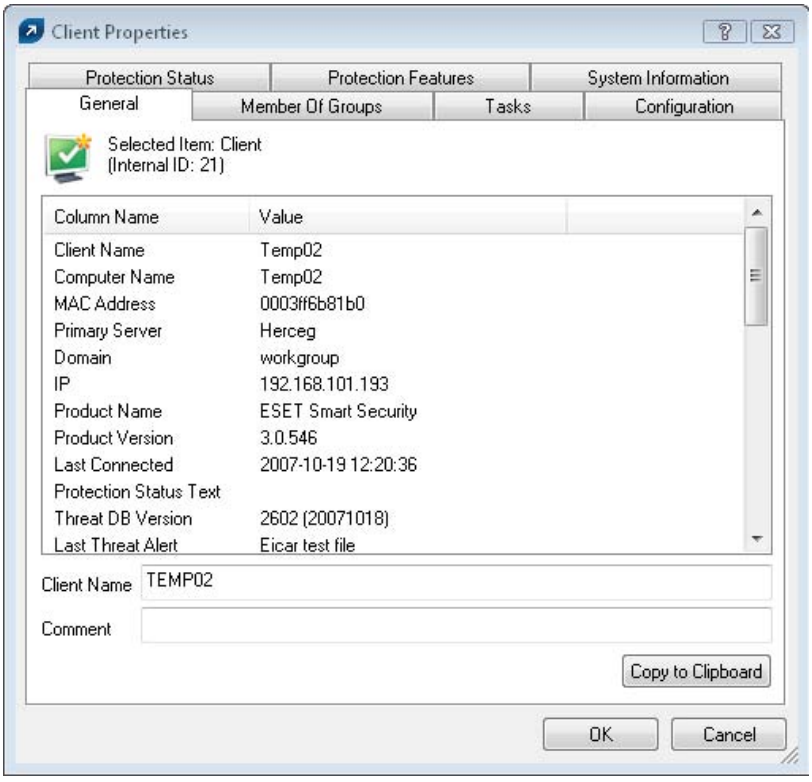


Figure 7

Configuration détaillée d'une station cliente.

L'onglet Clients affiche plusieurs éléments après avoir double-cliqué sur un client :

- **Onglet General**
  Contient les mêmes informations que celles affichées dans l'onglet 'Clients'. Vous pouvez y spécifier le nom du client – celui qui sera affiché dans ERA, ainsi qu'un commentaire éventuel.

- **Onglet Member Of Groups**
  Tous les groupes auquel appartient ce client seront affichés. Pour plus d'informations, voir la partie 4.3 "Filtrage des informations.

- **Onglet Tasks**
  Tâches relatives au client. Voir la partie "Tâches" dans le chapitre 5.

- **Onglet Configuration**
  Cet onglet vous permet de voir ou exporter la configuration courante du client sous forme de fichier .xml. Les fichiers .xml peuvent être utilisés pour générer des modèles de configuration pour d'autres clients. Pour plus d'informations, voir la partie " Tâches " dans le chapitre 5.

- **Onglet Protection Status**
  Etat général de la protection des programmes ESET. Certains éléments sont interactifs et il est alors possible d'intervenir directement. Cette fonctionnalité permet d'éviter d'avoir à faire des tâches de configuration afin de résoudre certains problèmes.

- **Onglet Protection Feature**
  Statut des différents composants des solutions de sécurité ESET (Antispam, Personal Firewall, etc.)

- **Onglet System Information**
  Informations détaillées à propos des programmes installés, versions des composants, etc.

4.4.4 Onglet Rapport des menaces

Cet onglet affiche les informations détaillées à propos divers virus ou menaces détectées.

Attribut	Description
Threat Id	ID de l'élément dans la base de données
Client Name	Nom du client ayant détecté cette menace
Computer Name	Nom de l'ordinateur du client ayant détecté cette menace
MAC Address	Adresse MAC du client ayant détecté cette menace
Primary Server	Nom du Serveur ERA avec lequel le client communique
Date Received	Date/heure de réception du l'évènement par le Serveur ERA
Date Occurred	Date/heure à laquelle l'évènement est survenu sur le client
Level	Niveau d'alerte
Scanner	Nom du module de sécurité ayant détecté l'alerte
Object	Type d'objet
Name	Répertoire dans lequel se trouve l'infiltration
Threat	Nom du code malicieux détecté
Action	Action menée par le module de sécurité
User	Nom de l'utilisateur connecté lorsque l'incident est survenu
Information	Défini par l'utilisateur

4.4.5 Onglet Rapport du pare-feu

Cet onglet affiche les informations relatives à l'activité du pare-feu sur les clients.

Attribut	Description
Firewall Id	ID de l'élément dans la base de données
Client Name	Nom du client rapportant l'évènement
Computer Name	Nom de l'ordinateur du client rapportant l'évènement
MAC Address	Adresse MAC du client rapportant l'évènement
Primary Server	Nom du Serveur ERA avec lequel le client communique
Date Received	Date/heure de réception du l'évènement par le Serveur ERA
Date Occurred	Date/heure à laquelle l'évènement est survenu sur le client
Level	Niveau d'alerte
Event	Description de l'évènement
Source	Adresse IP source
Target	Adresse IP cible
Protocol	Protocole concerné
Rule	Règle concernée
Application	Application concernée
User	Nom de l'utilisateur connecté lorsque l'incident est survenu

4.4.6 Onglet Rapport des évènements

Cet onglet affiche la liste de tous les évènements relatifs au système.

Attribut	Description
Event Id	ID de l'élément dans la base de données
Client Name	Nom du client rapportant l'évènement
Computer Name	Nom de l'ordinateur du client rapportant l'évènement
MAC Address	Adresse MAC du client rapportant l'évènement
Primary Server	Nom du Serveur ERA avec lequel le client communique
Date Received	Date/heure de réception du l'évènement par le Serveur ERA
Date Occurred	Date/heure à laquelle l'évènement est survenu sur le client
Level	Niveau de l'évènement
Plugin	Nom du composant de programme rapportant 'évènement
Event	Description de l'évènement
User	Nom de l'utilisateur connecté lorsque l'évènement est survenu

4.4.7 Onglet Rapport d'analyses

Cet onglet affiche la liste des résultats des analyses à la demande qui on été réalisées à distance, localement, ou en tant que tâche programmée.

Attribut	Description
Scan Id	ID de l'élément dans la base de données
Client Name	Nom du client sur lequel l'analyse a été exécutée
Computer Name	Nom de l'ordinateur du client sur lequel l'analyse a été exécutée
MAC Address	Adresse MAC du client sur lequel l'analyse a été exécutée
Primary Server	Nom du Serveur ERA avec lequel le client communique
Date Received	Date/heure de réception du l'évènement par le Serveur ERA
Date Occurred	Date/heure à laquelle l'évènement est survenu sur le client
Scanned Targets	Fichiers, répertoires et lecteurs analysés
Scanned	Nombre de fichiers vérifiés
Infected	Nombre de fichiers infectés
Cleaned	Nombre de fichiers nettoyés
Status	Statut de l'analyse
User	Nom de l'utilisateur connecté lorsque l'analyse a été effectuée
Type	Qui a démarré l'analyse
Scanner	Elément ayant effectué l'analyse
Details	Informations détaillées

4.4.8 Onglet des Tâches

Le fonctionnement de cet onglet est détaillé dans le chapitre 5, " Tâches ". Les éléments disponibles sont:

Attribut	Description
Task Id	ID de l'élément dans la base de données
State	Statut de la tâche (Active = en cours d'application, Finished = la tâche a été donnée aux clients)
Type	Type de tâche
Name	Nom de la tâche
Description	Description de la tâche
Date Received	Date/heure de réception du l'évènement par le serveur ERA
Comment	Description optionnelle

4.4.9 Onglet Rapports

Cet onglet est utilisé pour générer des informations statistiques – rapports– sous forme d'histogrammes ou de graphes. Ces éléments peuvent également être générés puis analysés ultérieurement (données sauvegardées sous forme de fichier CSV – virgule comme séparateur de données) en utilisant les options de génération de ERA. Par défaut, ERA sauvegarde les rapports générés au format HTML (les images sont au format PNG).

ERA fournit plusieurs modèles de rapports prédéfinis. Afin de sélectionner un modèle particulier, utiliser le menu déroulant se trouvant au milieu de la fenêtre, juste en dessous du bouton 'Generate Now'.

Liste des menaces les plus fréquemment détectées

- **Top Clients with most Threats**
  Liste des clients les plus "actifs" (en nombre de menaces détectées)

- **Threats Progress**
  Progression du nombre de menaces détectées

- **Threats Comparative Progress**
  Progression du nombre de menaces spécifiques détectées (utilisation de filtres) par rapport au total

- **Threats By Scanner**
  Nombre d'alertes de menaces pour un module spécifique du programme

- **Threats By Object**
  Nombre de menaces par en fonction de leur origine (emails, fichiers, secteur de boot)

- **Combined Top Clients / Top Threats**
  Combinaison des éléments cites

- **Combined Top Threats / Threats Progress**
  Combinaison des éléments cités

- **Combined Top Threats / Threats Comparative Progress**
  Combinaison des éléments cités

- **Clients Report, Threats Report, Events Report, Scans Report, Tasks Report**
  Rapports typiques concernant les enregistrements des onglets mentionnés

- **Comprehensive Report**
  Résumé des rapports suivants :
  - Combined Top Clients / Top Threats
  - Combined Top Threats / Threats Comparative Progress
  - Threats Progress

Dans la section 'Filter', vous pouvez sélectionner les clients ou menaces qui vont être inclus dans les rapports.

D'autres éléments peuvent également être configurés en cliquant sur le bouton 'Additional Settings...'. Ceux-ci concernent généralement le type d'affichage des éléments graphiques. Cependant, vous pouvez également filtrer les données en fonction de certains statuts concernant les clients (ex : ne montrer que les clients ayant un problème concernant l'état de la protection), ainsi que le format qui sera utilisé pour générer le rapport (HTML, CSV).

Interval tab – Dans cet onglet vous pouvez définir la période qui sera utilisée pour générer le rapport :

- **Current**
  Seuls les éléments survenus lors de la période déterminée seront pris inclus dans le rapport. – ex : si le rapport est crée le mercredi et que l'intervalle est défini sur 'week' (semaine) alors seuls les éléments survenus dimanche, lundi, mardi et mercredi seront inclus.

- **Completed**
  Seuls les évènements survenus dans une période déterminée et close seront pris en compte dans le rapport. Si l'option 'Add also the current period' est sélectionnée, alors le rapport inclura également les évènements survenus jusqu'au moment de création du rapport.

Exemple : Nous voulons créer un rapport incluant les évènements de la dernière semaine calendaire (de dimanche à samedi). Ce rapport devra alors être généré le mercredi suivant.

Dans la partie 'interval', sélectionnez 'Complete' et '1 week'. Dans la partie 'Scheduler' mettez la fréquence sur 'Weekly' et sélectionnez 'Wednesday' (mercredi). Configurez les autres paramètres en fonction de vos besoins.

- **From/To**
  Ce paramètre permet de définir la période sur laquelle le rapport sera généré.

Onglet tab – Dans cet onglet vous pouvez configurer et définir la génération automatique de rapport pour une date ou un intervalle donné (en utilisant la section 'Frequency' - fréquence).

En utilisant les éléments 'Run at' et 'Start' vous pouvez définir la date et l'heure de génération du rapport. Cliquez sur le bouton 'Select Target...' afin de spécifier l'endroit où le rapport sera sauvegardé. Les rapports peuvent être sauvegardés dans le Serveur ERA (défaut), envoyés par email ou exporté dans un répertoire donné. La dernière option est utile si le rapport est envoyé dans un répertoire partagé au sein de votre entreprise, afin qu'il puisse être vu par les autres personnes de l'entreprise.

Afin d'envoyer le rapport par email, vous devez spécifier le serveur SMTP et l'adresse d'expédition tel que décrit dans le chapitre 4.6 Configurer le Serveur ERA en utilisant la Console.

Pour définir une période Durant laquelle le rapport sera généré, utilisez les options de la partie 'Range'. Vous pouvez y définir le nombre de rapports générés, (End after), ou alors une date après laquelle le rapport ne sera plus généré (End by).

Afin de sauvegarder les paramètres dans un modèle, cliquez sur les boutons 'Save' ou 'Save as...'. Pour la création d'un nouveau modèle, cliquez sur le bouton 'Save as...' et donnez un nom au modèle.

Dans la partie supérieure de la console, section rapports, vous pouvez voir le nom des modèles déjà crées. Les informations concernant le temps/intervalle sont également affichées. Cliquez sur le bouton 'Generate Now' afin de générer un rapport sans tenir compte de la planification de celui-ci (veillez à bien sélectionner le nom du modèle auparavant).

Les rapports déjà générés peuvent être visualises via l'onglet 'Generated Reports'. En sélectionnant un ou plusieurs rapports et en utilisant le menu contextuel (clic droit) vous avez accès à plusieurs options telles que la copie vers un autre répertoire, l'ajout du modèle à la liste des favoris, etc.

Les modèles placés dans la liste des favoris peuvent être utilisés pour générer immédiatement de nouveaux rapports. Pour déplacer un modèle dans la liste des favoris, cliquez droit sur celui-ci et sélectionnez 'Add to Favorites' dans le menu contextuel.

4.4.10 Onglet Installation à distance

Dans cet onglet vous avez plusieurs options pour l'installation à distance de ESET Smart Security et ESET NOD32 Antivirus sur les clients. Pour de plus amples informations, voir la section "Installation à distance" dans le chapitre 6, "Installation des solutions clientes ESET ".

4.5 Configuration de la console ERA

La console ERA peut être configurée par le menu Tools / Console Options...

4.5.1 Onglet Connexion

Dans cet onglet vous avez les paramètres de communication entre la Console et le Serveur ERA. Pour plus de détails, voir le début du chapitre 4, "Console d'administration à distance en détail".

4.5.2 Onglet Colonnes - Afficher / Masquer

Vous pouvez spécifier ici les colonnes qui seront affichées dans les différentes parties de la console. Les changements affectent la visualisation de type 'Custom View Mode' uniquement. Les autres modes de visualisation ne peuvent pas être modifiés.

4.5.3 Onglet Couleurs

Vous pouvez définir ici les couleurs qui seront associées aux différents évènements. Par exemple, les clients dont la date de la base virale est légèrement dépassée (Clients: Previous Version) peuvent être distingués de ceux dont la base virale est obsolète (Clients: Older Versions or N/A).

4.5.4 Onglet Chemin

Vous pouvez définir ici le répertoire dans lequel la Console ERA sauvegardera les rapports téléchargés depuis ERAS. Par défaut, ceux-ci sont placés dans le répertoire :
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Console\reports

4.5.5 Onglet Date / Heure

Apparence des colonnes date / heure :

- **Absolute**
  La console affichera le temps absolu (ex : 14:30:00).

- **Relative**
  LA console affichera un temps relatif (ex : 2 weeks ago).

- **Regional**
  La console affichera l'heure en fonction des paramètres régionaux (définis dans les paramètres de Windows).

- **Recalculate UTC time to your local time (use local time)**
  Sélectionnez cette option pour recalculer l'heure en heure locale. Sinon, l'heure GMT – UTC sera affichée.

4.5.6 Onglet Autres Paramètres

- **Auto Apply Changes**
  Lorsque cette case est cochée, les filtres dans les différents onglets seront appliqués automatiquement après chaque modification des paramètres. Sinon, les changements seront effectués uniquement après avoir appuyé sur le bouton 'Apply Changes'.

- **Remote Administrator updates**
  Cette option permet de vérifier la disponibilité de nouvelles versions de ESET Remote Administrator. Nous recommandons de laisser le paramétrage par défaut – mensuelle (Monthly). Si une nouvelle version est disponible, la console affichera une notification lors de son démarrage.

- **Use automatic refresh**
  Les données dans les différentes parties seront automatiquement mise à jour en fonction de l'intervalle spécifié.

- **Empty console recycle bins at application exit**
  Permet de vider automatiquement la corbeille interne de la console lors de la fermeture. Vous pouvez également la vider en cliquant sur celle-ci dans l'onglet 'Reports'.

- **Show gridlines**
  Permet de séparer les différentes cellules par des lignes dans les tableaux

- **Prefer showing Client as "Server/Name" instead of "Server/Computer/MAC"**
  Affecte le mode d'affichage des clients dans certaines fenêtres de dialogue (ex : New task).

- **Use systray icon**
  L'icone de la Console ERA sera affichée dans la barre de notification de Windows.

- **Show on taskbar when minimized**
  Si la Console ERA est minimisée, elle sera accessible par la barre de notification de Windows.

- **Use highlighted systray icon when problematic clients found**
  Permet de définir (avec le bouton 'Edit') les évènements qui feront changer la couleur de l'icône de la Console ERA dans la barre de notification.

NOTE : Si la console est amenée à être constamment connectée sur le Serveur ERA, nous recommandons d'activer la visualisation dans la barre des tâches. Si un problème survient, l'icône sera alors rouge, ce qui indiquera à l'administrateur qu'il doit intervenir. Nous recommandons également de cocher l'option 'Use highlighted systray icon when problematic clients found' afin de définir les évènements qui provoqueront le changement de couleur de l'icône.

- **Show all groups in filter panes**
  Modifie la façon de filtrer les groupes.

- **Tutorial messages**
  Désactive (Disable All) ou active (Enable All) tous les messages informatifs

- **Warn if the server license is about to expire in X days**
  Le programme affichera une notification X jour savant la date d'expiration de la licence.

- **Warn if there is only X% free clients left in the server license**
  La console affichera une notification si moins de X% de places sont disponibles pour l'affichage des clients dans la console (chaque licence est définie par un nombre de clients administrables).

4.6 Configurer le Serveur ERA en utilisant la Console

Le Serveur ERA peut être configure facilement depuis la console. Dans le menu, cliquez sur Tools > Server Options...

4.6.1 Onglet Général

Vous avez dans l'onglet 'General' les informations générales à propos de ERAS, les informations a propos de la clé de licence et des informations statistiques concernant les opérations de ERAS.
Cliquez sur 'Renew License...' afin d'installer une nouvelle clé de licence et ainsi éviter que celle-ci arrive à expiration. Les clés de licence sont décrites en détail dans la section 7.1.2, "Installation du Serveur ERA".

4.6.2 Onglet Sécurité

Les versions 3.x des solutions de sécurité ESET (ESET Smart Security, etc.) permettent d'avoir une protection par mot de passe lors de la communications entre le client et ERAS (communication par le protocole TCP, port 2222).

Les anciennes versions (2.x) n'ont pas cette fonctionnalité. Afin d'avoir une compatibilité pour les anciennes versions, l'option 'Enable unauthenticated access for Clients' doit être activée.

L'onglet 'Security' contient certaines options permettant l'utilisation simultanée des générations 2.x et 3.x du programme.

- **Password for Console**
  Permet de définir un mot de passe pour accéder à la console

- **Password for Clients (ESET Security Products)**
  Définit un mot de passe pour l'accès des clients sur ERAS

- **Password for Replication**
  Définit un mot de passe pour la réplication des serveurs inférieurs vers ce serveur

- **Password for ESET Remote Installer (Agent)**
  Définit un mot de passe pour l'accès de l'agent d'installation au serveur ERAS. Ceci est en rapport avec l'installation à distance

- **Enable unauthenticated access for Clients (ESET Security Products)**
  Permet l'accès a ERAS pour les clients n'ayant pas de mot de passe valide (si le mot de passe est différent de celui défini dans la partie 'Password for Clients').

- **Enable unauthenticated access for Replication**
  Permet l'accès sur ERAS des clients des Serveurs ERA inférieurs et n'ayant pas de mot de passe valide de défini pour la réplication

- **Enable unauthenticated access for ESET Remote Installer (Agent)**
  Permet l'accès à ERAS pour les agents d'installation n'ayant pas de mot de passe valide.

NOTE : Si l'authentification est active sur ERAS et tous les clients (Génération 3.x), l'option Enable unauthenticated access for Clients peut être désactivée.

4.6.3 Onglet Maintenance du Serveur

Une fois cette configuration bien réalisée, la base de donnée sera automatiquement maintenue et optimisée, sans aucun besoin de configuration ultérieur. Par défaut, les données de plus de 6 mois sont effacées et une tâche de réparation et de compactage est effectuée tous les 15 jours.

La partie ‘Server Maintenance’ possède les options suivantes :

- **Only keep the latest X threats for each client**
  Conserve uniquement le nombre spécifié d’incidents viraux pour chaque client
- **Only keep the latest X firewall logs for each client**
  Conserve uniquement le nombre spécifié de log firewall pour chaque client
- **Only keep the latest X events for each client**
  Conserve uniquement le nombre spécifié d’évènements système pour chaque client
- **Only keep the latest X scan logs for each client**
  Conserve uniquement le nombre spécifié de rapports d’analyse à la demande pour chaque client
- **Delete clients not connected for the last X months (days)**
  Supprime tous les clients qui ne se sont pas connectés à ERAS depuis le nombre spécifié de mois / jours
- **Delete threat logs older than X months (days)**
  Supprime tous les incidents viraux plus anciens que la date spécifiée
- **Delete firewall logs older than X months (days)**
  Supprime toutes les entrées firewall plus anciennes que la date spécifiée
- **Delete event logs older than X months (days)**
  Supprime tous les évènements système plus anciens que la date spécifiée
- **Delete scan logs older than X months (days)**
  Supprime tous rapports d’analyse à la demande plus anciens que la date spécifiée

4.6.4 Onglet Journaux

Durant son fonctionnement, ERAS crée un journal configurable (Log verbosity) concernant son d’activité. Si l’option ‘Log to text file’ est sélectionnée, de nouveaux fichiers seront crées (Rotate when greater than X MB) et supprimés (Delete rotated logs older than X days) quotidiennement.

L’option ‘Log to OS application log’ permet de copier les informations dans l’observateur d’évènements du système (accessible depuis les outils d’administration du système).

L’option ‘Debug Log’ doit être désactivée lors d’un fonctionnement normal.

Par défaut, le fichier texte du journal est sauvegardé dans le répertoire suivant :
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\logs\era.log

NOTE : Nous recommandons de laisser la verbosité du journal à ‘Level 2 – Above + Session Errors’. Changez de niveau uniquement si vous rencontrez des problèmes ou si cela vous est demandé par le support ESET.

4.6.5 Onglet Réplication

Le concept de réplication a été abordé dans la section 2.1.2, “Hiérarchie du Serveur ERA dans de vastes réseaux ”. La réplication est généralement utilisée dans un grand réseau dans lequel de multiples serveurs ERA sont installés).
Les options dans la partie réplication sont divisées en 2 sections :

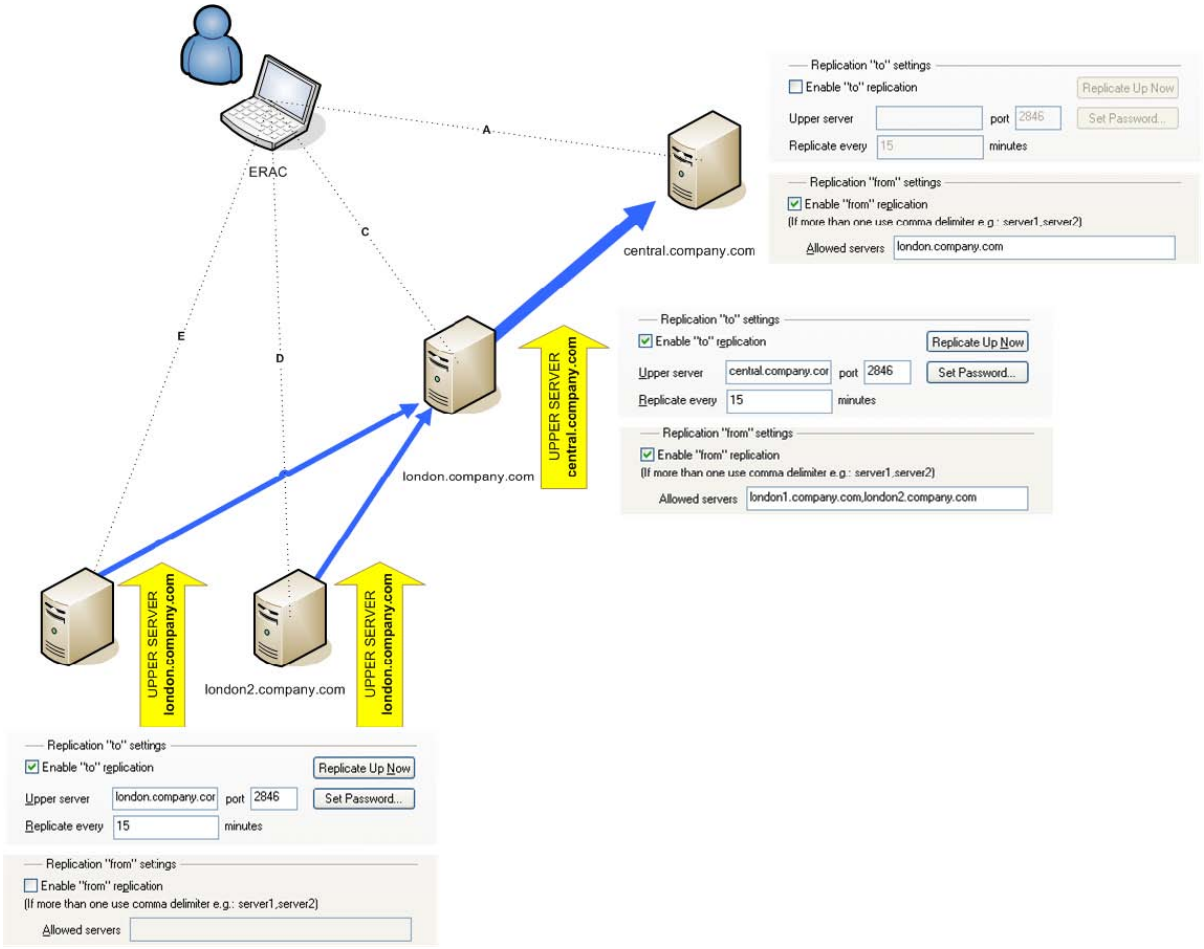
- Replication “to“ settings
- Replication “from“ settings

La section ‘Réplication “to“settings’ est utilisée pour configurer les Serveurs ERA inférieurs. La case ‘Enable “to“ réplication’ doit être cochée et l’adresse IP ou le nom du Serveur ERA maître (serveur supérieur) doit être indiqué. Les données du serveur inférieur seront alors répliquées sur le serveur supérieur.

La section ‘Réplication “from“ settings’ permet au Serveur ERA maître (serveur supérieur) d’accepter les données des Serveurs ERA inférieurs, ou de les transférer vers son serveur maître. La case ‘Enable “from“ réplication’ doit être cochés et les noms des serveurs inférieurs saisis (séparés par une virgule).

Ces 2 éléments doivent être activés pour les serveurs ERA situés au milieu de la hiérarchie de réplication (c-à-d s’ils ont à la fois des serveurs inférieurs et supérieurs).

Les scenarii abordés précédemment sont décris dans l’image ci-dessous. Les ordinateurs indiquent chacun un Serveur ERA. Chaque Serveur ERA est représenté par son nom (qui doit être le même que la variable %Computer Name%, afin d’éviter les confusions) et les paramètres de configuration correspondants sont affichés à côté.



Autres options ayant une influence sur la réplication de serveurs :

- **Replicate threat log, Replicate firewall log, Replicate event log, Replicate scan log**
  Si ces éléments sont sélectionnés, toutes les informations affichées dans les onglets les Clients, Threat Log, Firewall Log, Event Log, Scan Log, et Tasks seront répliquées individuellement. Cela comprend également les informations qui ne sont pas stockées directement dans la base de données, mais dans des fichiers individuels (.txt or .xml).

- **Automatically replicate threat log details, Automatically replicate scan log details, Automatically replicate client details**
  Ces options permettent la réplication automatique des informations complémentaires stockées dans des fichiers individuels. (Elles peuvent également être téléchargées en cliquant sur le bouton Request).

NOTE: La raison pour que certains éléments soient répliqués automatiquement et pas d'autres provient du fait que certains journaux contiennent un grand nombre d'informations qui ne sont pas toujours utiles quotidiennement.
Par exemple, rapport d'analyse avec l'option de lister tous les fichiers activée va prendre un espace disque non négligeable. De telles informations ne sont en général pas nécessaires et peuvent être demandées manuellement si besoin est.

4.6.6 Mises à jour

Dans cet onglet vous pouvez configurer les paramètres de la fonctionnalité de miroir qui est intégré dans ERAS. C'est une alternative à la même fonctionnalité présente dans les solutions clients ESET Smart Security Business Edition et ESET NOD32 Antivirus Business Edition.

- **Update server**
  Chemin ou adresse URL du serveur de mise à jour. Dans la plupart des cas, il n'est pas nécessaire de modifier la valeur par défaut 'Choose Automatically', permettant de faire les mises à jour depuis les serveurs ESET.

- **Update interval**
  Détermine l'intervalle de temps entre 2 mises à jour (la valeur recommandée est 60 minutes)

- **Update user name**
  Donnée d'authentification autorisant l'accès au serveur de mise à jour

- **Update password**
  Donnée d'authentification autorisant l'accès au serveur de mise à jour

- **Update now**
  Cliquez sur ce bouton pour faire une mise à jour immédiate

- **Create update mirror**
  Lorsque cette case est cochée, le programme permettra le téléchargement des mises à jour pour les clients dans le réseau, à partir du répertoire défini dans 'Folder to store mirrored files'. Si l'option 'Provide update files via internal HTTP server' est active, alors les fichiers de mise à jour seront accessibles via le serveur web interne (HTTP) au port spécifié (port du serveur HTTP – par défaut 2221).

- **Authentication**
  Permet de définir la méthode d'authentification pour les clients se connectant sur le miroir. Sélectionnez NONE pour permettre l'accès au serveur HTTP par tous les clients. Sélectionnez 'Basic' pour utiliser une méthode d'encryption base64. La méthode NTLM est la plus complexe disponible. Elle vérifie le compte utilisateur qui est indiqué du côté du client sous forme de nom d'utilisateur et mot de passe afin d'autoriser l'accès au serveur de mises à jour.

  Pour que le miroir fonctionne correctement, il est également nécessaire de configurer quels seront les composants téléchargés depuis les serveurs ESET (dans la fenêtre de configuration avancé), y compris les versions de langue. Ceci est disponible dans l'onglet 'Other Settings'.

4.6.7 Onglet Autres Paramètres

- **SMTP settings (Server, Sender address, Username, Password)**
  Certaines fonctionnalités dans ESET Remote Administrator nécessitent de paramétrer un serveur SMTP. Ceci inclus l'installation à distance par la méthode email, ou la génération de rapports devant être envoyés par email.

- **Allow new clients**
  Si cette option est désactivée, aucun nouveau client ne sera ajouté dans la liste des clients – même si les nouveaux clients communiquent avec le serveur ERA, ils ne seront pas visibles dans la liste.

- **Automatically reset "New" flag by new clients**
  Ceci permet de supprimer l'indication 'nouveau client' lorsqu'un client se connecte pour la première fois sur le Serveur ERA. Voir la section 4.4.3 "Onglet des Clients ".

- **Ports (Console, Client, Replication port of this server, ESET Remote Installer)**
  Détermine les ports sur lesquels ERAS va écouter et attendre des communications établies par :
  - Console (par défaut TCP 2223)
  - Client (par défaut TCP 2222)
  - Processus de réplication (par défaut TCP 2846)
  - Agent d'installation à distance (ESET Remote Installer, par défaut TCP 2224)

- **Enable ThreatSense.Net data forwarding to ESET servers**
  Dans certains cas, il n'est pas possible pour les clients d'envoyer directement ces informations.

- **Edit Advanced Settings...**
  Ce bouton ouvre l'éditeur de configuration ESET Configuration Editor, dans lequel ERAS peut être configuré en détail.

5. Tâches

ESET Remote Administrator permet d'effectuer à distance des tâches sur les stations clientes. Ces tâches sont effectuées lorsque le client se connecte sur le Serveur ERA (sur le port TCP 2222), connexion effectuée par défaut toutes les 5 minutes. Trois types de tâches sont possibles :

- Configuration – Modifie la configuration des clients
- On-Demand Scan – Effectue une analyse à la demande
- Update Now – Force une mise à jour

Pour ouvrir l'assistant de tâche, appuyez sur CTRL+N, cliquez sur File > New Task... ou cliquez sur l'icône 

Dans la barre d'outils de la console. Vous pouvez également l'ouvrir d'un clic droit sur un client (cette option saute certaines étapes – utilisez l'une des deux méthodes citées auparavant afin d'avoir toutes les options).

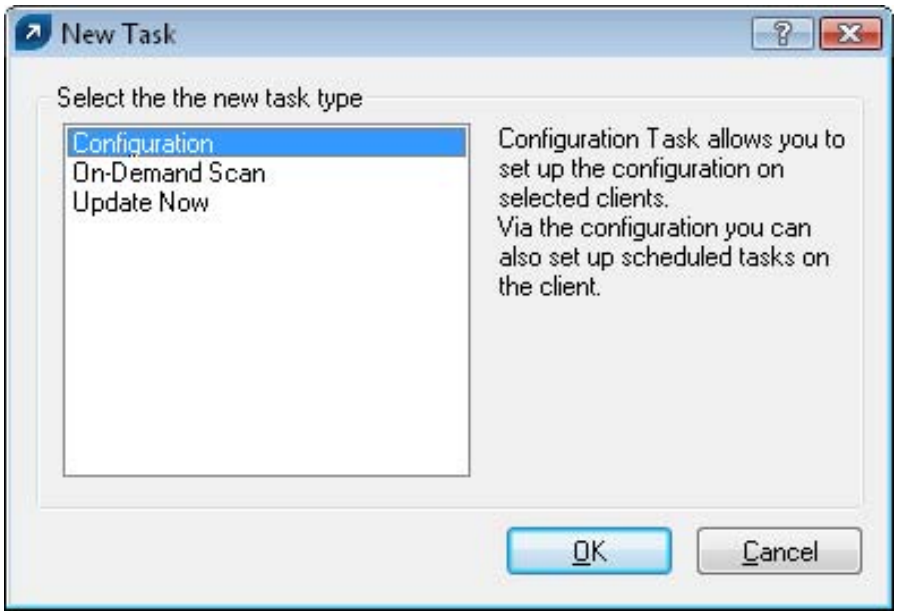


Figure 8
ERA propose 3 types de tâches

5.1 Tâche de Configuration

Cliquez sur le bouton 'Create...' afin de créer une nouvelle tâche (fichier .xml). Pour sélectionner un fichier de configuration existant, cliquez sur 'Select...'

NOTE : Les fichiers de configuration sont mutuellement compatibles quelle que soient leurs origines, ce qui signifie que vous pouvez utiliser un fichier .xml crée pour un package d'installation, téléchargé d'un client ou exporté localement (ex : depuis ESET Smart Security).

Les modifications des fichiers de configuration sont effectuées dans ESET Configuration Editor. Chaque paramètre qui sera modifié aura son icône en bleu. Afin de visualiser la configuration, cliquez sur le bouton 'View'. Pour modifier la configuration, cliquez sur 'Edit'.

Cliquez sur 'Create from Template...' afin d'ouvrir un fichier .xml existant et l'utiliser comme point de départ pour votre nouvelle configuration. Après modifications, le modèle restera inchangé.

Cliquez sur 'Next' et sélectionnez tous les clients (individuellement, par groupe ou serveur) sur lesquels le fichier .xml sera appliqué. Glissez les dans la colonne 'Selected items'. Pour ajouter des clients actuellement affichés dans la liste des clients, cliquez sur 'Add Special...', sélectionnez l'option 'Add clients loaded in the Clients pane' et cliquez sur le bouton 'Add'. Parmi les clients ajoutés depuis la liste des clients vous pouvez choisir des clients spécifiques en les sélectionnant depuis la colonne 'Servers' et en cochant l'option 'Only selected'.

Cliquez sur ‘Next’. L’étape finale consiste à donner un nom et une description à cette nouvelle tâche. Vous pouvez également dans cette même fenêtre indiquer si la tâche doit être différée (l’option ‘Apply task after’), ou encore automatiquement supprimée après que celle-ci ait été soumise avec succès sur les ordinateurs clients.

5.2 Tâche d’Analyse à la demande

Pour créer une tâche d’analyse à la demande, il est nécessaire d’indiquer sur quels ordinateurs clients celle-ci sera appliquée (il y a une légère différence technique dans la configuration des tâches d’analyse pour les générations 2.x et 3.x).

NOTE : La même tâche peut être utilisée à la fois pour les produits de génération 2.x et 3.x si les éléments On-demand Scan task for Windows NOD32 et On-demand Scan task for Windows ESET Security Product sont sélectionnés. Vous pouvez désactiver cette compatibilité en cochant la case ‘Exclude this section from On-Demand Scan’.

Pour effectuer une analyse sur un client avec ESET NOD32 version 2.x, sélectionnez ‘On-demand Scan task for Windows NOD32 version 2’ et procédez comme suit :

- Sélectionnez le profile à utiliser pour l’analyse – vous pouvez définir manuellement un nom qui n’est pas présent dans la liste.
- Sélectionnez les lecteurs à analyser (Drives to scan)
- Si besoins est, ajoutez un nouveau profile ou modifiez la configuration existante du profile (bouton Edit)
- Cliquez sur ‘Next’ afin de sélectionner les clients sur lesquels la tâche sera appliquée.
- Cliquez sur ‘Finish’

NOTE : L’analyse à la demande sur les clients utilisera le profile défini ainsi que la configuration définie dans le fichier .xml (bouton ‘Edit’). Le profile sera modifié temporairement sur le client, le temps d’exécution de la tâche.

L’option ‘The Scan without cleaning’ se réfère aux options ‘Analyser’ et ‘Nettoyer’ du module NOD32 dans ESET NOD32 for Windows 2.x. La différence entre ces deux options est la suivante :

- Scan without cleaning activé : aucune action ne sera effectuée sur les éléments infectés; un journal sera crée.
- Scan without cleaning désactivé : une action sera menée en fonction de la configuration définie pour les menaces nettoyables et non nettoyables.

Pour effectuer une analyse sur un client avec une solution de la génération 3.x sur l’ordinateur client (ESET Smart Security ou ESET NOD32 Antivirus), alors sélectionnez ‘On-demand Scan task for Windows ESET Security Product’ et procédez comme suit :

- Sélectionnez le profile à utiliser pour l’analyse – vous pouvez définir manuellement un nom qui n’est pas présent dans la liste.
- Sélectionnez les lecteurs à analyser (Drives to scan), ou indiquez des répertoires spécifiques (Add path).
- Cliquez sur ‘Next’ afin de sélectionner les clients sur lesquels la tâche sera appliquée.
- Cliquez sur ‘Finish’.

5.3 Tâche Mettre à jour maintenant

Pour exécuter une tâche de mise à jour, il est nécessaire d’indiquer sur quels ordinateurs clients celle-ci sera appliquée (il y a une légère différence technique dans la configuration des tâches pour les générations 2.x et 3.x).

La même tâche peut être utilisée à la fois pour les produits de génération 2.x et 3.x si les éléments On-demand Scan task for Windows NOD32 et On-demand Scan task for Windows ESET Security Produc sont sélectionnés. Vous pouvez désactiver cette compatibilité en cochant la case ‘Exclude this section from On-Demand Scan’.

Les étapes suivantes sont similaires pour les 2 versions du programme :

- Sélectionnez le profile à utiliser (Profile name) – Vous pouvez spécifier un nom non présent dans la liste. Il n’est généralement pas nécessaire de définir un profile spécifique (laissez l’option ‘Specify profile name’ désactivée).
- Cliquez sur ‘Next’ afin de sélectionner les clients sur lesquels la tâche sera appliquée.
- Cliquez sur ‘Finish’

NOTE : Les solutions de sécurité ESET (ESET NOD32 Antivirus, ESET Smart Security...) incluent par défaut une tâche de mise à jour automatique. La tâche ‘Update Now’ est donc une solution complémentaire et ponctuelle.

6. Installation des solutions clientes ESET

Ce chapitre est dédié à l'installation (directe et à distance) des solutions clientes pour les systèmes d'exploitation Microsoft Windows.

NOTE: Bien que cela soit techniquement faisable, nous recommandons de n'utiliser l'installation à distance des produits ESET que sur les stations de travail et non sur les serveurs.

6.1 Paramètres de ligne de commande pour une installation directe des solutions clientes

Plusieurs paramètres peuvent affecter le processus d'installation. Ils peuvent être utilises soit pour une installation directe ou alors lors d'une installation à distance. Pour l'installation à distance, les paramètres sont définis durant la configuration du package d'installation – les paramètres seront alors automatiquement appliqués sur les clients cibles.

Les paramètres additionnels pour ESET Smart Security et ESET NOD32 Antivirus doivent être inscrits après le nom du package d'installation .msi (ex : ea_nt64_ENU.msi /qn):

- **/qn**
  Mode d'installation silencieux– aucune fenêtre ne sera affichée

- **/qb!**
  Aucune intervention possible, mais le processus d'installation sera visible dans une barre de progression

- **REBOOT="ReallySuppress"**
  Inhibe le redémarrage après l'installation du programme

- **REBOOT="Force"**
  Redémarre automatiquement après l'installation

- **REBOOTPROMPT =" "**
  Après l'installation, une fenêtre s'affichera demandant à l'utilisateur de redémarrer l'ordinateur (ne peut pas être utilisé avec /qn).

- **ADMINCFG="path_to_xml_file"**
  Lors de l'installation, les paramètres définis dans un fichier .xml seront appliqués. Le paramètre n'est pas requis pour une installation à distance, le package d'installation comporte son propre fichier de configuration qui sera automatiquement appliqué.
  Les paramètres pour ESET NOD32 Antivirus version 2.x Antivirus doivent être inscrits après le fichier setup.exe, qui peut être extrait du package d'installation avec les autres fichiers (ex : setup.exe /silentmode):

- **/SILENTMODE**
  Mode d'installation silencieux– aucune fenêtre ne sera affichée.

- **/FORCEOLD**
  Force l'installation par dessus une version plus récente.

- **/CFG=" path_to_xml_file"**
  Lors de l'installation, les paramètres définis dans un fichier .xml seront appliqués. Le paramètre n'est pas requis pour une installation à distance, le package d'installation comporte son propre fichier de configuration qui sera automatiquement appliqué.

- **/REBOOT**
  Redémarre automatiquement après l'installation.

- **/SHOWRESTART**
  Après l'installation, une fenêtre s'affichera demandant à l'utilisateur de redémarrer l'ordinateur.

- **/INSTMFC**
  Installe les librairies MFC requise pour le système d'exploitation Microsoft Windows 9x. Ce paramètre peut être toujours utilisé même si les librairies MFC sont présentes.

6.2 Méthodes d'installation

6.2.1 Installation directe avec une configuration XML prédéfinie

Cette méthode ne demande pas de préparation et peut être utilisée avec de petits réseaux, ou alors si ESET Remote Administrator n'est pas utilisé.

Cette tâche peut cependant être grandement simplifiée par l'utilisation d'un fichier de configuration .xml prédéfini. Dans ce cas, aucun élément ne sera alors à configurer pendant ou après l'installation, tels que la définition des mises à jour (nom d'utilisateur / mot de passe, chemin vers le miroir, etc.), le mode silencieux, les analyses planifiées, etc.

L'application de ce fichier .xml est différente en fonction de l'utilisation de la version 3.x ou 2.x des solutions de sécurité ESET :

- Version 3.x: Téléchargez le fichier d'installation depuis le site d'ESET (ex : ess_nt32_enu.msi). Placez le fichier de configuration .xml (cfg.xml) dans le répertoire où se trouve le fichier d'installation. Lorsque vous lancer l'installation, il utilisera la configuration contenue dans le fichier.xml. Si ce dernier porte un autre nom ou se trouve dans un répertoire différent, le paramètre ADMINCFG="path_to_xml_file" sera à utiliser.

  (Ex: ess_nt32_enu.msi ADMINCFG="\\server\xml\settings.xml" pour utiliser la configuration se trouvant sur un répertoire réseau).

- Version 2.x: Téléchargez le fichier d'installation depuis le site d'ESET (ex : ndntenst.exe). Il faut ensuite extraire les fichiers dans un répertoire. Ce répertoire contiendra les fichiers d'installation, dont le fichier setup.exe. Copiez le fichier de configuration .xml configuration, que vous nommerez nod32.xml, dans ce répertoire. Exécutez le fichier setup.exe et la configuration du fichier nod32.xml sera automatiquement appliquée. Si le fichier .xml porte un autre nom ou se trouve dans un répertoire différent, le paramètre /cfg="path_to_xml_file" sera à utiliser.

  (Ex: setup.exe /cfg="\\server\xml\settings.xml" pour utiliser la configuration se trouvant sur un répertoire réseau).

NOTE : Les autres paramètres mentionnés précédemment peuvent également être utilisés.

6.2.2 Installation à distance en général

ESET Remote Administrator propose plusieurs méthodes d'installation à distance, listées ci-dessous. Les méthodes diffèrent dans la façon par laquelle le package est envoyé aux stations clientes.

- Remote push installation
- Logon script remote installation
- Email remote installation

Une installation à distance n'a pas nécessairement besoin d'être réalisée par les outils ERA – D'autres méthodes sont également disponibles (Distribution centralisée MSI, LANDesk, etc.). A final, le plus important est d'apporter le fichier d'installation (ou agent) aux clients, et de s'assurer que celui-ci est exécuté avec un compte d'administration. Pour cela, l'installation directe comme décrite précédemment peut également être utilisée.
L'installation à distance selon ESET consiste en :

- Création de packages d'installation
- Distribution des packages sur les stations clientes (push installation, logon script, e-mail, solution externe)

La première étape est réalisée avec la Console ERA, mais le package lui-même se trouve sur le Serveur ERA, dans le répertoire: *%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\packages*

Pour créer un package d'installation, allez dans l'onglet 'Remote Install' et cliquez sur le bouton 'Packages...'.
Chaque package d'installation est défini par un nom (voir (1) dans l'image 9). Les autres parties de cette fenêtre correspondent au contenu du package. Chaque package comporte :

- Fichiers d'installation (2) des solutions ESET
- Fichier de configuration.xml (3)
- Paramètre de ligne de commande (4)

La liste déroulante (1) étant les possibilités de ERA. En plus de l'installation à distance, les solutions clientes ESET peuvent être désinstallées à distance en sélectionnant 'Uninstall ESET Security Products and NOD32 version 2'. L'installation à distance d'une application externe peut également être configurée, en sélectionnant 'Custom package'.

NOTE : Pour des raisons techniques, l'installation des solutions ESET antérieures (version 2.x) est une fonction séparée de l'installation des solutions de la génération 3.x. Pour les mêmes raisons, les packages sont stockés dans des répertoires différents dans ERAS.

NOTE : L'option 'Custom package' offre une de nombreuses possibilités telles que la désinstallation de solutions de sécurité d'autres éditeurs (si une ligne de commande adéquate est utilisée).

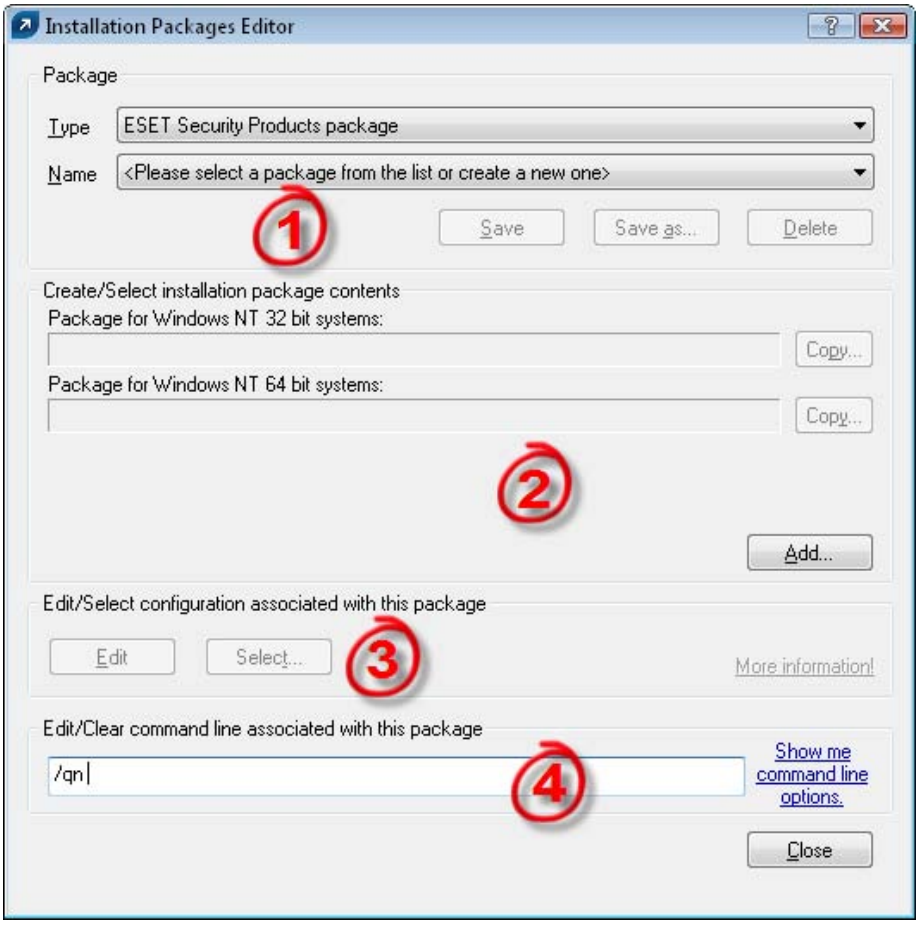


Figure 9
Fenêtre de dialogue de l'éditeur de packages d'installation

A chaque package est assigné un agent 'ESET Remote Installer', permettant l'installation et la communication entre la station cible et ERAS. Cet agent est nommé 'einstaller.exe' et comporte le nom du Serveur ERA, ainsi que le nom et le type de package dont il fait parti. Le chapitre suivant fournit une description détaillée de l'agent.

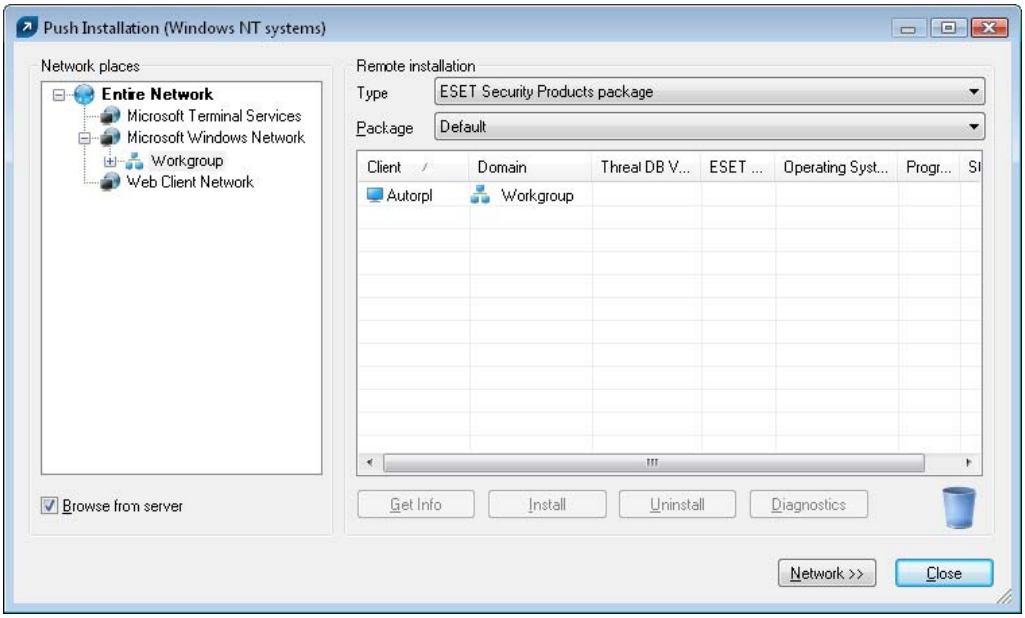
6.2.3 Installation par la méthode "push"

Cette méthode d'installation à distance pousse la solution cliente ESET sur les ordinateurs cibles. Ces ordinateurs doivent être en ligne. Voici également une liste d'éléments requis (voir le chapitre 2 "ERAS" pour plus d'éléments) :

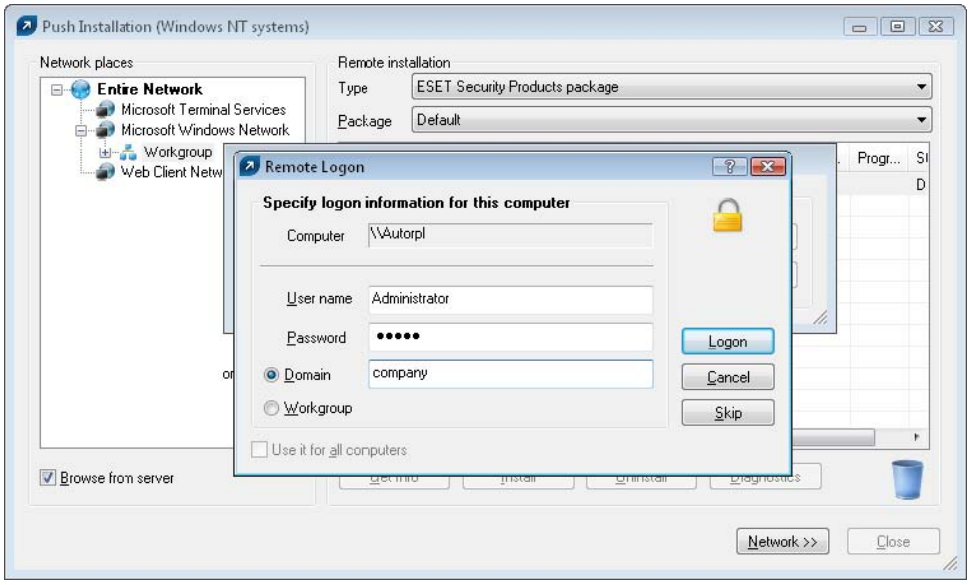
- Client réseau Microsoft activé (fonctionnalité de l'adaptateur réseau)
- Service de partage de fichiers activé (fonctionnalité de l'adaptateur réseau)
- Partage de fichiers autorisé sur le pare-feu
- Services: Accès à distance au registre, Remote Service Manager, Serveur
- Compte administrateur (nom d'utilisateur et mot de passe) pour la station cliente (de préférence, le compte administrateur du domaine).

Pour démarrer une installation par la méthode push, procédez comme suit :

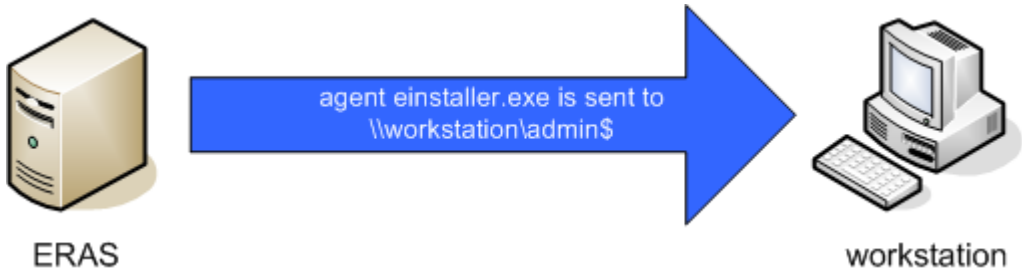
1) Cliquez sur le bouton 'Install...' dans la console ERA (onglet Remote Install).
2) Naviguez dans la partie 'Network places' à gauche, afin de trouver les stations sur lesquelles vous désirez installer le package. Déplacer-les vers la partie de droite (utilisez la méthode glisser/déplacer).
3) Sélectionnez le package à installer dans la liste déroulante.



4) Dans la liste de droite, sélectionnez les stations sur lesquelles va être installé le package.
5) Cliquez sur ‘Install’ (vous pouvez également cliquer sur ‘Get Info’ pour avoir des informations sur les clients).
6) Dans la plupart des cas, il vous sera demandé de saisir le nom d’utilisateur et le mot de passe du compte à utiliser pour effectuer l’installation (ce doit être un compte avec des droits administrateur).

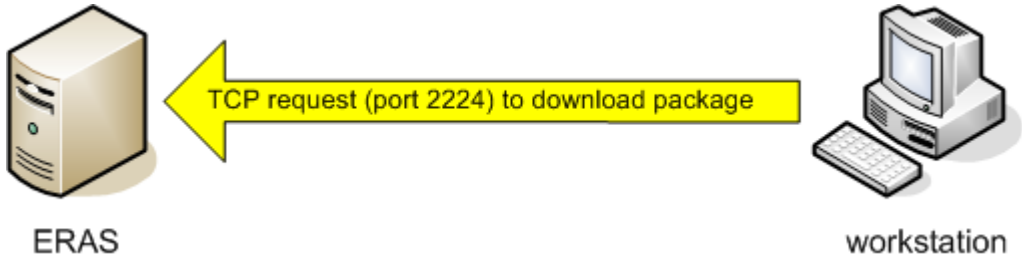


7) Les opérations suivantes sont indiquées par une barre de progression et un message. Ces opérations sont :
8) ERAS envoie l’agent einstaller.exe vers la station cible avec le partage administratif admin$.

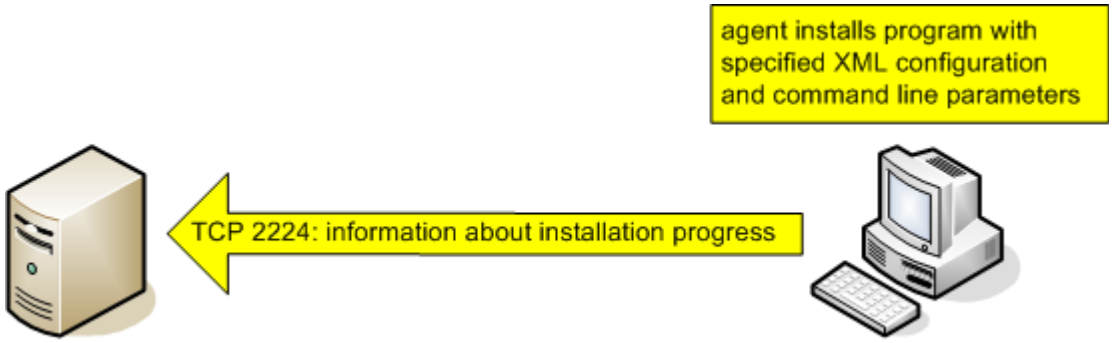


9) L'agent démarre en tant que service avec le compte spécifié à l'étape 6.

10) L'agent établi une communication avec son Serveur ERA 'mère' et télécharge le package correspondant par le port 2224.



11) L'agent installe le package avec le compte administrateur défini à l'étape 6; Le fichier .xml ainsi que les paramètres de ligne de commande correspondants seront appliqués.



12) Immédiatement après que l'installation soit terminée, l'agent renvoie un message à ERAS. Certaines solutions ESET nécessitent un redémarrage. Si tel est le cas, il y aura un message l'indiquant.

Le menu contextuel dans la fenêtre d'installation comporte les options suivantes :

- **Get Info**
  Permet de détecter le statut actuel de la solution cliente ESET sur la station cible (nécessite un compte administrateur). Cette fonctionnalité utilise le partage admin$.

- **Uninstall**
  Suppression du programme – l'agent va essayer de désinstaller à distance le programme. Ce mode ne prend pas en compte le package sélectionné dans la liste déroulante.

- **Diagnostics**
  Vérifie la disponibilité des clients et services qui seront utilises pour faire l'installation à distance. Pour plus d'informations, voir ci-après.

- **Remove Installer Leftovers**
  Supprime l'agent du gestionnaire de services sur la station cliente et le supprime du disque dur. Si ceci est réalisé avec succès, alors la balise permettant d'empêcher de multiples installations du package est enlevée (voir la section 6.4, "Empêcher les installations répétées").

- **Logon...**
  Ouvre la fenêtre permettant de spécifier le compte administrateur (sinon cette fenêtre s'affiche automatiquement - étape 6). Cette fonctionnalité force la connexion sur les stations.

- **Logoff**
  Déconnecte la session pour les stations sélectionnées.

- **Add Client...**
  Ajoute des clients dans la liste. Saisissez l'adresse IP ou le nom du client. Plusieurs clients peuvent être ajoutés simultanément.

6.2.4 Installation à distance par Logon / email

Les installations à distance de type Logon et email sont très similaires. Elles diffèrent uniquement dans la manière dont le l'agent einstaller.exe est envoyé aux clients. L'agent peut également être utilisé individuellement et exécuté par d'autres méthodes (voir le chapitre suivant pour plus de détails).

Tandis que le logon script s'exécute automatiquement, la méthode par email nécessite une intervention de la part de l'utilisateur, qui doit exécuter l'agent einstaller.exe joint au mail. S'il est lancé plusieurs fois, l'agent ne va pas déclencher une nouvelle installation des solutions ESET. Pour plus d'informations, voir la section 6.4, "Empêcher les installations répétées".

NOTE : La ligne appelant l'agent einstaller.exe depuis le logon script peut être insérée en utilisant un éditeur de texte ou tout autre outil spécifique. De même, l'agent peut être envoyé par email par n'importe quel client mail. Quelle que soit la méthode utilisée, assurez-vous d'utiliser le bon fichier einstaller.exe.

NOTE : Pour être exécuté, l'agent ne nécessite pas que l'utilisateur actuellement connecté soit un administrateur. Il utilise le mon d'utilisateur /mot de passe / domaine depuis ERAS. Pour plus d'informations, voir à la fin de ce chapitre.

Insertion de la ligne dans le logon script :

- Cliquez sur le bouton 'Export...' et sélectionnez le type et le nom du package devant être installé.
- Cliquez sur le bouton '... ' à côté de 'Folder' et sélectionnez le répertoire dans lequel einstaller.exe se trouvera et sera disponible sur le réseau.
- Dans le champ 'Share' assurez-vous que le chemin est correct, modifiez-le si nécessaire
- Cliquez sur le bouton '... ' à côté de 'Script Folder' pour sélectionner le répertoire dans lequel se trouve le script.
- Dans la partie inférieure, sélectionnez le fichier dans lequel la ligne (appelant einstaller.exe) sera insérée.
- Cliquez sur 'Export to Logon Script' pour y insérer la ligne.
- La position de la ligne peut être modifiée dans un mode avancé en cliquant sur 'Edit' et en sauvant avec le bouton 'Save'.

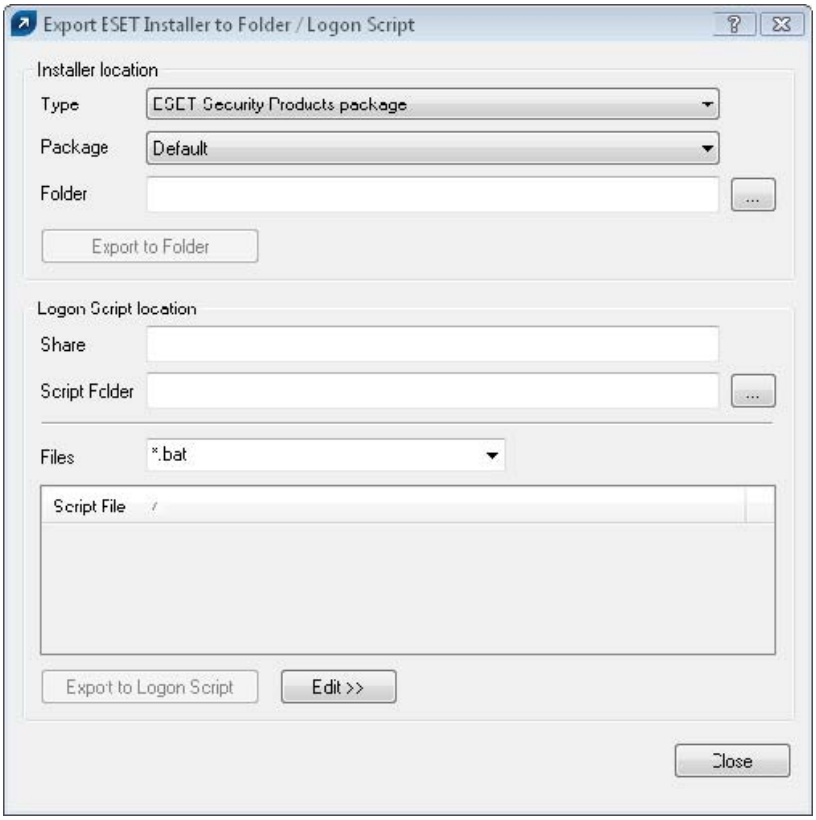


Figure 10
Fenêtre d'exportation vers un répertoire / script de connexion

Attacher l'agent (einstaller.exe) à un email :

- Cliquez sur 'Email...' et sélectionnez le type et le nom du package devant être installé.
- Cliquez sur 'To...' pour sélectionner les adresses dans le carnet d'adresses [3] (ou insérez les manuellement).
- Inscrivez un subject dans le champ correspondant.
- Inscrivez un message dans le champ 'Body'.
- Cliquez sur 'Send' afin d'envoyer le message.

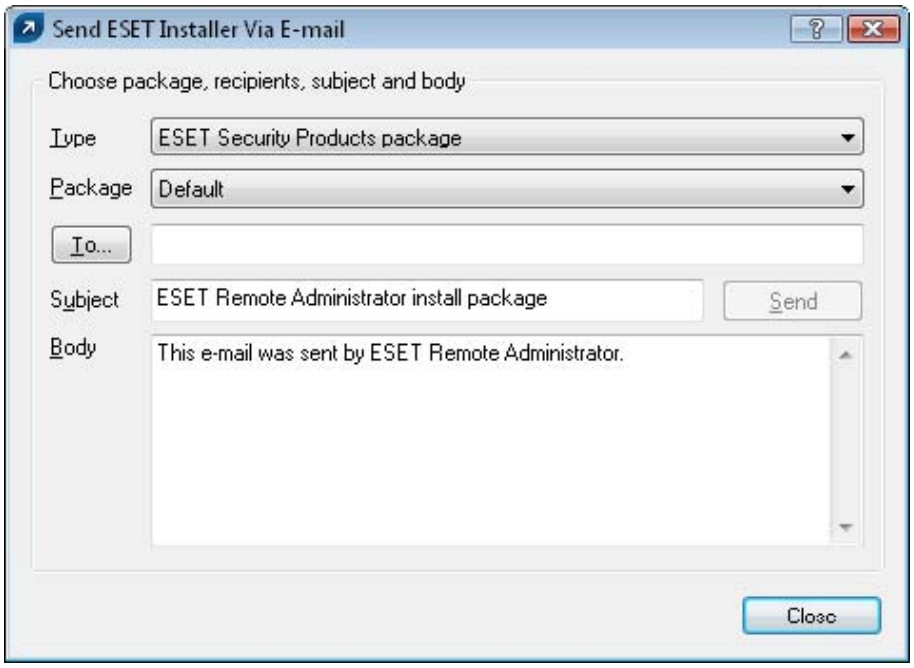


Figure 11
Fenêtre permettant d'envoyer l'agent par email

3. La console ERA ouvre le carnet d'adresses Microsoft Outlook (sous réserve que celui-ci soit installé sur le même ordinateur que ERAC.

Lors du processus d'installation à distance, une connexion est établie vers ERAS et l'agent (einstaller.exe) adopte les paramètres définis dans la partie 'Set Default Logon for E-mail and Logon Script', dans l'onglet 'Remote install'

Cliquez sur 'Logon...' pour indiquer le nom d'utilisateur et le mot de passe du compte qui sera utilisé pour effectuer l'installation du package. Ce doit être un compte avec des droits administrateur ou, de préférence, un compte administrateur du domaine).

NOTE : Les valeurs insérées à cet endroit sont supprimées à chaque redémarrage du service (ERAS).

6.2.5 Installation à distance personnalisée

Il n'est pas nécessaire d'utiliser les outils incorporés dans ESET Remote Administrator. Le plus important est de fournir et d'exécuter le fichier einstaller.exe sur les stations.

NOTE: Pour être exécuté, l'agent ne nécessite pas que l'utilisateur actuellement connecté soit un administrateur. Il utilise le mon d'utilisateur /mot de passe / domaine depuis ERAS. Pour plus d'informations, voir à la fin de ce chapitre.

Le fichier einstaller.exe peut être obtenu comme suit :

- Depuis l'onglet Remote Install, cliquez sur 'Export...' et sélectionnez le type et nom du package devant être installé
- Cliquez sur le bouton '...' à côté de 'Folder' et choisissez le répertoire dans lequel exporter le fichier.
- Cliquez sur le bouton 'Export'
- Vous pouvez utiliser le fichier einstaller.exe

NOTE : La méthode "Direct installation with predefined XML configuration" peut être utilisée dans les cas où il est possible de donner les droits d'administration pour l'installation. Le package MSI est lancé en utilisant le paramètre /qn (pour la version 3) ou le paramètre /silentmode (pour la version 2), ce qui lancera l'installation sans afficher d'interface utilisateur.

Durant le processus 'installation à distance, une connexion vers ERAS est établie et l'agent (einstaller.exe) adopte les paramètres d'utilisateur définis dans la partie 'Set Default Logon for E-mail and Logon Script settings' de l'onglet 'Remote Install'.

Cliquez sur 'Logon...' afin de définir le nom d'utilisateur et le mot de passé du compte utilisé pour effectuer l'installation du package. Ce doit être un compte avec les droits d'administration, ou, préférentiellement, le compte de l'administrateur du

domaine.

Si l'agent einstaller.exe est exécute manuellement sur la station cliente, l'installation se déroulera comme suit :

- L'agent envoie une requête à ERAS (sur le port TCP 2224)
- ERAS démarre l'installation à distance du package correspondant (envoyé via le partage admin$)
- L'installation du package est lancée, en appliquant le fichier de configuration .xml et les paramètres de ligne de commande, avec le compte utilisateur spécifié dans ERAS voir ci-dessus)

6.3 L'agent einstaller.exe en détail

A chaque package est automatiquement assigné un agent, ESET Remote Installer agent, permettant l'installation et la communication entre la station cible et le Serveur ERA. Cet agent et nommé einstaller.exe et continent les informations suivantes :

- Nom du Serveur ERA (+ adresse IP du ERAS)
- Nom et type du package d'installation

L'installation à distance utilisant l'agent einstaller.exe se déroule en deux phases. Premièrement, le petit installeur einstaller.exe (environ 200 KB) est envoyé à la station. Si tous les pré-requis sont bons, alors l'agent démarre le téléchargement du package d'installation complet (plusieurs MB) depuis ERAS.
L'activité de l'agent einstaller.exe est journalisée dans le fichier %TEMP%\einstaller.log et est renvoyé si cela est techniquement possible au Serveur ERA (port cible : TCP 2224).

Si l'agent einstaller.exe est exécuté sur une station avec comme système d'exploitation Microsoft Windows NT4/2000/XP/Vista :

1.einstaller.exe contacte ERAS sur le port TCP 2224 et utilise le nom d'utilisateur et le mot de passe définis dans ERA (soit lors de l'installation, soit avec le bouton 'Logon...').

2.(1) est le signal pour ERAS pour envoyer le package d'installation correspondant via admin$.

3.einstaller.exe récupère le package et démarre l'installation en utilisant le compte défini, appliquant la configuration .xml et les paramètres de ligne de commande.

Si les droits d'utilisateur sont insuffisants, ou que le nom d'utilisateur ou le mot de passe ne sont pas saisis correctement, einstaller.exe essaye de procéder à l'installation avec l'utilisateur courant (si il a les droits d'administration). Le package d'installation correspondant est téléchargé directement par einstaller.exe sur le port TCP/IP 2224.

Sur les systèmes d'exploitation Windows 95/98/Me, où il n'y a pas de hiérarchie de compte, les packages d'installation sont téléchargés par einstaller.exe (en s'affranchissant du processus d'authentification) et installés avec le compte utilisateur courant.

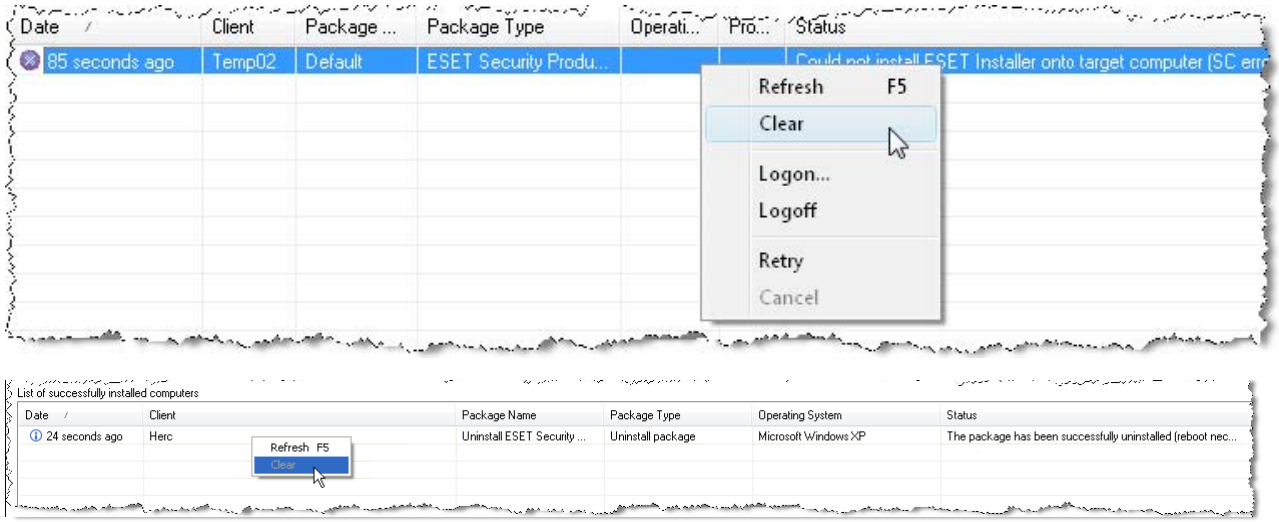
6.4 Empêcher les installations répétées

Immédiatement après que le processus d'installation à distance soit terminé, l'agent pose une "balise" sur le client empêchant l'installation répétés du même package d'installation. Cette balise est située dans la clé de registre suivante:
HKEY_LOCAL_MACHINE\Software\Eset\Eset Remote Installer

Si le type et le nom du package définis dans l'agent einstaller.exe correspondent avec la donnée dans la base de registre, alors aucune autre installation ne sera effectuée. Ceci permet d'éviter les installations répétées sur le client si l'agent est exécuté plusieurs fois.

Le Serveur ERA fournit un niveau supplémentaire de protection contre les installations répétées. Ceci est réalisé lorsque l'agent se connecte sur ERAS. Si il y a eu un message d'erreur en provenance de la station ou si l'installation est réalisée avec succès, toute autre tentative d'installation sera refusée.

L'activité de l'agent einstaller.exe est journalisée dans le fichier installer log situé dans %TEMP%\einstaller.log:
Status 20001: ESET Installer was told to quit by the server 'X:2224'.



Pour éviter que l'installation soit interdite niveau de ERAS, il faut supprimer la ligne correspondante dans l'onglet 'Remote Install'. Pour ceci, faite un clic droit sur la ligne et sélectionner 'Clear' dans le menu contextuel.

6.5 Processus d'installation – messages d'erreur

Lors de l'installation à distance, des erreurs peuvent se produire dans les 2 cas suivants :

- Lors de la distribution de l'agent einstaller.exe à la station distante
- Lors du lancement du service einstaller.exe, c-à-d durant l'installation elle-même

Lors de l'installation il se peut que l'agent affiche un message, constitué de code SC et GLE.

Par exemple : Could not set up IPC connection to target computer (SC error code 6, GLE error code 1326)

Les codes SC sont des codes d'identification internes. Les codes GLE sont plus importants pour l'utilisateur. Ils correspondent aux codes "Win32 Error Codes", que vous pouvez trouver à l'adresse :

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system_error_codes.asp

L'exemple ci-dessus – GLE error 1326 – est causé par un mon d'utilisateur ou mot de passe incorrect pour le compte utilisé lors de l'installation.

L'erreur la plus courante est GLE error 5 – Access Denied. Il peut y avoir plusieurs raisons pour interdire l'accès :

- Le pare-feu sur la station cliente peut avoir le partage de fichiers et d'imprimantes désactivé
- The service Server est désactivé, ou le partage de fichier et d'imprimante sur le réseau est désactivé
- La station cliente Windows XP n'est pas dans le domaine (policy)

Si des erreurs surviennent, elles sont reportées dans le fichier %TEMP%\einstaller.log. Les messages les plus importants sont renvoyés au Serveur ERA (TCP 2224). Bien évidemment, cela ne peut se faire que s'il n'y a pas de problème de communication entre la station et ERAS.

Vous pouvez rencontrer les messages suivants à cette phase de l'installation :

- Eset Installer was told to quit by the server 'X:2224'.
- Eset Installer could not connect to server X.

Le premier message est décrit au chapitre 6, " Empêcher les installations répétées". Le second message est un problème général indiquant que einstaller.exe n'a pas été capable de se connecter au serveur ERAS.

6.5.1 Diagnostique d'installation à distance

Pour utiliser l'outil diagnostique d'installation, cliquez sur le bouton 'Install...' dans l'onglet 'Remote Install'. Après avoir sélectionné le client, cliquez sur le bouton 'Diagnostics' afin de s'assurer qu'aucune erreur ne sera détectée et que le processus d'installation sera réalisé avec succès. L'administrateur pourra ainsi résoudre les erreurs détectées avant de procéder à l'installation.

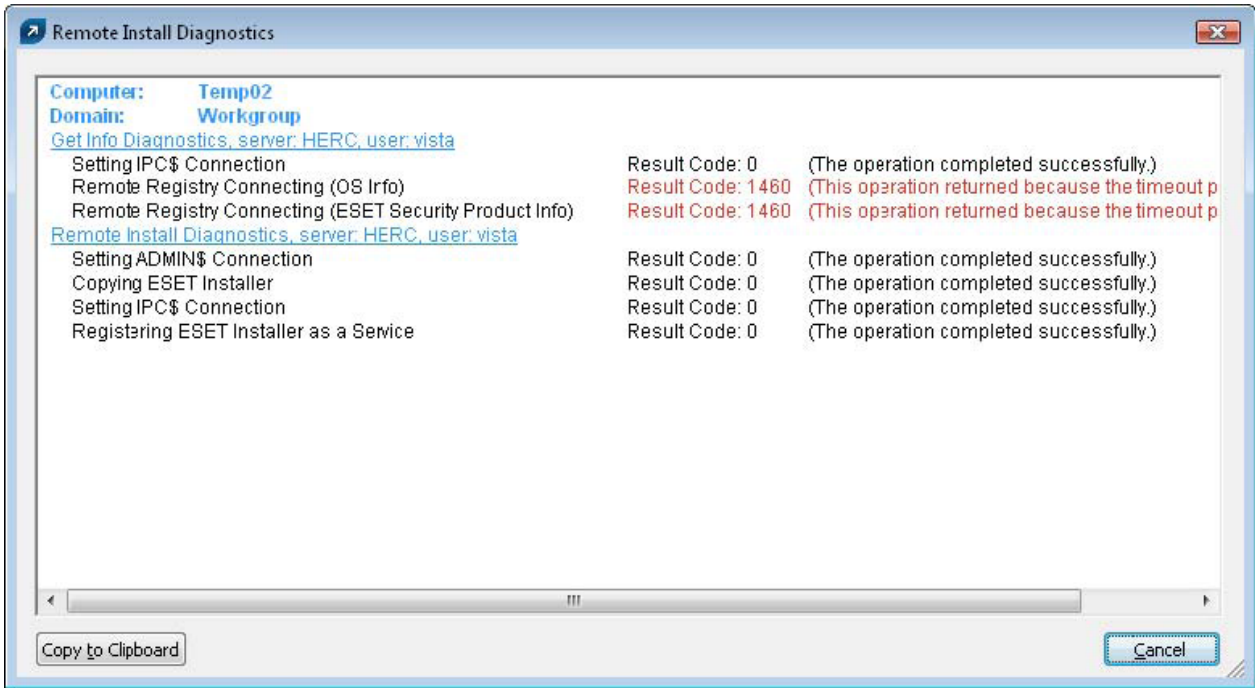


Figure 12
L'outil de diagnostic permettant de détecter d'éventuels problèmes avant l'installation

7. Scenario de déploiement pour ESET Remote Administrator, Serveur Miroir et Clients ESET

7.1 Petit réseau – 1x ERAS, 1x Serveur Miroir

En supposant que tous les clients sont des stations de travail et des ordinateurs portables fonctionnant sous Microsoft Windows 2000/XP et en réseau dans un domaine. Le serveur, nommé GHOST est en ligne 24/7 et peut être une station Windows, Professional, ou Server Edition (Il n'est pas nécessaire que ce soit un serveur Active Directory). De plus, supposons que les ordinateurs portables ne soient pas présents dans l'entreprise lors de l'installation des solutions client ESET. La structure du réseau pourrait ressembler à celle représentée ci-dessous :

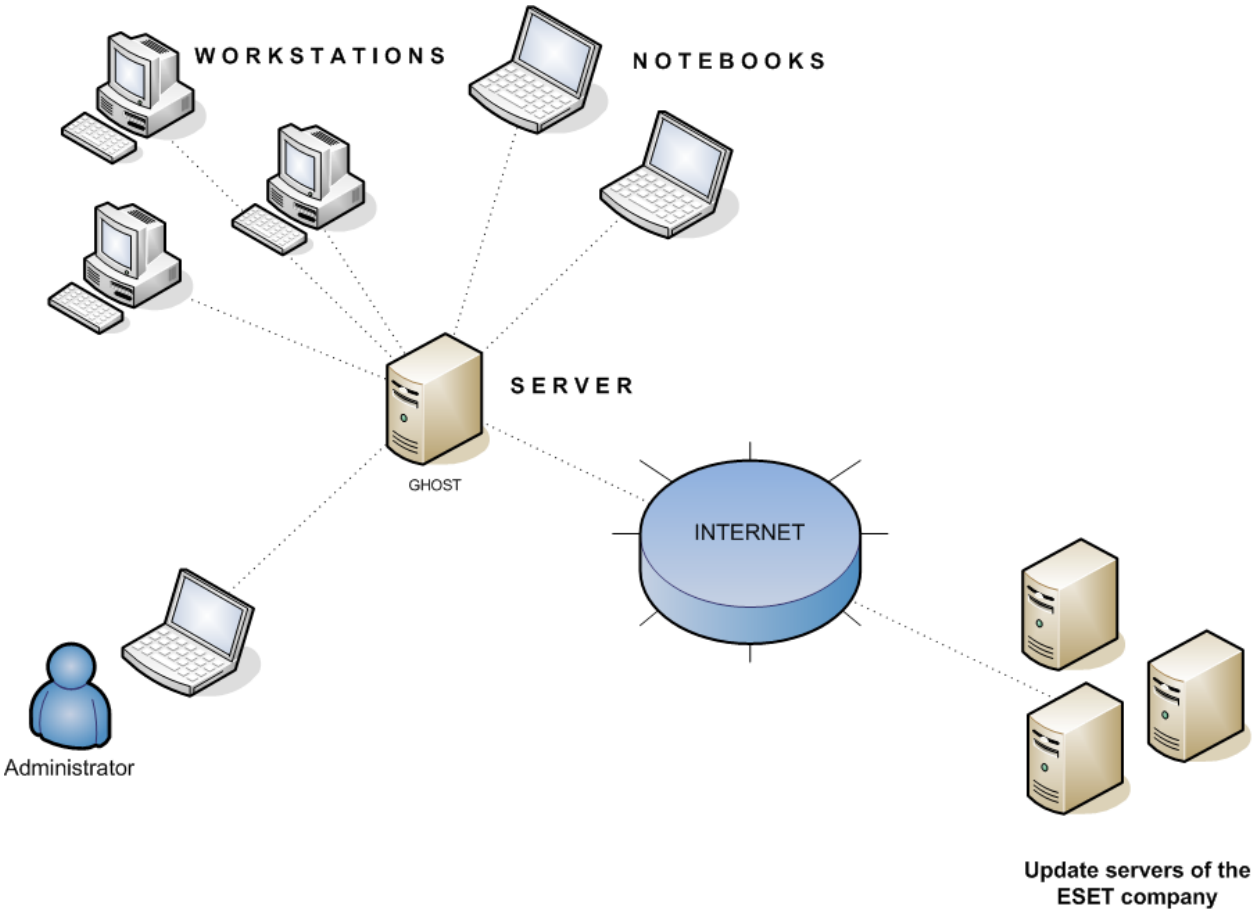


Figure 13
Structure réseau dans une petite entreprise

7.1.1 Installation du serveur Miroir HTTP

La première étape est l'installation d'un serveur miroir sur la machine nommée GHOST. Le package contenant cette fonctionnalité doit être installé (ESET Smart Security Business Edition ou ESET NOD32 Antivirus Business Edition). Lors de l'installation, inscrivez le nom d'utilisateur et le mot de passe obtenu lors de l'achat de votre licence – ce sont vos données d'authentification vous permettant le téléchargement des mises à jour des signatures virales. La prochaine étape est l'ajout de la licence au système. Ouvrez la fenêtre d'options avancées en appuyant sur F5. Dans l'arborescence, allez dans Miscellaneous > Licenses et cliquez sur le bouton 'Add...'. Ajoutez alors le fichier de licence .lic. La fonctionnalité de miroir est alors activée. Vérifiez que le miroir apparaît bien dans les paramètres avancés de mise à jour. Cliquez sur Update, puis sur le bouton 'Setup…' – l'onglet correspondent au miroir devrait alors être visible. Cliquez sur celui-ci et effectuez les modifications suivantes afin de configurer le miroir :

- Cochez la case 'Create update mirror'
- Cochez la case 'Select the Provide update files via internal HTTP server'
- Sélectionner le répertoire dans lequel vont être placés les fichiers de mise à jour (ex : C:\ESET)

- Dans la partie ‘Available versions’, sélectionnez les composants pour les systèmes d’exploitation que recevrons les mises à jour depuis le miroir. Si seules des stations Microsoft Windows 2000/XP/2003/Vista vont recevoir les mises à jour, alors sélectionnez uniquement ces systèmes dans la liste.
- Cliquez sur OK pour sauvegarder les paramètres.
- Maintenant, effectuez une mise à jour de la base de signatures virales en cliquant sur ‘Update > Update virus signature database’ depuis la fenêtre principale. Tous les fichiers nécessaires seront alors téléchargés dans le répertoire indiqué (ex : C:\ESET), et le miroir sera activé.

7.1.2 Installation du Serveur ERA

Nous recommandons d’installer le serveur ERA sur le même ordinateur que celui configuré pour le miroir – GHOST, dans notre exemple. Lors de l’installation, le fichier de licence (.lic) doit être fourni afin d’activer ERAS. Suite à l’installation, le service ERAS est démarré automatiquement. L’activité du service est journalisée dans le fichier suivant :
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\logs\era.log

7.1.3 Installation de la Console ERA

Installez ESET Remote Administrator Console sur l’ordinateur de l’administrateur. Si la console est installée sur le même ordinateur que ERAS, le nom du serveur ERAS (GHOST, dans notre exemple) devrait être automatiquement mis dans les paramètres de la console. Si la console et ERAS sont installés sur des ordinateurs différents, alors cliquez sur ‘File > Edit Connections...’ puis cliquez sur l’onglet ‘Connection’. Cliquez sur le bouton ‘Add/Remove...’ pour ajouter le nom du serveur ERA.

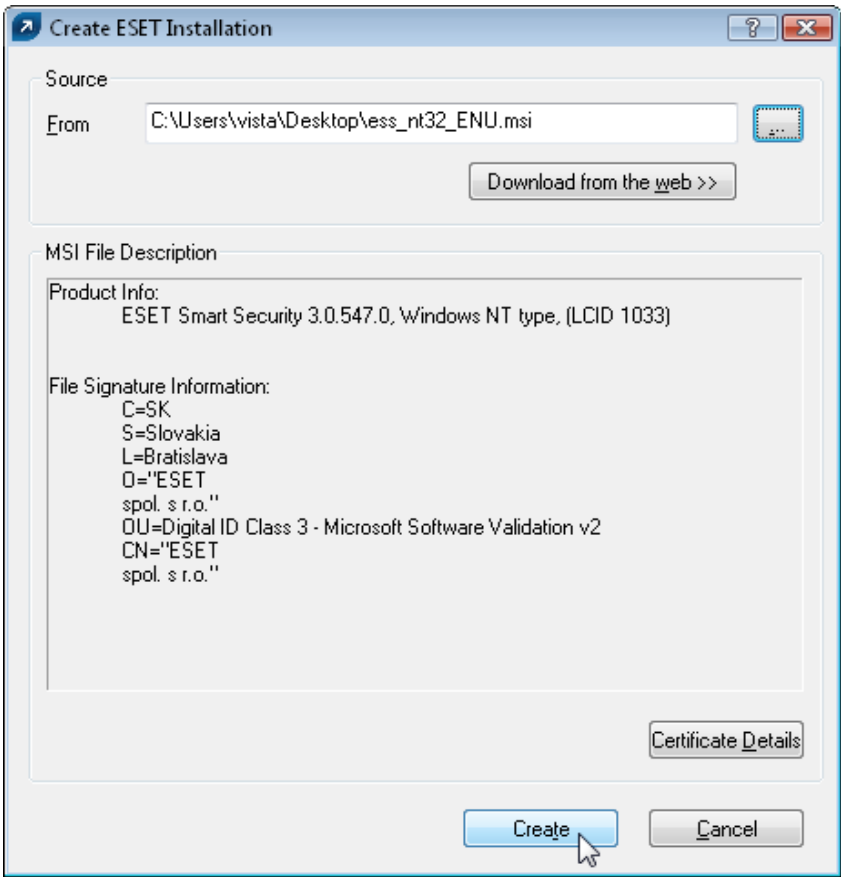
Pour plus d’information, voir la section 4.1, “Connecting to ERAS”).

7.1.4 Installation à distance sur les stations de travail présentes sur le réseau

En supposant que toutes les stations de travail sont allumées, la méthode d’installation ‘ push’ est alors la plus efficace. Avant de démarrer cette installation, vous devez télécharger les fichiers d’installation .msi pour ESET Smart Security ou ESET NOD32 Antivirus depuis le serveur web de ESET. Puis procédez comme suit :

- Ouvrez la console ERA et connectez-vous sur le serveur ERAS (GHOST, dans notre exemple). Dans l’onglet ‘Remote Install’, cliquez sur le bouton ‘Packages...’.

- Cliquez sur ‘Add...’ pour afficher la fenêtre ‘Create ESET Installation’, puis cliquez sur le bouton ‘...’ pour insérer le fichier .msi téléchargé auparavant.

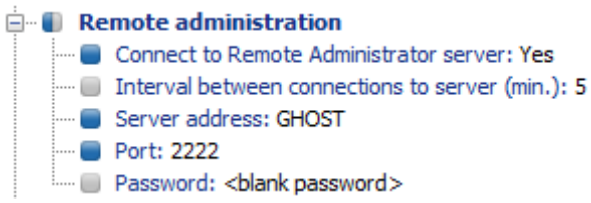


- Cliquez sur ‘Create’ afin de mettre le fichier d’installation dans le package (cela peut prendre quelques minutes pour que le fichier .msi soit incorporé).

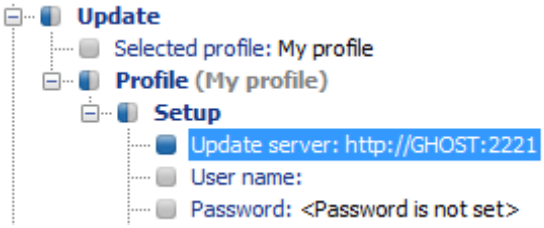
- Cliquez sur ‘Edit’ dans la fenêtre ‘Installation Packages Editor’ afin d’assigner un fichier de configuration .xml à ce package. Ce fichier sera utilisé lors de l’installation du package.

- Dans l’éditeur de configuration ESET (ESET Configuration Editor), concentrez-vous sur les points suivants :

- **ESET Smart Security > Kernel > Setup > Remote administration**
  Votre configuration devrait ressembler à celle de l’image ci-dessous (l’adresse IP peut également être utilisée)



- Dans ESET Smart Security, ESET NOD32 Antivirus > Update > Profile (My profile) > Setup’
  Indiquez le nom du serveur de mise à jour (GHOST).



- Ceux sont les éléments minima requis pour les stations de travail pour notre exemple. Cliquez sur ‘Console’ dans la partie droite de la fenêtre de l’éditeur de configuration pour retourner sur la fenêtre ‘Installation Packages Editor’.

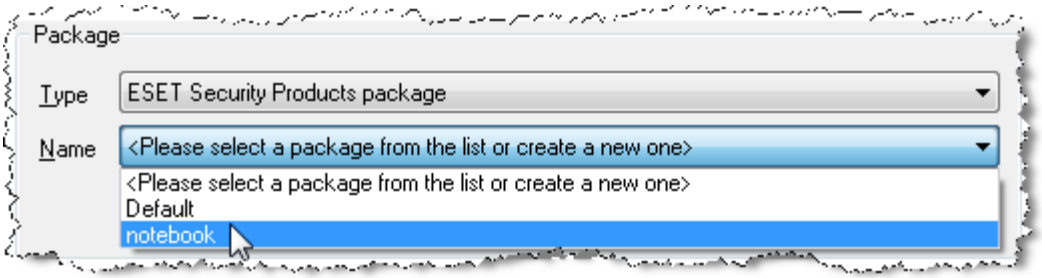
- Cliquez sur ‘Close’. Vous devrez alors indiquer un nom pour votre package (ex : workstation). Le package d’installation est maintenant créé.

- Maintenant l’installation par la méthode push va pouvoir être réalisée: Cliquez sur le bouton ‘Install...’ (onglet ‘Remote Install’) et suivez les instructions des chapitres précédents. Il est important de sélectionner le package ‘workstation’ comme indiqué dans l’image ci-dessous :

7.1.5 Installation distance sur les portables actuellement déconnecté du réseau

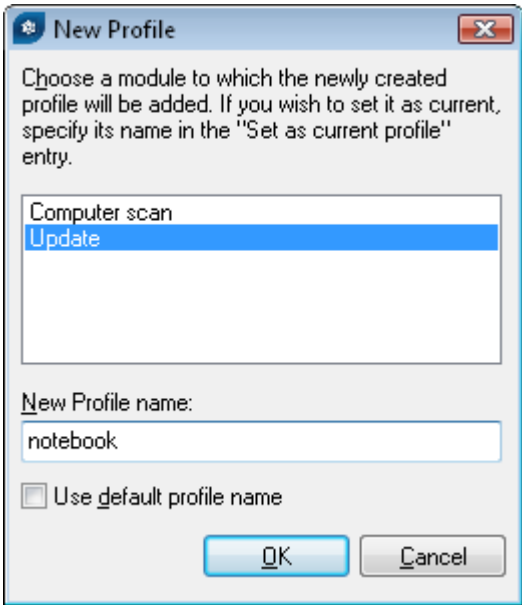
Les ordinateurs portables qui se trouvent quelquefois hors du réseau nécessitent un mode d’installation à distance différent. Pour ceux-ci, la méthode ‘logon script’ est suggérée. Procédez comme suit :

- Ouvrez la Console ERA et connectez-vous sur le serveur ERA (GHOST, dans notre exemple). Dans l’onglet ‘Remote Install’, cliquez sur le bouton ‘Packages...’.
- Sélectionnez le package d’installation ‘Notebooks’ dans le menu ‘Name’.

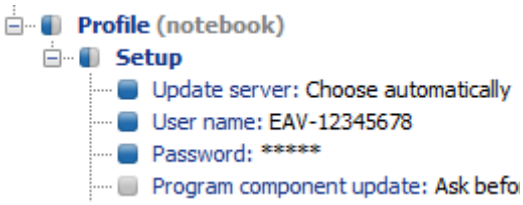


Pour permettre aux ordinateurs portables de recevoir les mises à jour depuis le serveur miroir “GHOST” (s’ils sont connectés au réseau) mais également depuis les serveurs ESET (s’ils ne sont pas connectés au réseau), procédez comme suit :

- Cliquez sur le bouton ‘Edit’ pour modifier le fichier .xml file crée dans la section 7.1.4.
- Allez dans ‘ESET Smart Security, ESET NOD32 Antivirus > Update > Profile (My profile)’.
- Cliquez droit sur ‘Profile (My profile)’ et sélectionnez ‘New Profile...’ dans me menu contextuel.
- Dans la fenêtre de création de profile, vérifiez bien que ‘Update’ est sélectionné, puis décochez la case ‘Use default profile name’.
- Saisissez le nom du nouveau profile (ex : notebooks).



- Cliquez sur ‘OK’ pour sauvegarder la configuration. Maintenant, en plus du ‘Profile (My profile)’, ‘Profile (notebook)’ apparaît. Cliquez sur ‘Profile (notebooks) > Setup’ et configurez les 3 éléments tels que dans l’image ci-dessous :



- L’option ‘Choose Automatically’ permet les mises à jour depuis les serveurs ESET au lieu du miroir local, et l’authentification sur ces serveurs est donnée par le nom d’utilisateur et le mot de passe qui vous ont été fournis lors de l’achat de votre licence.

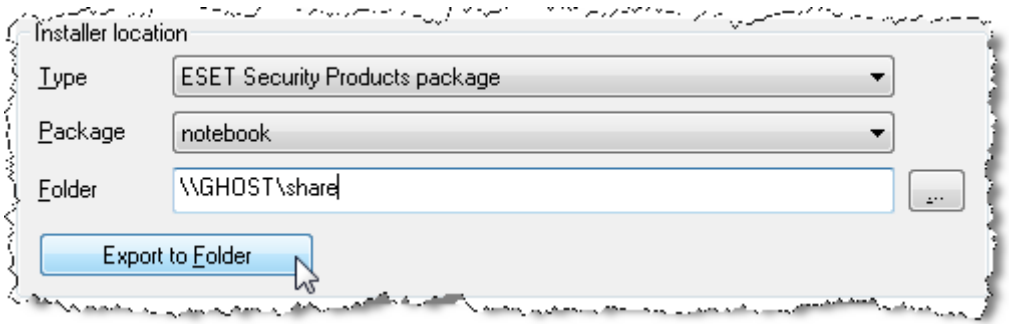
- Cliquez sur ‘Console’ dans la partie droite afin de retourner dans la fenêtre ‘Installation Packages Editor’.

- Cliquez sur ‘Yes’ puis sur ‘Save as...’ pour sauvegarder le package sous le nom de ‘notebooks’. Cliquez sur ‘Close’ pour retourner dans la console ERA.

Ensuite, il faut insérer l’agent einstaller.exe du package ‘notebooks’ dans le logon script. Procédez comme suit :

- Depuis l’onglet ‘Remote Install’, cliquez sur ‘Export...’

- Dans la liste des packages, sélectionnez ‘notebooks’ et cliquez sur le bouton ‘...’ pour définir le répertoire où sera placé l’agent einstaller.exe. Ce répertoire doit être accessible par les ordinateurs portables quand ils se connectent sur le réseau de l’entreprise (ou domaine). Dans notre exemple, nous allons prendre le répertoire défini par le chemin UNC \\GHOST\share



- Cliquez sur le bouton ‘Export to Folder’ puis cliquez sur ‘OK’. Le fichier einstaller.exe est maintenant dans le répertoire \\GHOST\share.

Si vous utilisez déjà un logon script, ERAC peut automatiquement ajouter une ligne au script existant. Ceci permettra aux ordinateurs portables d’installer le package dès qu’ils se connecteront au domaine. Pour ajouter cette ligne au script existant, procédez comme suit :

- Cliquez sur le bouton ‘...’ à droite du champ ‘Script Folder’ et sélectionnez le répertoire à résident les scripts.
- Depuis l’onglet ‘Remote Install’, cliquez sur ‘Logon...’. Saisissez le nom d’utilisateur Windows et le mot de passe (ainsi que le Domaine) de l’administrateur, et cliquez sur ‘OK’. Le logon script sera activé en utilisant ce compte.
- Maintenant, dès que l’ordinateur se connectera sur le domaine, le logon script se lancera automatiquement et installera le package.

7.2 Entreprise avec une filiale distante – 2x ERAS, 2x Serveur Miroir

Nous allons utiliser une copie du réseau précédent, auquel nous allons ajouter une filiale, avec plusieurs clients et un serveur appelé LITTLE. Supposons qu’il y ait une liaison VPN entre le siège et la filiale. Dans ce scénario, un serveur miroir devrait être installé sur le serveur LITTLE. Nous allons également installer un second Serveur ERA sur la machine LITTLE afin d’avoir un environnement convivial, et de minimiser le volume de données transférées.

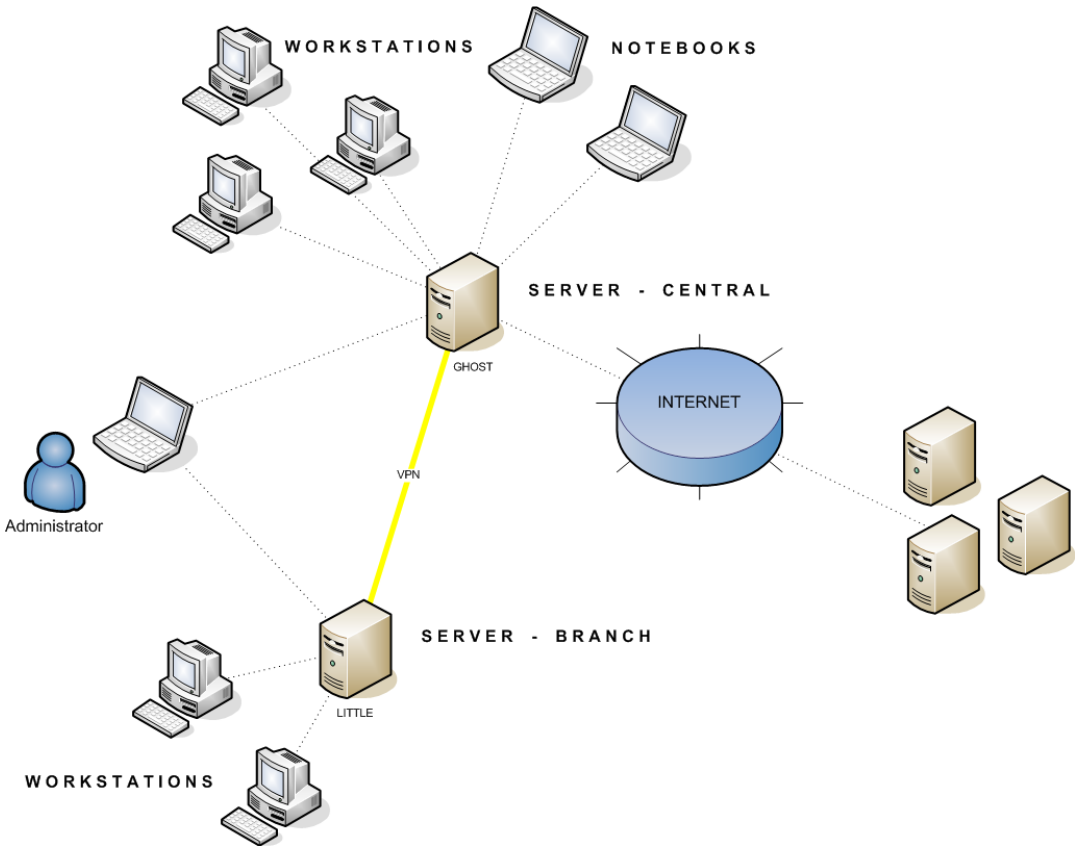
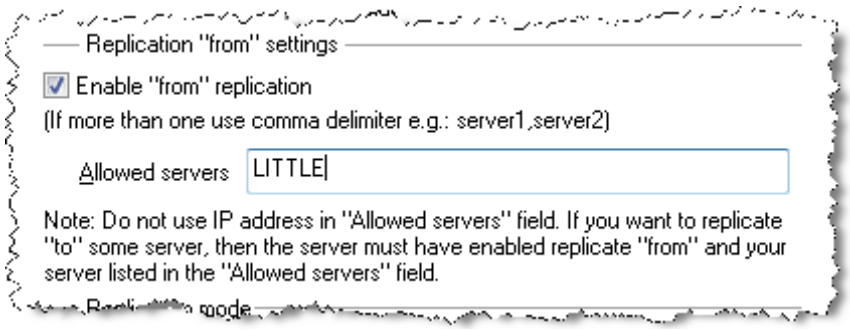


Figure 14
Structure réseau – entreprise avec une filiale

7.2.1 Installation au siège de l'entreprise

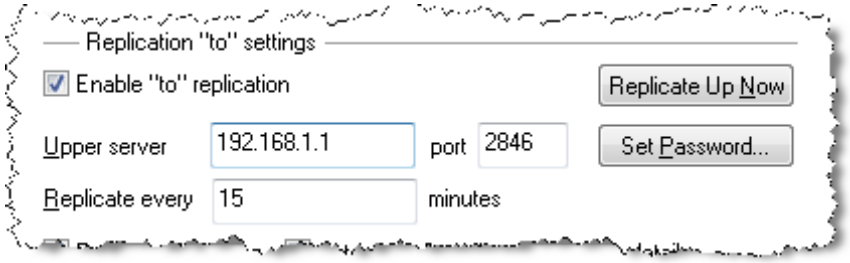
L'installation de ERAS, ERAC et des stations clients est très similaire au cas précédent. La seule différence est dans la configuration du serveur ERA maître (GHOST); il est nécessaire d'y spécifier que le serveur LITTLE est autorisé à recevoir les mises à jour depuis GHOST.

Pour cela, cliquez ouvrez la console ERA qui est connectée à GHOST. Cliquez sur Tools > Server Options... > Réplication. Cochez la case 'Enable "from" réplication' et inscrivez LITTLE dans le champ 'Allowed servers'.



7.2.2 Filiale : installation du Serveur ERA

Comme dans l'exemple précédent, installez le second serveur ERA. Configurez également les paramètres de réplication. Cochez la case 'Enable "to" replication' (Tools > Server Options... > Réplication) et saisissez l'adresse IP[4] du serveur ERA maître dans le champ 'Upper server'. Dans notre exemple, nous avons mis l'adresse IP du serveur GHOST.



7.2.3 Filiale : installation du Serveur Miroir HTTP

L'exemple précédent d'installation du serveur miroir peut également être utilisé dans ce cas. Les seuls changements concernent les parties :

- Source des fichiers de mise à jour (Source of update files)
- Nom d'utilisateur et mot de passé (User name and Password)

Comme indiqué dans l'image 14, les mises à jour pour la filiale ne sont pas téléchargées depuis les serveurs ESET, mais depuis le siège (GHOST). La source des mises à jour est définie par l'adresse URL : http://ghost:2221(ou http://IP_address_of_ghost:2221).

Il 'est pas nécessaire de spécifier de nom d'utilisateur ou de mot de passe, car le serveur web HTTP intégré ne requiers aucune authentification.

7.2.4 Filiale: installation à distance des clients

Là encore, le modèle précédent peut être utilisé, à la seule différence qu'il est plus pratique de faire les opérations avec la Console ERA connectée directement sur le Serveur ERA de la filiale (LITTLE)[5].

4. De façon à se prémunir de problèmes éventuels de DNS lors de la conversion du nom en adresse IP entre les réseaux (dépendant de la configuration DNS).
5. Ceci est fait dans le but de ne pas à avoir à transférer les packages d'installation via le VPN, ce qui est généralement plus lent

8. Trucs & Astuces

8.1 Export et autres caractéristiques de la configuration XML du client

Depuis la console, sélectionnez un client dans l'onglet 'Clients'. Cliquez droit et sélectionnez 'Configuration... dans le menu contextuel. Cliquez sur 'Save As...' pour exporter la configuration associée au client dans un fichier.xml[6]. Ce fichier .xml peut être ensuite utilisé pour différentes opérations :

- Pour les installations à distance, le fichier .xml peut être utilisé comme modèle de configuration prédéfinie. Ceci signifie qu'aucun nouveau fichier .xml ne sera créé et que le fichier .xml existant sera utilisé (Select...) dans le package.

- Pour configurer de multiples clients; les clients recevrons le fichier .xml sauvegardé précédemment et utiliseront les paramètres définis dans celui-ci (là encore, aucun autre fichier ne sera créé, mais uniquement assigné par le bouton 'Select...').

Exemple: Une solution ESET est installée uniquement sur une station de travail. Ajustez les paramètres sur cette machine directement depuis l'interface du programme. Ensuite, exportez les paramètres dans un fichier .xml. Ce fichier pourra alors être utilisé pour l'installation à distance sur les autres ordinateurs. Cette méthode peut s'avérer très utile pour des tâches telles que la configuration avancée des règles du pare-feu, si le mode "Policy-based" doit être utilisé.

8.2 Mises à jour combinées pour les ordinateurs portables

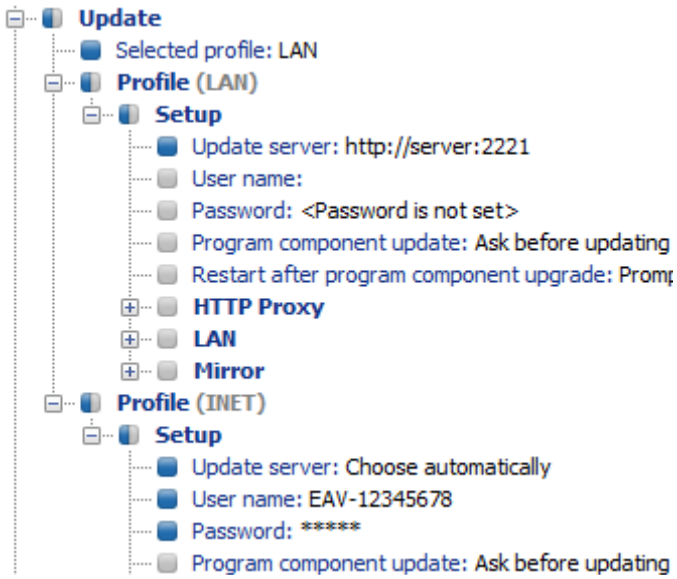
Si il y a des ordinateurs amenés à être déplacés (tels que les ordinateurs portables), nous recommandons de configurer les mises à jours combinées depuis 2 sources, les serveurs de ESET le miroir local. Le miroir sera contacté en premier, et si la connexion échoue (l'ordinateur est hors du bureau), alors les mises à jour seront téléchargées depuis les serveurs ESET. Procédez comme suit :

- Créez deux profiles de mise à jour, un qui se connectera au miroir (dans notre exemple, LAN), et l'autre aux serveurs ESET (dans notre exemple, INET)

- Créez une nouvelle tâche de mise à jour, ou modifiez-en une existante, dans le planificateur (Tools > Scheduler dans la fenêtre principale du programme ESET Smart Security ou ESET NOD32 Antivirus).

Cette configuration peut être réalisée directement sur l'ordinateur, ou alors à distance en utilisant l'éditeur de configuration. Ceci peut être appliqué lors de l'installation, mais également à n'importe quel autre moment grâce à une tâche de configuration dans ERA.
Pour créer un nouveau profile dans ESET Configuration Editor, cliquez droit dans la branche 'Update' et sélectionnez 'New profile' dans le menu contextuel.

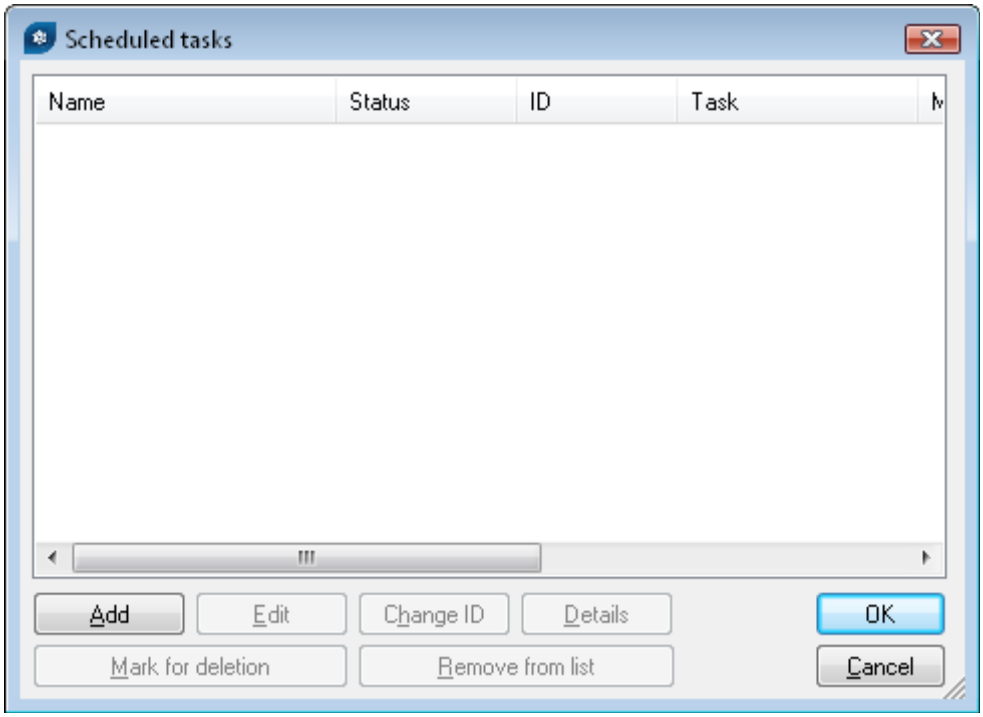
Le résultat des modifications devrait ressembler à la configuration affichée ci-dessous :



6. Les fichiers de configuration .xml peuvent également être générés depuis l'interface du programme ESET Smart Security.

Le profile LAN télécharge les mises à jour depuis le serveur miroir local de l'entreprise (http://server:8081), tandis que le profile INET se connecte aux serveurs de mise à jour ESET (Choose Automatically).

Ensuite, définissez une tâche de mise à jour qui utilisera les 2 profiles à la suite. Dans l'éditeur de configuration, allez dans 'ESET Smart Security, ESET NOD32 Antivirus > Kernel > Setup > Scheduler/Planner' ou NOD32 'version 2 > General > Setup > Scheduler/Planner'. Cliquez sur le bouton 'Edit' afin d'afficher la fenêtre 'Scheduled tasks'.



- Pour créer une nouvelle tâche, cliquez sur 'Add'. Dans la liste déroulante 'Scheduled task', sélectionnez 'Update' et cliquez sur 'Next'
- Donnez un nom à votre tâche (ex : "combined update"), sélectionnez 'Repeatedly' et cliquez sur 'Next'.
- Laissez l'intervalle 'Interval between task execution' à 60 minutes. Cliquez sur 'Next' 2 fois pour utiliser le paramétrage par défaut, et cliquez sur 'Finish'.
- Sélectionnez le profile de mise à jour principal et le secondaire (LAN, INET - ou vice versa) pour cette tâche.
- Si la mise à jour doit se faire en premier sur le miroir local, alors, le profile primaire (Primary profile) doit être LAN et le secondaire INET. Le profile INET ne sera utilisé que si la mise à jour n'arrive pas à être effectuée avec le profile LAN.
- Recommandation: Exportez la configuration d'un client dans un fichier .xml (pour plus d'informations, voir la section 8.1) et faites les modifications précédentes dans ce fichier. Vous éviterez ainsi toute duplication entre le planificateur et des profiles non fonctionnels.

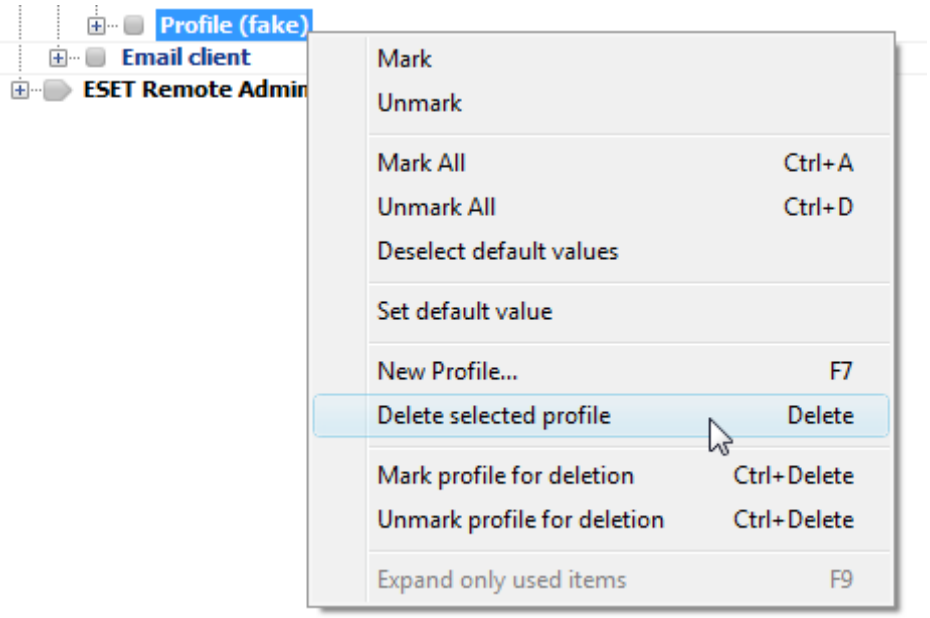
8.3 Suppression d'un profile existant

Si des profiles non utilisés ou dupliqués ont été créés par erreur sur les clients, ceux-ci peuvent être supprimés à distance. Procédez alors comme suit :

Dans la console ERA, onglet 'Clients', double-cliquez sur un client posant problème.

- Dans la fenêtre de propriété de ce client, cliquez sur l'onglet 'Configuration'.
- Cochez les cases 'Then Run ESET Configuration Editor to edit the file' et 'Use the downloaded configuration in the new configuration task' et cliquez sur le bouton 'New Task'.
- Dans l'assistant, cliquez sur 'Edit' afin d'ouvrir l'éditeur de configuration. Appuyez sur CTRL + D pour désélectionner tous les paramètres (gris). Ceci permettra d'éviter des changements accidentels, car tous les éléments qui seront modifiés seront marqués en bleu.
- Cliquez droit sur le profile que vous voulez supprimer et sélectionnez 'Mark profile for deletion' dans le menu contextuel.
- Cliquez sur 'File > Save' et fermez l'éditeur de configuration.
- Vérifiez que le client que vous avez sélectionné se trouve bien dans la colonne 'Selected items' sur la droite, et cliquez sur 'Next' puis sur 'Finish'.

Le profile non désiré sera alors supprimé de l'ordinateur sélectionné.



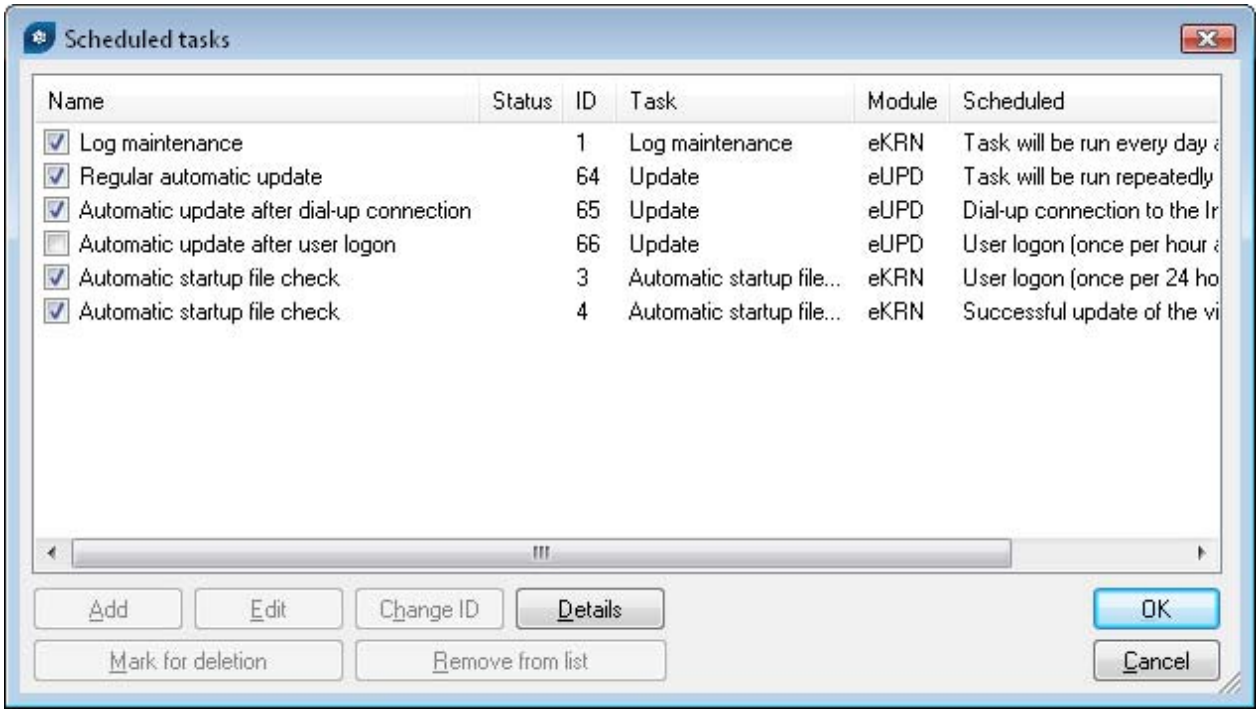
8.4 Configuration du planificateur

Pour modifier à distance les tâches dans le planificateur, allez dans Eset Smart Security / Kernel / Settings / Scheduler (ou NOD32 version 2 / General /Settings / Scheduler/Planner) dans l'éditeur de configuration ESET et cliquez sur le bouton Edit.

Si vous voulez ajouter des tâches, vous pouvez utiliser un fichier de configuration vierge. Si vous voulez modifier ou supprimer une tâche existante, il est nécessaire de :

- soit utiliser la configuration XML exportée depuis le client,
- ou utiliser les IDs des tâches que vous voulez modifier / supprimer.

Voici la fenêtre avec les tâches planifiées, si on utilise un fichier .xml exporté :



A chacune des tâche est assigné un identificateur (ID), Les tâches par défaut un ID décimal (1, 2, 3...) tandis que ceux des tâches personnalisées une valeur en hexadécimal (par exemple 4AE13D6C), qui est générée aléatoirement lors de la création de celles-ci.

Si une case est cochée, cela signifie que la tâche est active et sera exécutée sur le client.

Les fonctionnalités des boutons dans la fenêtre sont :

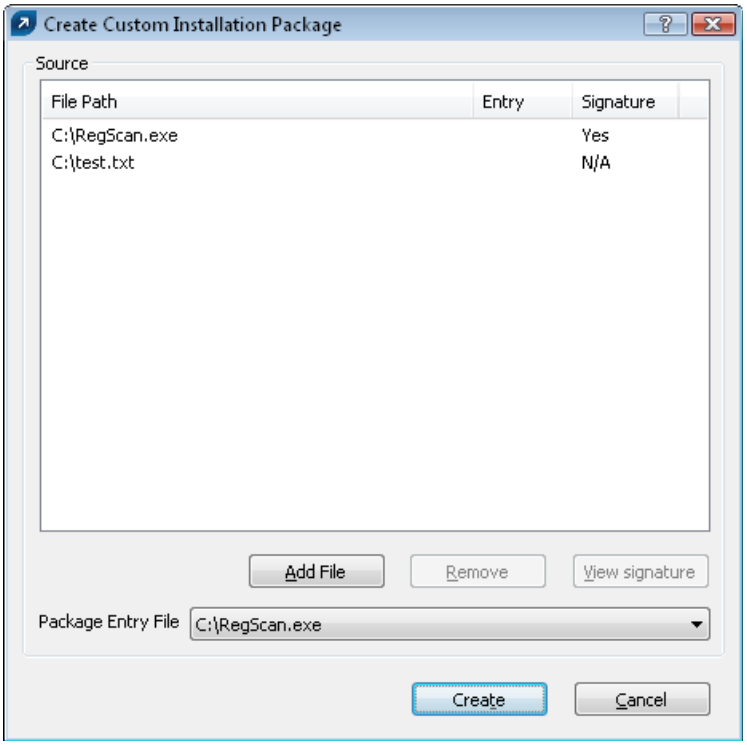
- Add... – Ajoute une nouvelle tâche.
- Edit. – Modifie la tâche sélectionnée.
- Change ID – Modifie l'ID la tâche sélectionnée.
- Details – Informations résumées à propos de la tâche sélectionnée.
- Select for deletion – L'application du fichier .xml va supprimer la tâche sélectionnée sur les ordinateurs cibles.
- Remove from list – Supprime la tâche sélectionnée de la liste. Attention, une tâche supprimée de la liste ne sera pas supprimée sur les ordinateurs cible.

NOTE : Vu que les valeurs des ID sont générées aléatoirement, certaines complications peuvent survenir si le même type de tâche est appliqué plusieurs fois. Exemple: il y a 40 PC dans le réseau. L'administrateur ajoute une nouvelle tâche nommée ABC (avec comme ID 4A2B8CA5). L'entreprise ajoute 10 nouveaux ordinateurs et l'administrateur applique une nouvelle tâche appelée également ABC (avec comme ID 8D5A6D1B). Plus tard, il décide de modifier la tâche ABC. Il exporte le fichier de configuration XML de l'un des 40 PC originaux, modifie la tâche et l'applique sur l'ensemble des 50 machines. Ceci créée un problème car le même type de tâche a deux ID différents (4A2B8CA5, 8D5A6D1B). La modification sera correctement réalisée sur les 40 premières machines, mais les 10 nouvelles auront une nouvelle tâche dupliquée de créée (la tâche originale a l'ID 8D5A6D1B, mais la modification porte sur la tâche avec l'ID 4A2B8CA5). Ceci peut être évité en changeant manuellement l'ID (cliquer sur le bouton 'Change ID') et en y inscrivant un ID commun, lors de la création d'une tâche du même type.

8.5 Packages d'installation personnalisés

L'éditeur de package d'installation permet la création de packages personnalisés.
Pour ouvrir l'éditeur, cliquez sur le bouton 'Package…' dans l'onglet 'Remote Install' de la console ERA. Dans la liste des types de package, choisissez 'Custom package', puis cliquez sur le bouton 'Add…'. Cliquez sur le bouton 'Add File' afin 'ajouter le fichier maître (celui qui sera exécuté en premier). Vous pouvez ensuite ajouter n'importe quel fichier de la même manière, en cliquant sur le bouton 'Add File'.

La distribution sur les clients à distance est similaire à celle des solutions client ESET. Le package est automatiquement extrait sur les ordinateurs cibles, et le fichier maître du package sera alors exécuté.



Ce type de package peut être très utile pour la désinstallation de logiciels de sécurité d'autres éditeurs.