ESET

REMOTE ADMINISTRATOR 6

Guide d'administration

Cliquez ici pour accéder à la dernière version de ce document.

ENJOY SAFER TECHNOLOGY™

ESET **REMOTE ADMINISTRATOR 6**

Service client : www.eset.com/support

RÉV. 26/01/2016

Table des

Table des

1. Administration

Cette section explique comment gérer et configurer ESET Remote Administrator. Les chapitres suivants décrivent les étapes initiales recommandées que vous devez suivre après l'installation d'ESET Remote Administrator.

- Premières étapes : commencez la configuration.
- Tâches de post-installation : découvrez comment tirer pleinement parti d'ESET Remote Administrator et effectuer les étapes recommandées pour une expérience utilisateur optimale.
- Console Web ERA : la principale interface utilisateur d'ESET Remote Administrator. Simple à utiliser n'importe où et sur tous les périphériques.
- Gestion des utilisateurs : vous pouvez créer un groupe d'utilisateurs, ajouter de nouveaux utilisateurs, modifier ceux existants et effectuer une synchronisation avec Active Directory.
- Gestion de licences : ESET Remote Administrator doit être activée à l'aide d'une clé de licence émise par ESET avant de pouvoir être utilisée. Reportez-vous à la section Gestion de licences pour des instructions sur l'activation de votre produit, ou consultez l'aide en ligne d'ESET License Administrator pour en savoir plus sur l'utilisation d'ESET License Administrator.
- Un tableau de bord entièrement personnalisable vous donne une vue d'ensemble de l'état de sécurité de votre réseau. La section Admin de la console Web d'ESET Remote Administrator (Console Web ERA) constitue un outil convivial puissant pour gérer les produits ESET.
- Déploiement d'ERA Agent : ERA Agent doit être installé sur tous les ordinateurs clients qui communiquent avec ERA Server.
- Les notifications vous donnent des informations pertinentes en temps réel et les rapports vous permettent de trier efficacement divers types de données que vous pouvez utiliser ultérieurement.
- Mobile Device Management vous permet d'installer, d'inscrire et de configurer vos périphériques mobiles.

2. Premières étapes

Une fois ESET Remote Administrator correctement installé, vous pouvez passer à l'étape de configuration.

Tout d'abord, ouvrez la console Web ERA dans votre navigateur et connectez-vous.

Découverte de la console Web ERA

Avant de commencer la configuration initiale, il est recommandé de découvrir la console Web ERA, car il s'agit de l'interface à utiliser pour gérer les solutions de sécurité ESET.

Quand vous ouvrez la console Web ERA la première fois, les tâches de post-installation vous indiquent les étapes à suivre pour configurer votre système.

Création/configuration des autorisations pour les nouveaux utilisateurs

Au moment de l'installation, vous avez créé un compte d'administrateur par défaut. Il est recommandé d'enregistrer le compte Administrateur et de créer un compte pour gérer les clients et configurer leurs autorisations.

Ajout des ordinateurs clients, des serveurs et des périphériques mobiles du réseau à la structure ERA

Au cours de l'installation, vous pouvez choisir de rechercher les ordinateurs (clients) sur votre réseau. Tous les clients détectés sont répertoriés dans la section Ordinateurs lorsque vous démarrez ESET Remote Administrator. Si les clients ne sont pas affichés dans la section Ordinateurs, exécutez la tâche Synchronisation des groupes statiques pour rechercher les ordinateurs et les afficher dans des groupes.

Déploiement de l'Agent
Une fois les ordinateurs détectés, déployez l'Agent sur les ordinateurs clients. L'Agent permet les communications entre ESET Remote Administrator et les clients.

Installation d'un produit ESET (activation comprise)
Pour protéger les clients et le réseau, installez des produits ESET. Cette installation est effectuée à l'aide de la tâche Installer un logiciel.

Création/modification de groupes
Il est recommandé de trier les clients en groupes statiques ou dynamiques selon divers critères. Vous pouvez ainsi gérer plus facilement les clients et avoir une vue d'ensemble du réseau.

Création d'une stratégie
Les stratégies servent à transmettre des configurations spécifiques aux produits ESET s'exécutant sur les ordinateurs clients. Elles vous évitent de devoir configurer manuellement les produits ESET sur chaque client. Une fois que vous avez créé une stratégie avec une configuration personnalisée, vous pouvez l'attribuer à un groupe (statique ou dynamique) en vue d'appliquer vos paramètres à tous les ordinateurs de ce groupe.

Attribution d'une stratégie à un groupe
Comme indiqué ci-dessus, une stratégie doit être attribuée à un groupe pour entrer en vigueur. Les ordinateurs appartenant au groupe se verront appliquer la stratégie. La stratégie est appliquée et mise à jour à chaque connexion d'un Agent à ERA Server.

Configuration de notifications et création de rapports
Nous vous recommandons d'utiliser des notifications et des rapports pour surveiller l'état des ordinateurs clients dans votre environnement. Par exemple, si vous voulez être informé de la survenue d'un événement en particulier, ou pour voir ou télécharger un rapport.

2.1 Ouverture d'ERA Web Console

Il existe plusieurs méthodes pour ouvrir ERA Web Console :

- Sur le serveur local (l'ordinateur hébergeant la console Web), saisissez cette URL dans le navigateur Web : *https://localhost/era/*

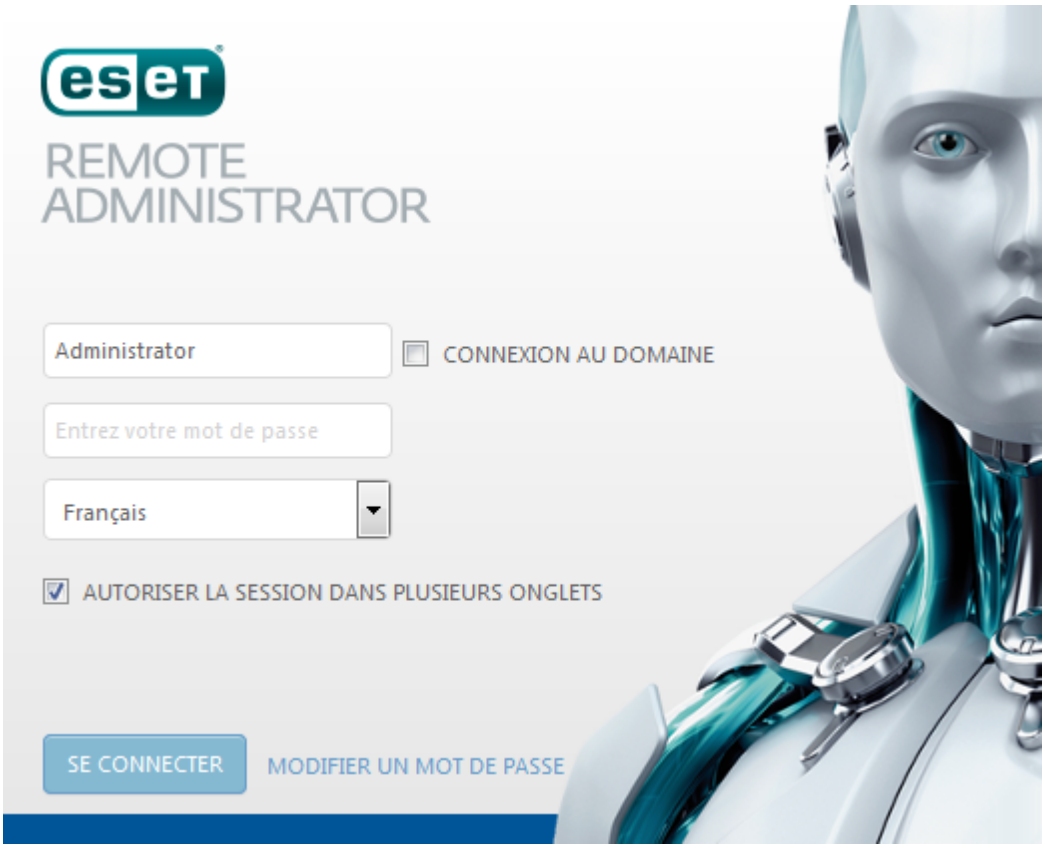
- À partir de n'importe quel emplacement ayant un accès Internet au serveur Web, saisissez l'URL dans le format suivant :
  https://yourservername/era/
  Remplacez « nomvotreserveur » par le nom ou l'adresse IP du serveur Web.

- Pour vous connecter à l'appliance virtuelle ERA, utilisez l'URL suivante :
  https://[IP address]:8443/
  Remplacez [adresse IP] par celle de votre machine virtuelle ERA. Si vous ne vous souvenez pas de l'adresse IP, reportez-vous à l'étape 9 des instructions pour le déploiement de l'appliance virtuelle.

- Sur le serveur local (l'ordinateur hébergeant la console Web), cliquez sur Démarrer > **Tous les programmes** > **ESET** > **ESET Remote Administrator** > **ESET Remote Administrator Webconsole**. Un écran de connexion s'affiche dans votre navigateur Web par défaut. Cela ne s'applique pas à l'appliance virtuelle ERA.

REMARQUE : comme la console Web utilise un protocole sécurisé (HTTPS), un message relatif à un certificat de sécurité ou à une connexion non approuvée peut s'afficher dans le navigateur Web (les termes exacts du message dépendent du navigateur utilisé). Ce message s'affiche, car le navigateur demande la vérification de l'identité du site auquel vous accédez. Cliquez sur **Poursuivre sur ce site Web** (Internet Explorer) ou **Je comprends les risques**, sur **Ajouter une exception...**, puis sur **Confirmer l'exception de sécurité** (Firefox) pour accéder à ERA Web Console. Cela s'applique uniquement lorsque vous accédez à l'URL de la console Web ESET Remote Administrator.

Lorsque le serveur Web (qui exécute la console Web ERA) est fonctionnel, l'écran suivant s'affiche.



S'il s'agit de votre première connexion, indiquez les informations d'identification saisies lors du processus d'installation. Pour plus d'informations sur cet écran, reportez-vous à la section Écran de connexion à la console Web.

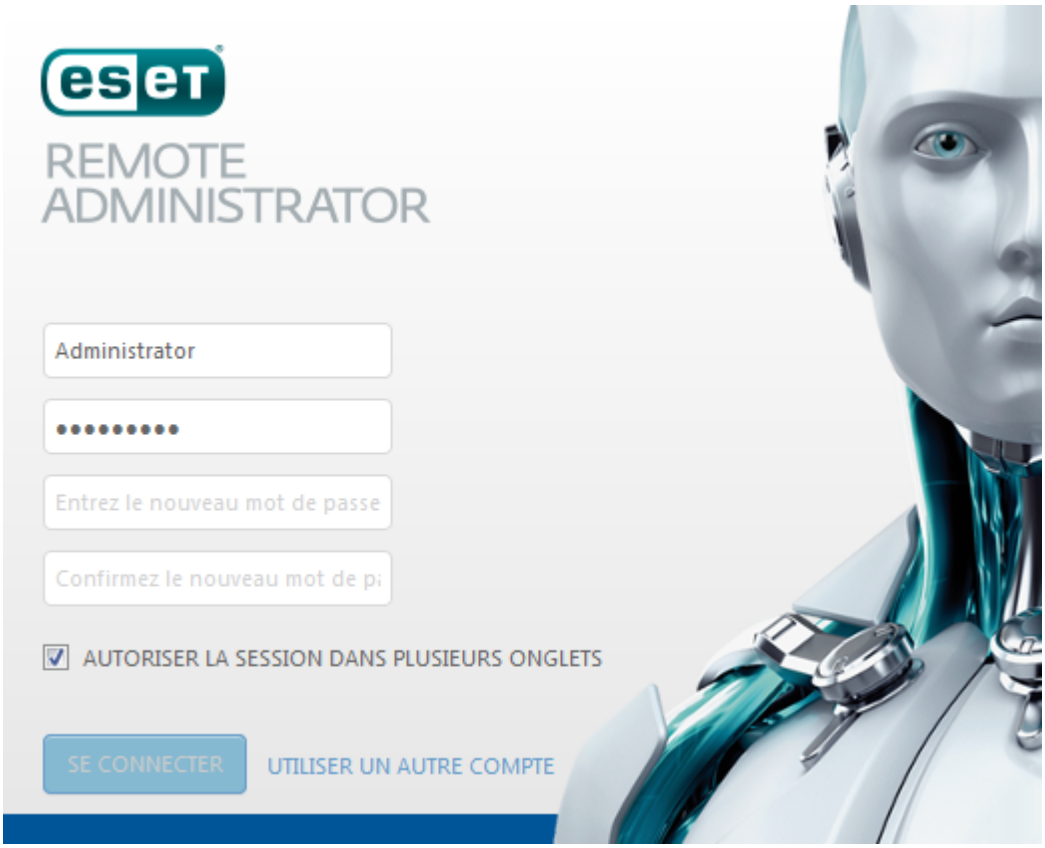
REMARQUE : si l'écran de connexion ne s'affiche pas ou s'il semble se charger sans cesse, redémarrez le service *ESET Remote Administrator Server*. Une fois le service *ESET Remote Administrator Server* fonctionnel et en cours d'exécution, redémarrez le service *Apache Tomcat*. Une fois cette opération terminée, l'écran de connexion de la console Web se charge correctement.

2.2 Écran de connexion d'ERA Web Console

Un utilisateur doit disposer d'informations d'identification (nom d'utilisateur et mot de passe) pour se connecter à la console Web. Il est également possible de se connecter en tant qu'utilisateur de domaine en cochant la case en regard de l'option **Connexion au domaine** (un utilisateur de domaine n'est pas associé à un groupe de domaines mappé). Vous pouvez sélectionner votre langue dans une liste située dans le coin supérieur droit de l'écran de connexion. Sélectionnez **Autoriser la session dans plusieurs onglets** pour permettre aux utilisateurs d'ouvrir la console Web ERA dans plusieurs onglets de leur navigateur Web.

REMARQUE : le message d'avertissement **Utilisation d'une connexion non chiffrée ! Configurez le serveur Web pour utiliser le protocole HTTPS** s'affiche quand vous accédez à la console Web ESET Remote Administrator (console Web ERA) via HTTP. Pour des raisons de sécurité, nous vous recommandons de configurer la console Web ERA pour utiliser HTTPS.

Modifier le mot de passe/Essayer avec un autre compte : permet de modifier le mot de passe ou de revenir à l'écran de connexion. Un utilisateur ne disposant pas de jeu d'autorisations est autorisé à se connecter à la console Web, mais ne peut pas afficher d'informations pertinentes.



Pour accorder des autorisations de lecture/écriture/modification à un utilisateur dans les modules de la console Web, un jeu d'autorisations doit être créé et attribué à l'utilisateur.

Gestion des sessions et mesures de sécurité :

- **Verrouillage de l'adresse IP de connexion**

  Après 10 tentatives infructueuses de connexion à partir d'une même adresse IP, les tentatives suivantes sont temporairement bloquées pendant environ 10 minutes. Le blocage de l'adresse IP n'a aucune incidence sur les sessions existantes.

- **Verrouillage de l'adresse d'ID de session incorrect**

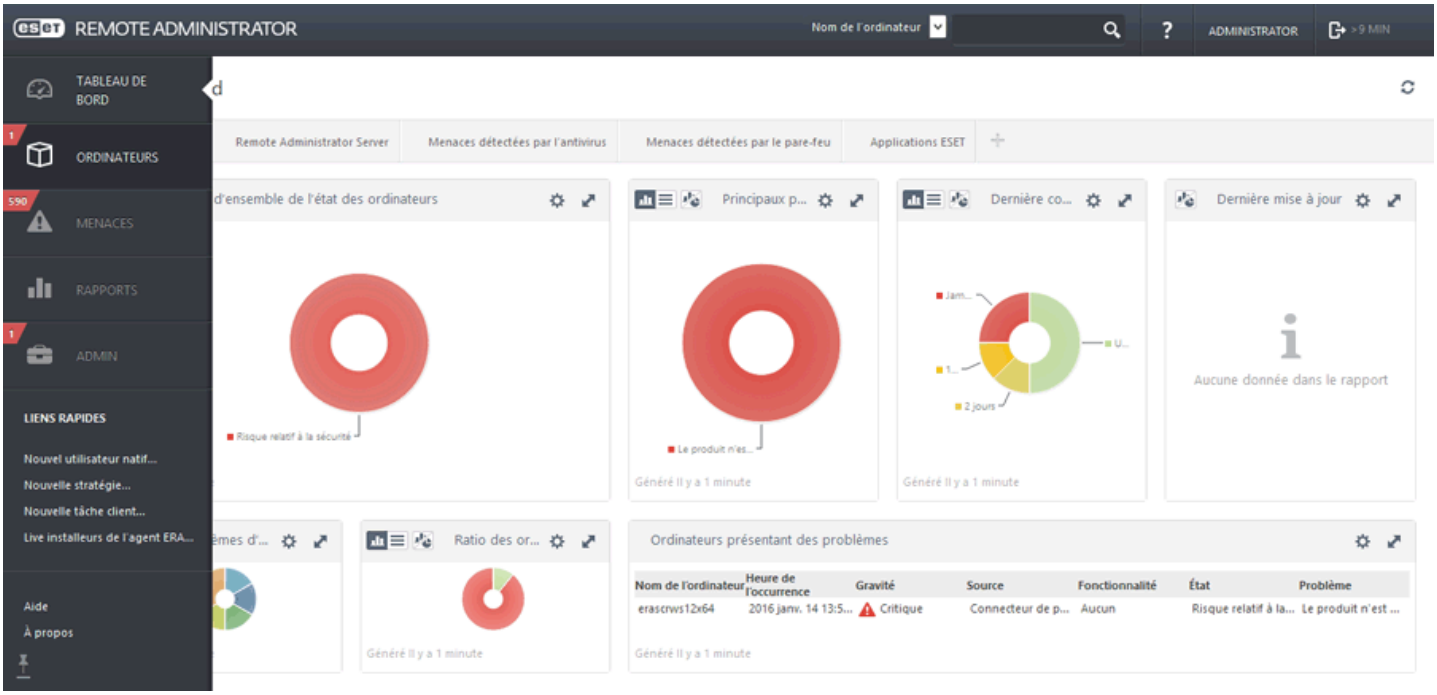
  Après avoir utilisé à 15 reprises un ID de session incorrect à partir d'une même adresse IP, les connexions suivantes à partir de cette adresse sont bloquées pendant environ 15 minutes. Les ID de session ayant expiré ne sont pas comptabilisés. Un ID de session expiré dans le navigateur n'est pas considéré comme une attaque. Le blocage de 15 minutes de l'adresse IP englobe toutes les actions (y compris les demandes valides).

2.3 Découverte de la console Web ERA

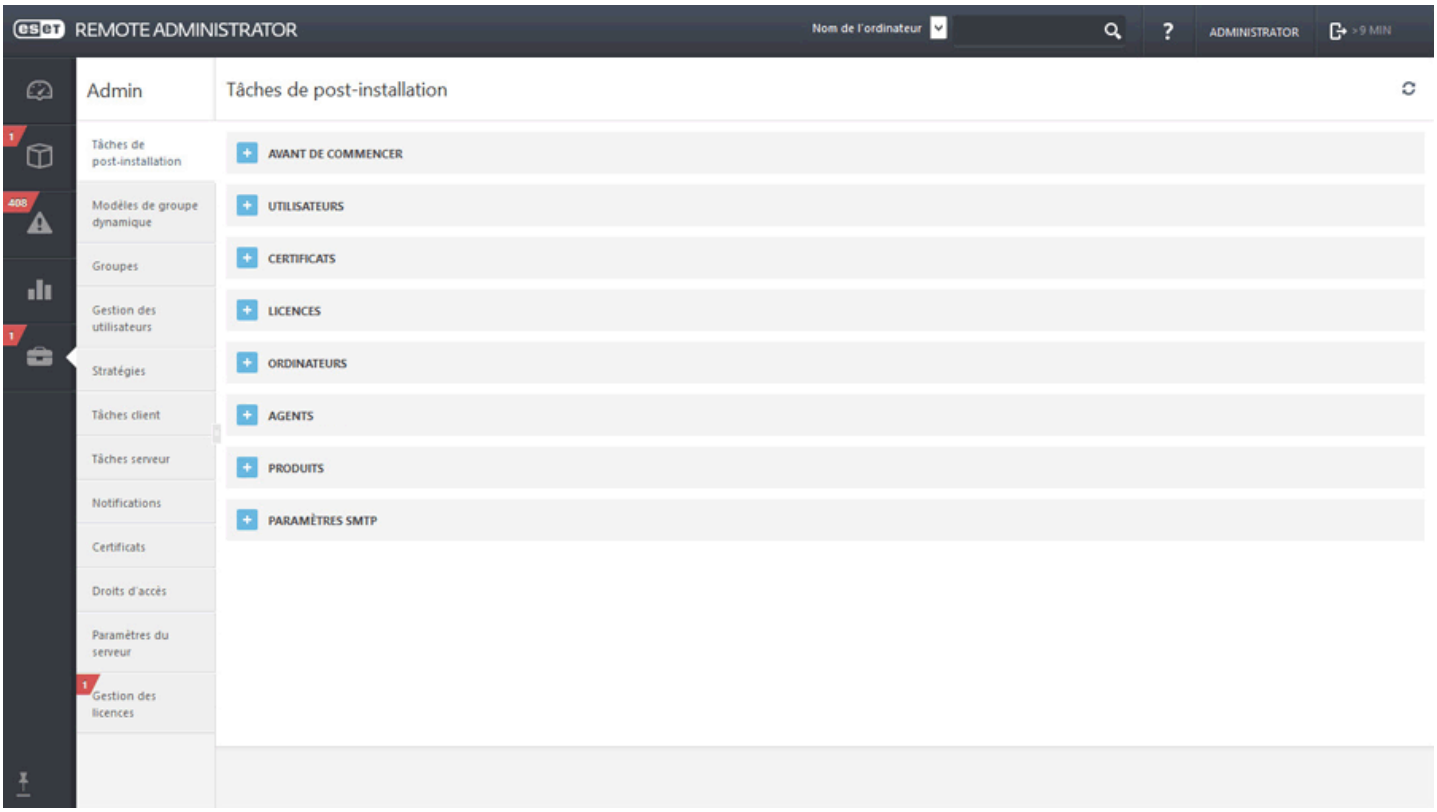
La console Web ESET Remote Administrator est l'interface principale pour communiquer avec ERA Server. Vous pouvez la comparer à un panneau de commandes centralisé à partir duquel vous pouvez gérer toutes les solutions de sécurité ESET. Il s'agit d'une interface Web qui est accessible à partir d'un navigateur (voir Navigateurs Web pris en charge) depuis n'importe quel emplacement et tout périphérique ayant accès à Internet.

Dans la présentation classique de la console Web ERA :

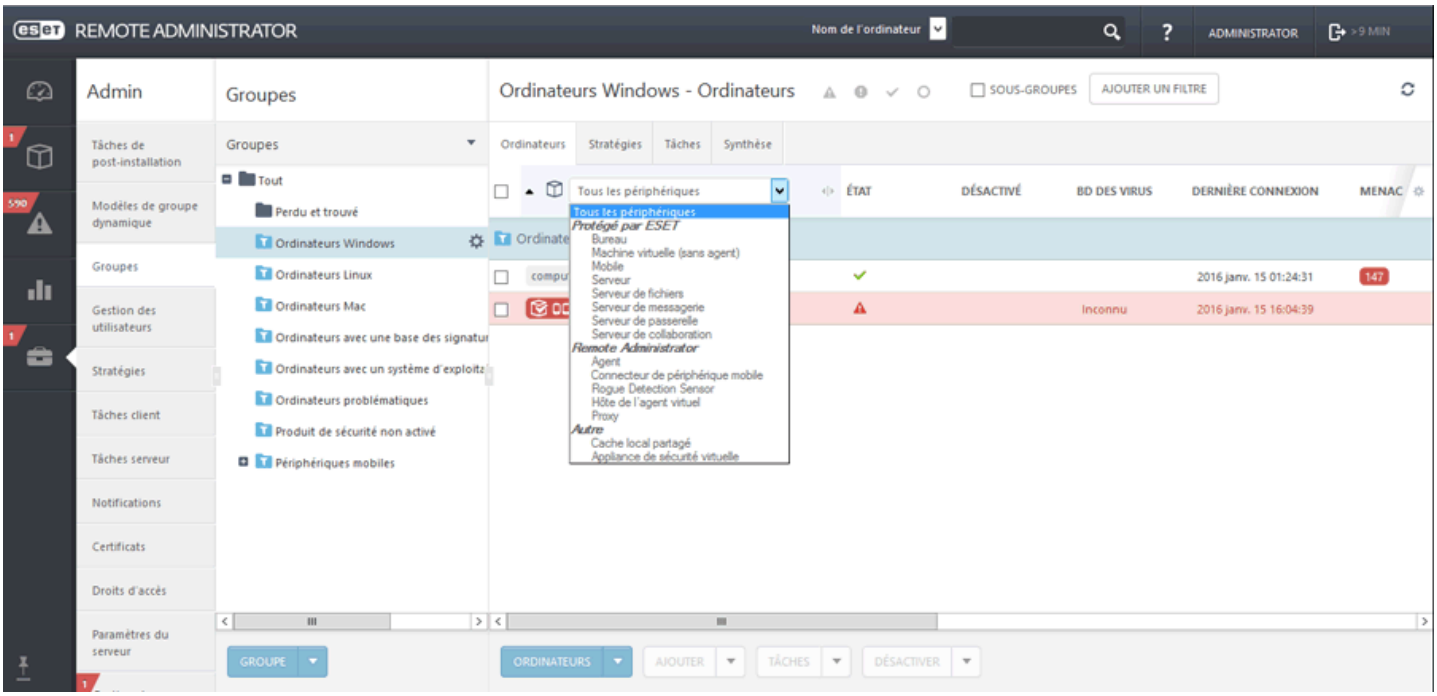
- L'utilisateur actuellement connecté est toujours affiché en haut à droite, où le délai d'expiration de la session fait l'objet d'un compte à rebours. Vous pouvez cliquez sur **Déconnexion** à tout moment pour vous déconnecter. Si une session expire (en raison de l'inactivité de l'utilisateur), l'utilisateur doit se reconnecter.
- Vous pouvez cliquer sur **?** dans la partie supérieure de n'importe quel écran pour afficher l'aide de cet écran.
- Le **menu** est accessible à tout moment à gauche, sauf lors de l'utilisation d'un assistant. Pour afficher le menu, placez le pointeur de votre souris dans la partie gauche de l'écran. Le menu contient également des **liens rapides** et la **version de votre console Web**.
- L'icône ⚙ signale toujours un menu contextuel.
- Cliquez sur **Rafraîchir** pour recharger/actualiser les informations affichées.



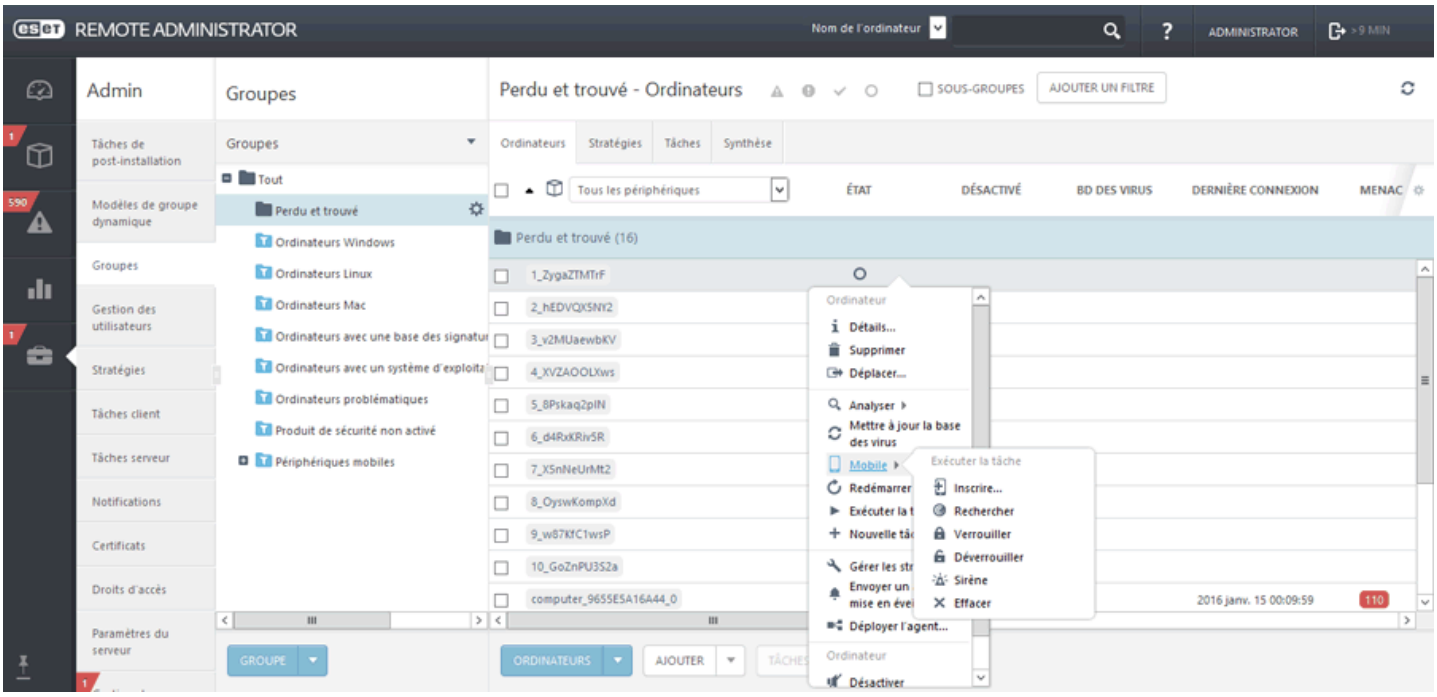
Les tâches de post-installation vous indiquent comment tirer pleinement parti d'ESET Remote Administrator. Elles vous guident tout au long des étapes recommandées.



Les écrans contenant une arborescence possède des contrôles spécifiques. L'arborescence est affichée à gauche et les actions apparaissent en dessous. Cliquez sur un élément de l'arborescence pour afficher des options pour celui-ci.

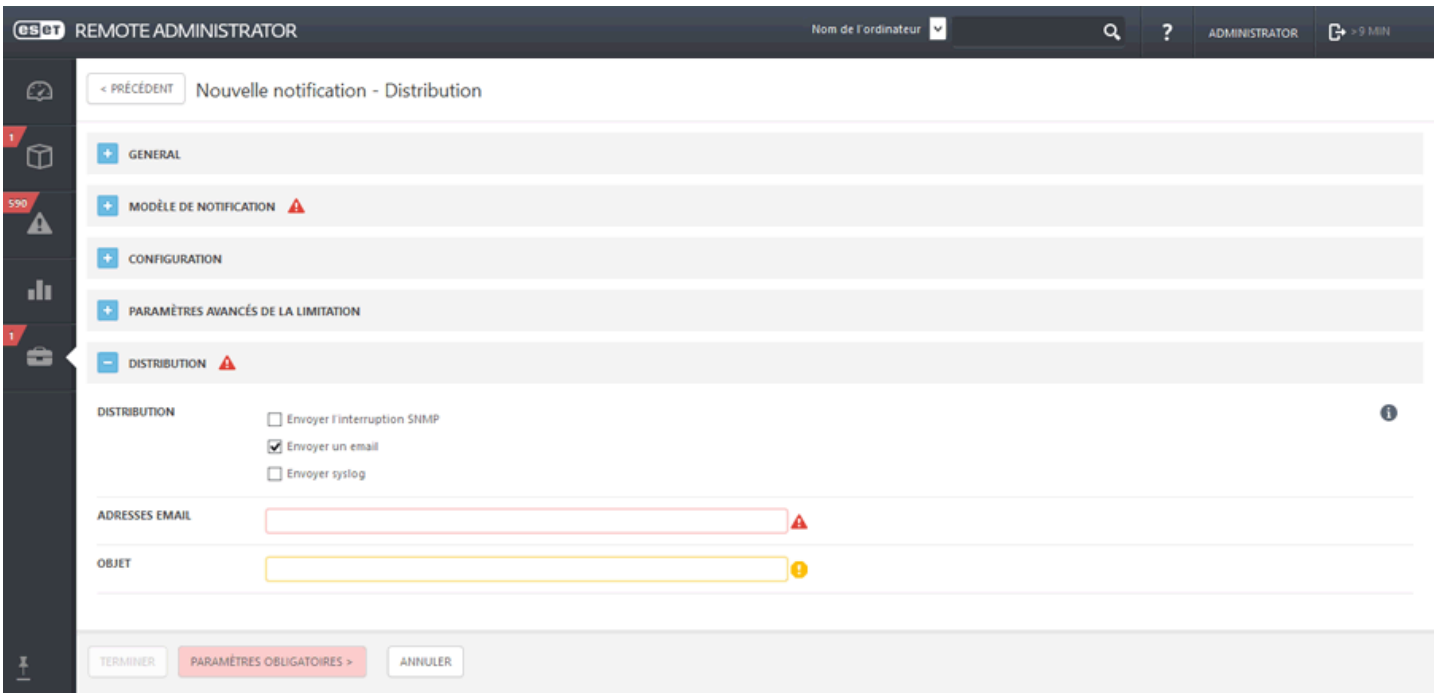


Les tables vous permettent de gérer les unités d'une ligne ou dans un groupe (lorsque plusieurs lignes sont sélectionnées). Cliquez sur une ligne pour afficher les options des unités de celle-ci. Les données des tables peuvent être filtrées et triées.



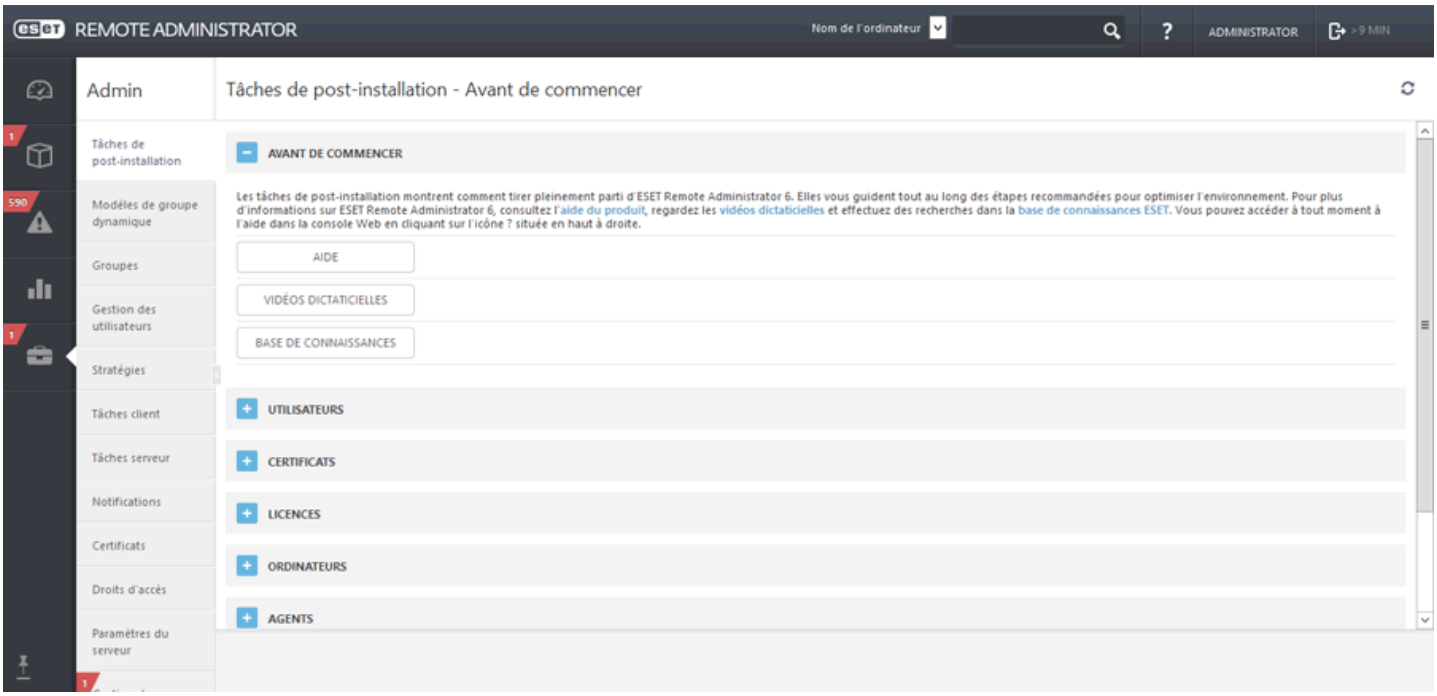
Dans ERA, les objets peuvent être modifiés à l'aide d'assistants. Tous les assistants partagent les comportements suivants :

- Les étapes s'affichent verticalement, de haut en bas.
- L'utilisateur peut revenir à une étape à tout moment.
- Les données d'entrée non valides sont signalées lorsque vous placez le curseur dans un nouveau champ. L'étape de l'assistant contenant des données d'entrée non valides est indiquée également.
- L'utilisateur peut vérifier à tout moment les données non valides en cliquant sur **Paramètres obligatoires**.
- Le bouton Terminer n'est pas disponible tant que toutes les données d'entrée ne sont pas correctes.



2.4 Tâches de post-installation

Nous vous recommandons vivement de prendre connaissance des **tâches de post-installation** qui vous seront utiles pendant la configuration initiale d'ESET Remote Administrator.



Avant de commencer
Nous vous invitons à consulter nos vidéos pédagogiques et la base de connaissances ESET.

Utilisateurs
Vous pouvez créer différents utilisateurs et configurer leurs autorisations pour permettre différents niveaux de gestion dans ESET Remote Administrator.

Certificats
Vous pouvez créer des autorités de certification et des certificats homologues pour des composants ESET Remote Administrator individuels afin d'autoriser la communication avec ERA Server.

Licences
À partir de la version 6, ESET Remote Administrator utilise un système de licences ESET entièrement nouveau. Sélectionnez la méthode de votre choix pour ajouter votre nouvelle licence.

Ordinateurs
Ajoutez des périphériques à des groupes dans ESET Remote Administrator.

Agents
Il existe plusieurs méthodes pour déployer ERA Agent sur les ordinateurs clients de votre réseau.

Produits
Vous pouvez installer le logiciel directement depuis le référentiel ESET ou spécifier un chemin d'accès vers un dossier partagé contenant des packages d'installation.

Paramètres SMTP
ESET Remote Administrator peut être configuré de manière à se connecter à votre serveur SMTP existant afin de permettre à ERA d'envoyer des courriers électroniques, par exemple des notifications, des rapports, etc.

2.5 Certificats

Les certificats représentent une partie importante de ESET Remote Administrator. Les certificats sont nécessaires pour que les composants ERA puissent communiquer avec ERA Server.

Vous pouvez utiliser les certificats créés lors de l'installation d'ERA. Vous avez aussi la possibilité d'utiliser votre autorité de certification et vos certificats personnalisés. Vous pouvez également Créer une autorité de certification (AC) ou Importer une clé publique que vous emploierez pour signer le certificat homologue de chacun des composants (ERA Agent, ERA Proxy, ERA Server, ERA MDM ou l'hôte de l'agent virtuel).

2.6 Déploiement

Après l'installation d'ESET Remote Administrator, il est nécessaire de déployer **ERA Agent** et **ESET Endpoint Protection (EES, EEA...)** sur les ordinateurs du réseau. Le déploiement est constitué des étapes suivantes :

1. Ajout des ordinateurs clients à la structure des groupes ESET Remote Administrator
2. Déploiement d'ERA Agent.
3. Déploiement d'ESET Endpoint Protection

Une fois ERA Agent déployé, vous pouvez effectuer une installation à distance d'autres produits de sécurité ESET sur vos ordinateurs clients. La procédure précise pour l'installation à distance est décrite dans le chapitre Installation du produit.

2.6.1 Ajouter un ordinateur client à la structure ERA

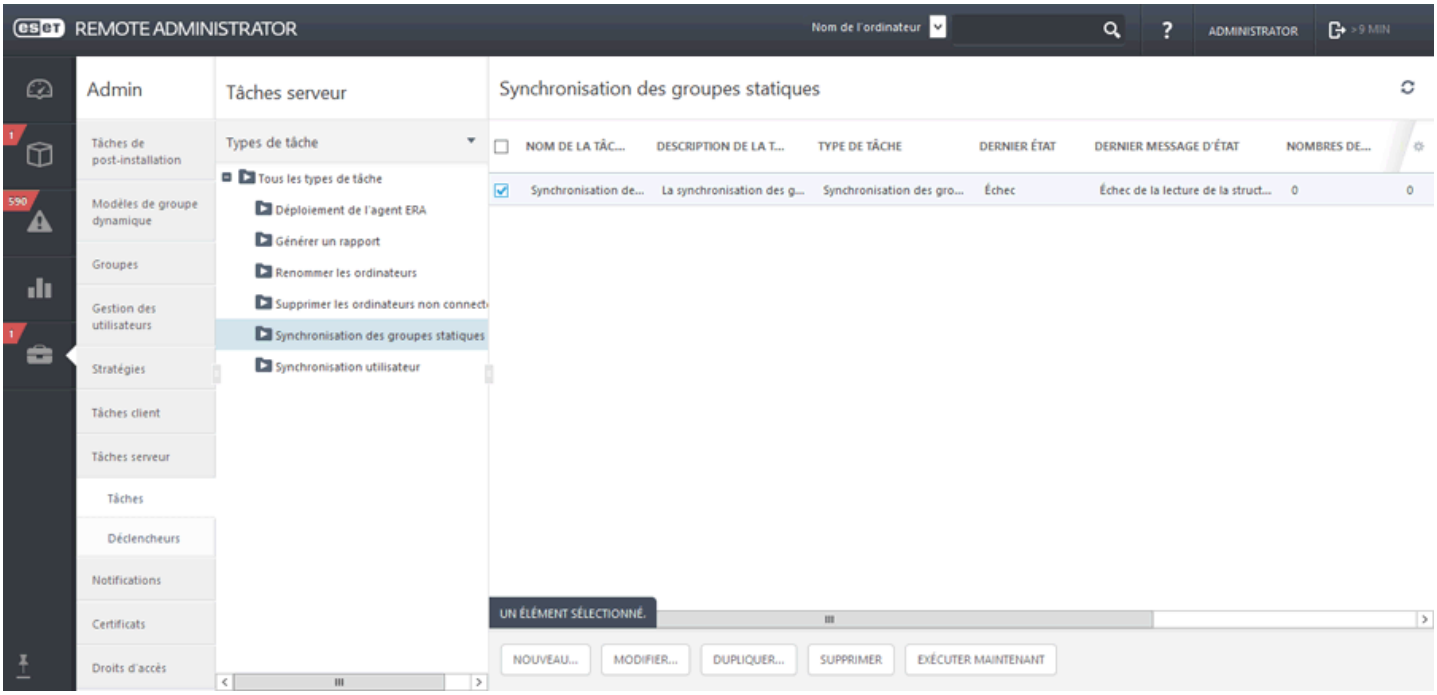
Il existe trois méthodes pour ajouter un ordinateur client à ESET Remote Administrator :

- Synchronisation d'Active Directory
- Saisie manuelle du nom/de l'adresse IP
- Utilisation de RD Sensor

2.6.1.1 Utilisation de la synchronisation d'Active Directory

La synchronisation d'Active Directory est effectuée en exécutant la tâche de serveur **Synchronisation des groupes statiques**.

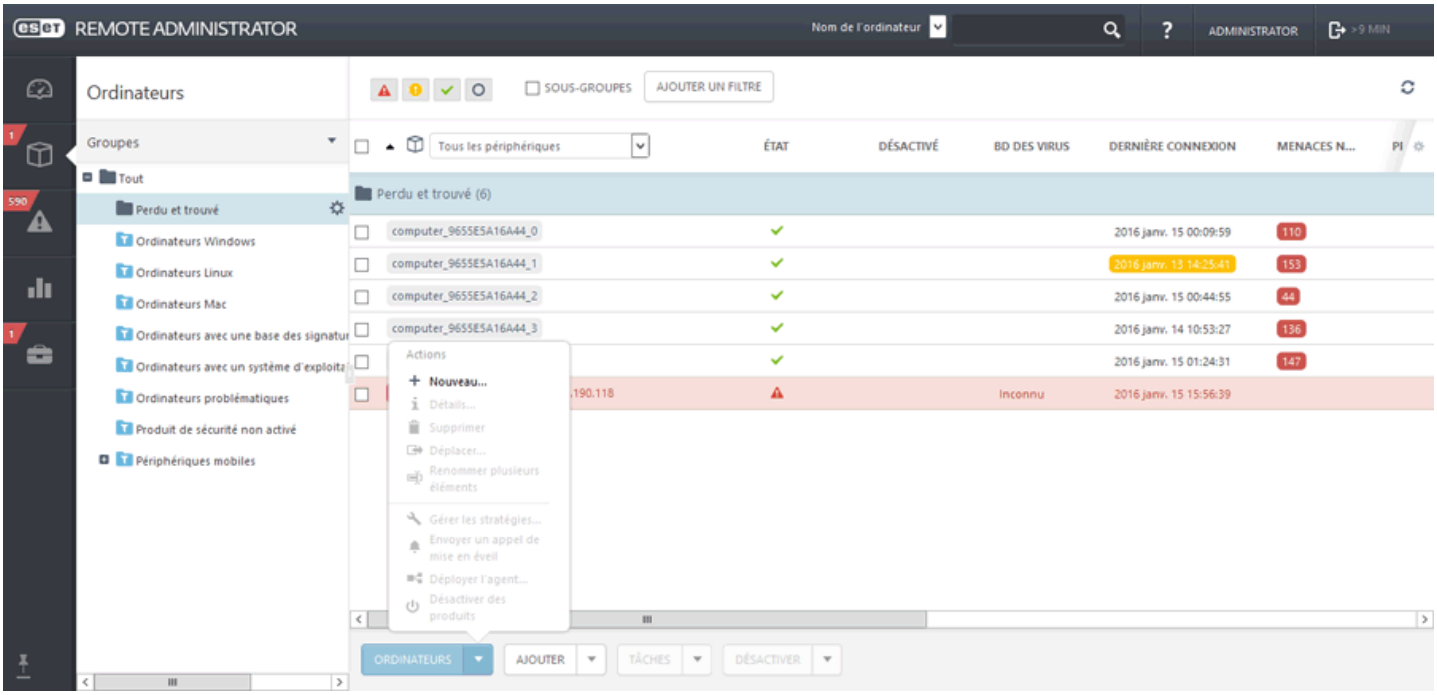
Admin> **Tâche de serveur** est une tâche par défaut prédéfinie que vous pouvez choisir d'exécuter automatiquement lors de l'installation de ESET Remote Administrator. Si l'ordinateur se trouve dans un domaine, la synchronisation est effectuée, et les ordinateurs d'Active Directory sont classés dans le groupe **Tous** par défaut.



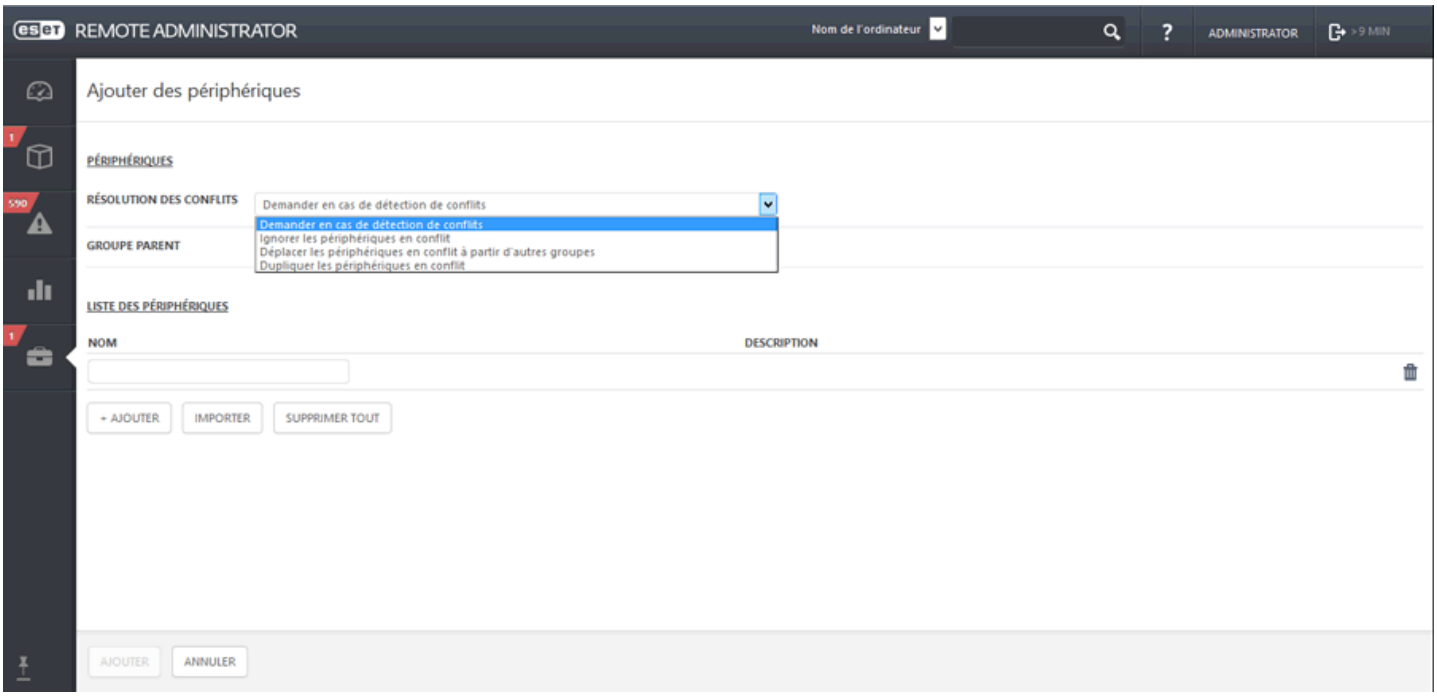
Pour démarrer le processus de synchronisation, cliquez sur la tâche et sélectionnez **Exécuter maintenant**. Si vous devez créer une autre tâche de synchronisation d'Active Directory, sélectionnez un groupe auquel ajouter les nouveaux ordinateurs depuis Active Directory. Sélectionnez également les objets d'Active Directory à partir desquels effectuer la synchronisation et l'action à exécuter sur les doublons. Saisissez les paramètres de connexion au serveur Active Directory, puis définissez le mode de synchronisation sur **Active Directory/Open Directory/LDAP**. Suivez les instructions détaillées de cet article de la base de connaissances ESET.

2.6.1.2 Saisie manuelle du nom/de l'adresse IP

L'onglet **Ordinateurs** vous permet d'ajouter de **nouveaux** ordinateurs. Vous pouvez ainsi manuellement ajouter les ordinateurs qui ne sont pas détectés ou automatiquement ajoutés.



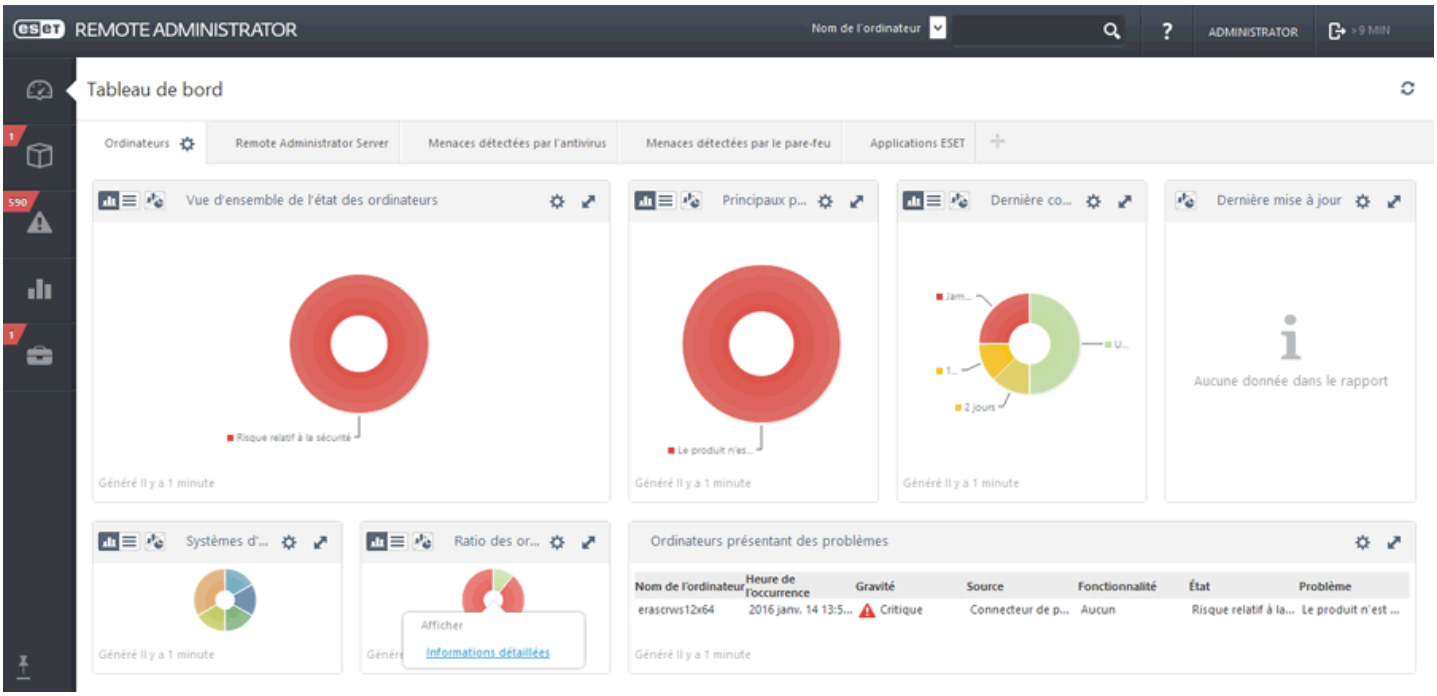
Saisissez l'**adresse IP** ou le **nom d'hôte** d'un ordinateur à ajouter. ESET Remote Administrator le recherche sur le réseau.



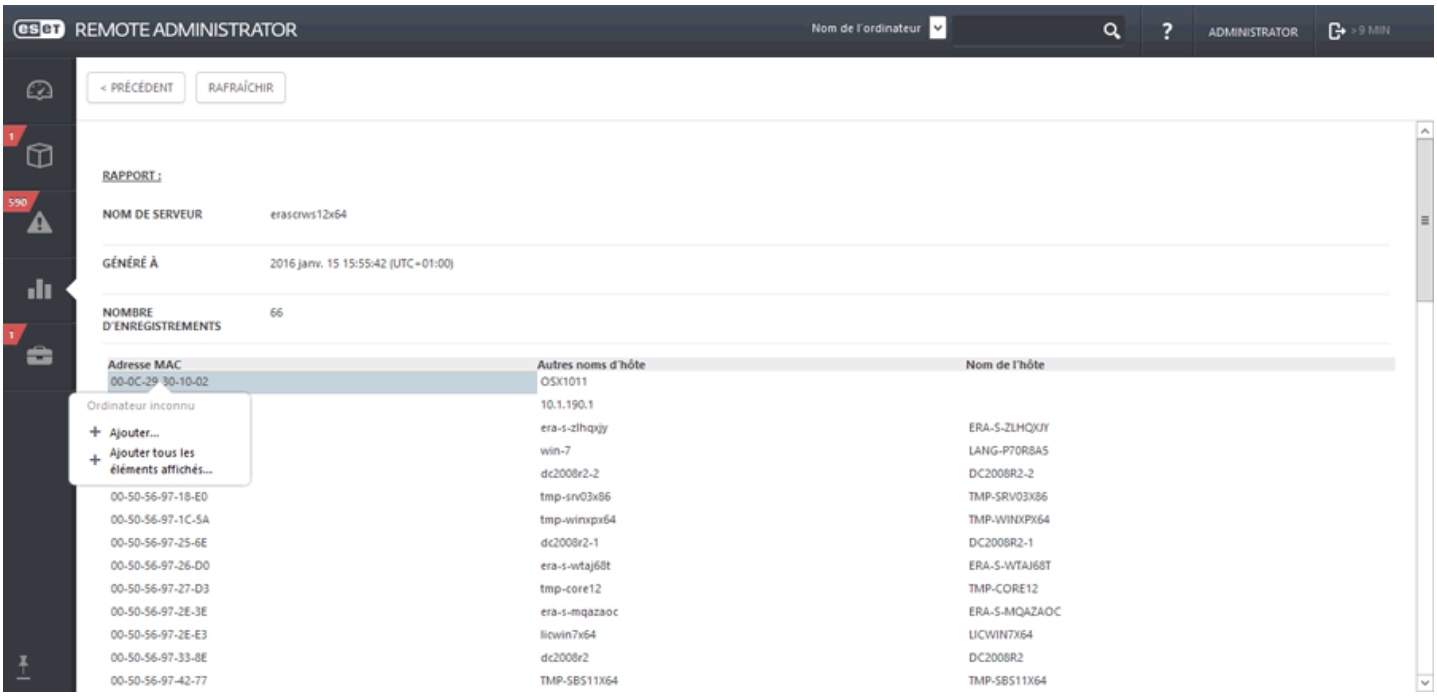
Cliquez sur **Ajouter**. Les ordinateurs sont visibles dans la liste de droite lorsque vous sélectionnez le groupe auquel ils appartiennent. Une fois l'ordinateur ajouté, une fenêtre indépendante s'affiche avec l'option **Déployer l'agent**.

2.6.1.3 Utilisation de RD Sensor

Si vous n'utilisez pas la synchronisation d'Active Directory, la méthode la plus simple pour ajouter un ordinateur à la structure ERA consiste à utiliser **RD Sensor**. Le composant RD Sensor fait partie du programme d'installation. Vous pouvez facilement explorer au niveau du détail le rapport **Ratio des ordinateurs non administrés**. Un graphique situé dans la partie inférieure du tableau de bord Ordinateurs vous permet de voir les ordinateurs non administrés (cliquez sur la partie rouge du graphique).

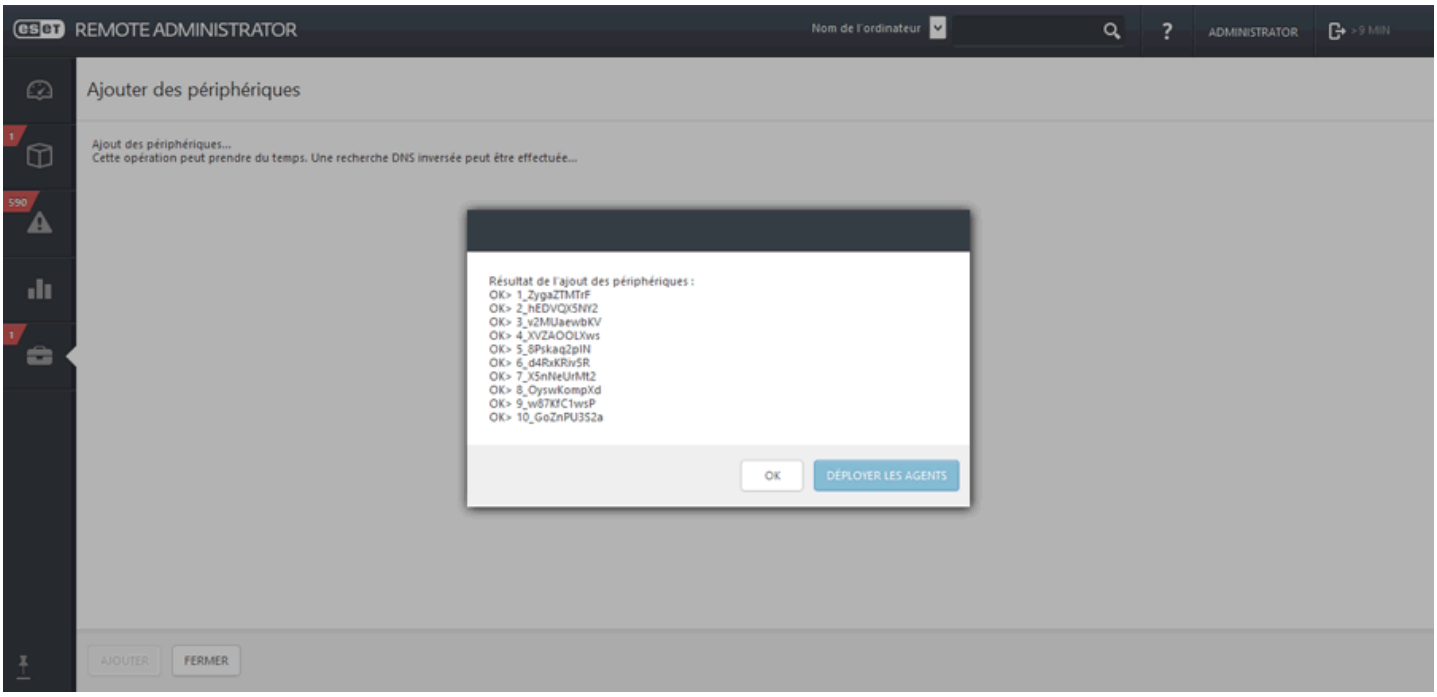


Dans le tableau de bord, le rapport **Ordinateurs non administrés** répertorie maintenant les ordinateurs détectés par RD Sensor. Pour ajouter un ordinateur, cliquez dessus, puis sur **Ajouter**. Vous pouvez également utiliser l'option **Ajouter tous les éléments affichés**.



Si vous ajoutez un seul ordinateur, suivez les instructions à l'écran. Vous pouvez utiliser un nom prédéfini ou indiquer le vôtre (il s'agit d'un nom d'affichage qui sera utilisé uniquement par la console Web ERA, et non d'un nom d'hôte réel). Vous pouvez également ajouter une description si vous le souhaitez. Si cet ordinateur existe déjà dans votre répertoire ERA, vous en êtes averti et pouvez choisir l'action à exécuter sur le doublon. Les options disponibles sont les suivantes : **Déployer l'agent**, **Ignorer**, **Réessayer**, **Déplacer**, **Dupliquer** et **Annuler**. Une fois l'ordinateur ajouté, une fenêtre indépendante s'affiche avec l'option **Déployer l'agent**.

Si vous cliquez sur **Ajouter tous les éléments affichés**, la liste des ordinateurs à ajouter s'affiche. Cliquez sur X en regard du nom d'un ordinateur spécifique si vous ne souhaitez pas l'inclure pour l'instant dans votre répertoire ERA. Lorsque vous avez terminé de supprimer des ordinateurs de la liste, cliquez sur Ajouter. Après avoir cliqué sur **Ajouter**, sélectionnez l'action à exécuter lorsqu'un doublon est détecté (l'affichage peut prendre quelques instants en fonction du nombre d'ordinateurs dans la liste) : **Ignorer**, **Réessayer**, **Déplacer**, **Dupliquer** et **Annuler**. Une fois une option sélectionnée, une fenêtre indépendante répertoriant tous les ordinateurs ajoutés s'affiche. Elle propose une option **Déployer les agents** pour effectuer le déploiement sur ces ordinateurs.



Les résultats de l'analyse de RD Sensor sont écrits dans un fichier journal appelé `detectedMachines.log`. Ce fichier contient la liste des ordinateurs détectés sur votre réseau. Vous pouvez trouver le fichier `detectedMachines.log` ici :

- Windows
  C:\ProgramData\ESET\Rouge Detection Sensor\Logs\detectedMachines.log
- Linux
  /var/log/eset/RogueDetectionSensor/detectedMachines.log

2.6.2 Déploiement d'agent

Le déploiement de l'Agent ERA peut être effectué de plusieurs manières différentes : Vous pouvez déployer l'Agent :

Utiliser GPO et SCCM à distance : cette méthode est recommandée pour le déploiement en masse d'ERA Agent sur des ordinateurs clients (vous pouvez aussi utiliser une tâche de serveur pour déployer ERA Agent).
Localement : à l'aide d'un package d'installation de l'Agent ou des programmes d'installation Agent Live, en cas de problème lors du déploiement à distance, par exemple.

Le déploiement local peut être effectué de trois manières différentes :

- Programmes d'installation Agent Live : à l'aide d'un script généré à partir de la console web ERA, vous pouvez distribuer les programmes d'installation Agent Live par courrier électronique ou les exécuter à partir d'un support amovible (clé USB, etc.).
- Installation assistée du serveur : à l'aide du package d'installation de l'Agent, cette méthode permet de télécharger automatiquement les certificats d'ERA Server (méthode de déploiement local recommandée).
- Installation hors ligne : à l'aide du package d'installation de l'Agent, vous devez exporter manuellement les certificats et les utiliser avec cette méthode de déploiement.

La tâche de serveur de déploiement d'agent à distance peut être utilisée pour la distribution en masse de l'Agent aux ordinateurs clients. Il s'agit de la méthode de distribution la plus pratique, car elle est peut être effectuée à partir de la console Web sans avoir à déployer manuellement l'Agent sur chaque ordinateur.

ERA Agent est un composant très important, car les solutions de sécurité ESET s'exécutant sur les clients communiquent avec ERA Server exclusivement par le biais de l'Agent.

REMARQUE : si vous rencontrez des problèmes lors du déploiement à distance d'ERA Agent (la tâche de serveur **Déploiement d'agent** échoue), reportez-vous au guide Dépannage.

2.6.2.1 Étapes de déploiement - Windows

1. Vérifiez que toutes les **conditions préalables requises** sont remplies :

- **ERA Server** et **ERA Web Console** sont installés (sur un ordinateur serveur).
- Un certificat d'Agent est créé et préparé sur votre lecteur local.
- Une autorité de certification est préparée sur le lecteur local.
- L'**ordinateur serveur** doit être accessible depuis le réseau.

REMARQUE : si vous rencontrez des problèmes lors du déploiement à distance d'ERA Agent (la tâche de serveur **Déploiement d'agent** se termine avec un état d'échec), reportez-vous au guide Dépannage.

2. Double-cliquez sur le package d'installation pour commencer l'installation.
3. Saisissez un **hôte du serveur** (nom d'hôte ou adresse IP) et le **port du serveur** (2222 par défaut) dans les champs correspondants. Ces paramètres sont utilisés pour la connexion à ERA Server.
4. Sélectionnez un certificat homologue et un mot de passe pour ce certificat. Vous pouvez éventuellement ajouter une autorité de certification. Elle n'est nécessaire que pour les certificats non signés.
5. Sélectionnez un dossier d'installation pour ERA Agent ou conservez le dossier prédéfini.
6. Cliquez sur **Installer**. ERA Agent est installé sur votre ordinateur.

REMARQUE : si un journal détaillé de l'installation est nécessaire, l'utilisateur doit démarrer l'installation par le biais du programme *msiexec* et indiquer les paramètres nécessaires :

```
msiexec /i program_installer.msi /lv* c:\temp\installer_log.txt
```

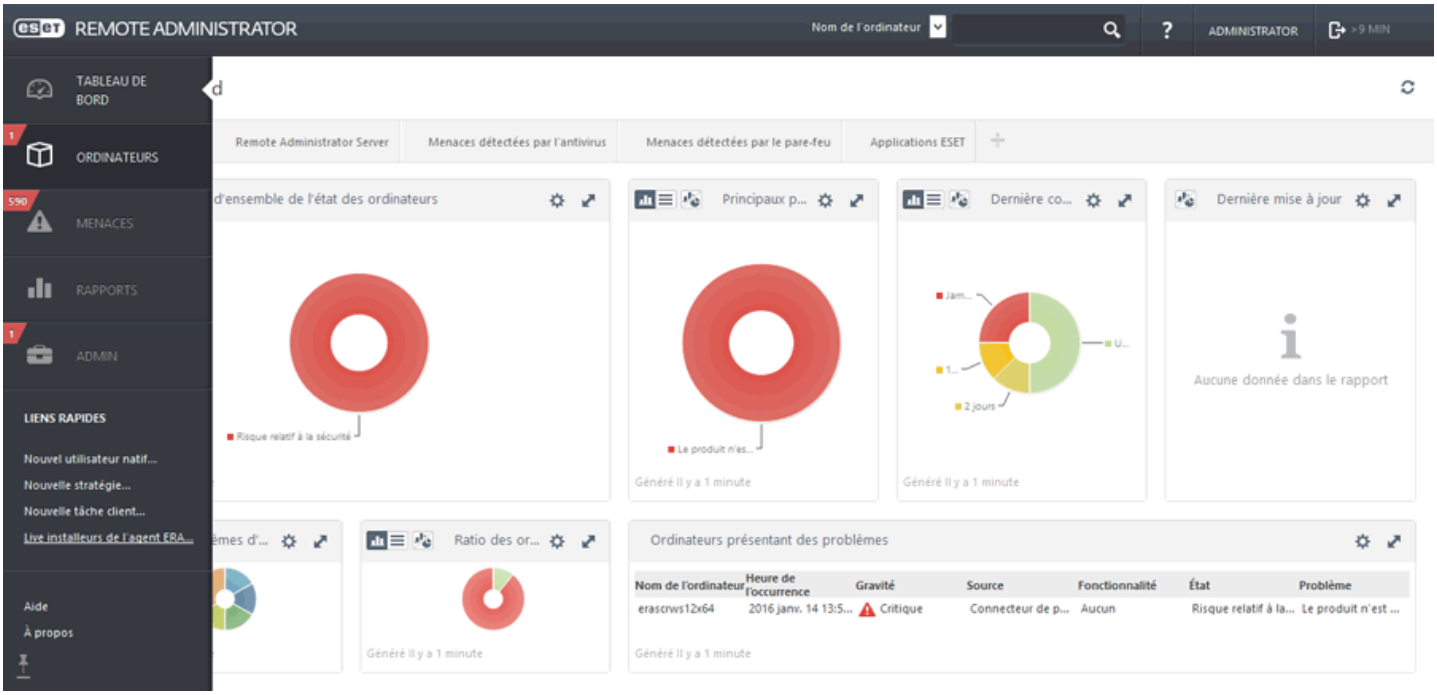
- Avant d'exécuter cette commande, le dossier *c:\temp* doit être créé.
- Vous pouvez consulter le journal d'état de l'ordinateur client *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html* pour vérifier qu'ERA Agent fonctionne correctement.

2.6.2.1.1 Programmes d'installation Agent Live

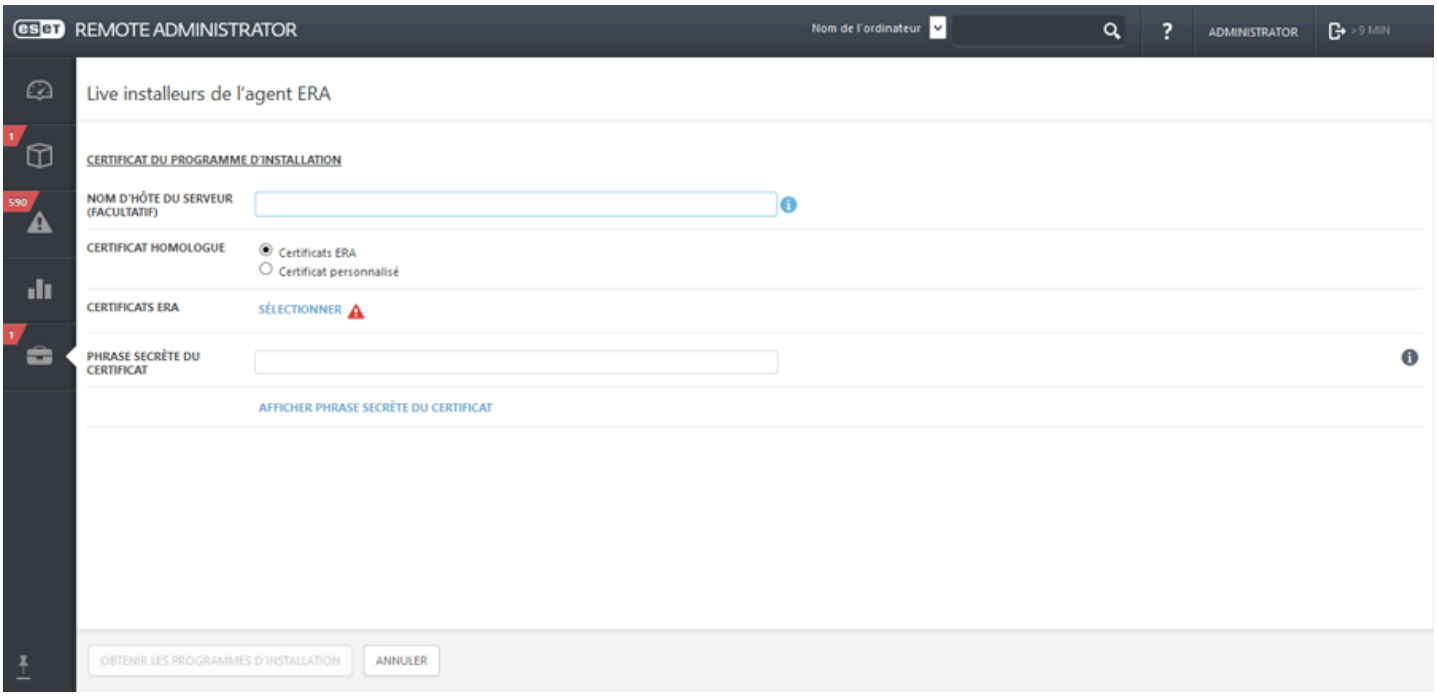
Ce type de déploiement d'agent s'avère utile lorsque les options de déploiement local et à distance ne vous conviennent pas. Dans ce cas, vous pouvez distribuer le programme d'installation Agent Live par courrier électronique et laisser l'utilisateur le déployer. Vous pouvez également l'exécuter à partir d'un support amovible (clé USB, etc.).

REMARQUE : l'ordinateur client doit disposer d'une connexion Internet pour télécharger le package d'installation de l'Agent. Il doit être également en mesure de se connecter à ERA Server. Vous pouvez suivre les instructions de l'article de la base de connaissances.

1. Dans la section **Accès rapides** de la barre de menus, cliquez sur **Programmes d'installation Agent Live...** pour créer le programme d'installation.



2. Saisissez l'adresse IP ou le nom d'hôte du serveur, puis sélectionnez l'**autorité de certification ERA** que vous avez créée lors de l'installation initiale. Saisissez la **phrase secrète de l'autorité de certification** créée lors de l'**installation du serveur** lorsque vous êtes invité à fournir le mot de passe du certificat.



3. Cliquez sur **Obtenir les programmes d'installation** pour générer les liens pour les fichiers du programme d'installation de l'Agent Windows, Linux et MAC.

4. Cliquez sur le lien **Télécharger** situé en regard du ou des fichiers du programme d'installation à télécharger, puis enregistrez le fichier **zip**. Décompressez le fichier sur l'ordinateur client sur lequel vous souhaitez déployer ERA Agent, puis exécutez le script `EraAgentOnlineInstaller.bat` (Windows) ou `EraAgentOnlineInstaller.sh` (Linux et Mac) pour exécuter le programme d'installation. Pour savoir comment déployer l'Agent ERA sur un client MAC OS X à l'aide du programme d'installation Agent Live, consultez notre article de la base de connaissances.

REMARQUE : si vous exécutez le script sous Windows XP SP2, vous devez installer Microsoft Windows Server 2003 Administration Tools Pack. Sinon, le programme d'installation Agent Live ne s'exécutera pas correctement. Une fois le pack d'administration installé, vous pouvez exécuter le script du programme d'installation Agent Live.

Vous pouvez consulter le journal d'état de l'ordinateur client *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html* pour vérifier qu'ERA Agent fonctionne correctement. En cas de problème lié à l'Agent (s'il ne se connecte pas à ERA Server, par exemple), reportez-vous à la section de dépannage.

- Si vous souhaitez déployer ERA Agent à l'aide du programme d'installation Agent Live à partir de votre dossier partagé local sans ESET Repository Download Server, procédez comme suit :

1. Modifiez le fichier `EraAgentOnlineInstaller.bat` (Windows) ou le script `EraAgentOnlineInstaller.sh` (Linux et Mac).
2. Modifiez les lignes 28 et 30 pour pointer vers les fichiers téléchargés localement. Par exemple :

```
27
28  set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.1.365.0/Agent_x64.msi
29  if defined IsArch_x86 (
30    set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.1.365.0/Agent_x86.msi
31  )
```

3. Utilisez votre propre URL (au lieu de celle indiquée ci-dessous) :

```
26  )
27
28  set url=\\server\share\Agent_x64.msi
29  if defined IsArch_x86 (
30    set url=\\server\share\Agent_x86.msi
31  )
```

4. Modifiez la ligne 80 pour remplacer " **^& packageLocation ^&** "

```
79  echo.
80  echo.Dim params: params = "/qr /i " ^& packageLocation ^& " /l*v %temp%\ra-agent-install.log" ^&_
```

par **!url!**

```
79  echo.
80  echo.Dim params: params = "/qr /i !url! /l*v %temp%\ra-agent-install.log" ^&_
```

5. **Enregistrez** le fichier.

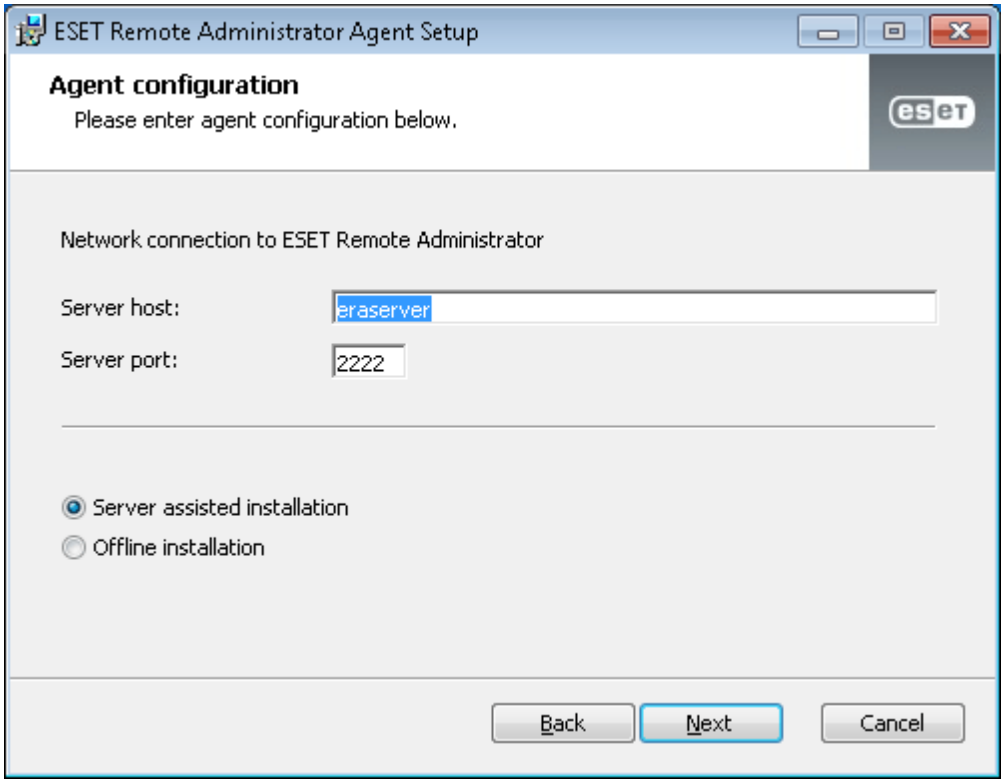
2.6.2.1.2 Déployer l'agent localement

Pour déployer ERA Agent localement sur un ordinateur client à l'aide de l'assistant d'installation, procédez comme suit :

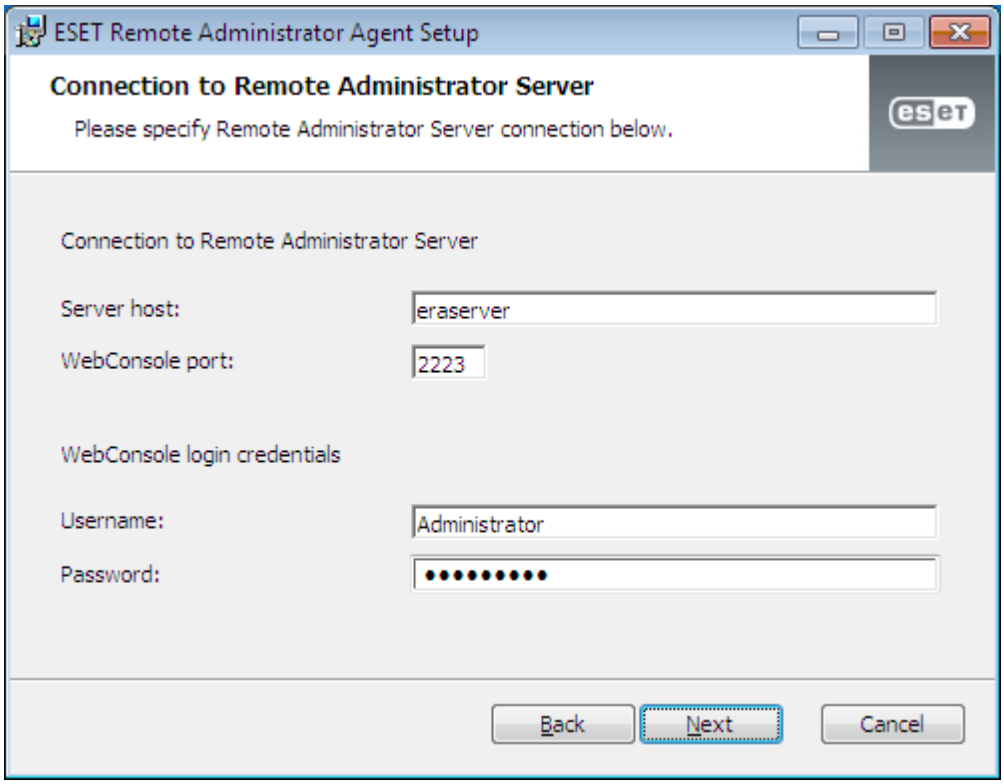
Téléchargez le package d'installation d'ERA Agent depuis la section des téléchargements du site Web ESET sous **Remote Administrator 6** (cliquez sur le signe **+** pour développer la catégorie) dans ESET Remote Administrator. Des **programmes d'installation autonomes** sont disponibles en téléchargement sous forme de composants. Exécutez le programme d'installation sur l'ordinateur client sur lequel vous souhaitez déployer l'Agent. Vous pouvez également consulter cet article de la base de connaissances ESET qui contient des instructions détaillées et illustrées.

1. **Installation assistée du serveur** :

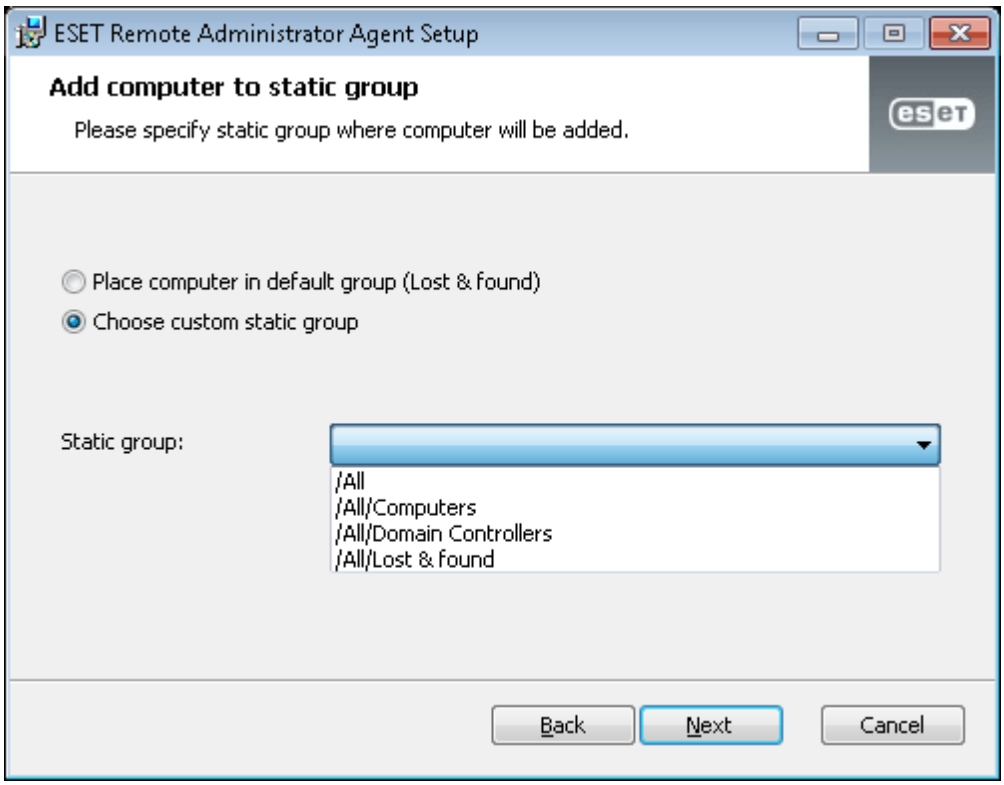
Vérifiez que l'option **Installation assistée du serveur** est sélectionnée, indiquez le **hôte du serveur** (nom ou adresse IP) et le **port du serveur** d'ERA Server, puis cliquez sur **Suivant**. Le port du serveur par défaut est 2222. Si vous utilisez un autre port, remplacez le port par défaut par le numéro de port personnalisé.



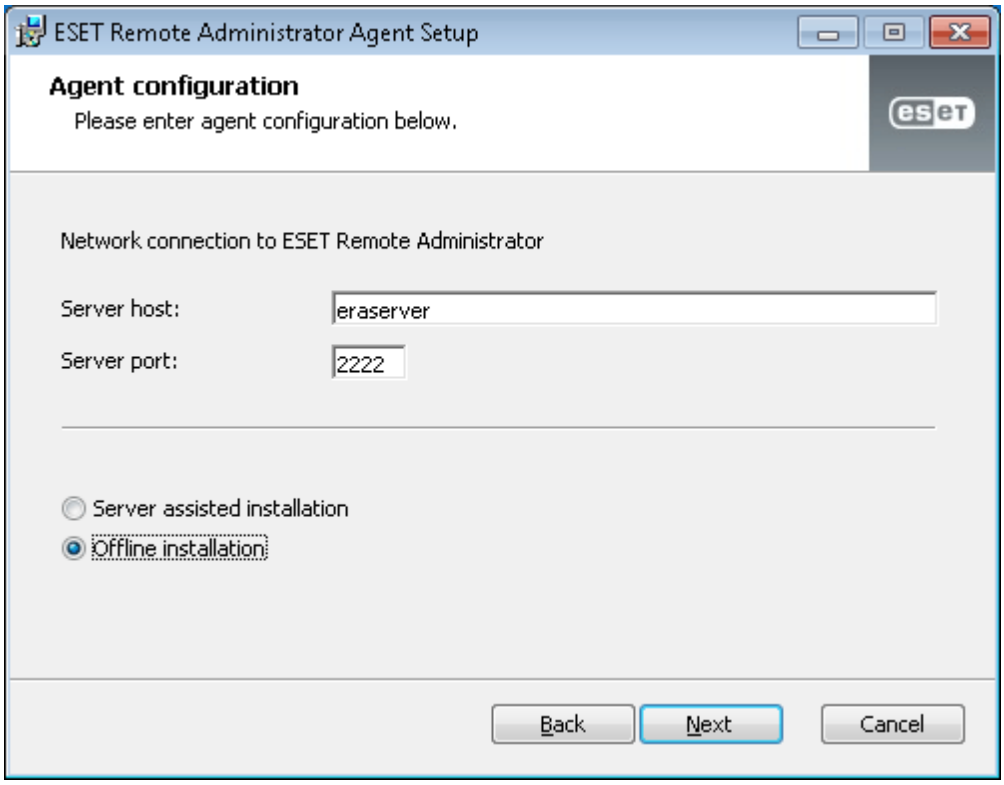
Indiquez la méthode utilisée pour les connexions à Remote Administrator Server : **ERA Server** ou **ERA Proxy Server** et le port d'ERA Web Console, puis saisissez les informations d'identification de connexion à ERA Web Console : **nom d'utilisateur** et **mot de passe**.



Cliquez sur **Choisir un groupe statique personnalisé** et sélectionnez dans le menu déroulant le groupe statique auquel l'ordinateur client sera ajouté.

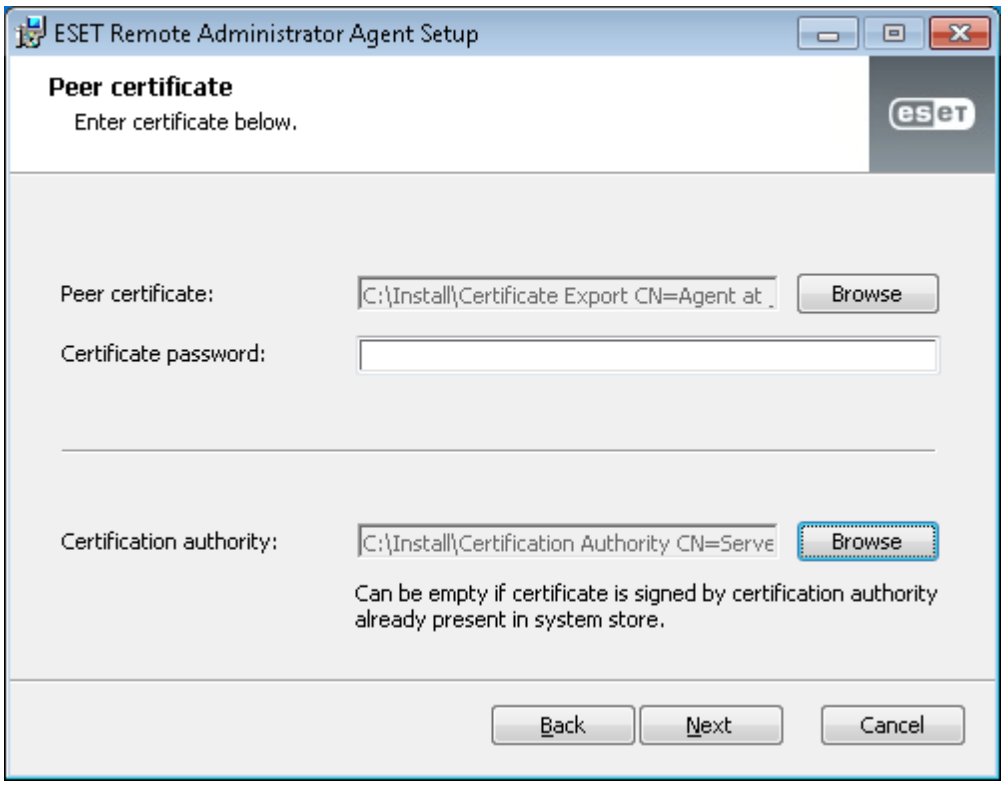


2. **Installation hors connexion** :



Pour effectuer une **installation hors connexion**, saisissez **2222** dans le champ **Port du serveur**, sélectionnez **Installation hors connexion**, puis cliquez sur **Suivant**. Pour cette méthode, vous devez indiquer un **certificat homologue** et une **autorité de certification**.

Pour plus d'informations sur l'exportation et l'utilisation d'un **certificat homologue** et d'une **autorité de certification**, cliquez ici.



REMARQUE : vous pouvez consulter le journal d'état d'un ordinateur client (situé dans *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html ou C:\Documents and Settings\All Users\Application Data\Eset\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.hmtl)*) pour vérifier qu'ERA Agent fonctionne correctement. En cas de problème lié à l'Agent (s'il ne se connecte pas à ERA Server, par

exemple), reportez-vous à la section de dépannage.

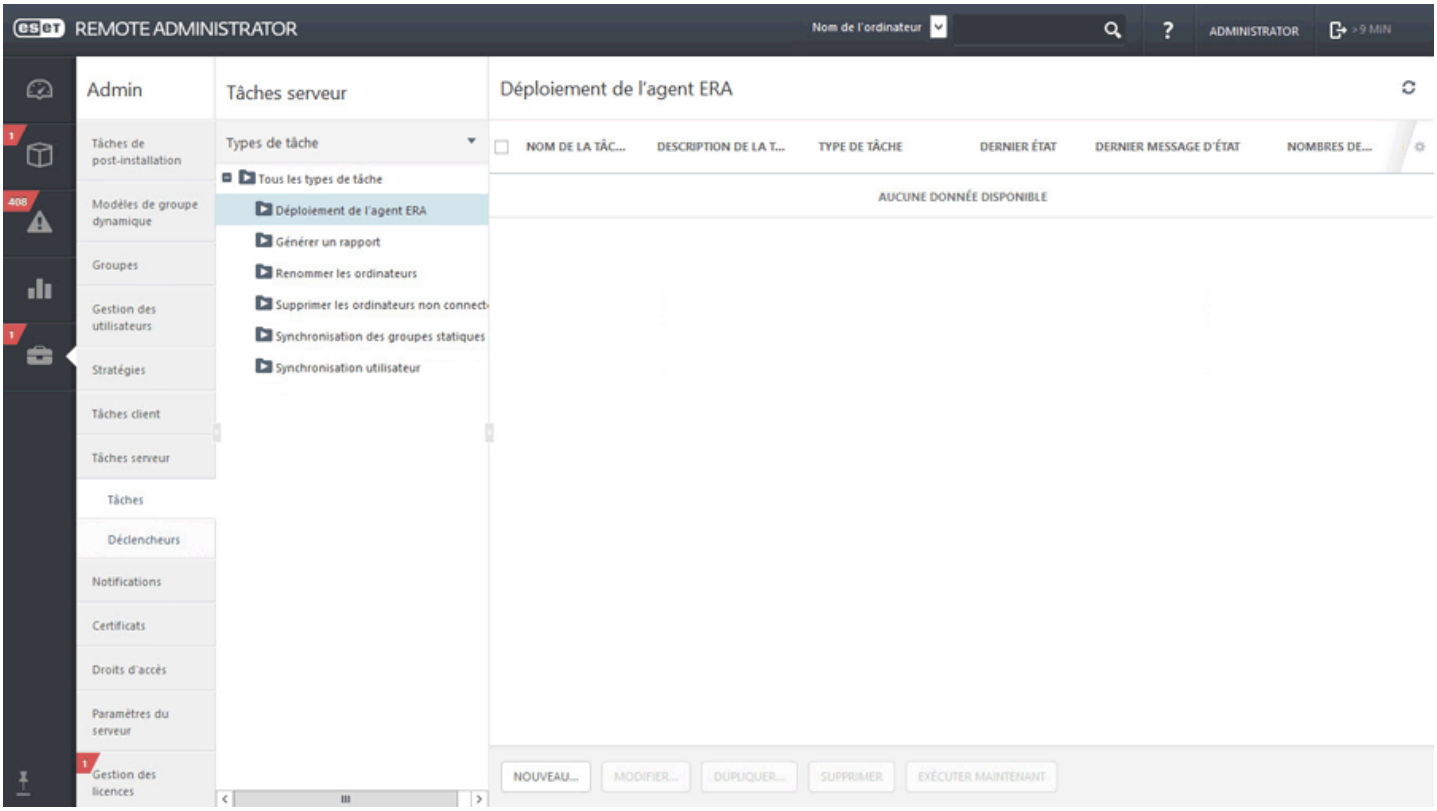
2.6.2.1.3 Déployer l'agent à distance

Vous pouvez déployer à distance ERA Agent de deux manières différentes. Vous pouvez utiliser une tâche de serveur comme décrit ci-dessous ou déployer l'Agent à l'aide de GPO et SCCM.

Le déploiement à distance d'ERA Agent à l'aide d'une tâche de serveur est effectué dans la section **Admin**. Vous pouvez suivre les instructions de l'article de la base de connaissances.

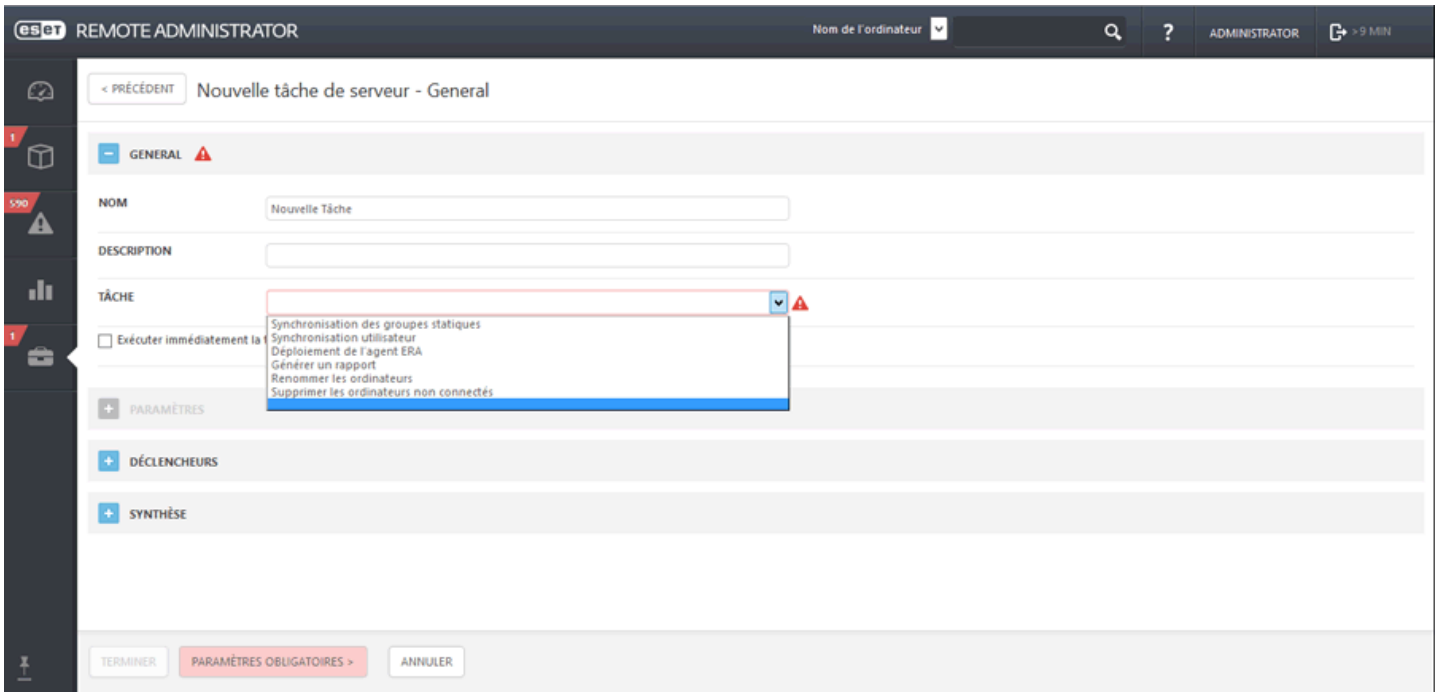
REMARQUE : il est recommandé de tester le déploiement en masse de l'Agent dans votre environnement avant de déployer ERA Agent dans des groupes importants de clients. Avant de tester le déploiement en masse, définissez l'intervalle de connexion de l'Agent selon vos besoins.

Cliquez sur **Tâche de serveur** > **Déploiement d'agent** > **Nouveau** pour configurer une nouvelle tâche.



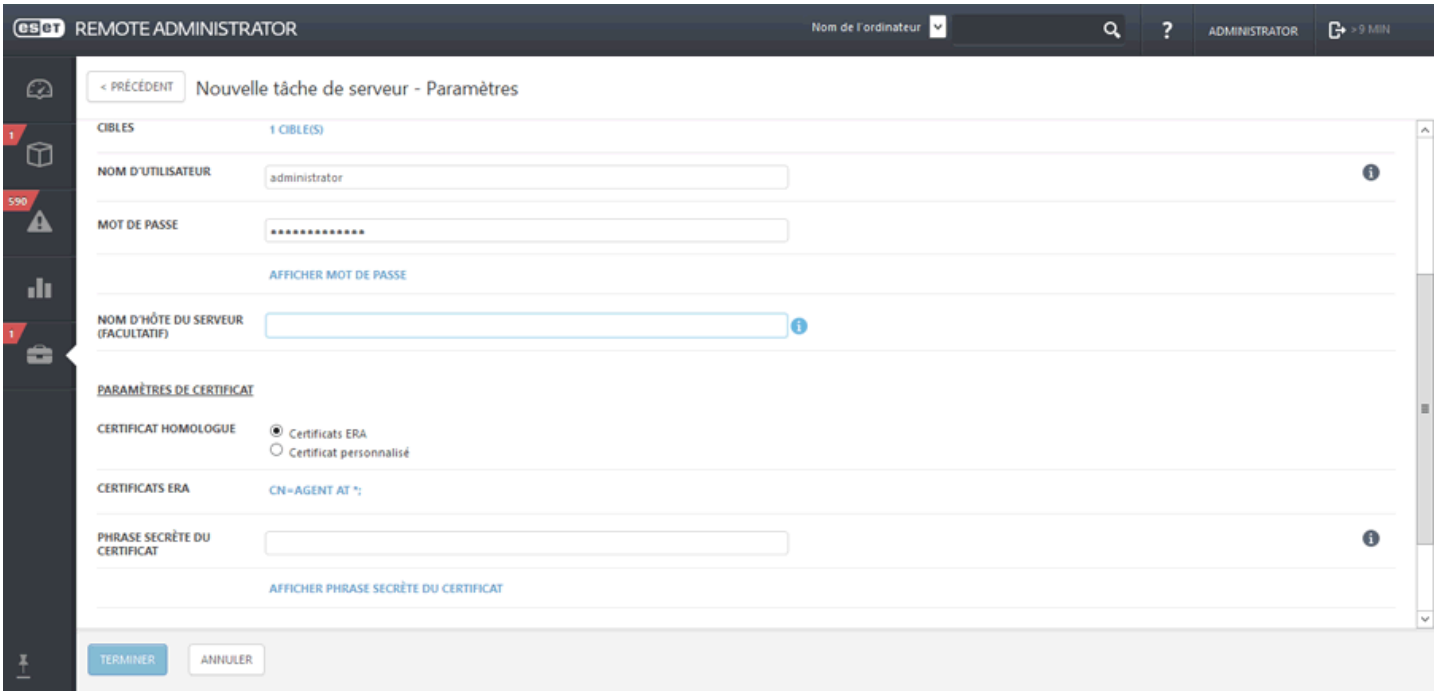
General

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** définit les paramètres et le comportement de la tâche.



Paramètres

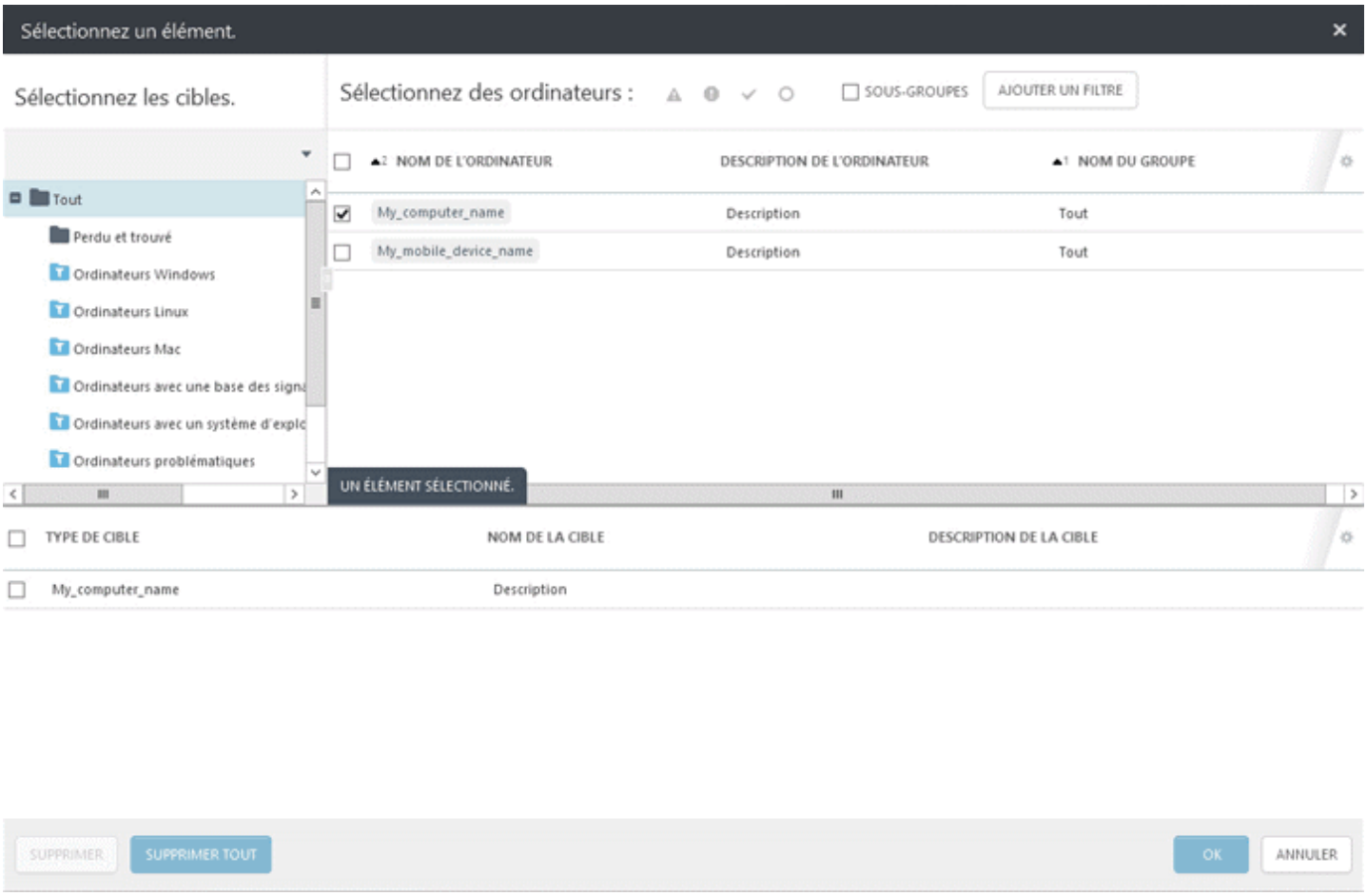
- **Résolution automatique de l'ERA Agent adéquat** : si vous disposez de plusieurs systèmes d'exploitation (Windows, Linux, Mac OS) dans votre réseau, sélectionnez cette option. La tâche recherche automatiquement le package d'installation de l'Agent adéquat compatible avec le serveur pour chaque système.
- **Cibles** : cliquez sur cette option pour sélectionner les clients destinataires de cette tâche.
- **Nom d'utilisateur/Mot de passe** : il s'agit du nom d'utilisateur et du mot de passe de l'utilisateur disposant de droits suffisants pour effectuer une installation à distance de l'Agent.
- **Nom d'hôte du serveur (facultatif)** : vous pouvez saisir un nom d'hôte du serveur s'il est différent du côté client et serveur.
- **Certificat homologue/Certificat ERA** : il s'agit du certificat de sécurité et de l'autorité de certification pour l'installation de l'Agent. Vous pouvez utiliser le certificat et l'autorité de certification par défaut ou des certificats personnalisés. Pour plus d'informations, reportez-vous au chapitre Certificats.
- **Certificat personnalisé** : si vous utilisez un certificat personnalisé pour l'authentification, accédez à celui-ci et sélectionnez-le lors de l'installation de l'Agent.
- **Phrase secrète du certificat** : il s'agit du mot de passe du certificat que vous avez saisi lors de l'installation du serveur (à l'étape de création d'une autorité de certification) ou du mot de passe de votre certificat personnalisé.



REMARQUE : ERA Server peut automatiquement sélectionner le package d'installation de l'ERA Agent adéquat pour les systèmes d'exploitation. Pour sélectionner manuellement un package, décochez l'option **Résolution automatique de l'Agent adéquat**, puis choisissez le package à utiliser parmi la liste des Agents disponibles dans le référentiel ERA.

Cible

La fenêtre **Cible** vous permet de spécifier les clients (ordinateurs ou groupes) destinataires de cette tâche. Cliquez sur **Ajouter des cibles** pour afficher tous les groupes statiques et dynamiques et leurs membres.



Sélectionnez des clients, cliquez sur **OK**, puis passez à la section Déclencheur.

Déclencheur : détermine l'événement qui déclenche la tâche.

- **Dès que possible** : exécute la tâche dès que le client se connecte à ESET Remote Administrator Server et la reçoit. Si la tâche ne peut pas être effectuée avant la **date d'expiration**, elle est retirée de la file d'attente. La tâche n'est pas supprimée, mais elle ne sera pas exécutée.
- **Déclencheur planifié** : exécute la tâche à une date sélectionnée. Vous pouvez planifier la tâche une seule fois, de manière répétée ou à l'aide d'une expression CRON.
- **Déclencheur lié au Journal des événements** : exécute la tâche selon les événements spécifiés dans cette zone. Ce déclencheur est invoqué lorsqu'un événement d'un certain type se produit dans les journaux. Définissez le **type de journal**, l'**opérateur logique** et les critères de **filtrage** qui déclencheront cette tâche.
- **Déclencheur A rejoint le groupe dynamique** : ce déclencheur exécute la tâche lorsqu'un client rejoint le groupe dynamique sélectionné dans l'option cible. Si un groupe statique ou un client a été sélectionné, cette option ne sera pas disponible.

REMARQUE : pour plus d'informations sur les déclencheurs, reportez-vous au chapitre Déclencheurs.

Paramètres avancés de la limitation : une limitation sert à limiter l'exécution d'une tâche si cette dernière est déclenchée par un événement qui se produit fréquemment, comme dans les cas **Déclencheur lié au Journal des événements** et **Déclencheur A rejoint le groupe dynamique** (voir ci-dessus). Pour plus d'informations, reportez-vous au chapitre Limitation.

Lorsque vous avez défini les destinataires et les déclencheurs de cette tâche, cliquez sur **Terminer**.

Résumé

Toutes les options configurées sont affichées dans cette section. Examinez les paramètres et s'ils sont corrects, cliquez sur Terminer. La tâche est alors créée et prête à être utilisée.

REMARQUE : si vous rencontrez des problèmes lors du déploiement à distance d'ERA Agent (la tâche de serveur **Déploiement d'agent** échoue), reportez-vous à la section Dépannage de ce guide.

2.6.2.2 Étapes de déploiement - Linux

Ces étapes s'appliquent à l'installation locale de l'Agent. Si vous souhaitez déployer l'Agent sur plusieurs ordinateurs, reportez-vous à la section Déploiement de l'Agent.

Vérifiez que les conditions préalables requises suivantes sont remplies :

- ERA Server et ERA Web Console sont installés (sur un ordinateur serveur).
- Un certificat d'agent a été créé et placé sur votre lecteur local.
- L'autorité de certification est préparée sur le lecteur local.
- L'**ordinateur serveur** doit être accessible depuis le réseau.
- Le fichier d'installation de l'Agent doit être défini comme exécutable (chmod +x).

L'Agent est installé en exécutant une commande sur le terminal (voir l'exemple ci-dessous).

Exemple
(Les nouvelles lignes sont signalée par une barre « \ » pour faciliter la copie de cette chaîne sur le terminal.)

```
./Agent-Linux-i686-1.0.387.0.sh --skip-license --cert-path=/home/adminko/Desktop/agent.pfx \
--cert-auth-path=/home/adminko/Desktop/CA.der --cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 --port=2222
```

ERA Agent et eraagent.service sont installés à l'emplacement suivant :
/opt/eset/RemoteAdministrator/Agent

Paramètres d'installation

Attribut	Description
`--skip-license`	L'installation ne demande pas à l'utilisateur de confirmer le contrat de licence.
`--cert-path`	Chemin d'accès au fichier de certificat de l'Agent.
`--cert-auth-path`	Chemin d'accès au fichier d'autorité de certification du serveur.
`--cert-password`	Doit correspondre au mot de passe du certificat de l'Agent.
`--hostname`	Connexion au serveur (ou au proxy) dans l'un des formats suivants : nom d'hôte, IPv4, IPv6 ou enregistrement SRV
`--port`	Port d'écoute : pour le serveur et le proxy (2222).

Pour vérifier si l'installation a été effectuée correctement, exécutez la commande suivante :

```
sudo service eraagent status
```

REMARQUE : lorsque vous utilisez un certificat que vous avez créé et qui a été signé par une autorité autre que l'autorité de certification ERA, vous devez laisser le paramètre *--cert-auth-path* en dehors du script d'installation, car l'autre autorité de certification est déjà installée sur votre système d'exploitation Linux (et votre ordinateur serveur).

REMARQUE : si vous rencontrez des problèmes lors du déploiement à distance d'ERA Agent (la tâche de serveur **Déploiement d'agent** se termine avec un état d'échec), reportez-vous au guide Dépannage.

Vous pouvez consulter le journal d'état de l'ordinateur client */var/log/eset/RemoteAdministrator/Agent/trace.log* ou */var/log/eset/RemoteAdministrator/Agent/status.html* pour vérifier qu'ERA Agent fonctionne correctement.

2.6.2.3 Étapes de déploiement - OS X

1. Vérifiez que toutes les **conditions préalables requises** sont remplies :

- **ERA Server** et **ERA Web Console** sont installés (sur un ordinateur serveur).
- Un certificat d'Agent est créé et préparé sur votre lecteur local.
- Une autorité de certification est préparée sur le lecteur local.

REMARQUE : si vous rencontrez des problèmes lors du déploiement à distance d'ERA Agent (la tâche de serveur **Déploiement d'agent** se termine avec un état d'échec), reportez-vous au guide Dépannage.

2. Double-cliquez sur le fichier *.dmg* pour démarrer l'installation.

3. Saisissez les données de **connexion du serveur** : l'**hôte du serveur** (nom d'hôte ou adresse IP d'ERA Server) et le **port du serveur** (2222 par défaut).

4. Sélectionnez un certificat homologue et un mot de passe pour ce certificat. Vous pouvez éventuellement ajouter une autorité de certification. Elle n'est nécessaire que pour les certificats non signés.

5. Examinez l'emplacement d'installation, puis cliquez sur **Installer**. L'**Agent** est installé sur votre ordinateur.

6. Le fichier journal d'ERA Agent se trouve à cet emplacement : */Library/Application Support/com.eset.remoteadministrator.agent/Logs/* ou */Users/%user%/Library/Logs/EraAgentInstaller.log*

2.6.2.4 Protection de l'agent

L'Agent ERA est protégé par un mécanisme d'autodéfense. Rôles de cette fonctionnalité :

- Protection des entrées de Registre de l'Agent ERA contre la modification (HIPS)
- Protection des fichiers de l'agent ERA contre la modification, le remplacement, la suppression ou l'altération (HIPS)
- Protection du processus de l'Agent ERA contre l'arrêt
- Protection du service de l'Agent ERA contre l'arrêt, la pause, la désactivation, la désinstallation ou toute autre mise en péril

Une partie de la protection est assurée par la fonctionnalité HIPS, qui fait partie de votre produit de sécurité ESET (par exemple ESET Endpoint Security).

REMARQUE : Pour garantir une totale protection de l'Agent ERA, HIPS doit être activé sur un ordinateur client.

Configuration protégée par mot de passe
En plus de l'autodéfense, vous pouvez protéger par mot de passe l'accès à l'Agent ERA (disponible pour Windows uniquement). Quand un mot de passe est utilisé, l'Agent ERA ne peut pas être désinstallé ni réparé sans la fourniture du mot de passe correct. Pour définir un mot de passe pour l'Agent ERA, vous devez créer une stratégie pour l'Agent ERA.

2.6.2.5 Dépannage - Déploiement de l'Agent

Il est possible que vous rencontriez des problèmes lors du déploiement d'ERA Agent. Si c'est le cas, les causes de l'échec peuvent être multiples. Cette section vous permet d'effectuer les opérations suivantes :

- rechercher les raisons de l'échec du déploiement d'ERA Agent ;
- rechercher les causes possibles dans le tableau ci-dessous ;
- résoudre le problème et réussir le déploiement.

Windows

1. Pour déterminer les raisons de l'échec du déploiement de l'Agent, accédez à **Rapports** > **Automatisation**, sélectionnez Informations sur les tâches de déploiement d'agent au cours des 30 derniers jours**, puis** cliquez sur Générer maintenant.
Un tableau comportant des informations sur le déploiement s'affiche. La colonne **Progression** affiche les messages d'erreur associés à l'échec du déploiement de l'Agent.

Si vous avez besoin d'informations plus détaillées, vous pouvez modifier le niveau de détail du journal de suivi d'ERA Server. Accédez à **Admin** > **Paramètres du serveur** > **Paramètres avancés** > **Journalisation**, puis sélectionnez **Erreur** dans le menu déroulant. Réexécutez le déploiement de l'Agent et au moment de l'échec, recherchez les dernières entrées du fichier journal de suivi d'ERA Server dans la partie inférieure du fichier. Le rapport comprend des suggestions pour la résolution du problème.

Le dernier fichier journal d'ERA Server se trouve à cet emplacement : *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\trace.log*

Le dernier fichier journal d'ERA Agent se trouve à cet emplacement : *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* *C:\Documents and Settings\All Users\Application Data\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs*

Pour activer la journalisation complète, créez un fichier factice appelé **traceAll** sans extension dans le dossier d'un fichier journal trace.log. Redémarrez le service ESET Remote Administrator Server pour activer la journalisation complète dans le fichier **trace.log**.

REMARQUE : en cas de problèmes liés à la connexion d'ERA Agent, consultez Dépannage - Connexion de l'Agent pour obtenir des informations supplémentaires.

Si l'installation échoue avec l'erreur 1603, vérifiez le fichier *ra-agent-install.log*. Il figure à cet emplacement : *C:\Users\%user%\AppData\Local\Temp\ra-agent-install.log* sur l'ordinateur cible.

2. Le tableau suivant contient les raisons possibles de l'échec du déploiement de l'Agent :

Message d'erreur	Cause possible
Connexion impossible.	Le client n'est pas accessible sur le réseau. Impossible de résoudre le nom d'hôte du client. Le pare-feu bloque les communications. Les ports 2222 et 2223 ne sont pas ouverts dans le pare-feu (du côté client et serveur).
Accès refusé.	Aucun mot de passe n'est défini pour le compte administrateur. Les droits d'accès sont insuffisants. Le partage administratif ADMIN$ n'est pas disponible. Le partage administratif IPC$ n'est pas disponible. L'option Utiliser le partage de fichiers simple est activée.
Package introuvable dans le référentiel.	Le lien vers le référentiel est incorrect. Le référentiel n'est pas disponible. Le référentiel ne contient pas le package requis.

3. Suivez la procédure de dépannage qui correspond à la cause possible :

- Le client n'est pas accessible sur le réseau. - Effectuez un test ping du client à partir d'ERA Server. Si vous obtenez une réponse, essayez de vous connecter à distance à l'ordinateur client (via le Bureau à distance, par exemple).
- Impossible de résoudre le nom d'hôte du client. - Les solutions possibles aux problèmes DNS peuvent inclure, entre autres, les solutions suivantes :

  Utilisation de la commande `nslookup` de l'adresse IP et du nom d'hôte du serveur et/ou des clients rencontrant des problèmes liés au déploiement de l'Agent. Les résultats doivent correspondre aux informations de l'ordinateur. Par exemple, une commande `nslookup` d'un nom d'hôte doit être résolue en l'adresse IP affichée par la commande `ipconfig` sur l'hôte en question. La commande `nslookup` doit être exécutée sur les clients et le serveur.

  Recherche manuelle de doublons dans les enregistrements DNS.
- Le pare-feu bloque les communications. - Vérifiez les paramètres du pare-feu sur le serveur et le client, ainsi que de tout autre pare-feu existant entre ces deux ordinateurs (le cas échéant).

- Les ports 2222 et 2223 ne sont pas ouverts dans le pare-feu. - Comme ci-dessus, vérifiez que ces ports sont ouverts sur tous les pare-feu entre les deux ordinateurs (client et serveur).
- Aucun mot de passe n'est défini pour le compte administrateur. - Définissez un mot de passe correct pour le compte administrateur (n'utilisez pas de mot de passe vide).
- Les droits d'accès sont insuffisants. - Essayez d'utiliser les informations d'identification de l'administrateur de domaine lors de la création d'une tâche de déploiement d'agent. Si l'ordinateur client se trouve dans un groupe de travail, utilisez le compte Administrateur local sur cet ordinateur spécifique.
- Le partage administratif ADMIN$ n'est pas disponible. - La ressource partagée ADMIN$ doit être activée sur l'ordinateur client. Vérifiez qu'elle se trouve parmi les autres partages (**Démarrer** > **Panneau de configuration** > **Outils d'administration** > **Gestion de l'ordinateur** > **Dossiers partagés** > **Partages**).
- Le partage administratif IPC$ n'est pas disponible. - Vérifiez que le client peut accéder à IPC en saisissant la commande suivante dans l'invite de commandes du client :

  ```
  net use \\nom_serveur\IPC$
  ```

  où *nom_serveur* correspond au nom d'ERA Server.
- L'option Utiliser le partage de fichiers simple est activée. - Si un message d'erreur « Accès refusé » s'affiche et si vous disposez d'un environnement mixte (composé d'un domaine et d'un groupe de travail), désactivez la fonctionnalité **Utiliser le partage de fichiers simple** ou **Utiliser l'Assistant Partage** sur tous les ordinateurs rencontrant un problème lié au déploiement de l'Agent. Sous Windows 7, par exemple, procédez comme suit :
  - Cliquez sur **Démarrer**, saisissez `dossier` dans la zone de rechercher, puis cliquez sur **Options des dossiers**. Cliquez sur l'onglet **Affichage**, puis, dans la zone Paramètres avancés, faites défiler la liste jusqu'à la case à cocher **Utiliser l'Assistant Partage** et décochez-la.
- Le lien vers le référentiel est incorrect. - Dans ERA Web Console, accédez à **Admin** > **Paramètres du serveur**, puis cliquez sur **Paramètres avancés** > **Référentiel**. Vérifiez que l'URL du référentiel est correcte.
- Package introuvable dans le référentiel - Ce message d'erreur s'affiche généralement lorsqu'il n'existe aucune connexion au référentiel ERA. Vérifiez la connexion Internet.

REMARQUE : pour les systèmes d'exploitation Windows plus récents (Windows 7, Windows 8, etc.), il est nécessaire d'activer le compte d'utilisateur Administrateur pour exécuter la tâche de déploiement d'agent.

Pour activer le compte d'utilisateur Administrateur :

1. Ouvrez une invite de commandes d'administration.
2. Saisissez la commande suivante :

   ```
   net user administrator /active:yes
   ```

Linux et Mac OS

Si le déploiement de l'Agent ne fonctionne pas sous Linux ou Mac OS, il s'agit généralement d'un problème lié à SSH. Vérifiez l'ordinateur client pour vous assurer que le démon SSH est en cours d'exécution. Une fois ce problème résolu, réexécutez le déploiement de l'Agent.

2.6.2.6 Dépannage - Connexion de l'Agent

Lorsqu'un ordinateur client ne semble pas se connecter à ERA Server, il est recommandé d'effectuer le dépannage d'ERA Agent localement sur l'ordinateur client.
Par défaut, ERA Agent effectue une synchronisation avec ERA Server toutes les 20 minutes. Vous pouvez modifier ce paramètre en créant une stratégie pour l'intervalle de connexion d'ERA Agent.

Consultez le dernier fichier journal d'ERA Agent. Il figure à cet emplacement :
C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs
C:\Documents and Settings\All Users\Application Data\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs

REMARQUE : pour activer la journalisation complète, créez un fichier factice appelé **traceAll** sans extension dans le dossier d'un fichier journal trace.log. Redémarrez ensuite le service ESET Remote Administrator Server pour activer la journalisation complète dans le fichier **trace.log**.

- **last-error.html** : protocole (tableau) qui affiche la dernière erreur enregistrée pendant l'exécution d'ERA Agent.
- **software-install.log** : protocole de texte de la dernière tâche d'installation à distance effectuée par ERA Agent.
- **status.html** : tableau indiquant l'état actuel des communications (synchronisation) d'ERA Agent avec ERA Server.
- **trace.log** : rapport détaillé de toutes les activités d'ERA Agent, y compris les erreurs consignées.

Les problèmes les plus courants qui peuvent empêcher ERA Agent de se connecter à ERA Server sont les suivants :
- Votre réseau interne n'est pas configuré correctement. Vérifiez que l'ordinateur sur lequel ERA Server est installé peut communiquer avec les ordinateurs client sur lesquels ERA Agent est installé.
- ERA Server n'est pas configuré pour l'écoute sur le port 2222.
- DNS ne fonctionne pas correctement ou les ports sont bloqués par un pare-feu : consultez la liste des ports utilisés par ESET Remote Administrator ou l'article Quels adresses et ports dois-je ouvrir sur mon pare-feu tiers pour permettre un fonctionnement optimal de mon produit ESET ? de la base de connaissances.
- Un certificat généré par erreur qui contient des fonctionnalités limitées ou incorrectes et qui ne correspond pas à la clé publique de l'autorité de certification ERA Server est présent. Créez un autre certificat ERA Agent pour résoudre ce problème.

2.6.3 Déploiement de l'Agent à l'aide de GPO et SCCM

Après l'installation d'ESET Remote Administrator, il est nécessaire de déployer **ERA Agent** et les produits de sécurité ESET sur les ordinateurs clients du réseau.

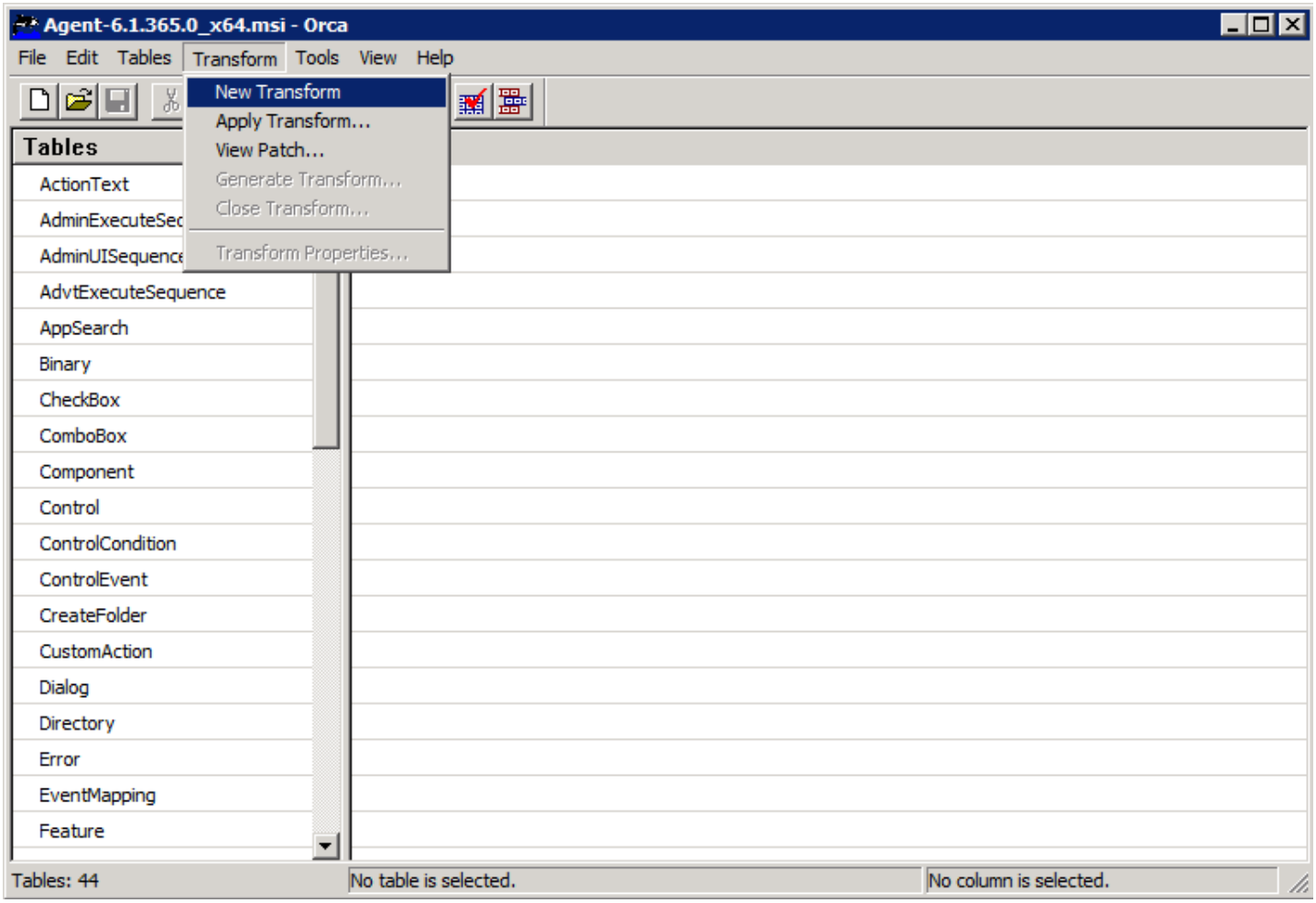
En dehors d'un déploiement local ou d'un déploiement à distance à l'aide d'une tâche de serveur, vous pouvez également utiliser des outils d'administration tels que GPO, SCCM, Symantec Altiris ou Puppet. Pour obtenir des instructions détaillées relatives aux deux méthodes de déploiement courantes d'ERA Agent, cliquez sur le lien adéquat suivant :

1. Déploiement d'ERA Agent à l'aide de GPO
2. Déploiement d'ERA Agent à l'aide de SCCM

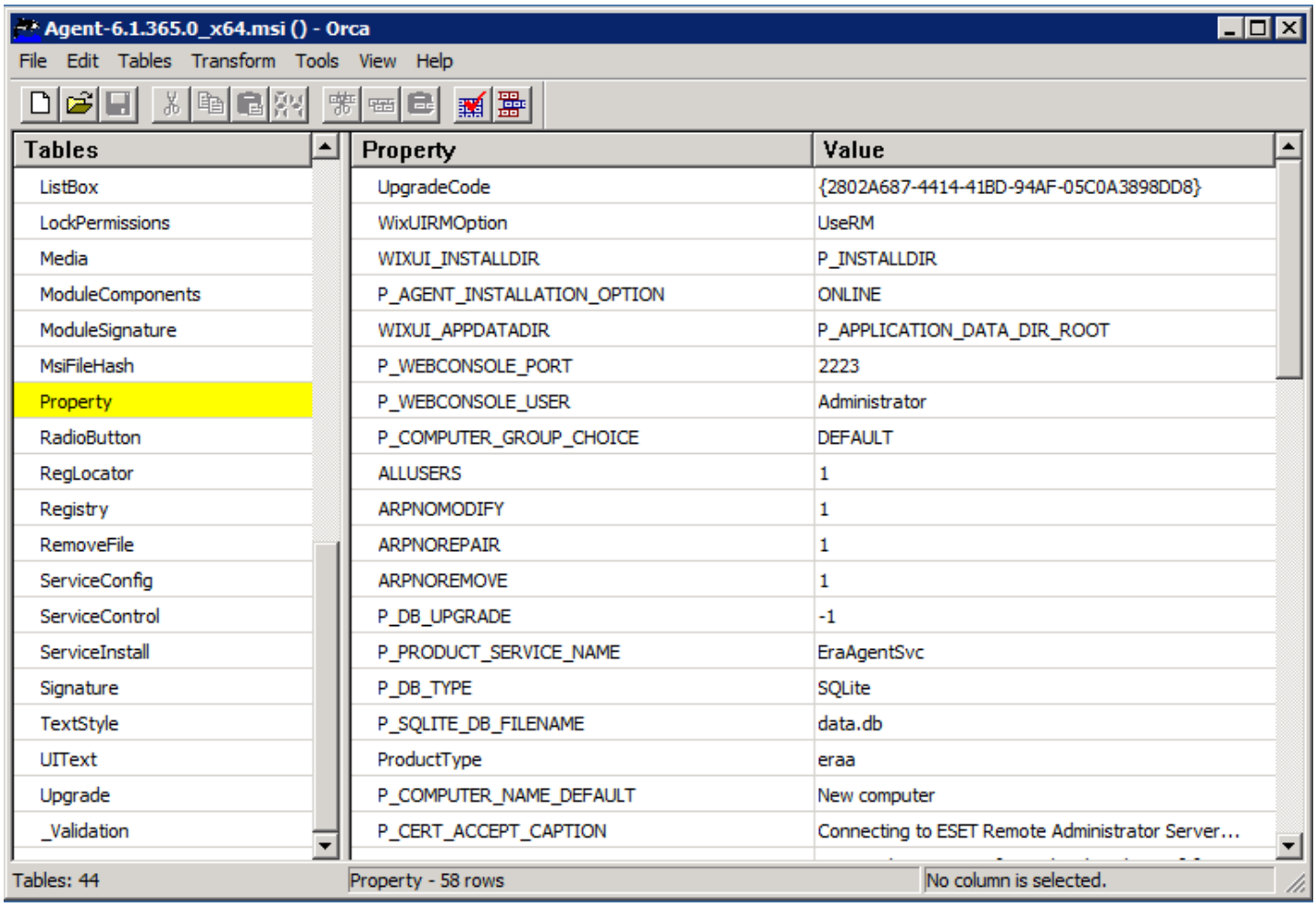
2.6.3.1 Création d'un fichier MST

Avant de déployer le fichier d'installation d'ERA Agent, vous devez créer un fichier de transformation `.mst` avec des paramètres pour ERA Agent. Installez Orca (cet éditeur fait partie du Kit de développement logiciel (SDK) Windows). Pour plus d'informations sur Orca, reportez-vous à l'article http://support.microsoft.com/kb/255905/.

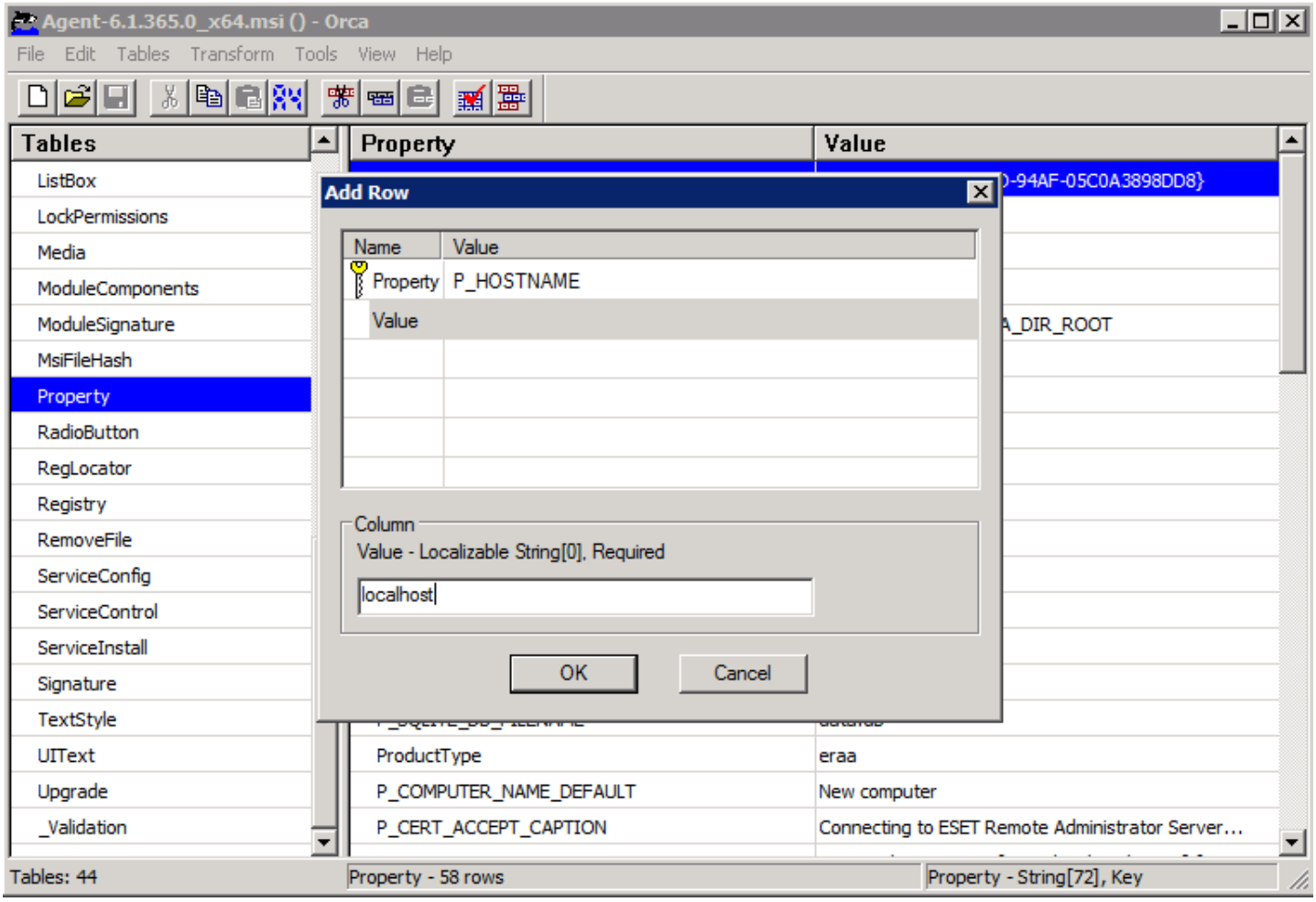
1. Téléchargez le programme d'installation d'**ERA Agent**. Vous pouvez par exemple utiliser le fichier `Agent-6.1.365.0_x64.msi` qui est un composant d'ERA version 6.1.28.0 pour les systèmes 64 bits. Pour obtenir la liste des versions du composant ERA, consultez notre base de connaissances.
2. Ouvrez Orca en cliquant sur Démarrer > **Programmes** > **Orca**.
3. Cliquez sur **File (Fichier)** dans le menu supérieur, sur **Open (Ouvrir)**, puis accédez au fichier `Agent-6.1.365.0_x64.msi`.
4. Cliquez sur **Transform (Transformation)** dans le menu supérieur, puis sélectionnez **New Transform (Nouvelle transformation)**.



6. Cliquez sur **Property (Propriété)**.



7. Cliquez avec le bouton droit n'importe où dans la liste des valeurs de propriété, puis sélectionnez **Add Row (Ajouter une ligne)** dans le menu contextuel.
8. Ajoutez la propriété **P_HOSTNAME**, puis saisissez le nom d'hôte ou l'adresse IP d'ERA Server dans le champ **Value (Valeur)**.
9. Répétez les étapes 7 à 8 pour ajouter la propriété P_PORT, où la valeur correspond au port par défaut utilisé pour se connecter à ERA Server (2222).



10. Pour ERA Agent, ajoutez le certificat homologue (`.pfx`) signé par l'autorité de certification et stocké dans la base de données d'ERA Server. Ajoutez la clé publique de l'autorité de certification (fichier `.der`) qui a été utilisé pour signer le certificat homologue ERA Server.

- **Pour ajouter des certificats, vous pouvez procéder de deux manières différentes :**

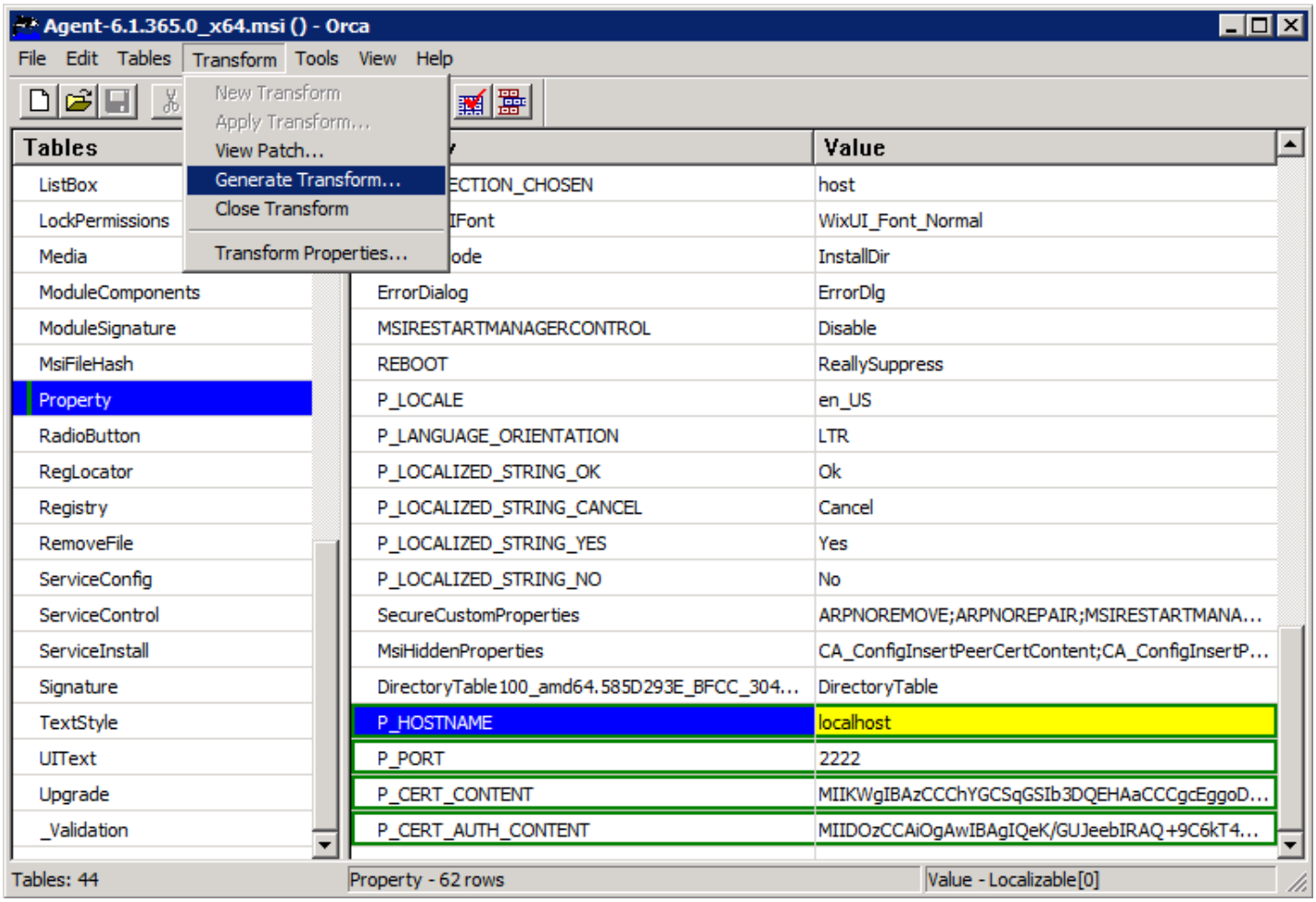
1. Vous pouvez ajouter le contenu du certificat et de la clé publique codé au **format Base64** (aucun fichier de certificat n'est nécessaire).

- Dans ERA Web Console, accédez à **Admin** > **Certificats** > **Certificat homologue**, cliquez sur **Certificat de l'Agent**, puis sélectionnez **Exporter en Base64...**.
- Accédez à **Admin** > **Certificats** > **Autorités de certification**, cliquez sur Autorité de certification ERA, puis sélectionnez **Exporter la clé publique en Base64**.
- Dans Orca, ajoutez le contenu du certificat et de la clé publique exportés au tableau des propriétés à l'aide des noms de propriété suivants :

Nom de la propriété	Valeur
P_CERT_CONTENT	<certificat homologue au format Base64>
P_CERT_PASSWORD	<mot de passe du certificat homologue (n'ajoutez pas cette valeur lorsque le mot de passe est vide)>

P_CERT_AUTH_CONTENT	<clé publique exportée de l'autorité de certification au format Base64>
P_CERT_AUTH_PASSWORD	<mot de passe de l'autorité de certification (n'ajoutez pas cette valeur lorsque le mot de passe est vide)>

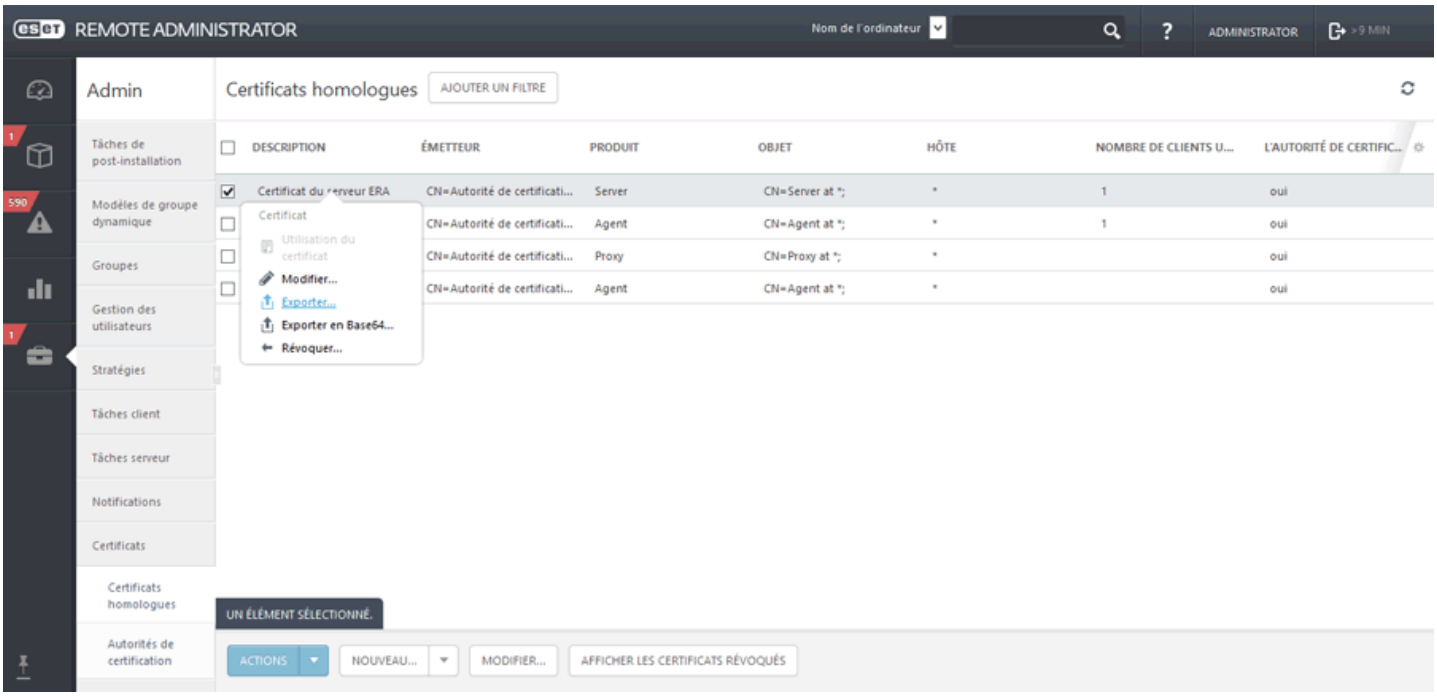
- Les nouvelles propriétés sont surlignées en vert. Cliquez sur **Transform (Transformation)**, puis sélectionnez **Generate transform...(Générer une transformation)** pour créer un fichier `.mst`.



2. Vous pouvez télécharger les fichiers de certificat et les rendre accessibles à partir de l'ordinateur cible. Exportez le **certificat homologue de l'Agent** et le fichier de la **clé publique** à partir de l'**autorité de certification** d'ERA Server et placez-les dans un dossier accessible à partir de l'ordinateur cible sur lequel est installé ERA Agent.

- Accédez à **Admin** > **Certificats** > **Certificat homologue**, cliquez sur **Certificat de l'Agent**, puis sélectionnez **Exporter...**

- Accédez à **Admin** > **Certificats** > **Autorités de certification**, cliquez sur **Autorité de certification**, puis sélectionnez **Exporter la clé publique**.



- Utilisez les fichiers exportés et ajoutez leur chemin d'accès dans le tableau des propriétés d'Orca à l'aide des noms de propriété suivants :

Nom de la propriété	Valeur
P_CERT_PATH	<chemin d'accès au certificat `.pfx` > (spécifiez le chemin d'accès au fichier de certificat en incluant l'extension)
P_CERT_PASSWORD	<mot de passe du certificat `.pfx` (n'ajoutez pas cette valeur si le mot de passe est vide)>
P_CERT_AUTH_PATH	<chemin d'accès à la clé publique exportée de l'autorité de certification>
P_CERT_AUTH_PASSWORD	<mot de passe de l'autorité de certification (n'ajoutez pas cette valeur lorsque le mot de passe est vide)>

- Les propriétés ajoutées sont surlignées en vert. Cliquez sur **Transform (Transformation)**, puis sélectionnez **Generate transform...(Générer une transformation)** pour créer un fichier `.mst`.

Commande (si vous avez généré un fichier de transformation portant le nom AgentSettings) : `msiexec /i Agent-6.1.265.0_x64.msi /qn TRANSFORMS="AgentSettings.mst"`

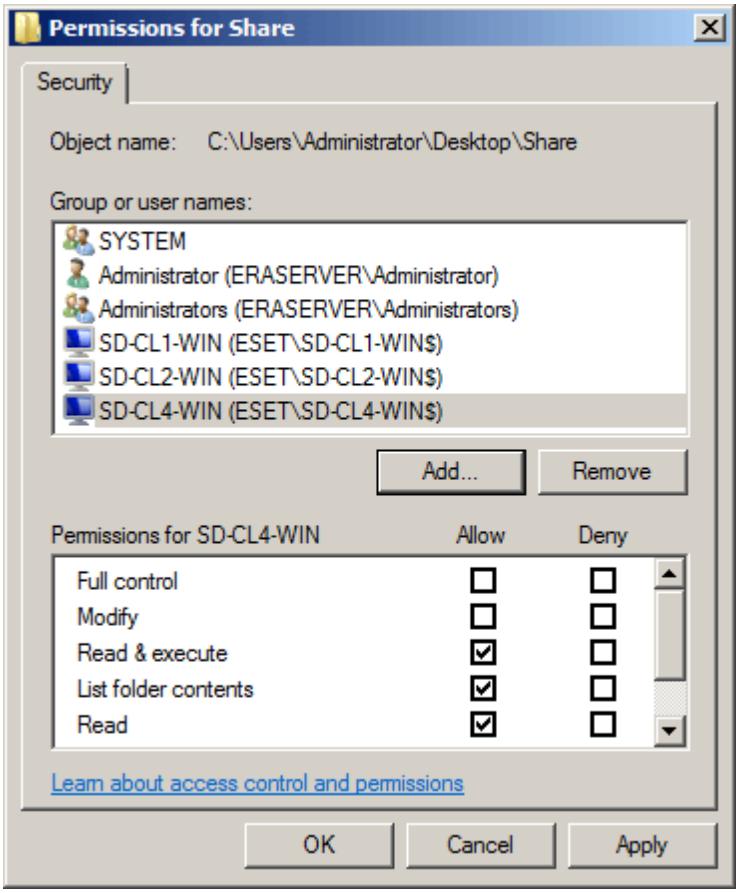
Pour créer un journal d'installation, exécutez plutôt cette commande : `msiexec /i Agent-6.1.265.0_x64.msi /qn TRANSFORMS="AgentSettings.mst" /L*v! log.txt`

2.6.3.2 Étapes de déploiement - GPO

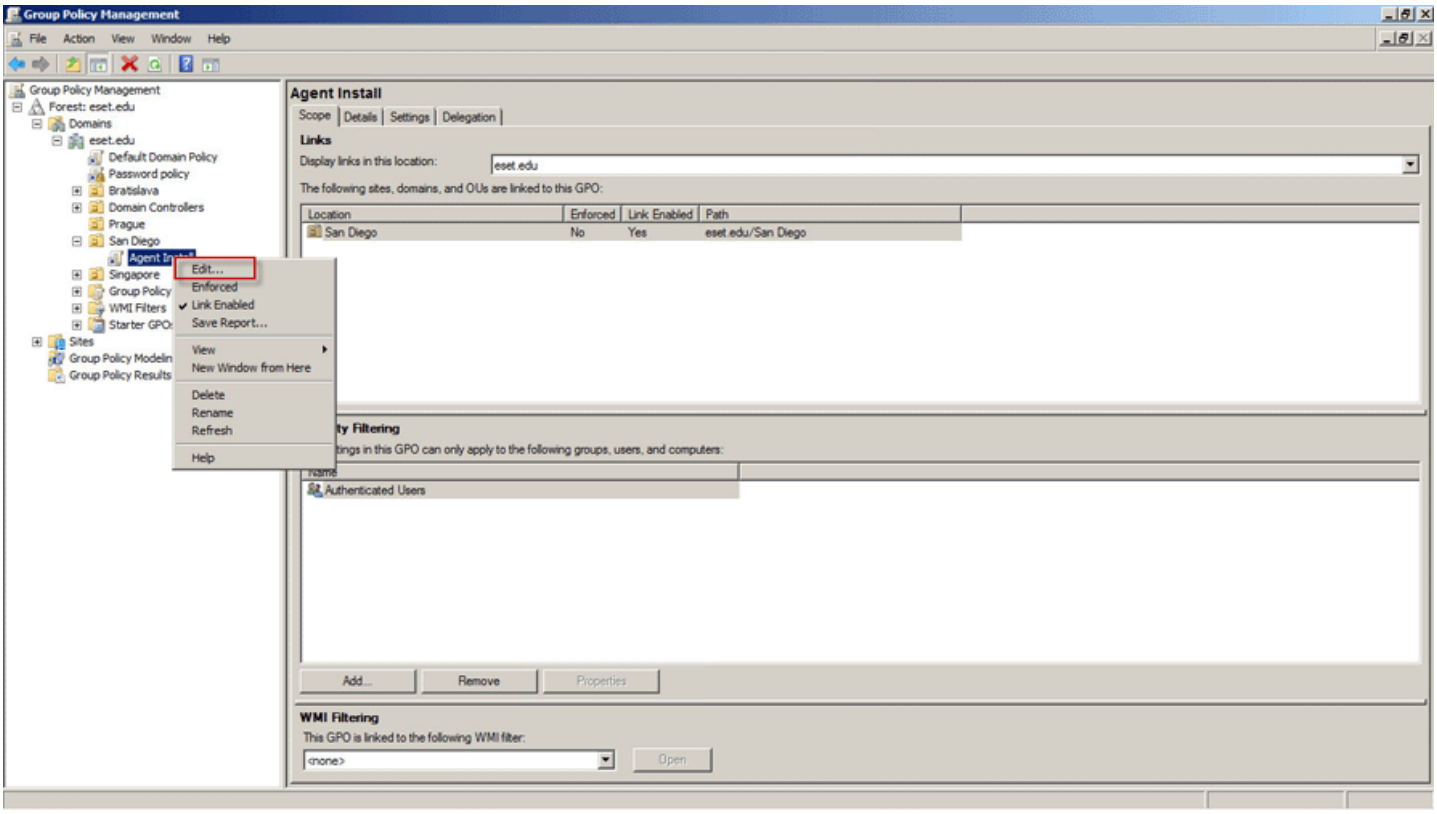
Pour déployer ERA Agent sur les clients à l'aide de GPO, suivez la procédure décrite ci-dessous ou consultez l'article de la base de connaissances :

1. Téléchargez le fichier `.msi` du programme d'installation d'ERA Agent à partir de la page de téléchargement ESET.
2. Créez un fichier .mst de transformation du programme d'installation d'ERA Agent.
3. Placez le fichier `.msi` du programme d'installation d'ERA Agent et le fichier `.mst` de transformation dans un dossier partagé accessible par le ou les clients cibles.

REMARQUE : les ordinateurs clients nécessitent un accès en lecture/exécution à ce dossier partagé.

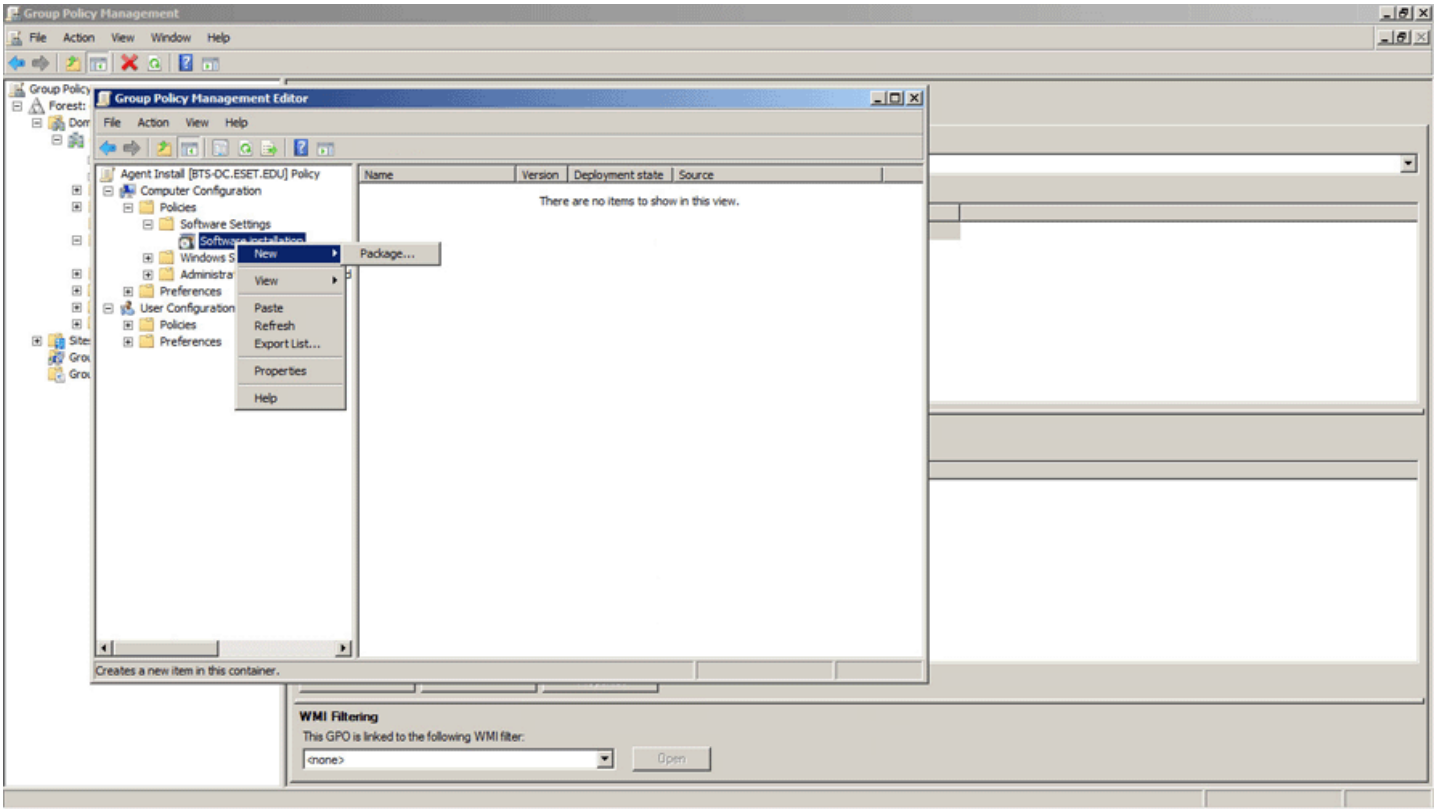


4. Utilisez un objet de stratégie de groupe existant ou créez-en un (cliquez avec le bouton droit sur GPO, puis cliquez sur **Nouveau**). Dans l'arborescence GPMC (Console de gestion des stratégies de groupe), cliquez avec le bouton droit sur l'objet de stratégie de groupe à utiliser, puis sélectionnez **Modifier...**.



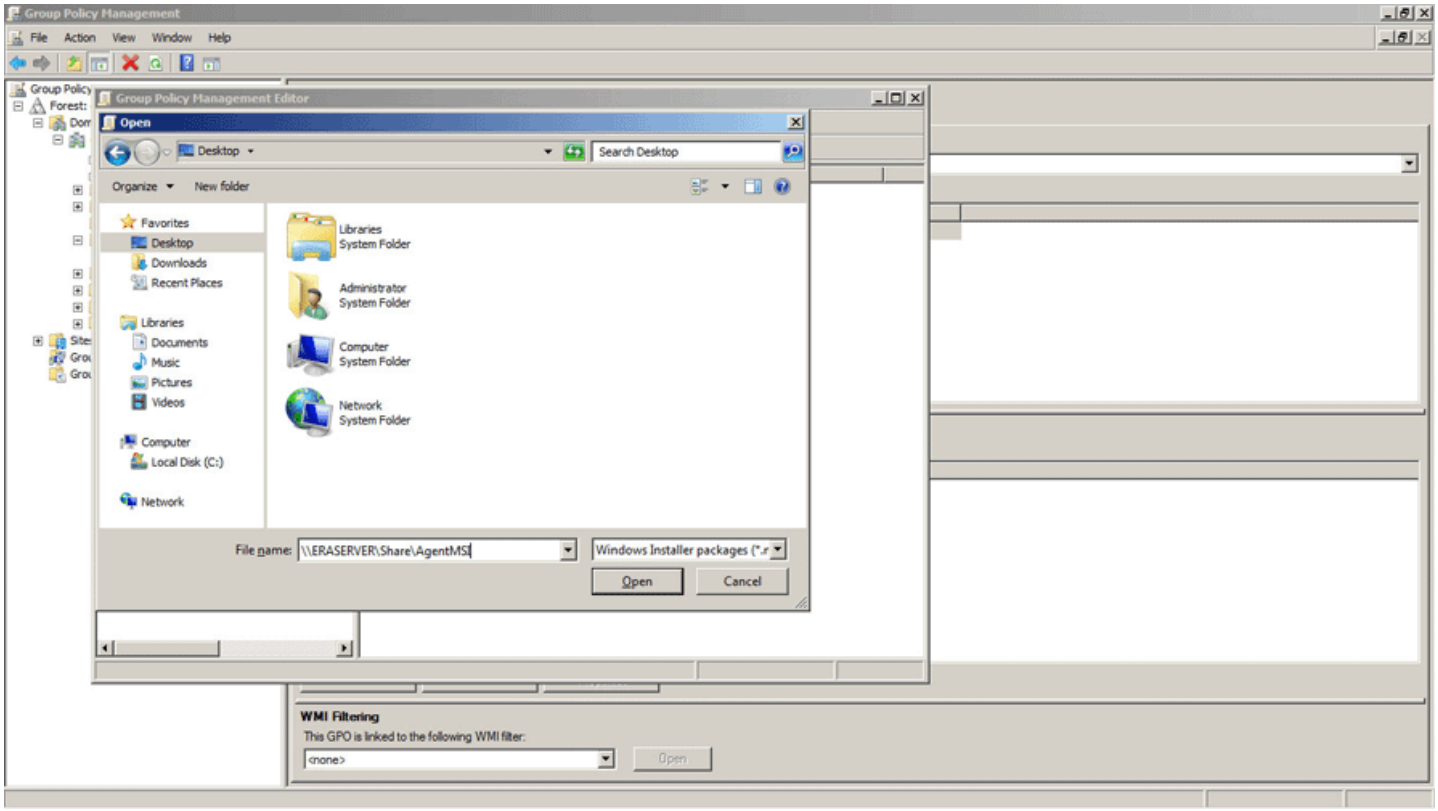
5. Dans Configuration ordinateur, accédez à **Stratégies** > **Paramètres du logiciel** > **Paramètres du logiciel**.

6. Cliquez avec le bouton droit sur **Installer un logiciel**, sélectionnez **Nouveau**, puis cliquez sur **Package...** pour créer une configuration de package.

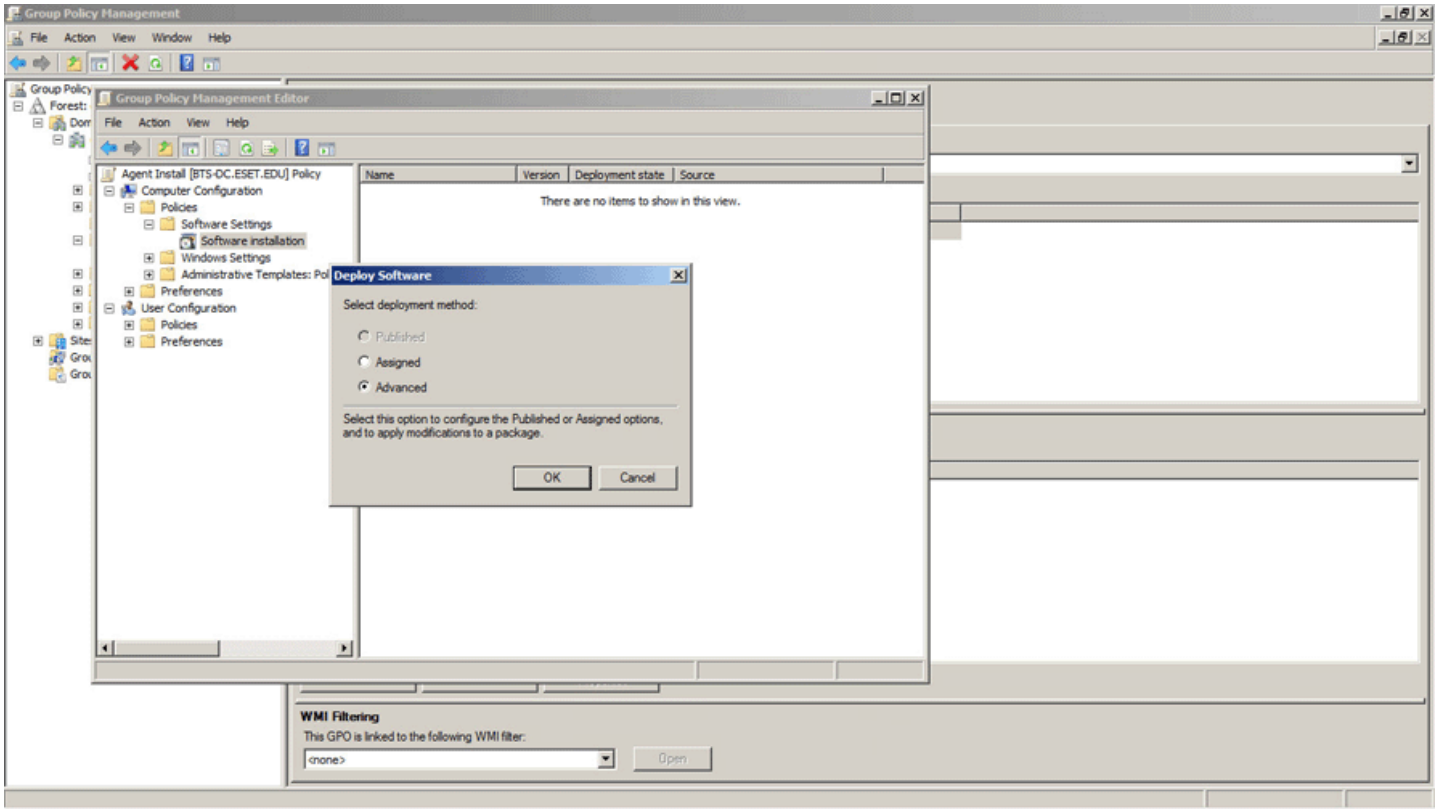


7. Accédez à l'emplacement du fichier `.msi` d'ERA Agent. Dans la boîte de dialogue Ouvrir, saisissez le chemin UNC complet au package d'installation partagé que vous souhaitez utiliser, Par exemple : `\\fileserver\share\filename.msi`

REMARQUE : veillez à utiliser le chemin UNC du package d'installation partagé.

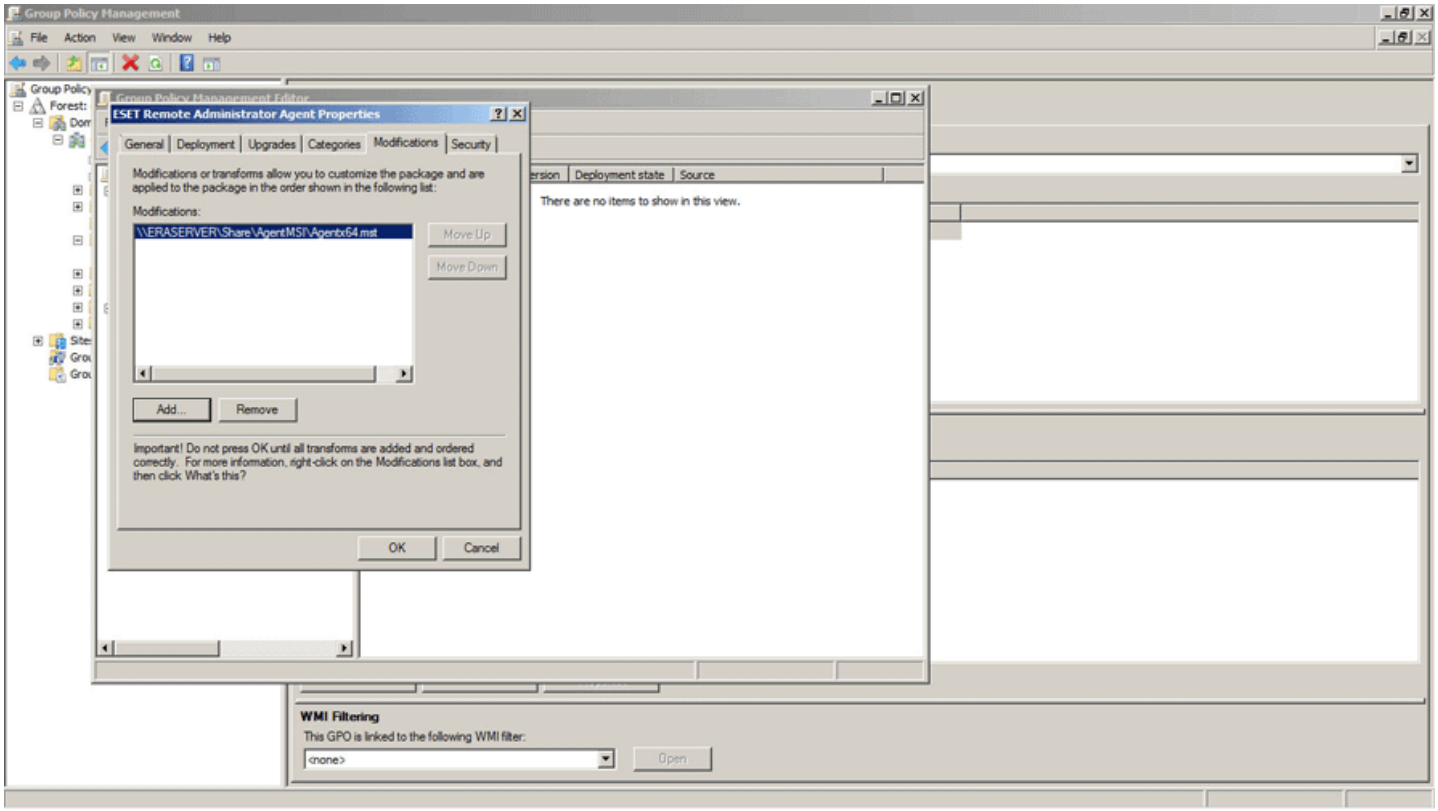


8. Cliquez sur **Ouvrir**, puis choisissez la méthode de déploiement **Avancé**.

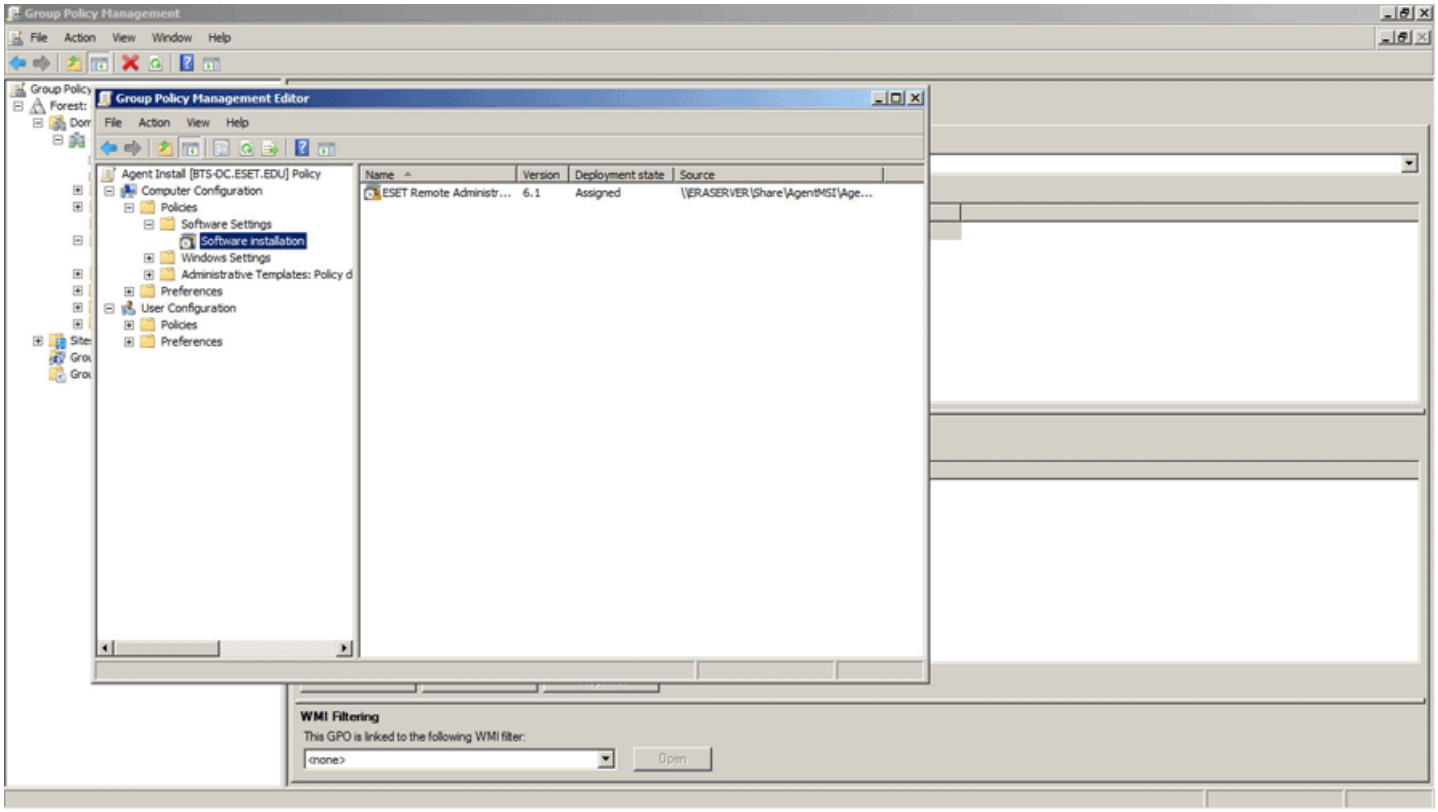


9. Vous pouvez ainsi configurer des options de déploiement. Sélectionnez l'onglet **Modifications**, puis accédez au fichier `.mst` de transformation du programme d'installation d'ERA Agent.

REMARQUE : le chemin d'accès doit pointer vers le même dossier partagé que celui utilisé à l'étape 7.



10. Confirmez la configuration du package, puis poursuivez le déploiement GPO.

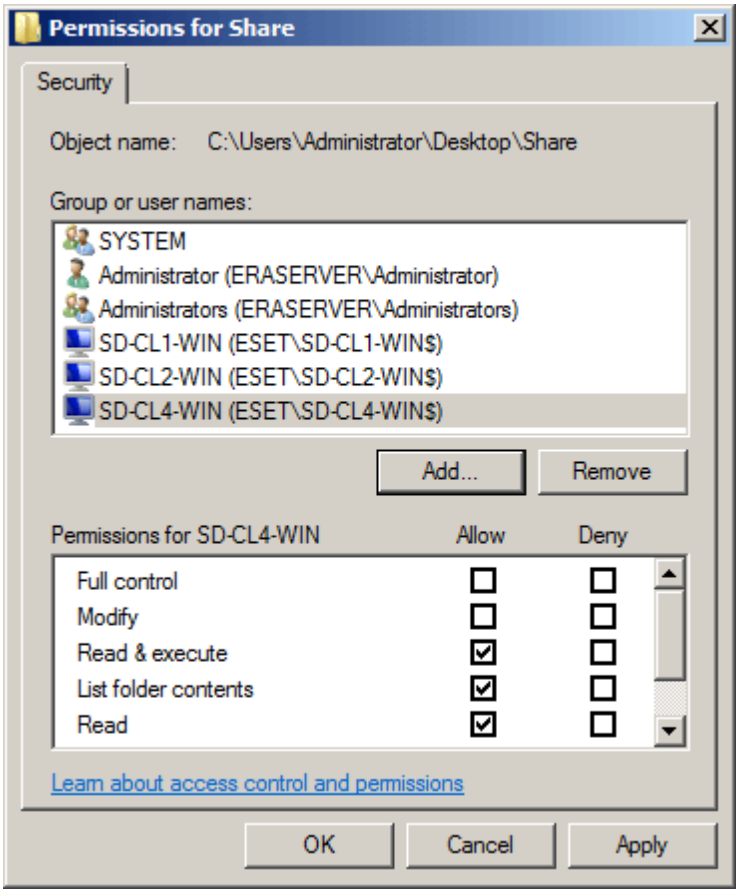


2.6.3.3 Étapes de déploiement - SCCM

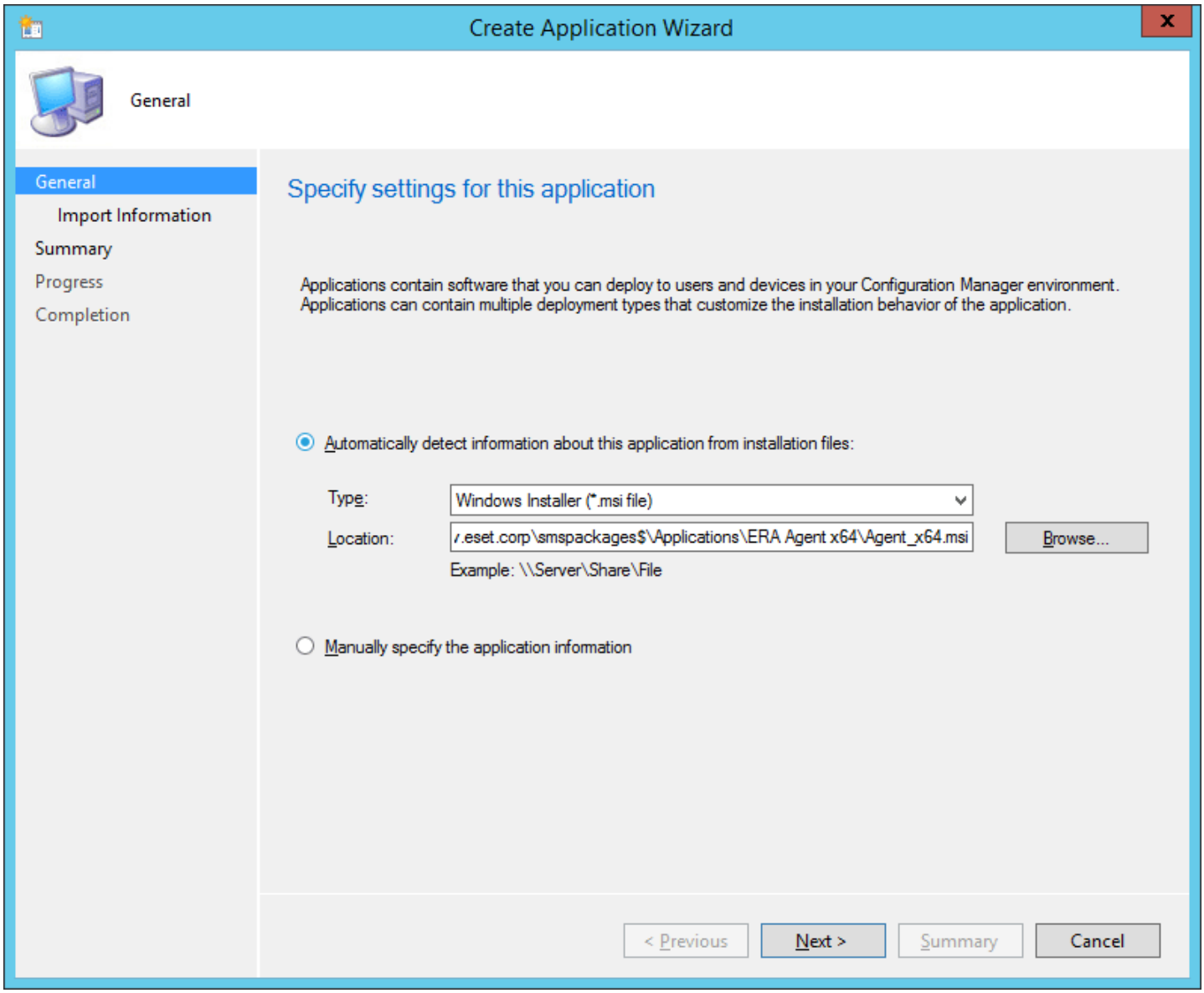
Pour déployer ERA Agent sur les clients à l'aide de SCCM, suivez la procédure décrite ci-dessous ou consultez l'article de la base de connaissances :

1. Téléchargez le fichier `.msi` du programme d'installation d'ERA Agent à partir de la page de téléchargement ESET.
2. Créez un fichier .mst de transformation du programme d'installation d'ERA Agent.
3. Placez les fichiers `.msi` du programme d'installation ERA Agent et .mst de transformation dans un dossier partagé.

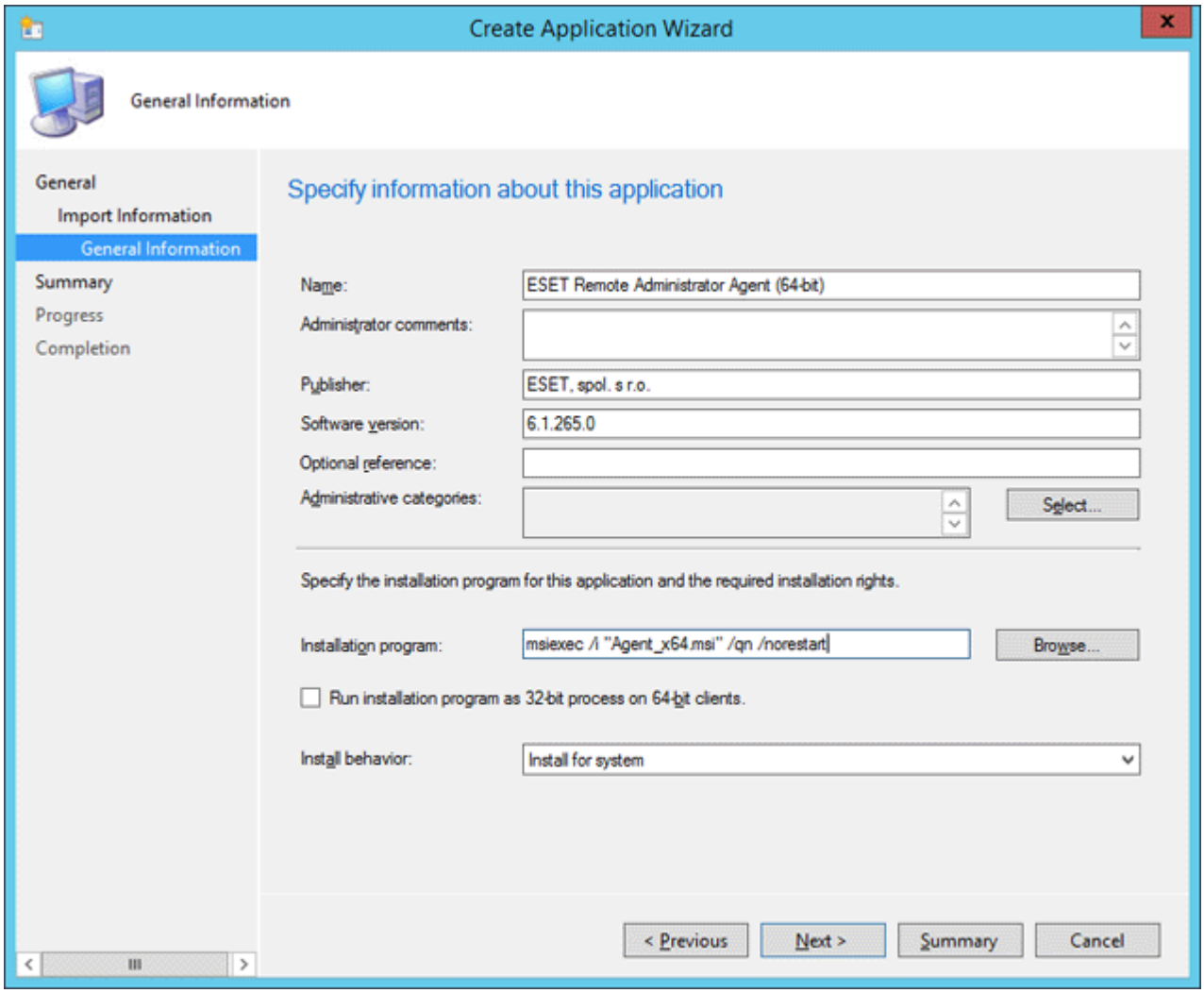
REMARQUE : les ordinateurs clients nécessitent un accès en lecture/exécution à ce dossier partagé.



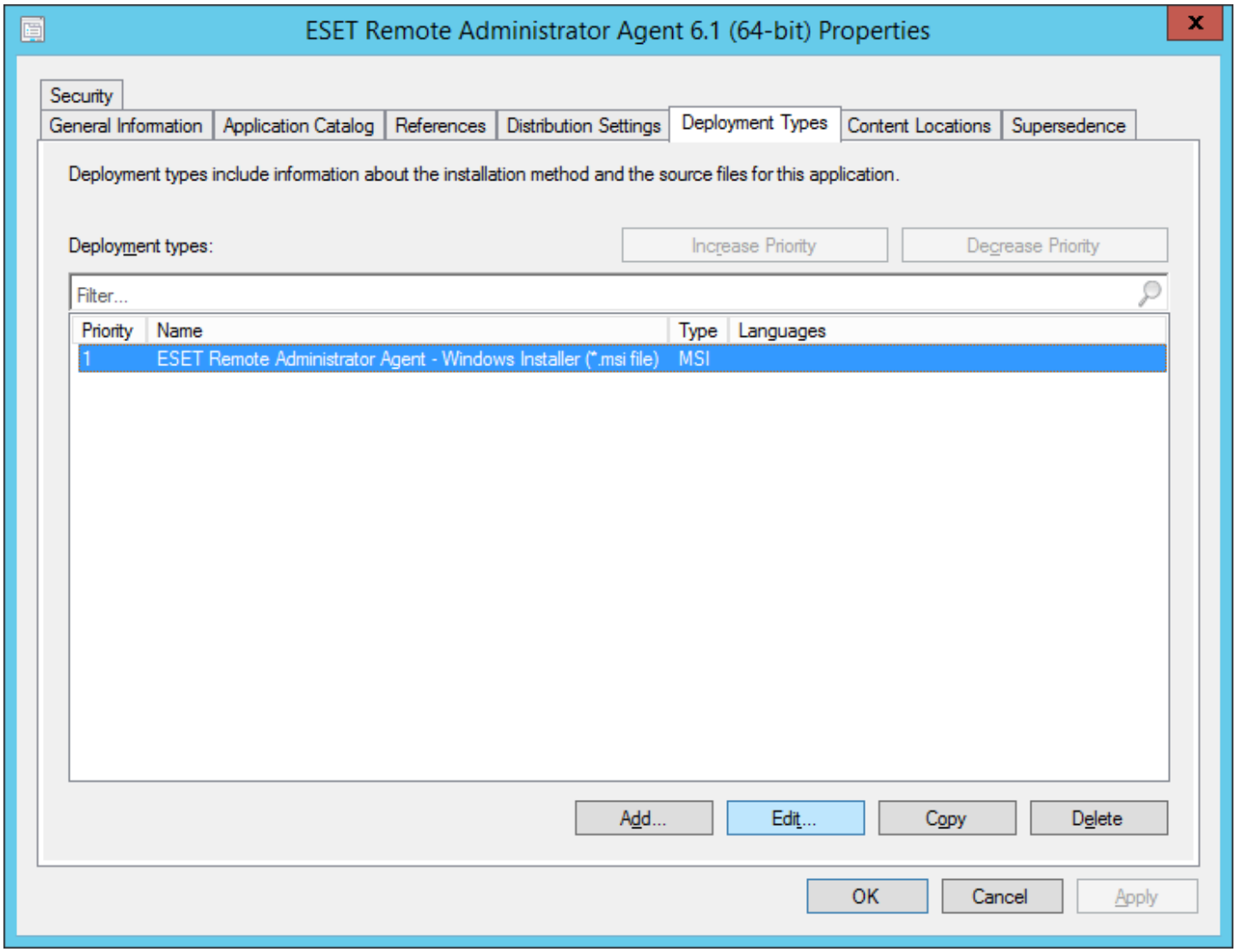
4. Ouvrez la console SCCM, puis cliquez sur **Bibliothèque de logiciels**. Dans **Gestion des applications**, cliquez avec le bouton droit sur **Applications**, puis choisissez **Créer une application**. Choisissez **Windows Installer (fichier *.msi)**, puis recherchez le dossier source dans lequel vous avez enregistré le fichier `.msi`.



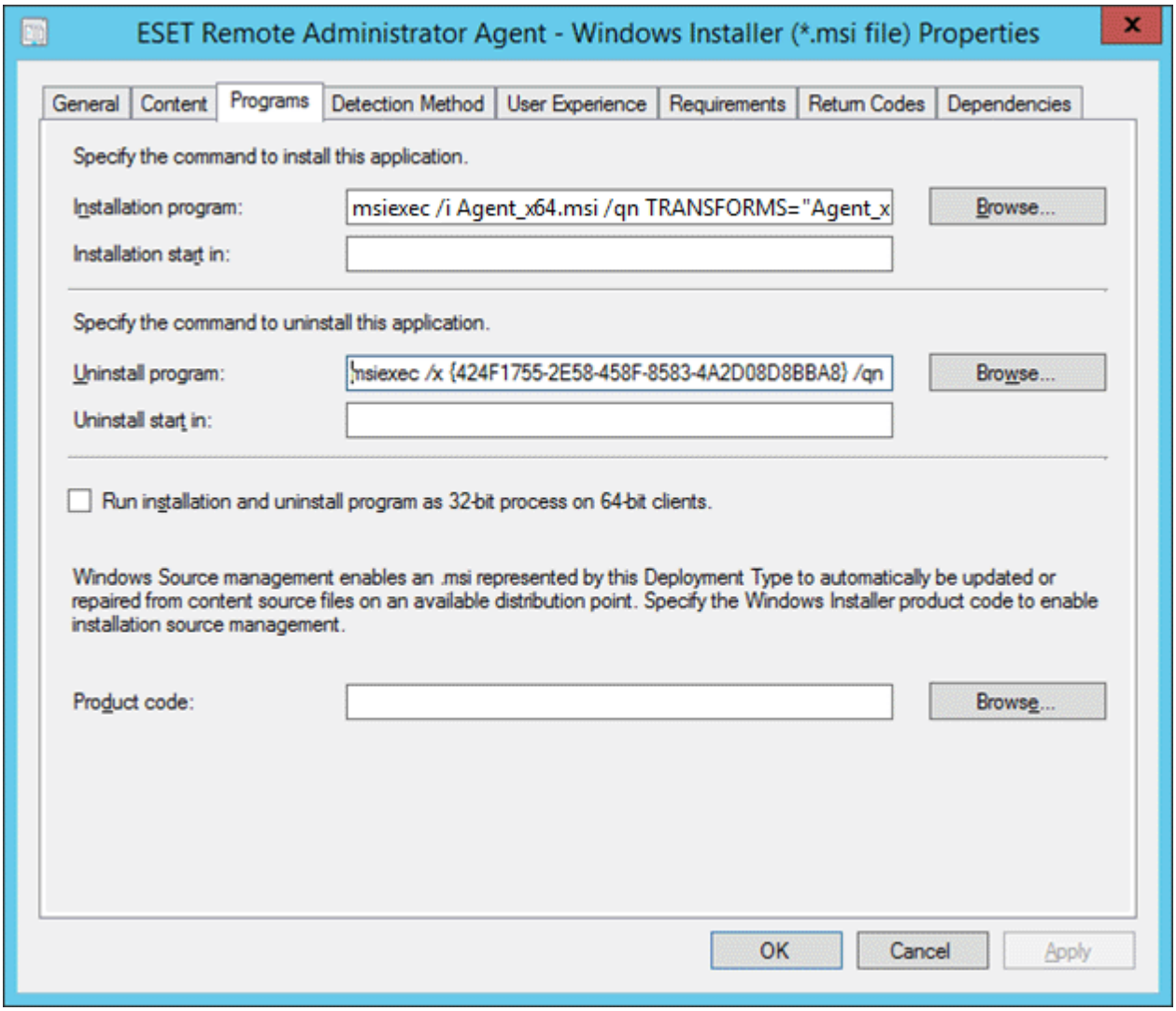
5. Fournissez toutes les informations obligatoires sur l'application, puis cliquez sur **Suivant**.



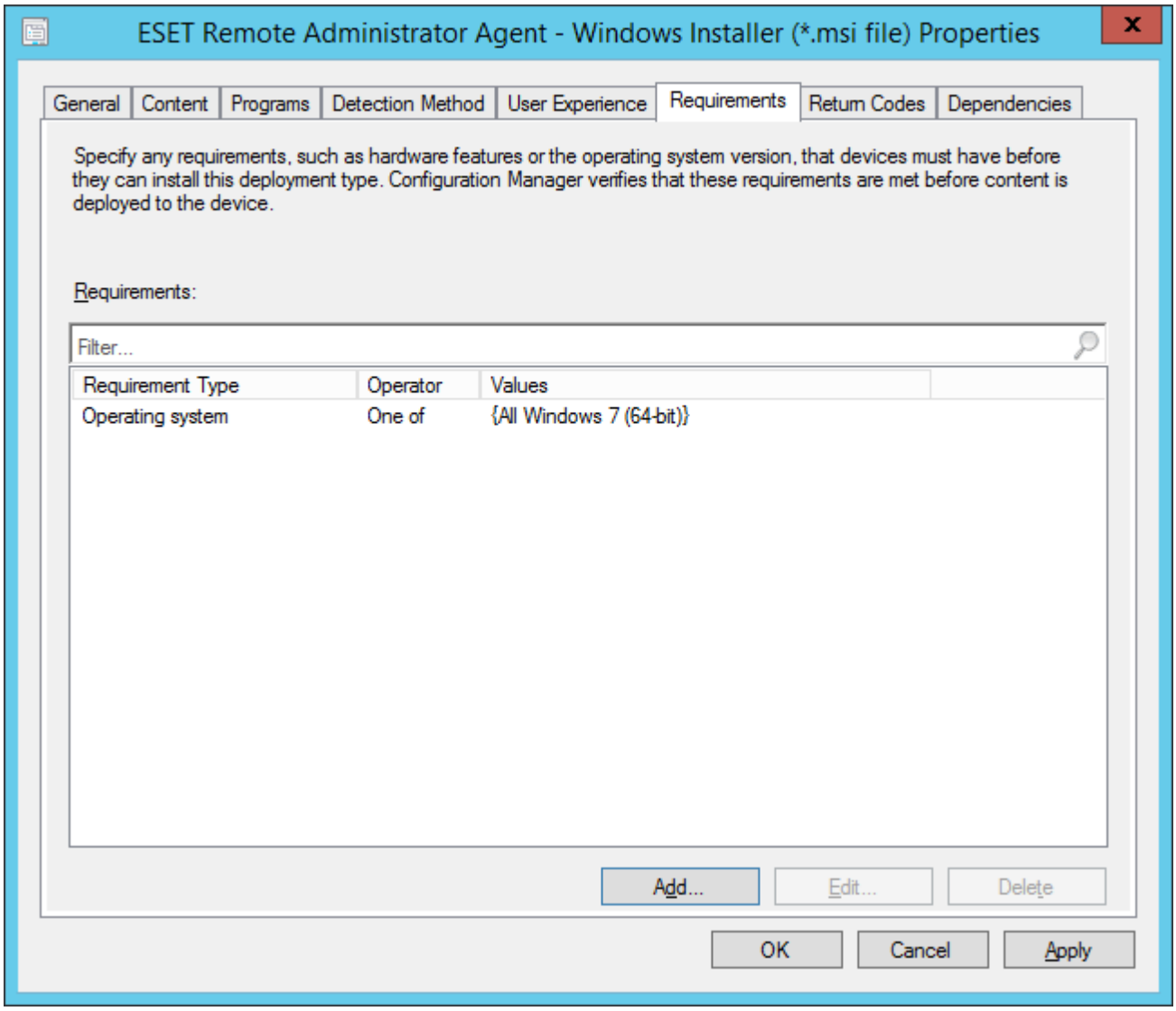
6. Cliquez avec le bouton droit sur l'application ESET Remote Administrator Agent, cliquez sur l'onglet **Types de déploiement**, sélectionnez la seule option de déploiement, puis cliquez sur **Modifier**.

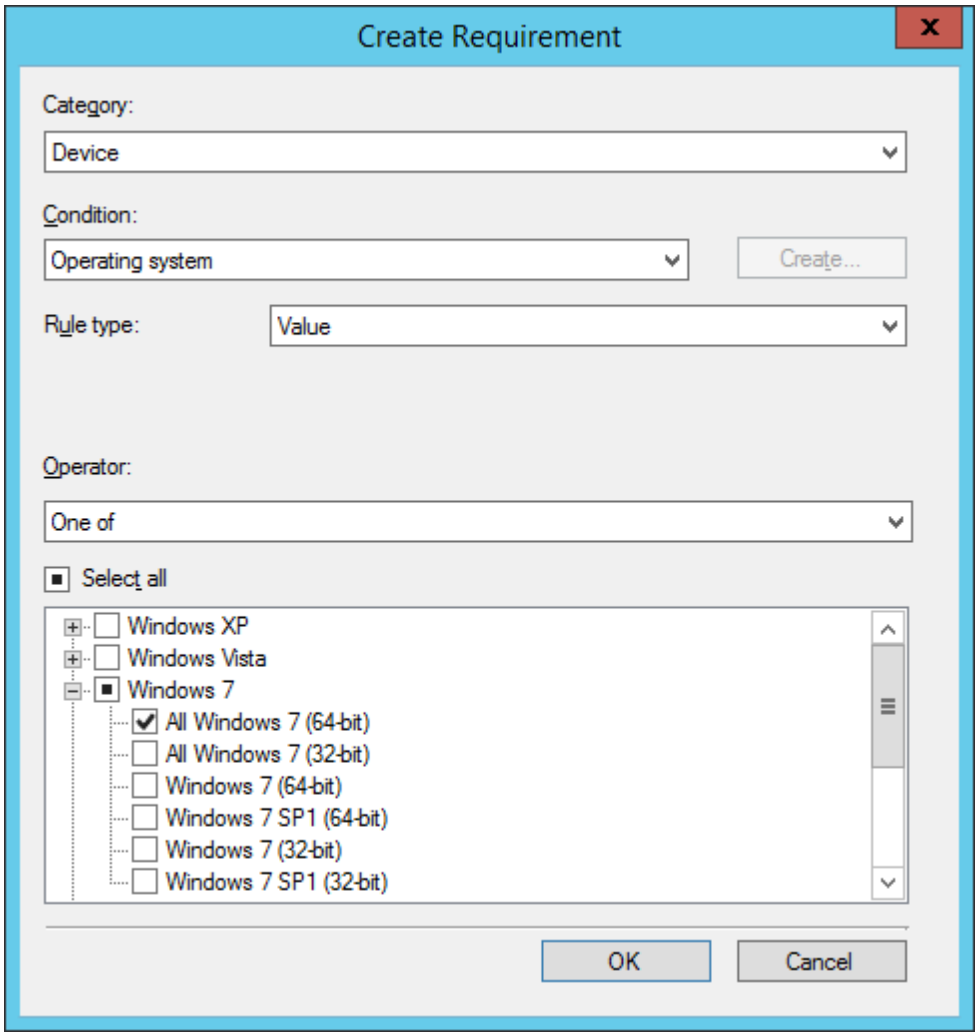


7. Cliquez sur l'onglet Programmes et modifiez le champ Programme d'installation avec les informations suivantes : msiexec/iAgent_x64.msi/qn TRANSFORMS="Agent_x64.mst (si vous utilisez des packages 32 bits, la chaîne sera légèrement différente dans la mesure où « x32 » apparaîtra à la place de « x64 » dans cet exemple).
8. Modifiez le champ Programme de désinstallation avec les informations suivantes : msiexec/x {424F1755-2E58-458F-8583-4A2D08D8BBA8} /qn/norestart.

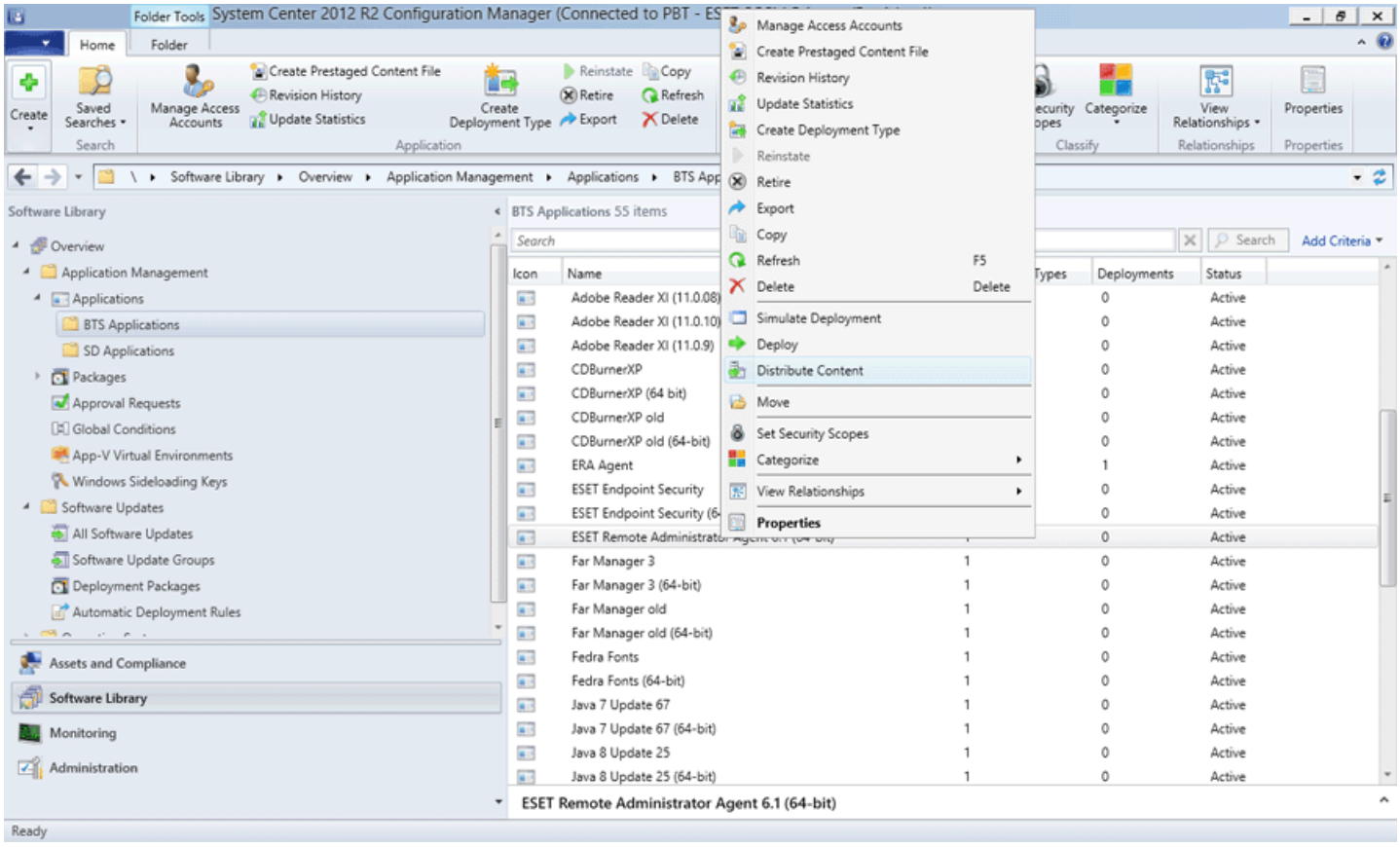


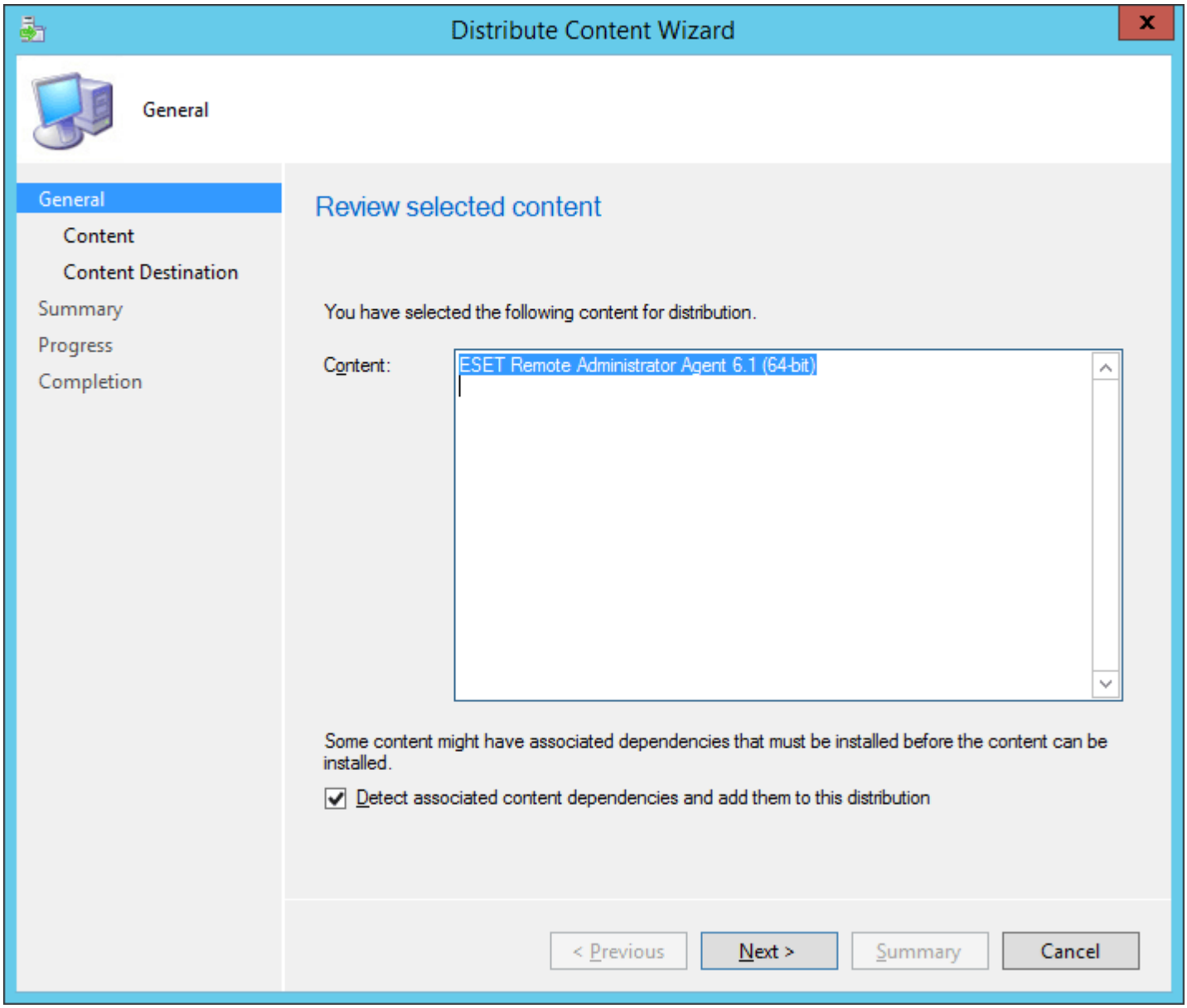
9. Cliquez sur l'onglet **Spécifications**, puis sur Ajouter. Dans le menu déroulant Condition, sélectionnez Système d'exploitation. Dans le menu Opérateur, sélectionnez L'un des, puis spécifiez les systèmes d'exploitation que vous allez installer en cochant les cases adéquates. Cliquez sur OK lorsque vous avez terminé. Pour fermer toutes les fenêtres et enregistrer vos modifications, cliquez sur OK.

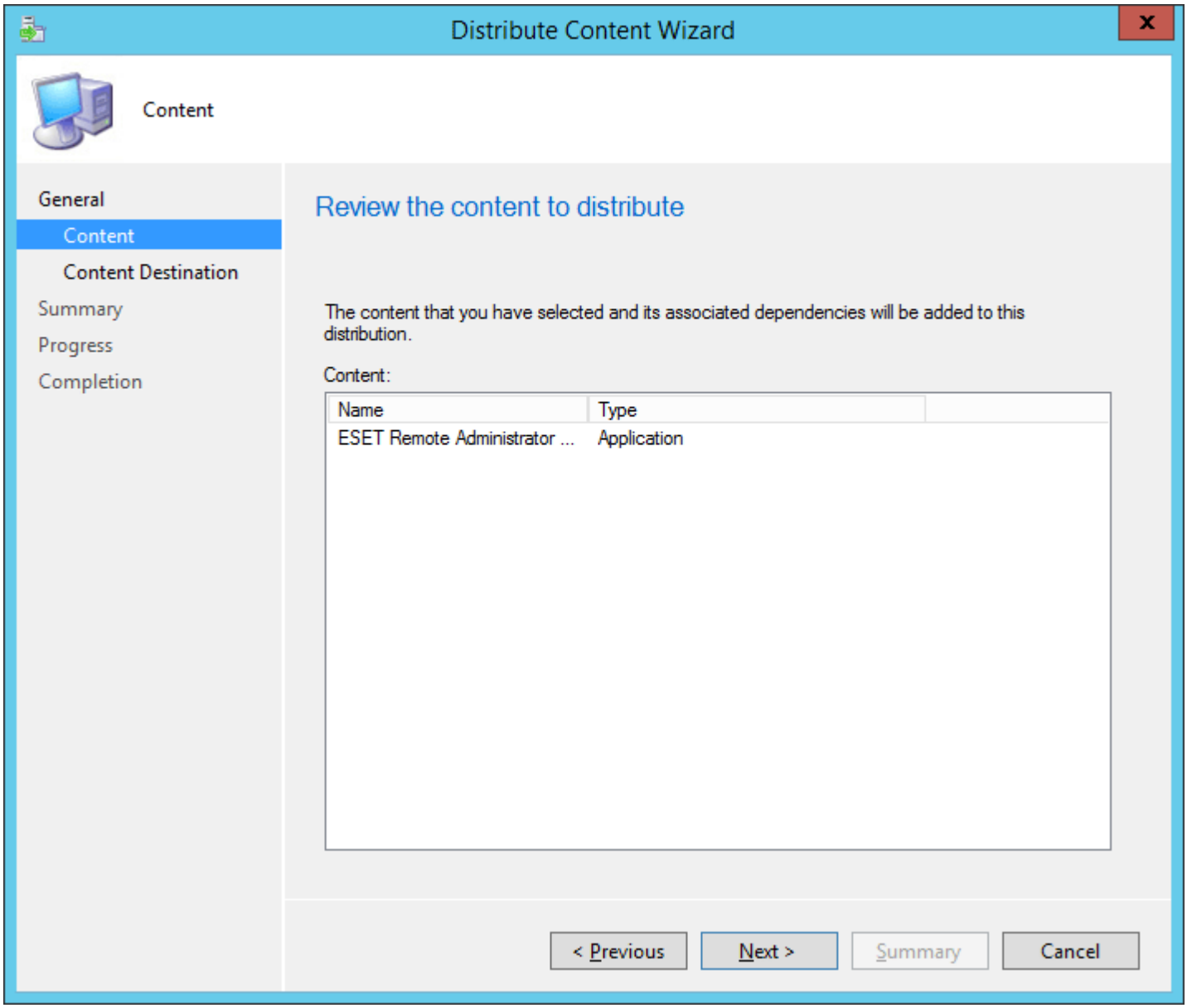

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.
Requirements:
Filter...
Requirement Type
Operator
Values
Operating system
One of
{All Windows 7 (64-bit)}
Add...
Edit...
Delete
OK
Cancel
Apply



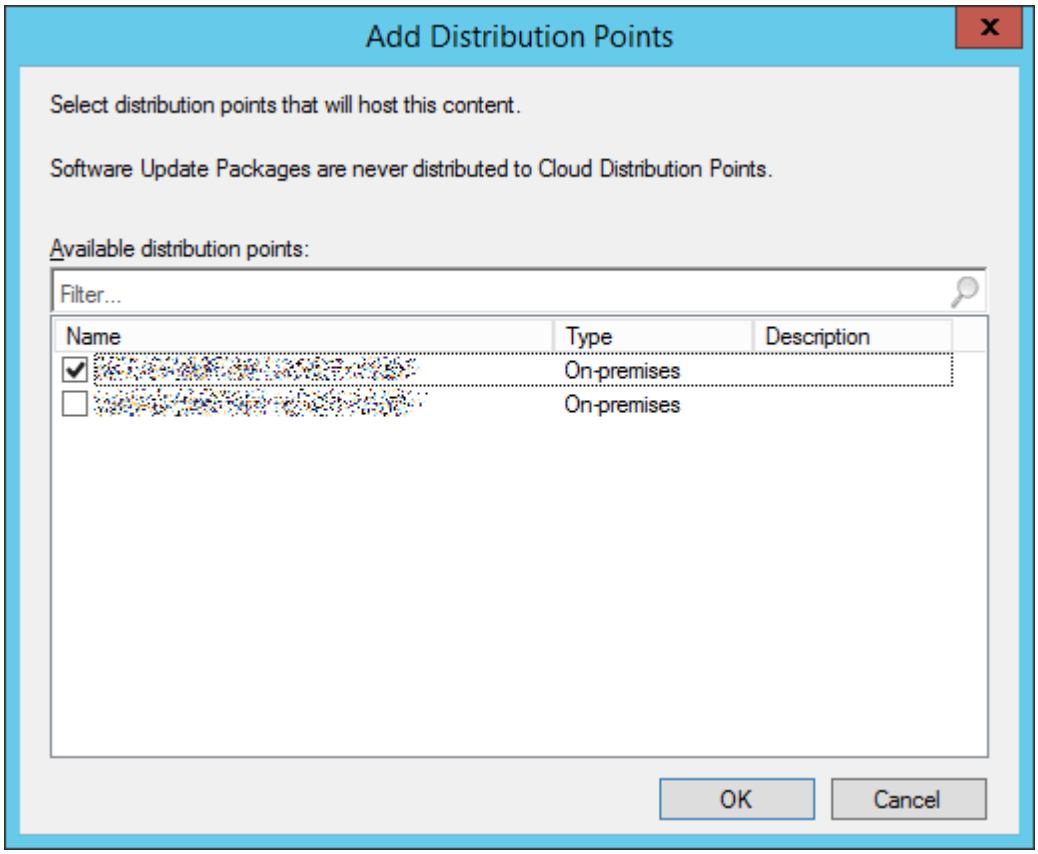
10. Dans la bibliothèque de logiciels System Center Configuration Manager, cliquez avec le bouton droit sur la nouvelle application, puis sélectionnez Distribuer du contenu dans le menu contextuel. Suivez les instructions de l'Assistant Déploiement logiciel pour terminer le déploiement de l'application.

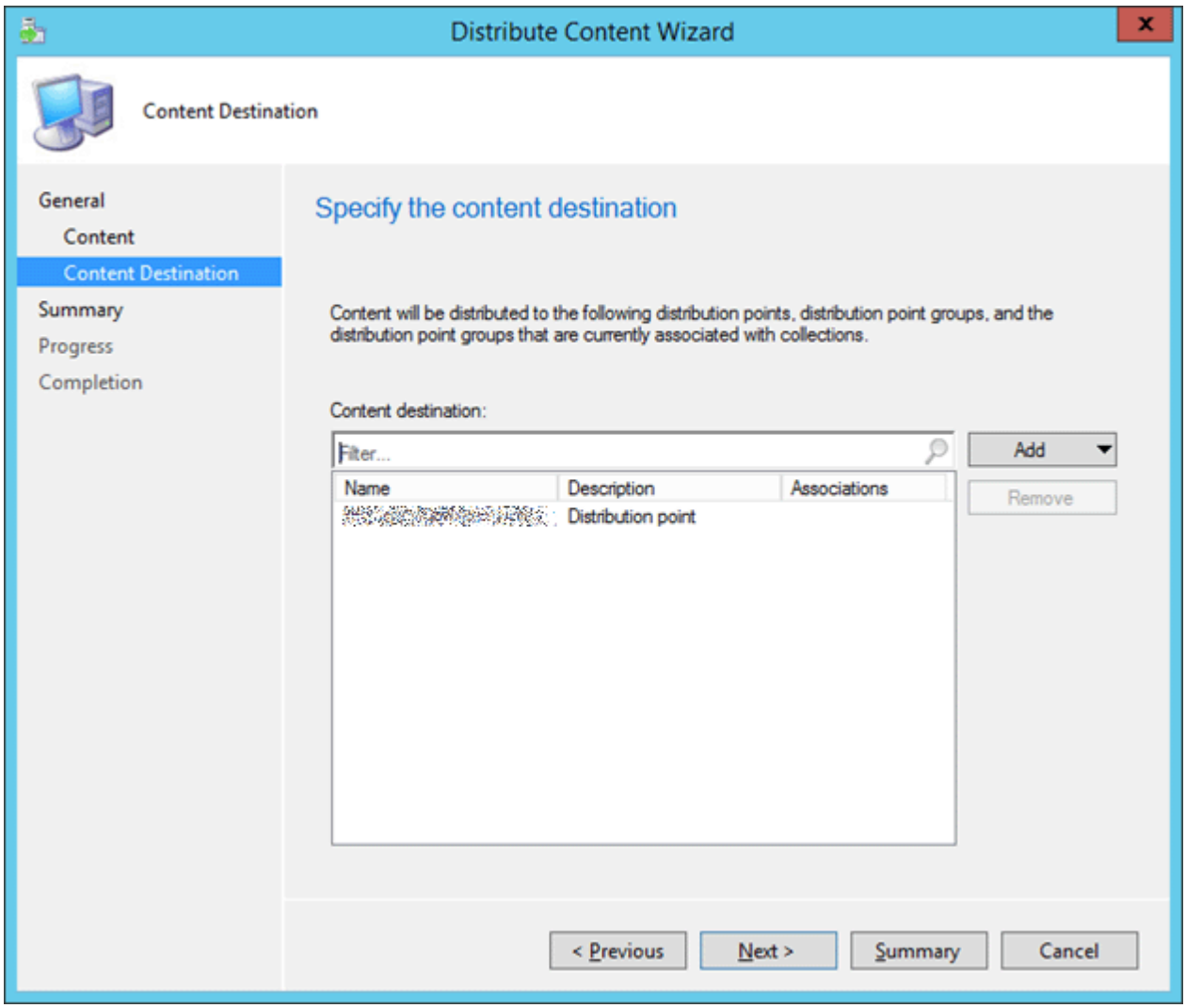


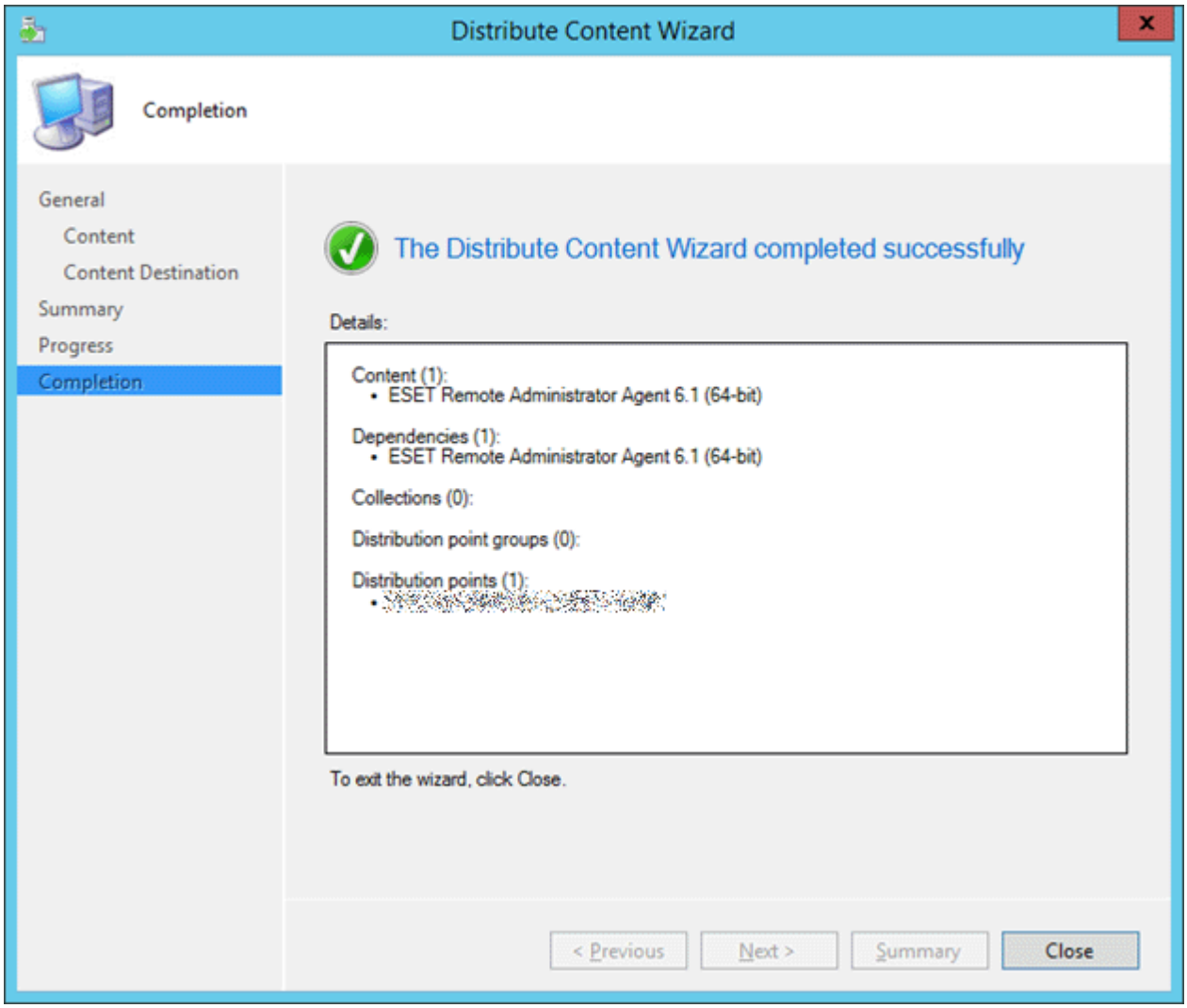

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent 6.1 (64-bit)
Some content might have associated dependencies that must be installed before the content can be installed.
Detect associated content dependencies and add them to this distribution
< Previous
Next >
Summary
Cancel

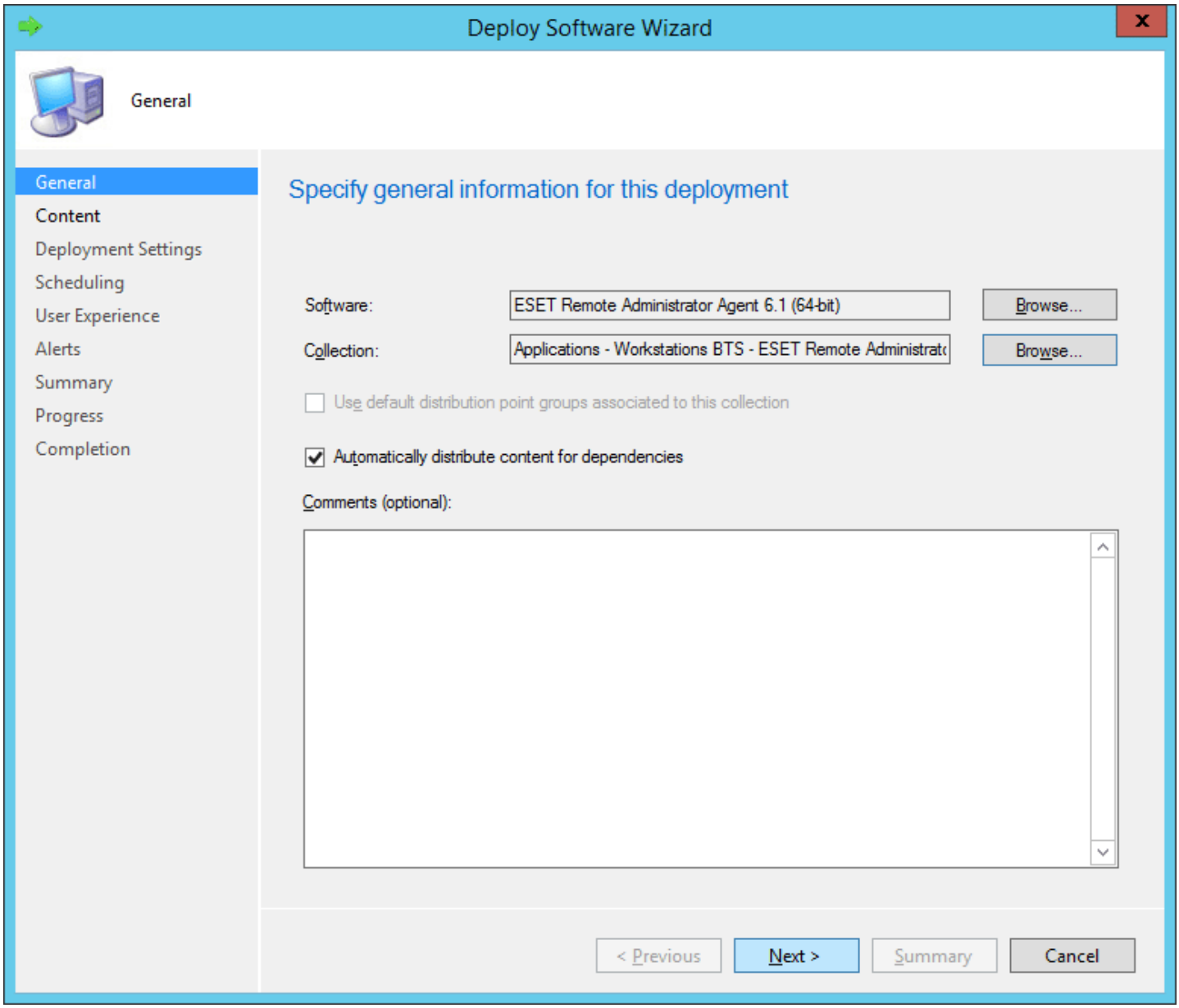


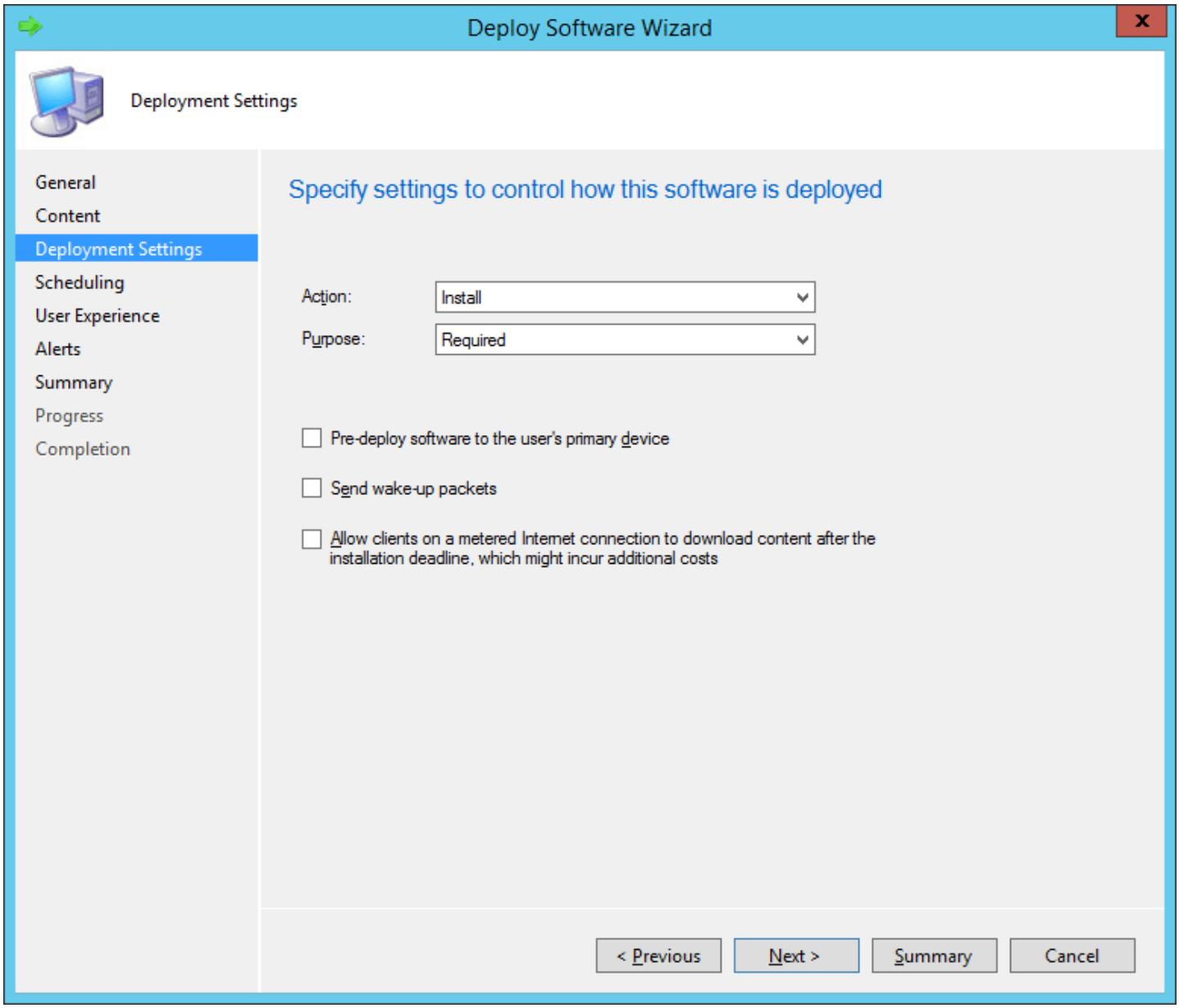
11. Cliquez avec le bouton droit sur l'application, puis sélectionnez **Déployer**. Suivez les instructions de l'assistant et choisissez la destination et la collection vers lesquelles déployer l'Agent.

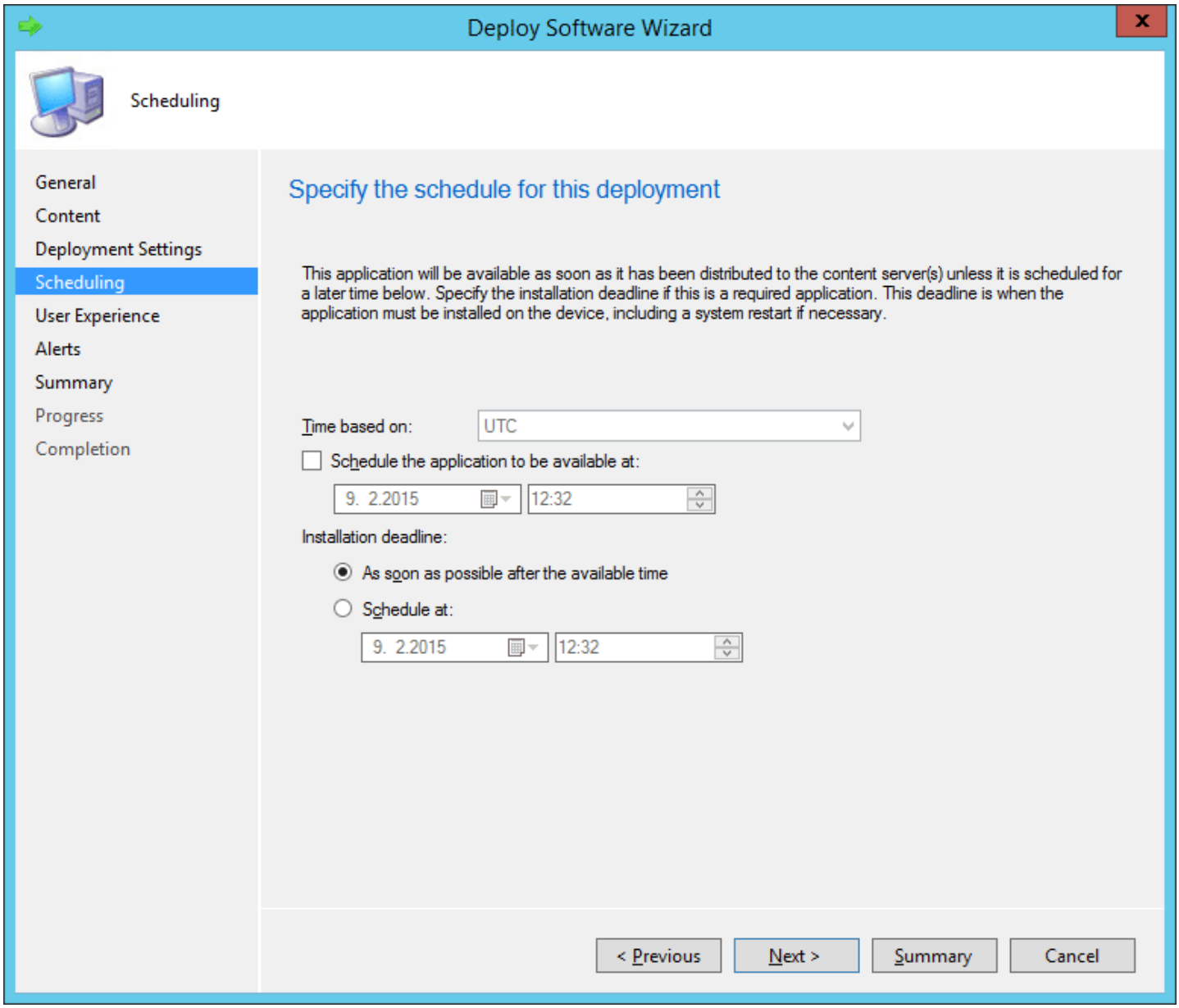

Add Distribution Points
Select distribution points that will host this content.
Software Update Packages are never distributed to Cloud Distribution Points.
Available distribution points:
Filter...
Name
Type
Description
On-premises
On-premises
OK
Cancel

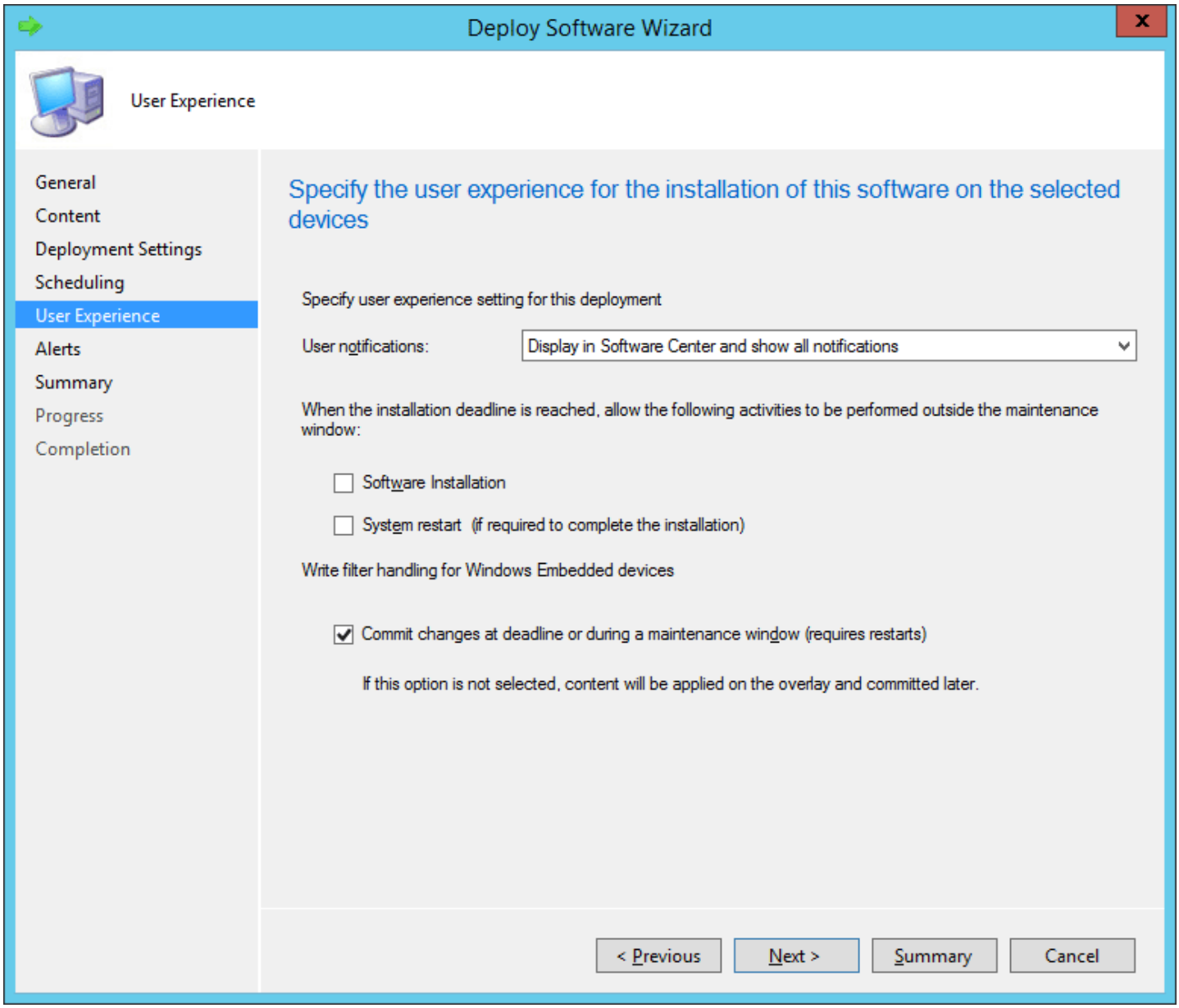

Distribute Content Wizard
Content Destination
General
Content
Content Destination
Summary
Progress
Completion
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.
Content destination:
Filter...
Add
Remove
Name
Description
Associations
Distribution point
< Previous
Next >
Summary
Cancel

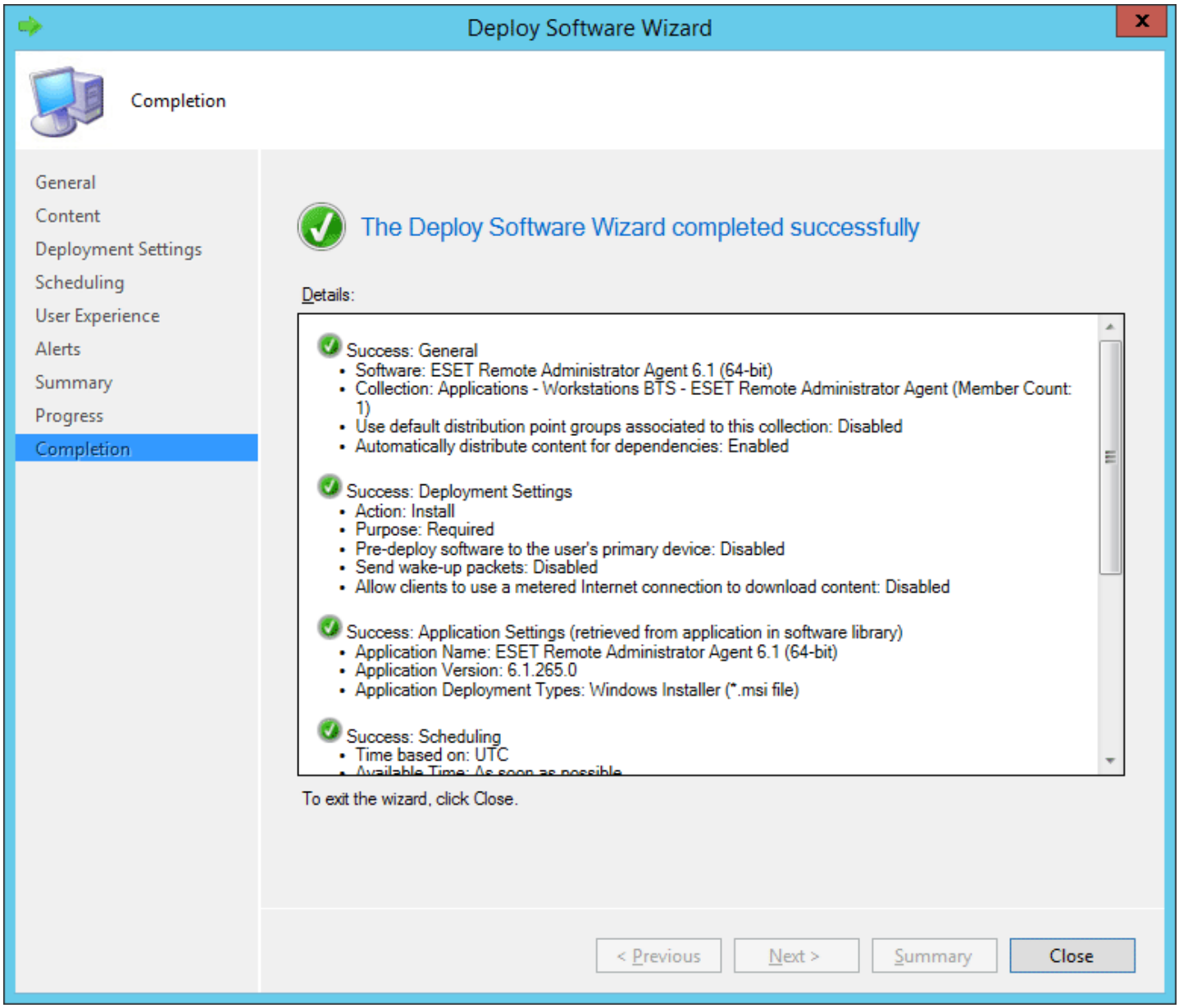

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent 6.1 (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent 6.1 (64-bit)
Collections (0):
Distribution point groups (0):
Distribution points (1):
To exit the wizard, click Close.
< Previous
Next >
Summary
Close


Deploy Software Wizard
General
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify general information for this deployment
Software:
ESET Remote Administrator Agent 6.1 (64-bit)
Browse...
Collection:
Applications - Workstations BTS - ESET Remote Administrat
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Comments (optional):
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Deployment Settings
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Scheduling
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the schedule for this deployment
This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.
Time based on:
UTC
Schedule the application to be available at:
9. 2.2015
12:32
Installation deadline:
As soon as possible after the available time
Schedule at:
9. 2.2015
12:32
< Previous
Next >
Summary
Cancel

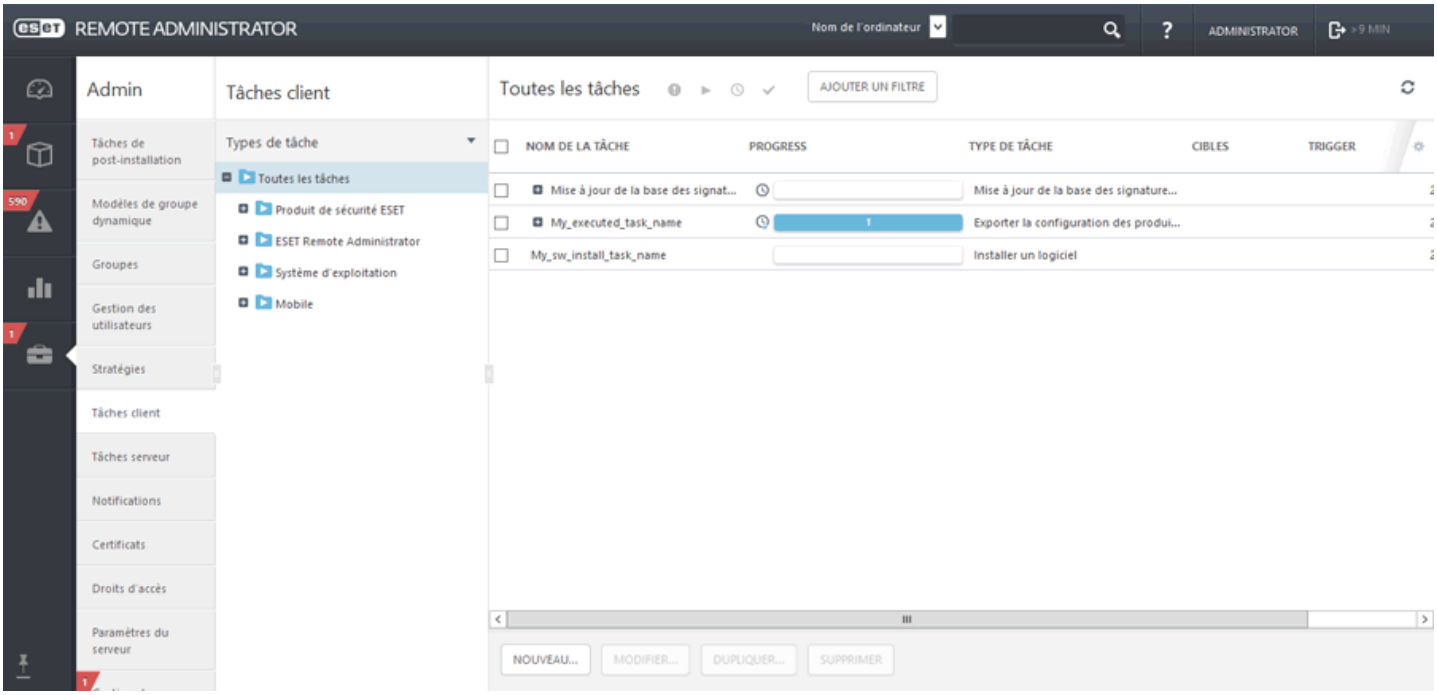

Deploy Software Wizard
User Experience
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center and show all notifications
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Completion
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
The Deploy Software Wizard completed successfully
Details:
Success: General
Software: ESET Remote Administrator Agent 6.1 (64-bit)
Collection: Applications - Workstations BTS - ESET Remote Administrator Agent (Member Count: 1)
Use default distribution point groups associated to this collection: Disabled
Automatically distribute content for dependencies: Enabled
Success: Deployment Settings
Action: Install
Purpose: Required
Pre-deploy software to the user's primary device: Disabled
Send wake-up packets: Disabled
Allow clients to use a metered Internet connection to download content: Disabled
Success: Application Settings (retrieved from application in software library)
Application Name: ESET Remote Administrator Agent 6.1 (64-bit)
Application Version: 6.1.265.0
Application Deployment Types: Windows Installer (*.msi file)
Success: Scheduling
Time based on: UTC
To exit the wizard, click Close.
< Previous
Next >
Summary
Close

2.6.4 Installation du produit

Les produits de sécurité ESET peuvent être installés à distance en cliquant sur l'ordinateur client souhaité et en sélectionnant **Nouveau**, ou en créant une tâche **Installer un logiciel** dans le menu **Admin** > **Tâches client**. Cliquez sur **Nouveau...** pour commencer à configurer la nouvelle tâche.

- L'exécution de la tâche client vous indique l'état en cours des tâches client et comprend un indicateur de progression de la tâche sélectionnée.

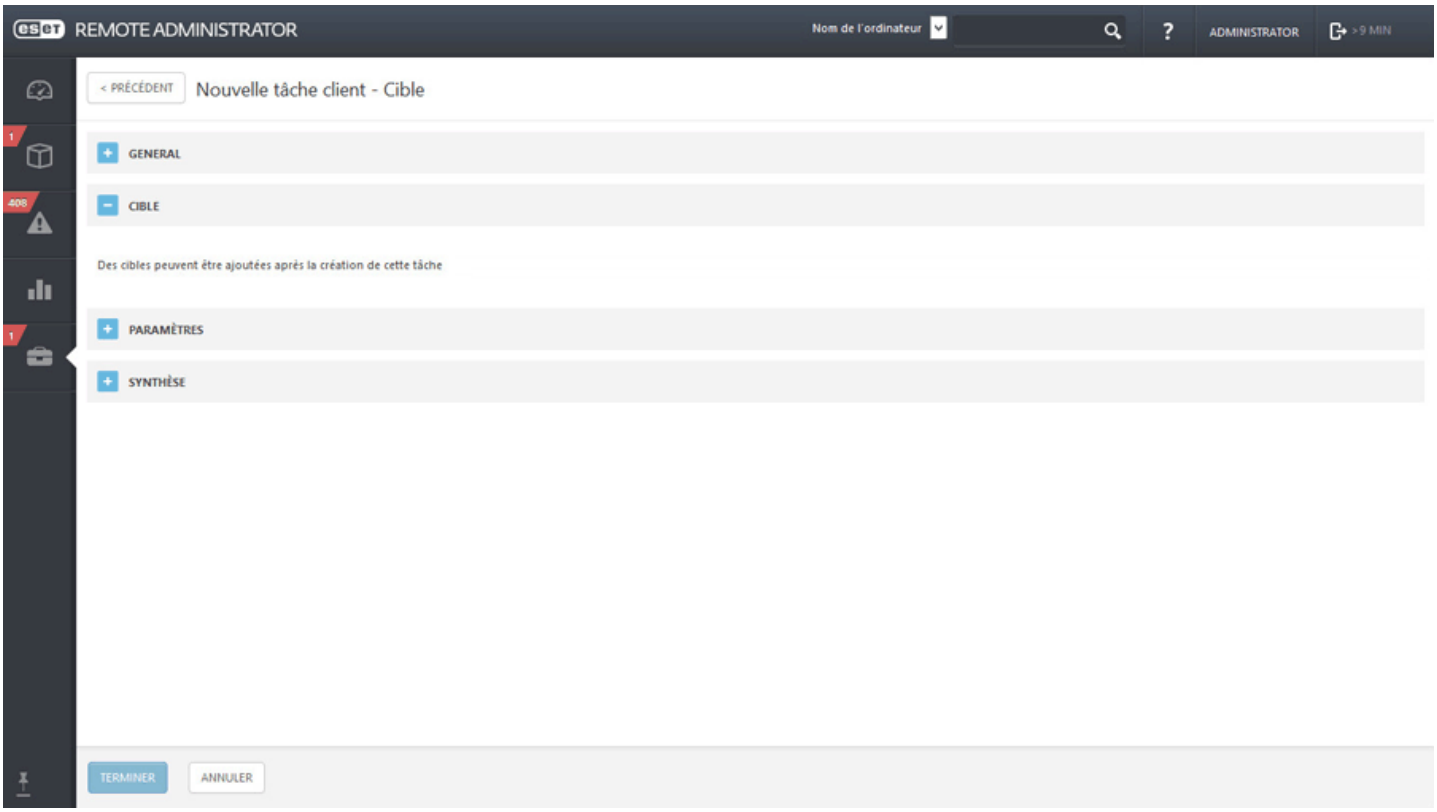


General

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche.

Cible

IMPORTANT : Une tâche client doit être définir avant de pouvoir être attribuée à des cibles. Pour commencez, configurez la tâche sous Paramètres, puis cliquez sur Terminer. Vous pourrez alors attribuer des cibles et configurer les éventuels déclencheurs que vous souhaitez utiliser pour cette tâche.



Paramètres

Cliquez sur **<Choisir une licence ESET>**, puis sélectionnez la licence adéquate pour le produit installé dans la liste des licences disponibles. Cochez la case en regard de l'option **J'accepte les termes du Contrat de Licence Utilisateur Final de l'application** si vous les acceptez. Pour plus d'informations, reportez-vous à Gestion de licences ou CLUF.

Cliquez sur **<Sélectionner un package>** pour sélectionner un package d'installation dans le référentiel ou indiquez une URL de package. Une liste de packages disponibles s'affiche dans laquelle vous pouvez sélectionner le produit ESET à installer (ESET Endpoint Security, par exemple). Sélectionnez le package d'installation souhaité, puis cliquez sur **OK**. Si vous souhaitez indiquer une URL de package d'installation, saisissez-la ou copiez-la et collez-la (par exemple, *file://\\pc22\install\ees_nt64_ENU.msi*) dans le champ de texte (n'utilisez pas d'URL qui requiert une authentification).

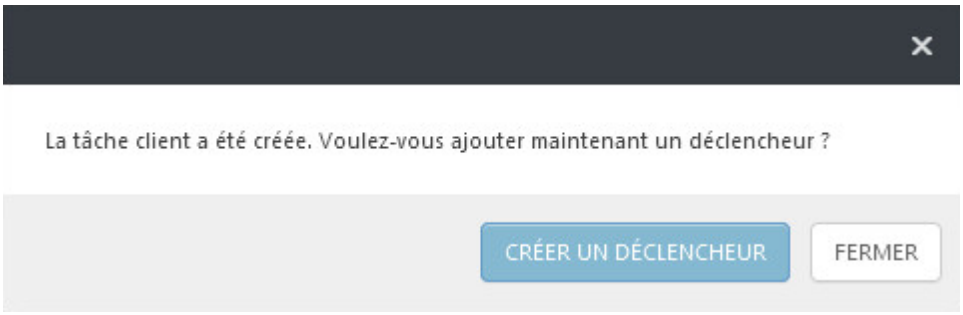
http://server_address/ees_nt64_ENU.msi : si vous effectuez l'installation à partir d'un serveur Web public ou de votre serveur HTTP.
file://\\pc22\install\ees_nt64_ENU.msi : si vous effectuez l'installation à partir d'un chemin d'accès réseau.
file://C:\installs\ees_nt64_ENU.msi : si vous effectuez l'installation à partir d'un chemin d'accès local.

REMARQUE : notez qu'ERA Server et ERA Agent doivent avoir accès à Internet pour accéder au référentiel et effectuer l'installation. Si vous ne disposez pas d'un accès Internet, vous pouvez installer manuellement le logiciel client.

Si nécessaire, vous pouvez spécifier des paramètres dans le champ Paramètres d'installation. Sinon, laissez ce champ vide. Cochez la case en regard de l'option **Redémarrage automatique si nécessaire** pour forcer un redémarrage automatique de l'ordinateur client après l'installation. Vous pouvez également ne pas cocher cette case pour laisser la décision de redémarrer l'ordinateur client à un utilisateur.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une boîte de dialogue s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



2.6.4.1 Installation du produit (ligne de commande)

Les paramètres suivants doivent être utilisés **uniquement avec les paramètres réduits, de base ou néant** de l'interface utilisateur. Pour connaître les paramètres de ligne de commande appropriés, reportez-vous à la documentation de la version de **msiexec** utilisée.

Paramètres pris en charge :

APPDIR=<chemin>
- chemin : chemin d'accès valide au répertoire.
- Répertoire d'installation de l'application.
- Par exemple : `ees_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<chemin>
- chemin : chemin d'accès valide au répertoire.
- Répertoire d'installation des données de l'application.

MODULEDIR=<chemin>
- chemin : chemin d'accès valide au répertoire.
- Répertoire d'installation du module.

ADDEXCLUDE=<liste>
- La liste ADDEXCLUDE est séparée par des virgules et contient les noms de toutes les fonctionnalités à ne pas installer ; elle remplace la liste obsolète REMOVE.
- Lors de la sélection d'une fonctionnalité à ne pas installer, le chemin d'accès dans son intégralité (c.-à-d., toutes ses sous-fonctionnalités) et les fonctionnalités connexes invisibles doivent être explicitement inclus dans la liste.
- Par exemple : `ees_nt64_ENU.msi /qn ADDEXCLUDE=Firewall,Network`

REMARQUE : La liste **ADDEXCLUDE** ne peut pas être utilisée avec **ADDLOCAL**.

ADDLOCAL=<liste>
- Installation du composant : liste des fonctionnalités non obligatoires à installer localement.
- Utilisation avec les packages .msi ESET : `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Pour plus d'informations sur la propriété **ADDLOCAL**, voir http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

Règles

- La **liste ADDLOCAL** est une liste séparée par des virgules qui contient le nom de toutes les fonctionnalités à installer.
- Lors de la sélection d'une fonctionnalité à installer, le chemin d'accès entier (toutes les fonctionnalité parent) doit être explicitement inclus.
- Pour connaître l'utilisation correcte, reportez-vous aux règles supplémentaires.

Présence de la fonctionnalité

- **Obligatoire** : la fonctionnalité sera toujours installée.
- **Facultative** : la fonctionnalité peut être désélectionnée pour l'installation.
- **Invisible** : fonctionnalité logique obligatoire pour que les autres fonctionnalités fonctionnent correctement.
- **Espace réservé** : fonctionnalité sans effet sur le produit, mais qui doit être répertoriée avec les sous-fonctionnalités.

L'arborescence des fonctionnalités d'Enpoint 6.1 est la suivante :

Arborescence des fonctionnalités	Nom de la fonctionnalité	Présence de la fonctionnalité
Ordinateur	Ordinateur	Obligatoire
Ordinateur/Antivirus et antispyware	Antivirus	Obligatoire
Ordinateur/Antivirus et antispyware > Protection en temps réel du système de fichiers	Protection en temps réel	Obligatoire
Ordinateur/Antivirus et antispyware > Analyse de l'ordinateur	Analyser	Obligatoire
Ordinateur/Antivirus et antispyware > Protection des documents	DocumentProtection	Facultative
Ordinateur/Contrôle de périphérique	Contrôle de périphérique	Facultative
Réseau	Réseau	Espace réservé
Réseau/Pare-feu personnel	Pare-feu	Facultative
Internet et messagerie	Internet et messagerie	Espace réservé
Internet et messagerie/Filtrage des protocoles	Filtrage des protocoles	Invisible
Internet et messagerie/Protection de l'accès Web	Protection de l'accès Web	Facultative
Internet et messagerie/Protection du client de messagerie	Protection du client de messagerie	Facultative
Internet et messagerie/Protection du client de messagerie/Plugins de messagerie	Plugins de messagerie	Invisible
Internet et messagerie/Protection du client de messagerie/Protection antispam	Antispam	Facultative
Internet et messagerie/Filtrage Internet	Filtrage Internet	Facultative
Miroir de mise à jour	Miroir de mise à jour	Facultative
Prise en charge de Microsoft NAP	Microsoft NAP	Facultative

Règles supplémentaires

- Si l'une des fonctionnalités **Internet et messagerie** est sélectionnée en vue de son installation, la fonctionnalité **Filtrage des protocoles** invisible doit être explicitement incluse dans la liste.
- Si l'une des sous-fonctionnalités **Protection du client de messagerie** est sélectionnée en vue de son installation, la fonctionnalité **Plugins de messagerie** invisible doit être explicitement incluse dans la liste.

Exemples :

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Liste des propriétés CFG_ :

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0 : Désactivé, 1 : Activé
• Application potentiellement indésirable

CFG_LIVEGRID_ENABLED=1/0
• 0 : Désactivé, 1 : Activé
• LiveGrid

FIRSTSCAN_ENABLE=1/0
• 0 : Désactiver, 1 : Activer
• Planifier une nouvelle première analyse après l'installation.

CFG_EPFW_MODE=0/1/2/3
• 0 : Automatique, 1 : Interactif, 2 : Stratégie, 3 : Apprentissage

CFG_PROXY_ENABLED=0/1
• 0 : Désactivé, 1 : Activé

CFG_PROXY_ADDRESS=<ip>
• Adresse IP du proxy.

CFG_PROXY_PORT=<port>
• Numéro de port du proxy.

CFG_PROXY_USERNAME=<user>
• Nom d'utilisateur pour l'authentification.

CFG_PROXY_PASSWORD=<pass>
• Mot de passe pour l'authentification.

2.6.4.2 Liste des problèmes en cas d'échec de l'installation

- Package d’installation introuvable.
- Une version plus récente du service Windows Installer est requise.
- Une autre version ou un produit en conflit est déjà installé.
- Une autre installation est déjà en cours. Terminez cette installation avant de démarrer l’autre.
- L’installation ou la désinstallation est correctement terminée. L’ordinateur doit être toutefois redémarré.
- Échec de la tâche. Une erreur s'est produite. Vous devez rechercher dans le journal de suivi de l'Agent le code de retour du programme d'installation.

2.6.5 Mise en service d'un poste de travail

Voir Environnements de mise en service de poste de travail pris en charge pour plus de détails.

2.7 Utilisation d'ESET Remote Administrator

Tous les clients sont gérés par le biais d'ERA **Web Console**. Cette console est accessible à l'aide d'un navigateur compatible depuis n'importe quel périphérique. La console Web est divisée en trois sections principales :

1. Dans la partie supérieure de la console Web, vous pouvez utiliser l'outil **Recherche rapide**. Saisissez un **nom de client** ou une **adresse IPv4/IPv6**, puis cliquez sur le symbole de la loupe ou appuyez sur **Entrée**. Vous êtes alors redirigé vers la section Groupes dans laquelle le client est affiché.

2. Le menu situé à gauche contient les sections principales d'ESET Remote Administrator et les liens rapides suivants :

- Tableau de bord
- Ordinateurs
- Menaces
- Rapports
- Admin

Accès rapides

- Nouvel utilisateur natif
- Nouvelle stratégie
- Nouvelle tâche client
- Programmes d'installation Agent Live

3. Les boutons situés dans la partie inférieure de la page sont uniques à chaque section et chaque fonction. Ils sont décrits en détail dans les chapitres correspondants.

REMARQUE : un bouton est commun à tous les nouveaux éléments : **Paramètres obligatoires**. Ce bouton rouge est affiché lorsque des paramètres obligatoires n'ont pas été configurés et que la création ne peut donc pas être effectuée. Ces paramètres obligatoires sont également indiqués par un point d'exclamation rouge en regard de chaque section. Cliquez sur **Paramètres obligatoires** pour accéder à la section dans laquelle se trouvent les paramètres en question.

Règles générales

- Les paramètres requis (obligatoires) sont toujours signalés par un point d'exclamation rouge situé en regard de la section et des paramètres correspondants. Pour accéder aux paramètres obligatoires (le cas échéant), cliquez sur **Paramètres obligatoires** dans la partie inférieure de chaque page.
- Si vous avez besoin d'aide lors de l'utilisation d'ESET Remote Administrator, cliquez sur l'icône **?** dans le coin supérieur droit ou accédez à la partie inférieure du volet gauche, puis cliquez sur **Aide**. La fenêtre d'aide correspondant à la page actuelle s'affiche alors.
- La section **Admin** est destinée à une configuration spécifique. Pour plus d'informations, reportez-vous au chapitre Admin. Cette section décrit comment ajouter un ordinateur ou des périphériques mobiles à des groupes. Comment créer une stratégie et en attribuer une à un groupe.

2.7.1 Ajouter des ordinateurs à des groupes

Les ordinateurs clients peuvent être ajoutés à des groupes. Vous pouvez ainsi les classer et les structurer selon vos préférences. Vous pouvez ajouter des ordinateurs à un groupe statique ou dynamique.

Les groupes statiques sont manuellement gérés. Les groupes dynamiques sont automatiquement organisés selon les critères spécifiques d'un modèle. Une fois que les ordinateurs se trouvent dans des groupes, vous pouvez attribuer des stratégies, des tâches ou des paramètres à ces derniers. Les stratégies, tâches ou paramètres sont ensuite appliqués à tous les membres du groupe. La corrélation entre les groupes et les tâches/stratégies est décrite ci-dessous :

Groupes statiques

Les groupes statiques sont des groupes de clients sélectionnés et configurés manuellement. Leurs membres sont statiques et ne peuvent être ajoutés/supprimés que manuellement, et non selon des critères dynamiques.

Groupes dynamiques

Les groupes dynamiques sont des groupes de clients dont l'appartenance est déterminée par des critères spécifiques. Si un client ne répond pas aux critères, il est supprimé du groupe. Les ordinateurs qui en revanche répondent aux critères sont automatiquement ajoutés au groupe (raison pour laquelle il s'appelle dynamique).

2.7.1.1 Groupes statiques

Les groupes statiques servent à trier manuellement les ordinateurs clients en **groupes** et **sous-groupes**. Vous pouvez créer des groupes statiques personnalisés et déplacer les ordinateurs de votre choix vers ceux-ci.

Les groupes statiques peuvent être uniquement créés manuellement. Les ordinateurs clients peuvent ensuite être déplacés manuellement vers ces groupes. Un ordinateur ne peut appartenir qu'à un seul groupe statique.

Il existe deux groupes statiques par défaut :

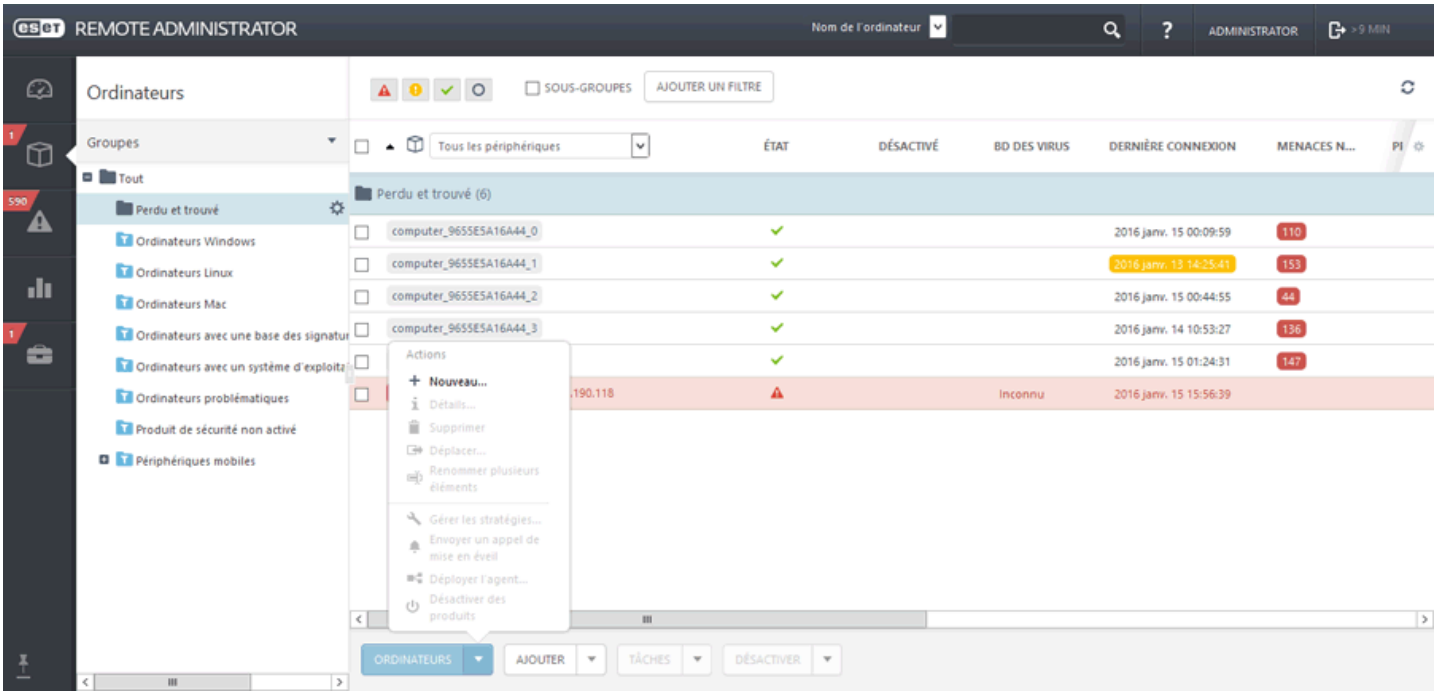
- **Tous** : il s'agit d'un groupe principal pour tous les ordinateurs d'un réseau ERA Server. Il permet d'appliquer des stratégies à chaque ordinateur en tant que stratégies par défaut. Ce groupe est toujours affiché. Il n'est pas autorisé de modifier le nom des groupes en modifiant le groupe.
- **Perdu et trouvé** en tant que groupe enfant du groupe **Tous** : chaque nouvel ordinateur qui se connecte la première fois avec l'agent au serveur est automatiquement affiché dans ce groupe. Ce groupe peut être renommé et copié, mais il ne peut pas être supprimé ni déplacé.

Vous pouvez créer des groupes statiques dans la section **Groupe** de l'onglet **Admin** en cliquant sur le bouton Groupes et en sélectionnant Nouveau groupe statique.

2.7.1.1.1 Ajouter un ordinateur à un groupe statique

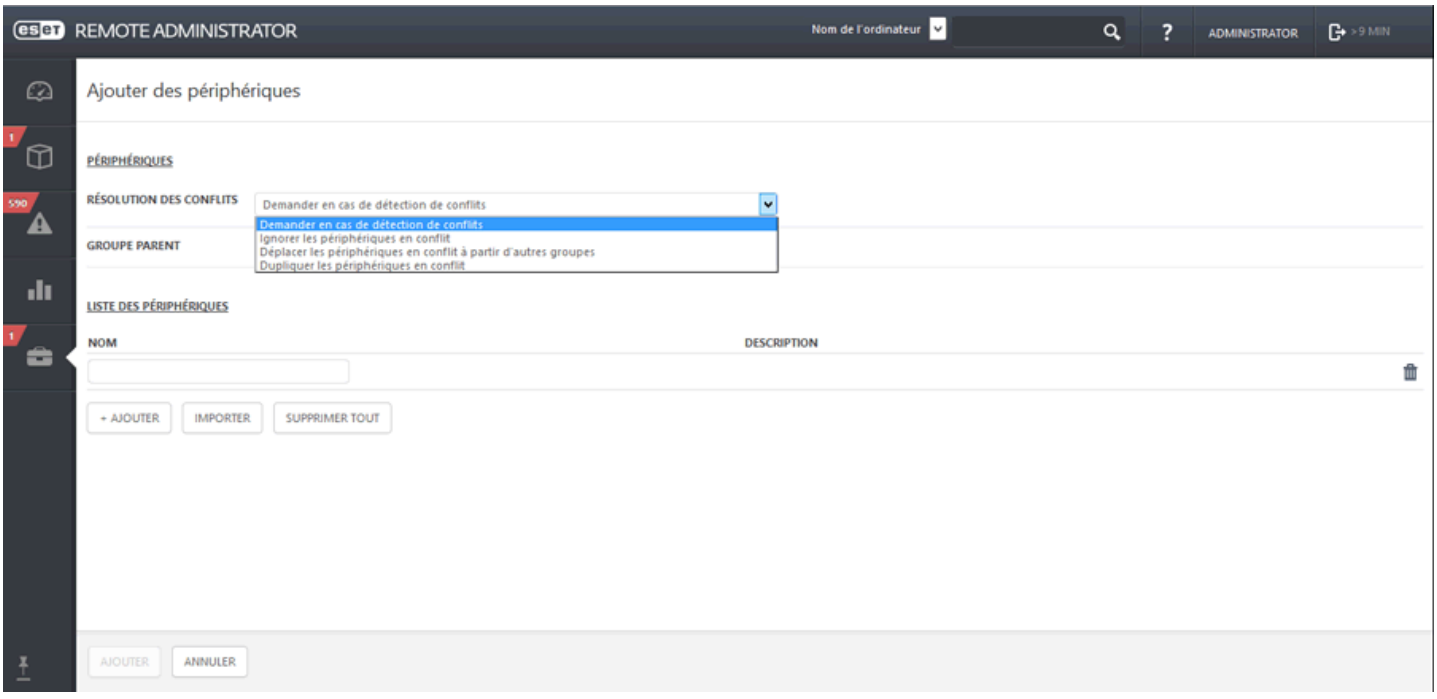
Créez des groupes statiques ou sélectionnez l'un des groupes statiques par défaut.

Cette fonctionnalité permet d'ajouter manuellement des ordinateurs ou des périphériques mobiles qui ne sont pas détectés ou ajoutés automatiquement. Cliquez sur l'onglet **Ordinateurs**, sélectionnez un **groupe statique**, puis cliquez sur **Ajouter**, sélectionnez **Ordinateurs**.



Saisissez le nom de l'ordinateur à ajouter dans le champ **Nom**. Utilisez le menu déroulant **Résolution des conflits** pour sélectionner l'action à exécuter si un ordinateur que vous ajoutez existe déjà dans ERA :

- **Demander en cas de détection de conflits :** lorsqu'un conflit est détecté, le programme vous demande de sélectionner une action (voir les options ci-dessous).
- **Ignorer les ordinateurs en conflit :** les ordinateurs en double ne sont pas ajoutés.
- **Déplacer les ordinateurs en conflit vers d'autres groupes :** les ordinateurs en conflit sont déplacés de leur groupe d'origine vers le groupe **Tous**.
- **Dupliquer les ordinateurs en conflit :** les nouveaux ordinateurs sont ajoutés avec des noms différents.

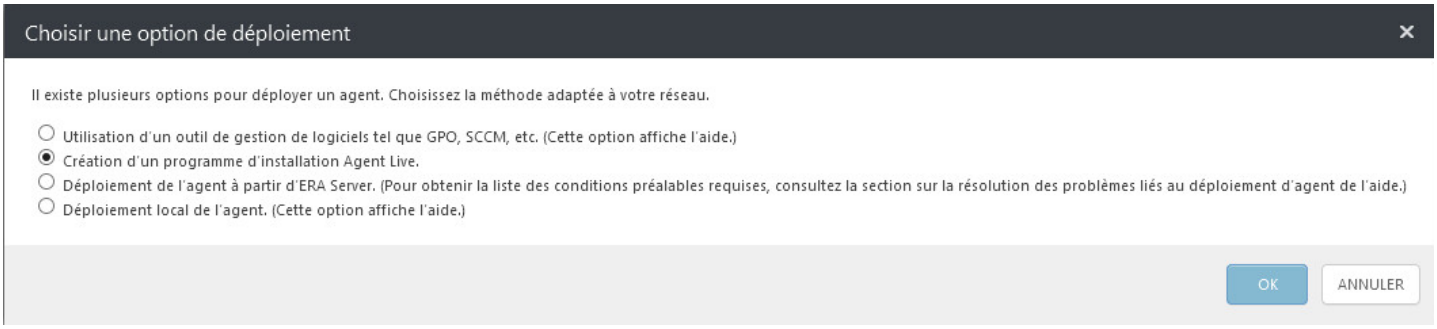


- Cliquez sur + **Ajouter** pour ajouter d'autres ordinateurs. Vous pouvez également cliquer sur **Importer** pour charger un fichier `.csv` qui contient la liste des ordinateurs à ajouter. Vous pouvez éventuellement saisir une **description** des ordinateurs. Lorsque vous avez terminé vos modifications, cliquez sur **Ajouter**.

REMARQUE : l'ajout de plusieurs ordinateurs peut prendre plus de temps. Une recherche DNS inversée peut être effectuée.

Les ordinateurs sont visibles dans la liste de droite lorsque vous sélectionnez le groupe auquel ils appartiennent. Une fois l'ordinateur ajouté, une fenêtre indépendante s'affiche avec l'option **Déployer l'agent**.

Choisissez le type de déploiement à utiliser parmi les options disponibles :



2.7.1.2 Groupes dynamiques

Chaque groupe dynamique utilise un modèle pour filtrer les ordinateurs clients. Une fois défini, un modèle peut être utilisé dans un autre groupe dynamique pour filtrer les clients. ERA contient plusieurs modèles de groupe dynamique par défaut prêts à l'emploi qui simplifient le classement des ordinateurs clients.

Les groupes dynamiques sont des groupes de clients sélectionnés selon des critères spécifiques. Si un ordinateur client ne répond pas aux critères, il est supprimé du groupe. S'il satisfait aux conditions définies, il sera ajouté au groupe. La sélection du groupe s'effectue automatiquement selon les paramètres configurés, sauf dans le cas d'un groupe statique.

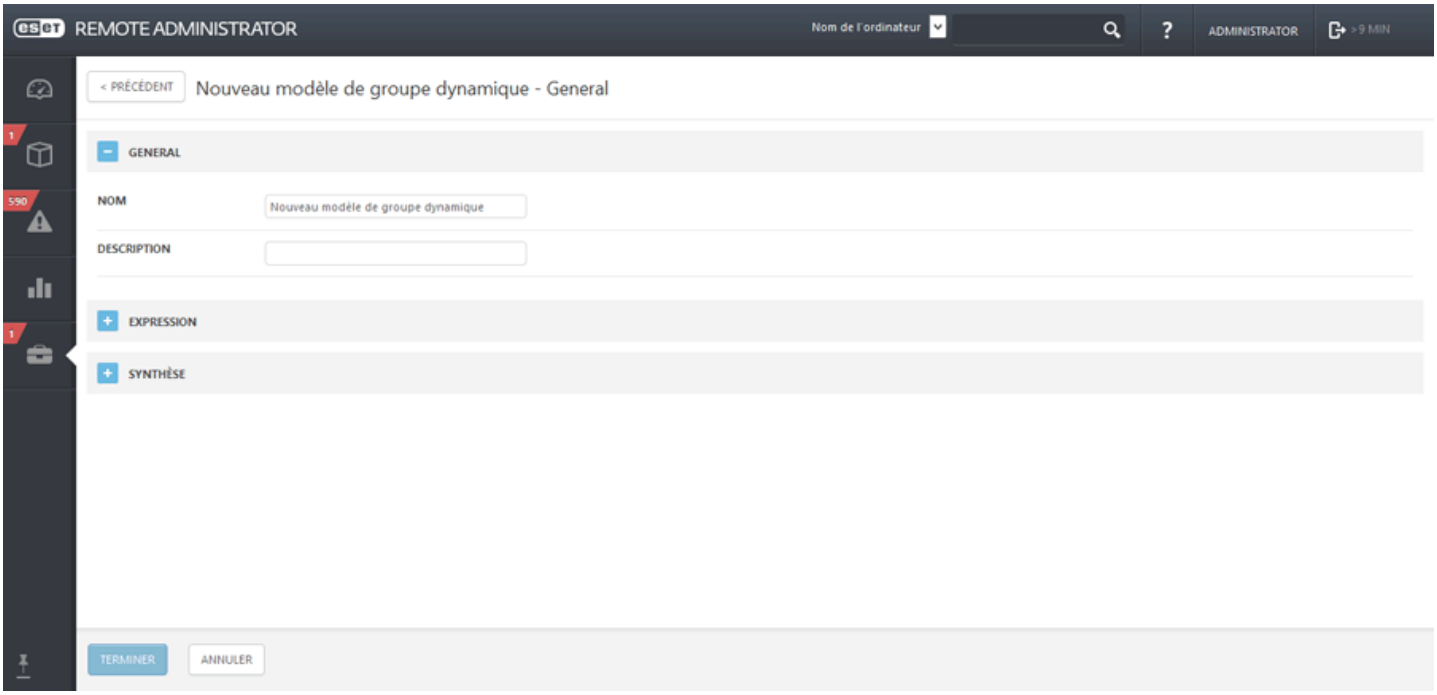
La section Modèles de groupe dynamique contient des modèles prédéfinis et personnalisés selon des critères différents. Tous les modèles sont affichés dans une liste. Lorsque vous cliquez sur un modèle existant, vous pouvez le modifier. Pour créer un modèle de groupe dynamique, cliquez sur **Nouveau modèle**.

2.7.1.2.1 Nouveau modèle de groupe dynamique

Cliquez sur **Nouveau modèle** sous **Admin** > **Modèles de groupe dynamique**.

General

Saisissez un **nom** et une **description** pour le nouveau modèle de groupe dynamique.

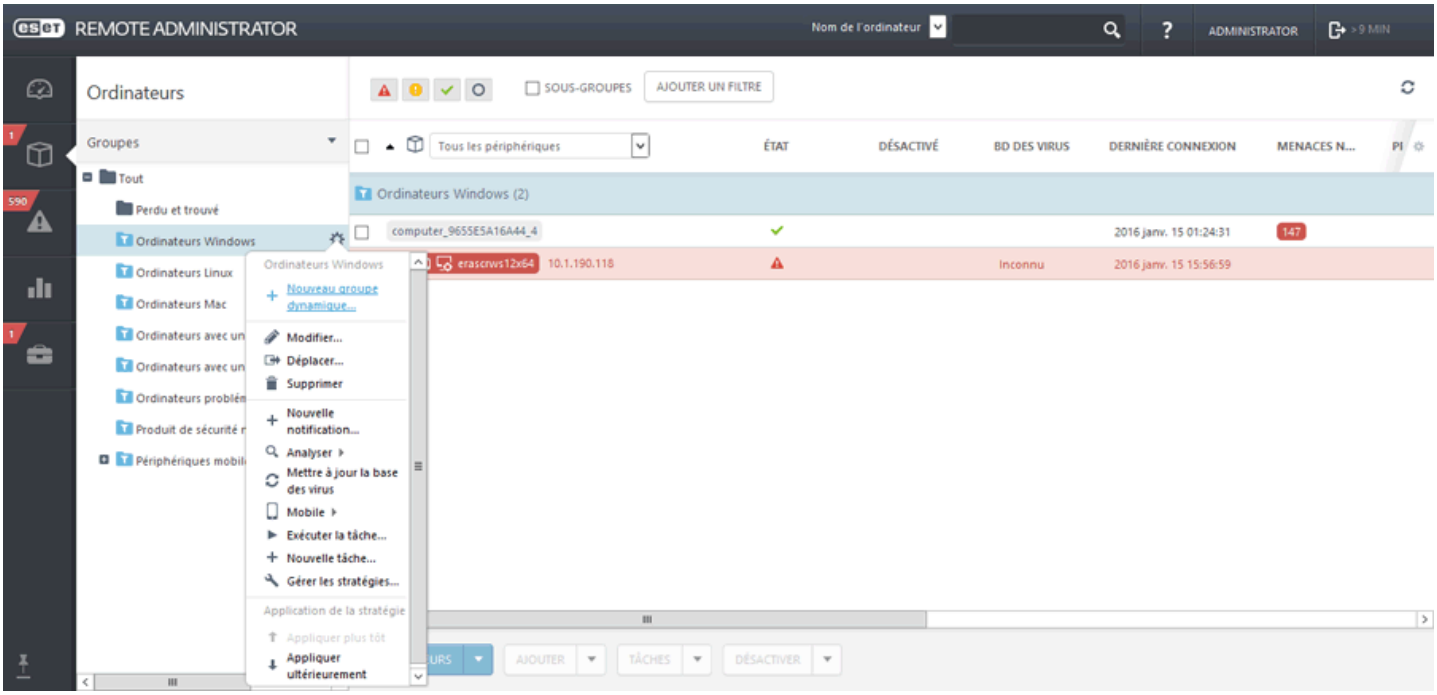


Pour découvrir comment utiliser des groupes dynamiques sur votre réseau, consultez nos exemples avec des instructions détaillées illustrées.

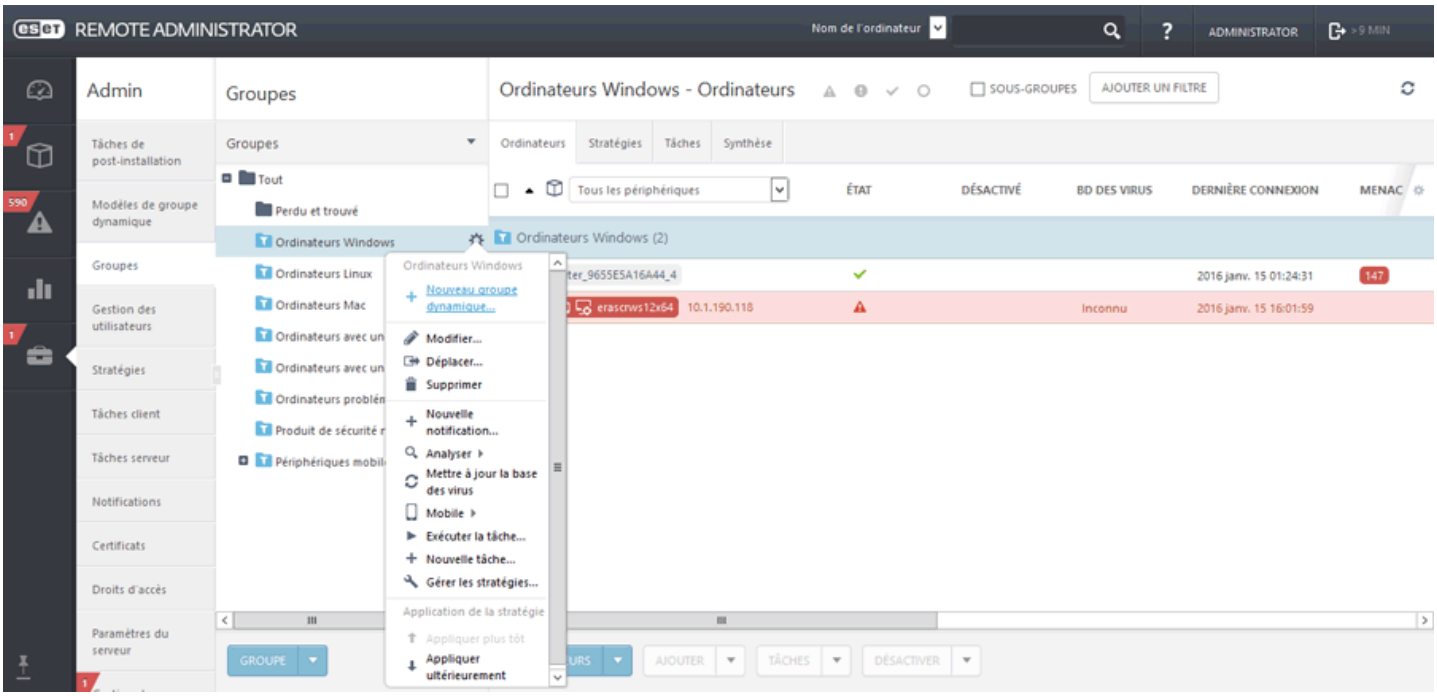
2.7.1.2.2 Créer un groupe dynamique

Trois méthodes permettent de créer un groupe dynamique :

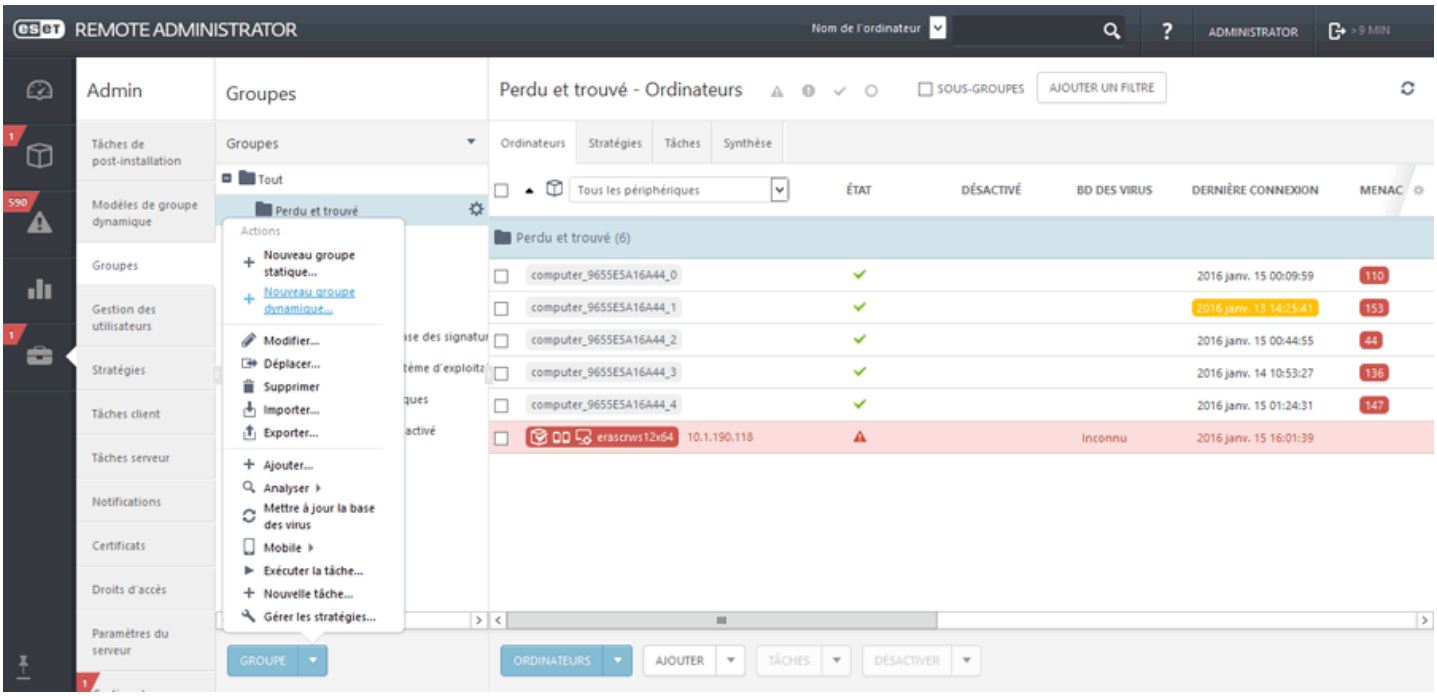
1. Cliquez sur **Ordinateurs** > **Groupes** > ⚙, puis sélectionnez **Nouveau groupe dynamique...**.



2. Cliquez sur **Admin** > **Groupes** > ⚙ > **Nouveau groupe dynamique...**.



3. Cliquez sur **Admin** > **Groupes**, sur le bouton **Groupe**, puis sur **Nouveau groupe dynamique...**.

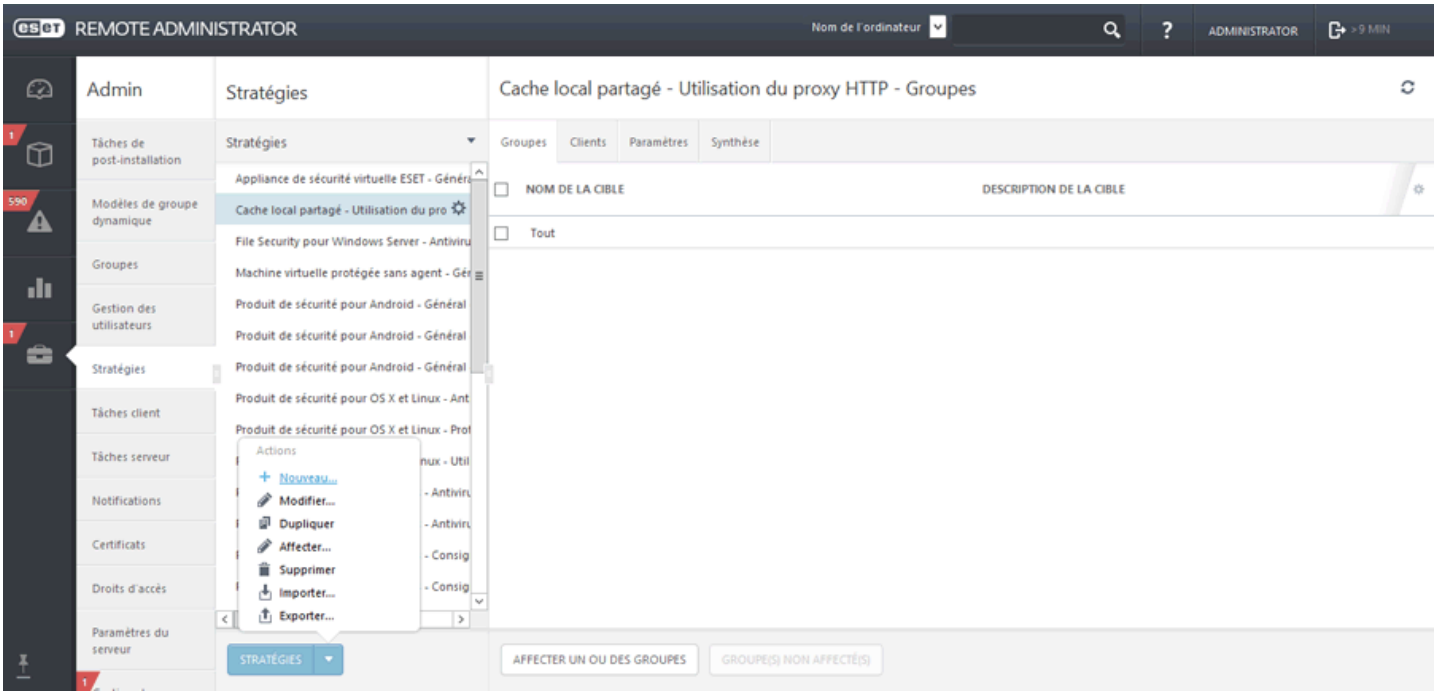


L'Assistant Nouveau groupe dynamique s'affiche. Pour obtenir d'autres cas d'utilisation sur la création d'un groupe dynamique avec des règles pour un modèle de groupe dynamique.

2.7.2 Créer une stratégie

Dans cet exemple, une stratégie pour l'intervalle de connexion d'ERA Agent est créée. Il est recommandé d'effectuer cette opération avant de tester le déploiement en masse dans votre environnement.

Créez un groupe statique. Ajoutez une nouvelle stratégie en cliquant sur **Admin** > **Stratégies**. Cliquez ensuite sur **Stratégies** dans la partie inférieure, puis sélectionnez **Nouveau...**.

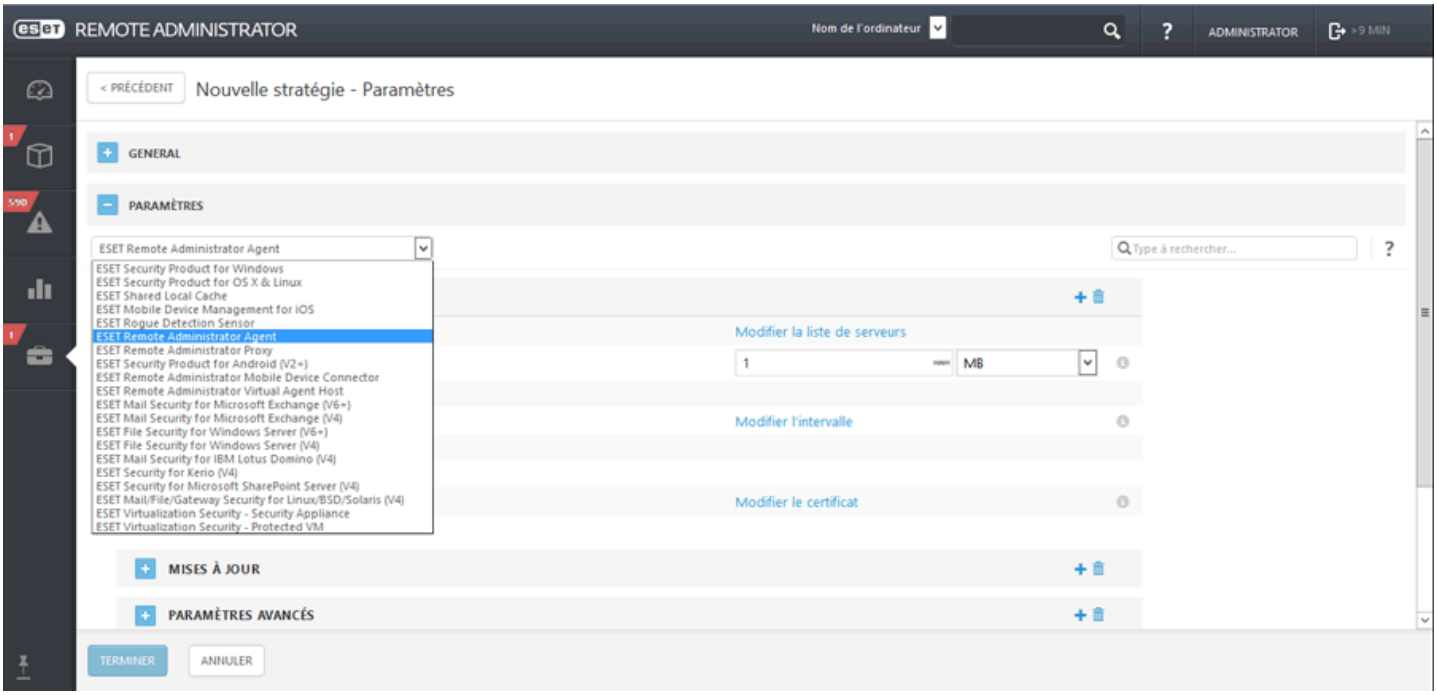


General

Saisissez un **nom** pour la nouvelle stratégie (« Intervalle de connexion de l'Agent », par exemple). Le champ **Description** est facultatif.

Paramètres

Sélectionnez **ESET Remote Administrator Agent** dans le menu déroulant **Produit**.



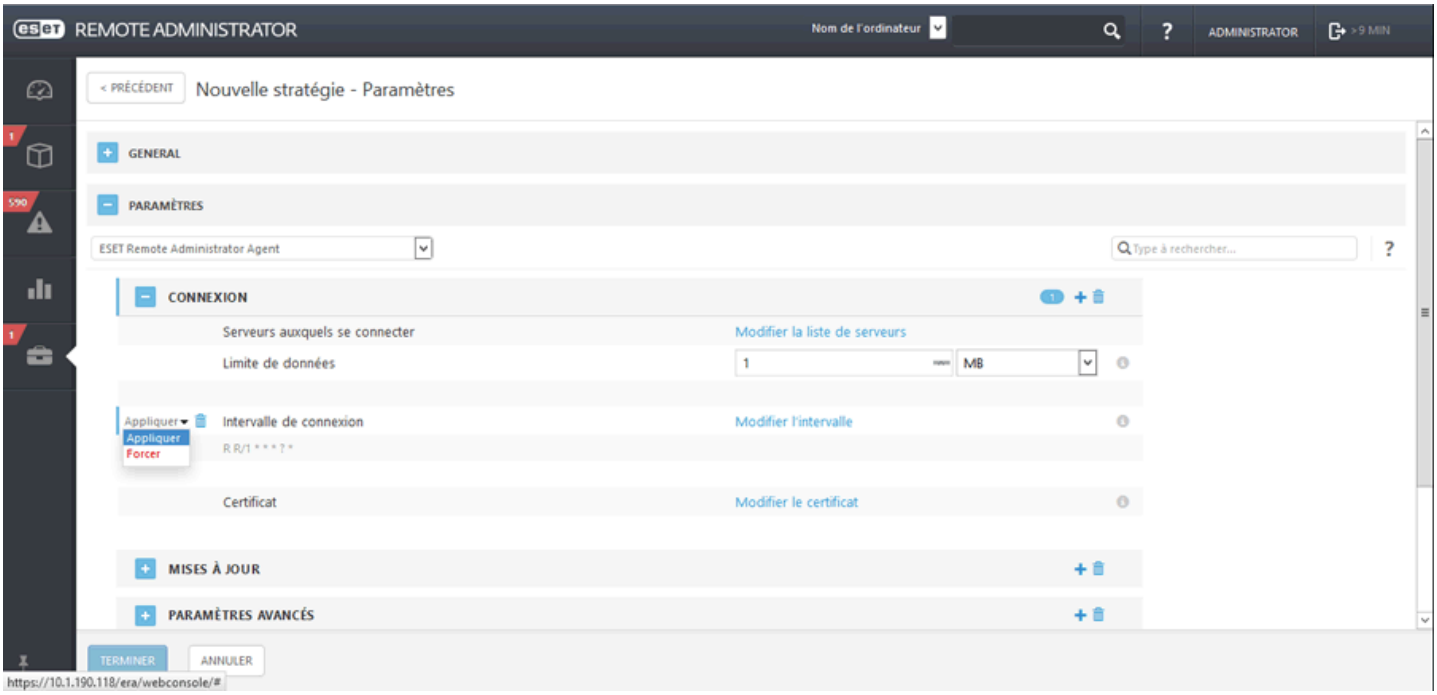
Connexion

Sélectionnez une catégorie dans l'arborescence située à gauche. Dans le volet droit, modifiez les paramètres au besoin. Chaque paramètre est une règle pour laquelle vous pouvez définir un indicateur. Pour faciliter la navigation, toutes les règles sont comptabilisées. Le nombre de règles que vous avez définies dans une section spécifique s'affiche automatiquement. Un nombre apparaît également en regard du nom d'une catégorie dans l'arborescence de gauche. Il indique la somme des règles dans toutes ses sections. Vous pouvez ainsi rapidement déterminer l'emplacement et le nombre de paramètres/règles définis.

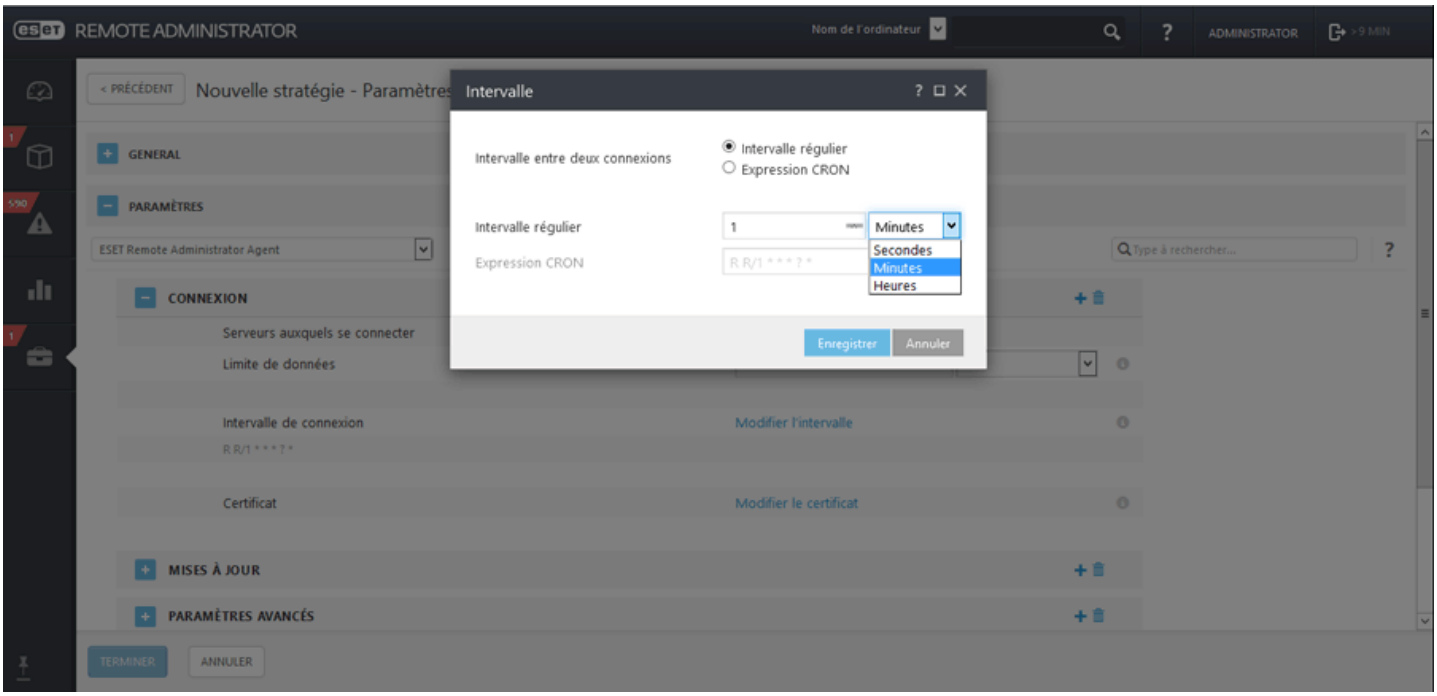
Pour faciliter la modification des stratégies, vous pouvez également suivre ces suggestions :

- utiliser + pour définir l'indicateur **Appliquer** sur tous les éléments actuels d'une section ;
- supprimer des règles à l'aide de l'icône **Corbeille**.

Cliquez sur Modifier l'intervalle.



Dans le champ **Intervalle régulier**, remplacez la valeur par l'intervalle de votre choix (60 secondes est la valeur recommandée), puis cliquez sur Enregistrer.



Une fois la stratégie Intervalle de connexion de l'Agent créée, attribuez-la au groupe statique créé à l'étape 1.

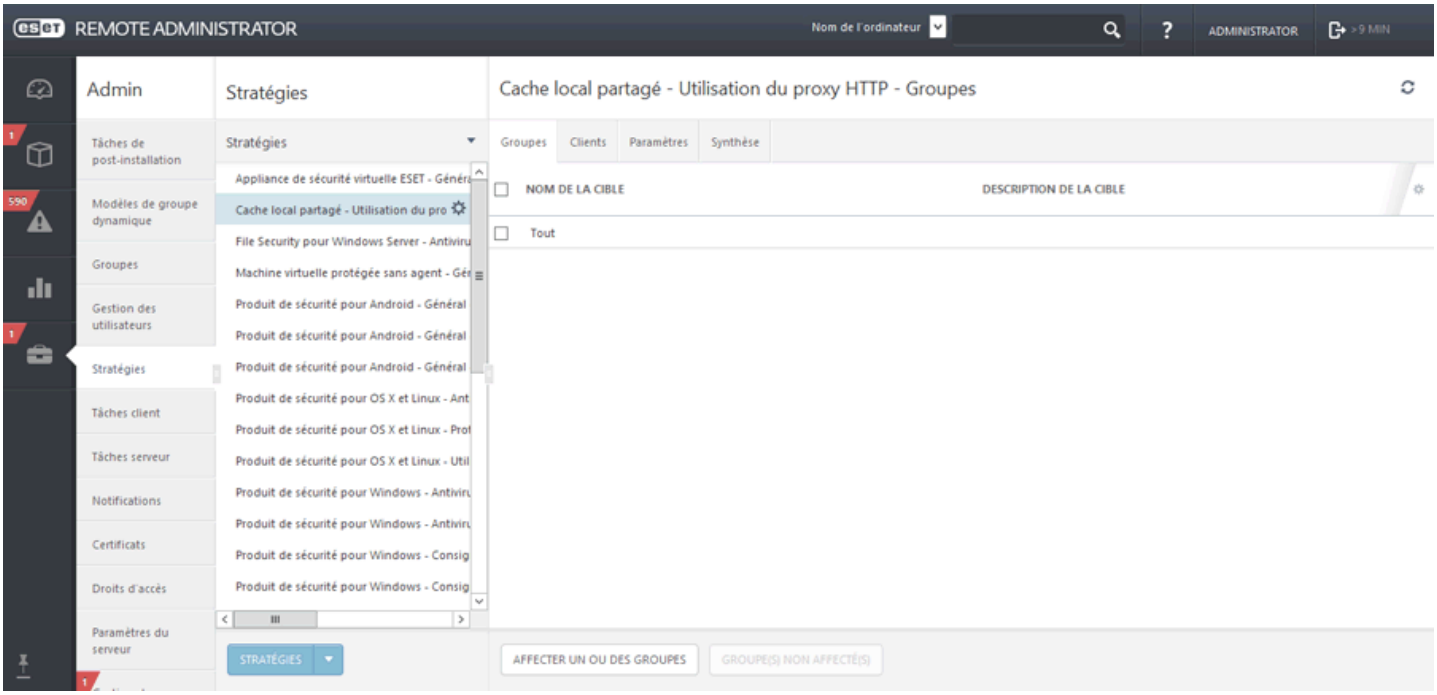
Une fois que vous avez terminé le test du déploiement en masse, modifiez les paramètres de la stratégie Intervalle de connexion de l'Agent créée à l'étape 2.

Cliquez sur **Admin** > **Groupes**, puis sélectionnez l'onglet **Stratégies**. Cliquez sur la stratégie Intervalle de connexion de l'Agent, choisissez **Modifier**, puis cliquez sur **Paramètres** > **Connexion**. Cliquez sur **Modifier l'intervalle** et définissez l'intervalle de connexion sur 20 minutes.

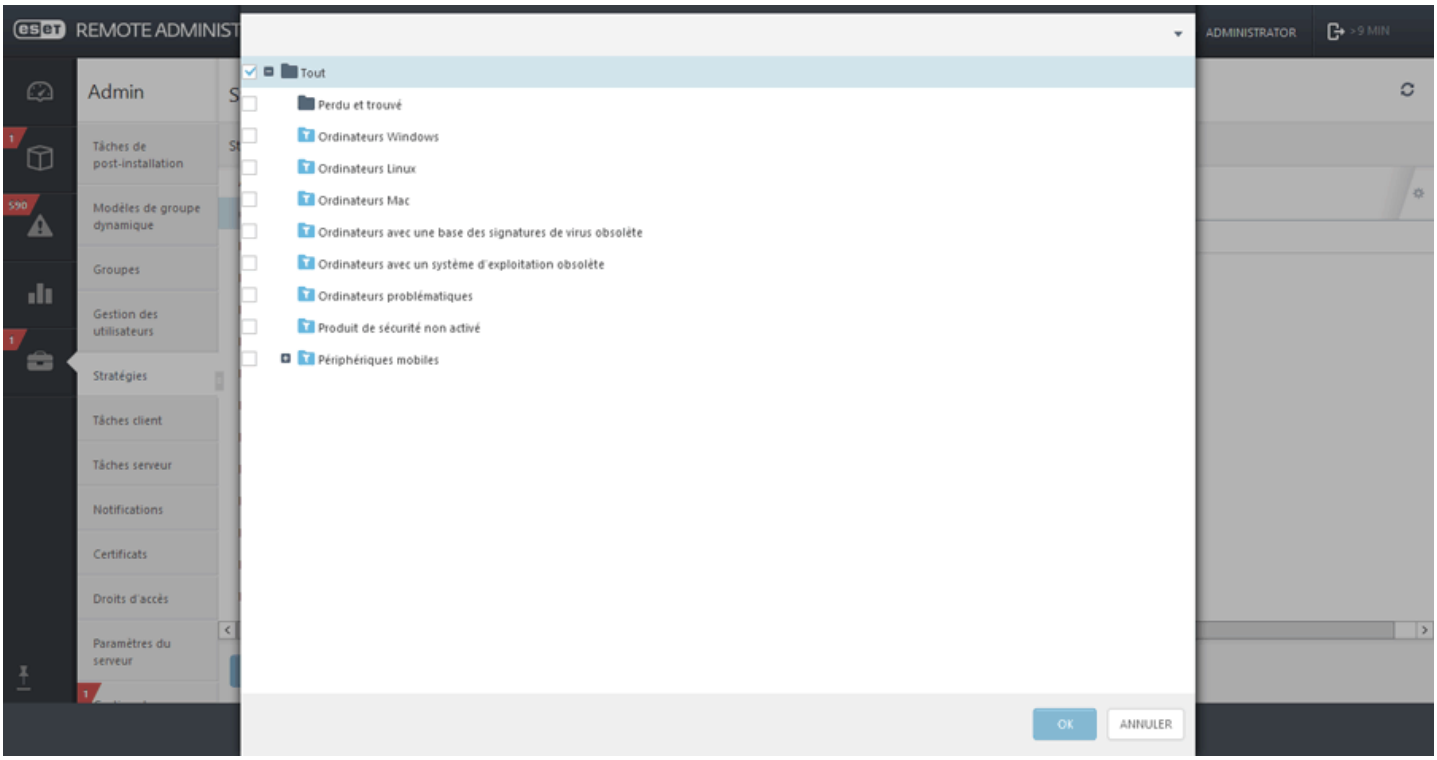
2.7.3 Attribuer une stratégie à un groupe

Une fois une stratégie créée, vous pouvez l'attribuer à un **groupe statique** ou **dynamique**. Il existe deux méthodes pour attribuer une stratégie :

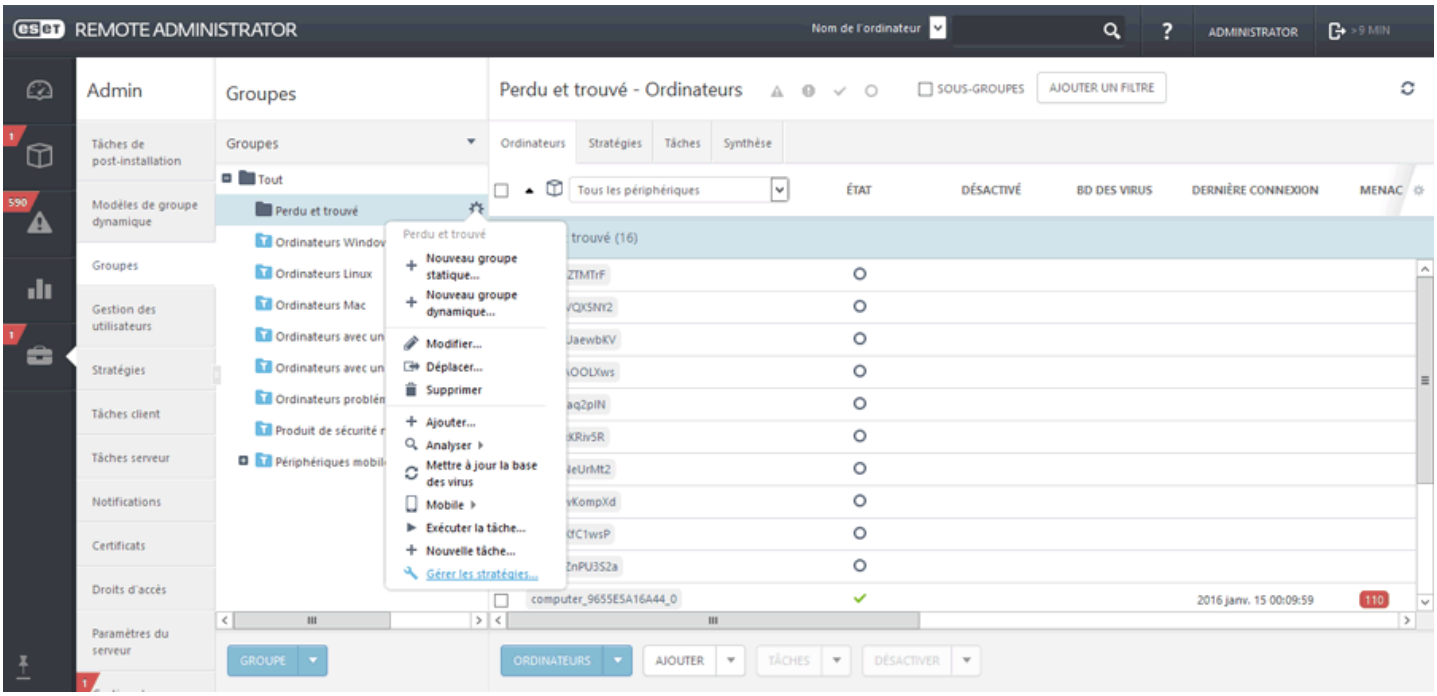
1. Sous **Admin** > **Stratégies**, sélectionnez une stratégie, puis cliquez sur **Affecter un ou des groupes**. Sélectionnez un groupe statique ou dynamique, puis cliquez sur **OK**.



Dans la liste, sélectionnez **Groupe**.



2. Cliquez sur **Admin** > **Groupes** > **Groupe** ou sur l'icône ⚙ située en regard du nom du groupe, puis sélectionnez **Gérer les stratégies**.



Dans la fenêtre **Ordre d'application de la stratégie**, cliquez sur **Ajouter une stratégie**. Cochez la case située en regard de la stratégie à attribuer à ce groupe, puis cliquez sur **OK**.
Cliquez sur **Enregistrer**. Pour afficher la liste des stratégies attribuées à un groupe spécifique, sélectionnez le groupe, puis cliquez sur l'onglet **Stratégies**.

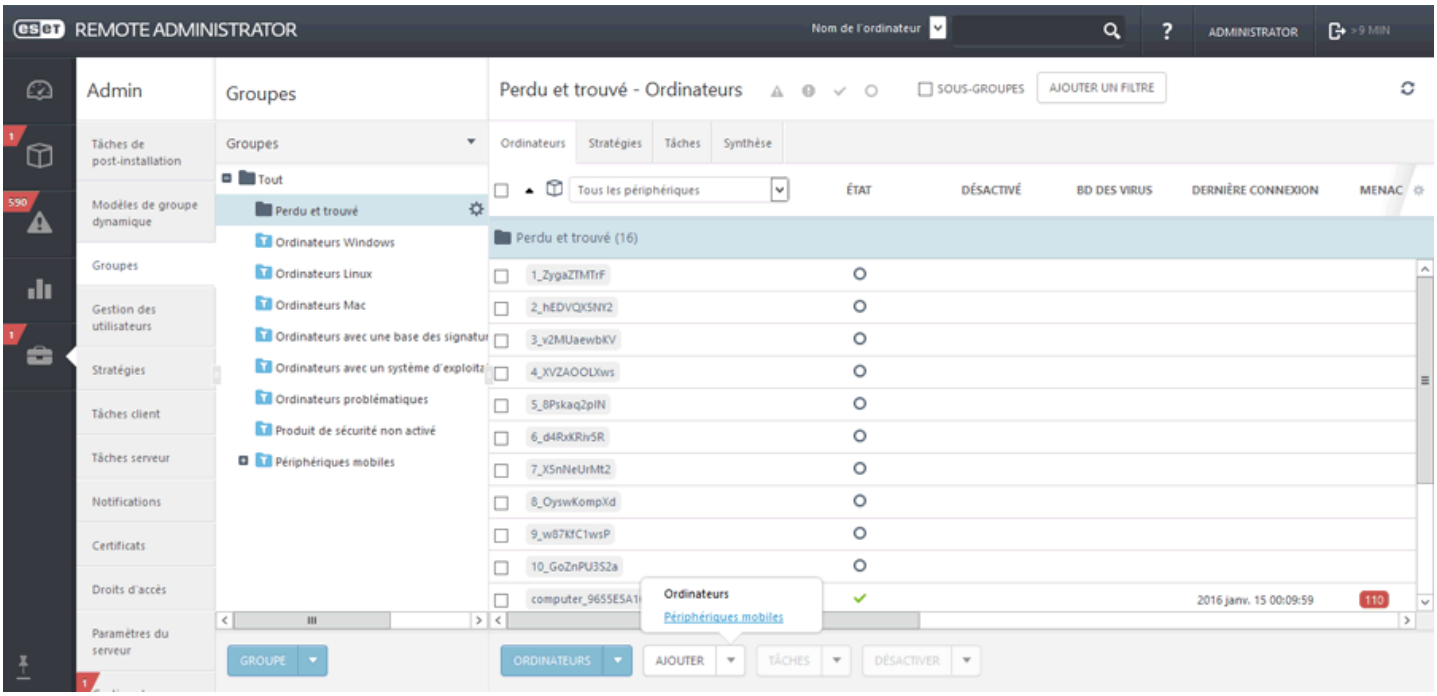
ℹ **REMARQUE** : pour plus d'informations sur les stratégies, reportez-vous au chapitre Stratégies.

2.7.4 Inscription de périphériques mobiles à partir de groupes

Les périphériques mobiles peuvent être gérés par ERA Server ainsi que depuis l'application mobile Android ESET Endpoint Security proprement dite. Pour commencer à gérer les périphériques mobiles, vous devez les ajouter à partir de groupes et les inscrire dans ERA.

Vous pouvez ajouter des périphériques mobiles à votre structure ERA de la même manière que vous le feriez pour de nouveaux ordinateurs :

1. Cliquez sur l'onglet **Admin**.
2. Sélectionnez le **groupe statique** auquel vous souhaitez ajouter le périphérique, puis cliquez sur **Ajouter** Nouveau > Périphériques mobiles.
3. L'assistant de la tâche client vous guide tout au long de la procédure d'ajout du nouveau périphérique.



Vous pouvez également utiliser la tâche client **Inscription de périphérique** :

- Inscription de périphérique Android
- Inscription de périphérique iOS

2.8 Tableau de bord

La page Tableau de bord est la page par défaut qui s'affiche lorsqu'un utilisateur se connecte à ERA Web Console pour la première fois. Elle affiche des rapports prédéfinis sur votre réseau. Vous pouvez passer d'un tableau de bord à un autre à l'aide des onglets situés dans la barre de menus supérieure. Chaque tableau de bord est composé de plusieurs rapports. Vous pouvez personnaliser les tableaux de bord selon vos préférences en ajoutant des rapports, en modifiant ceux existants, en les redimensionnant et en les déplaçant. Vous obtenez ainsi une vue d'ensemble complète d'ESET Remote Administrator et de ses composants (clients, groupes, tâches, stratégies, utilisateurs, compétences, etc.). ESET Remote Administrator contient quatre tableaux de bord préconfigurés :

Ordinateurs
Ce tableau de bord vous donne une vue d'ensemble des ordinateurs clients : état de la protection, systèmes d'exploitation, état de mise à jour, etc.

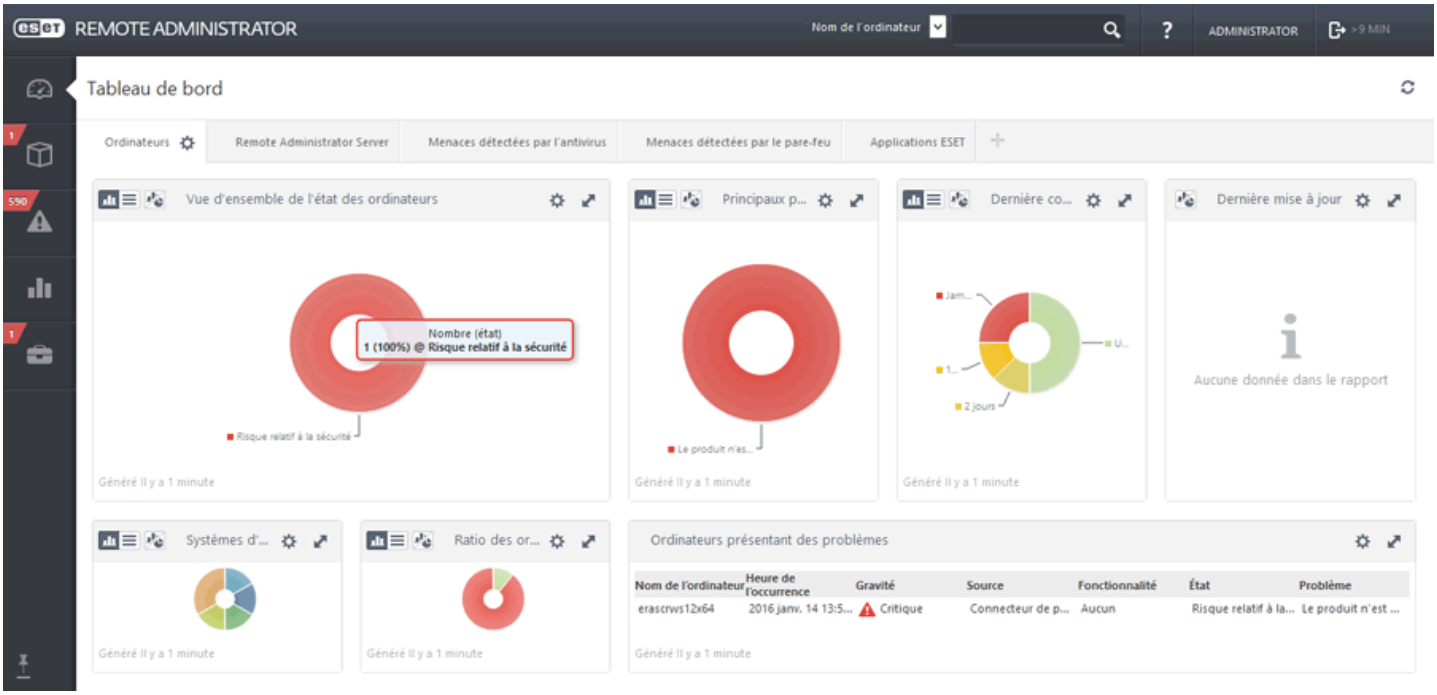
Remote Administrator Server
Ce tableau de bord affiche des informations sur ESET Remote Administrator Server : charge du serveur, clients présentant des problèmes, charge CPU, connexions de base de données, etc.

Menaces virales
Ce tableau de bord contient des rapports sur le module antivirus des produits de sécurité des clients : menaces actives, menaces au cours des 7/30 derniers jours, etc.

Menaces liées au pare-feu
Événements de pare-feu des clients connectés selon la gravité, l'heure de signalement, etc.

Applications ESET
Ce tableau de bord permet de consulter des informations sur les applications ESET installées.

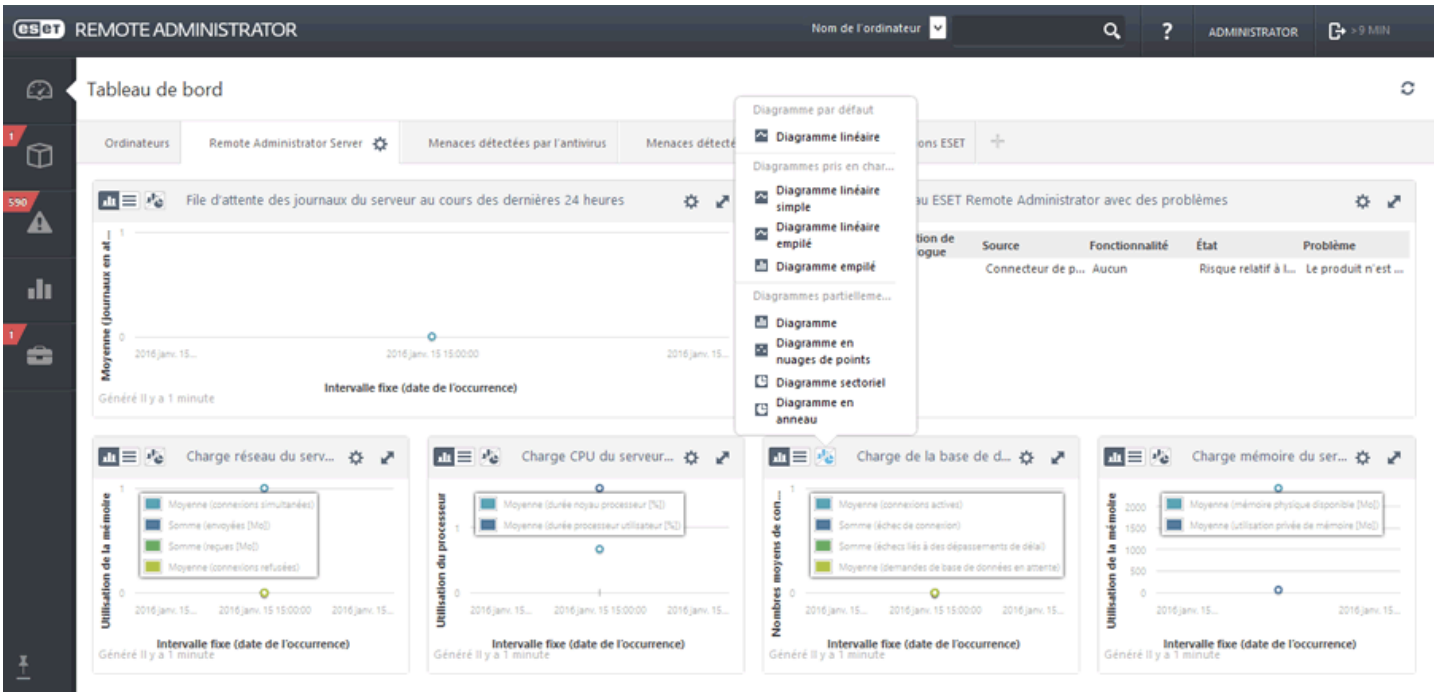
Fonctionnalités des tableaux de bord :



2.8.1 Paramètres de tableau de bord

Les paramètres de tableau de bord sont disponibles pour tous les tableaux de bord, qu'ils soient prédéfinis ou nouvellement créés. Ils vous permettent de gérer vos tableaux de bord. Les options disponibles sont décrites ci-dessous.

- **Ajouter un nouveau tableau de bord** : cliquez sur le symbole + situé dans la partie supérieure du titre Tableau de bord. Saisissez le nom du nouveau tableau de bord, puis cliquez sur **OK** pour confirmer l'opération. Un tableau de bord avec un champ de rapport vide est créé. Une fois le tableau de bord configuré, vous pouvez commencer à y ajouter des rapports.
- **Dupliquer un tableau de bord** : sélectionnez le tableau de bord à dupliquer, puis cliquez sur le symbole d'⚙ situé en regard de son nom. Sélectionnez **Dupliquer** dans la liste. Un tableau de bord en double est créé.
- Cliquez sur ↻ **Rafraîchir la page** pour recharger/actualiser les informations affichées.
- **Déplacer un tableau de bord** : cliquez sur le nom d'un tableau de bord et faites-le glisser pour modifier sa position par rapport aux autres tableaux de bord.
- **Modifier la taille du tableau de bord (nombre de rapports affichés)** : cliquez sur le symbole ⚙ > **Changer de structure**. Sélectionnez le nombre de rapports à afficher dans le tableau de bord (faites glisser) et cliquez sur ces derniers. La structure du tableau de bord change.
- **Renommer un tableau de bord** : cliquez sur le symbole ⚙ situé en regard du nom du tableau de bord, puis sur **Renommer**. Saisissez un nouveau nom pour le tableau de bord, puis cliquez sur **OK**.
- **Renommer un tableau de bord** : cliquez sur le symbole ⚙ situé en regard du nom du tableau de bord, sur **Supprimer**, puis confirmez la suppression.
- **Redimensionner** : cliquez sur le symbole de **flèche à deux pointes** à droite du rapport pour redimensionner ce dernier. Les rapports les plus pertinents sont plus grands, tandis que les moins pertinents sont plus petits. Vous pouvez également basculer en mode Plein écran pour afficher un rapport plein écran.



- **Changer de type de diagramme** : cliquez sur le symbole de **diagramme** situé dans le coin supérieur gauche, puis sélectionnez **Diagramme sectoriel**, **Diagramme linéaire** ou une autre option pour modifier le type de diagramme.
- Cliquez sur **Rafraîchir** pour actualiser les informations affichées.
- Cliquez sur **Modifier** pour afficher un autre rapport.
- Cliquez sur Modifier le modèle de rapport pour ajouter ou modifier un modèle.
- Cliquez sur **Définir l'intervalle de rafraîchissement** pour définir la fréquence de rafraîchissement des données d'un rapport. **L'intervalle de rafraîchissement par défaut est 120 secondes**.
- **Renommez/Supprimez** le rapport.

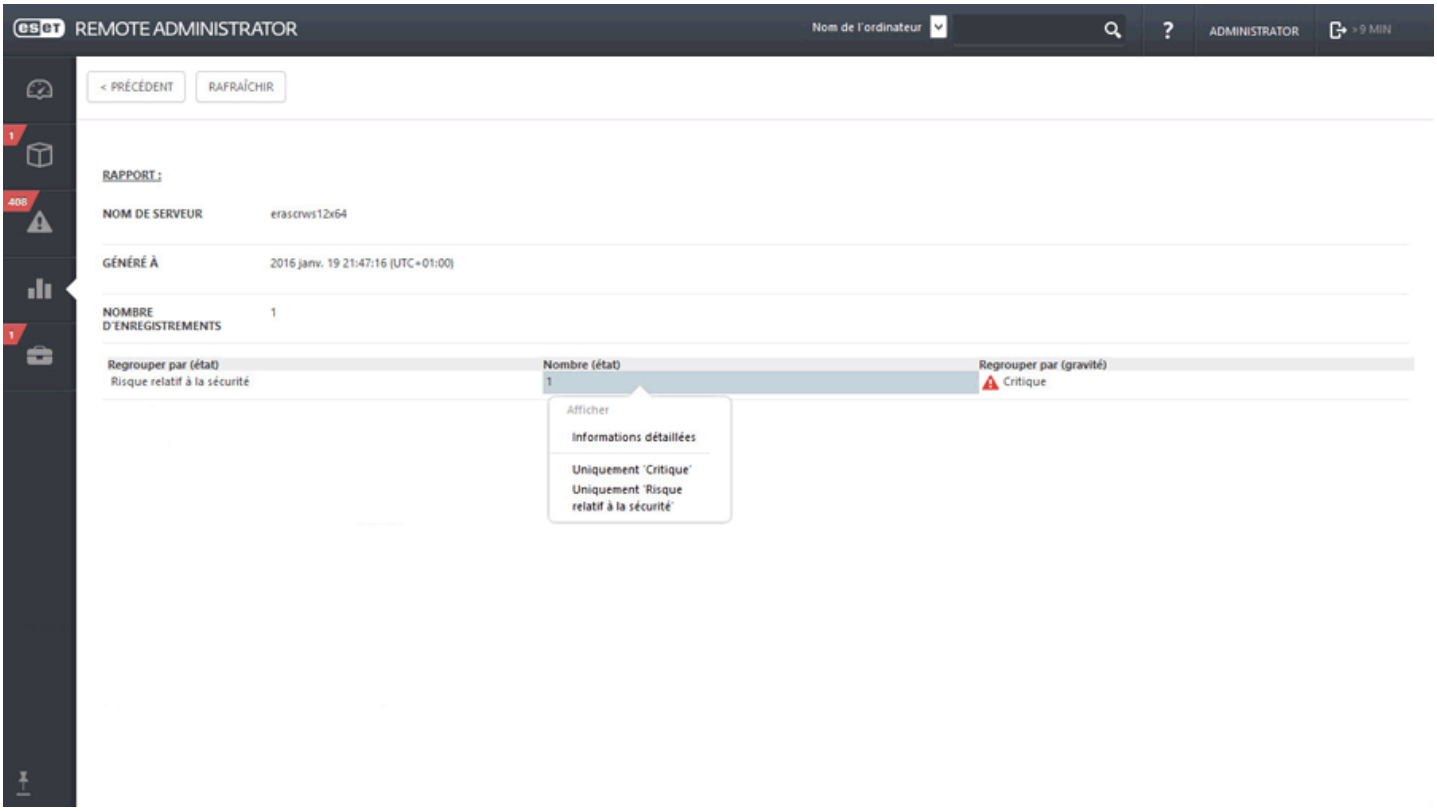
2.8.2 Descendre dans la hiérarchie

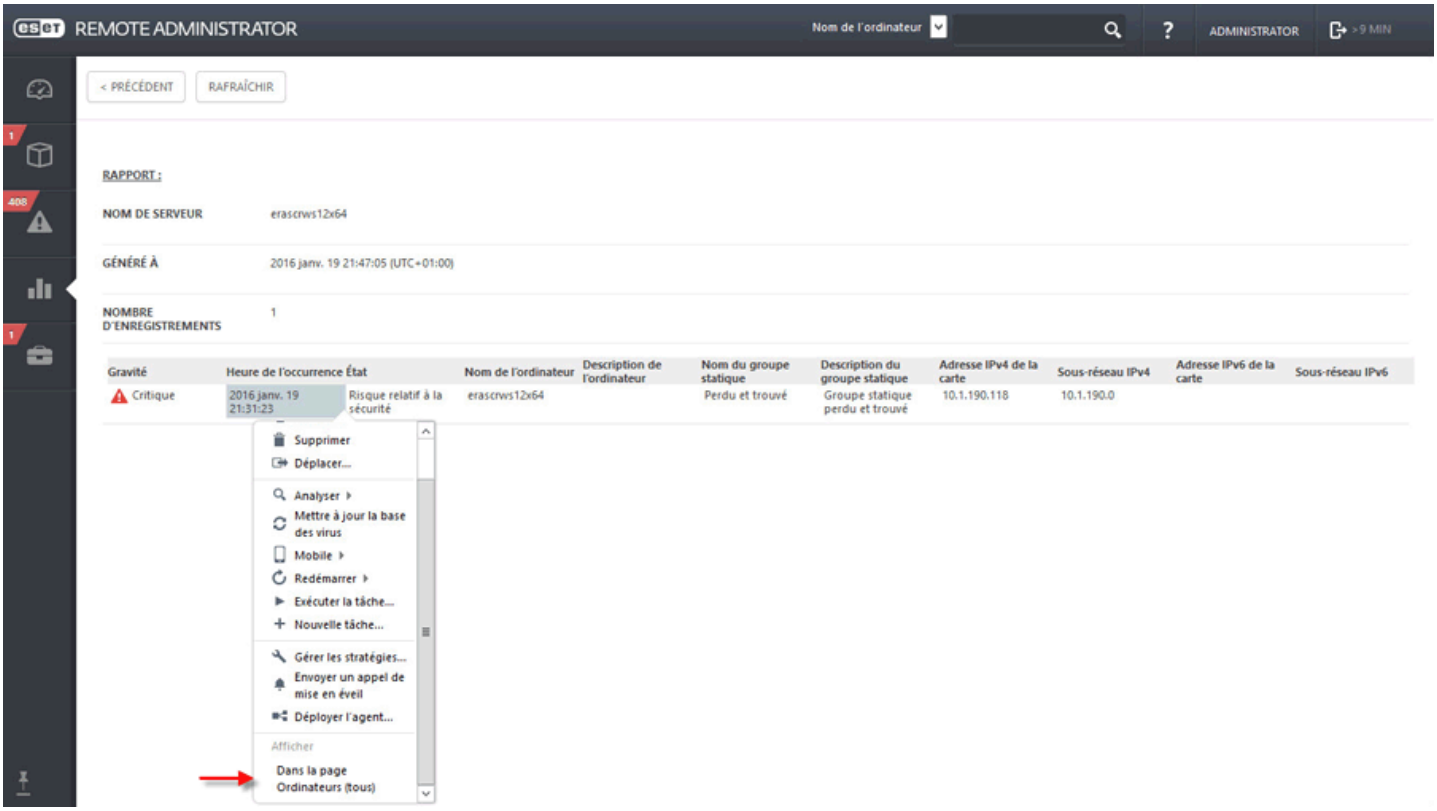
Cette fonctionnalité de tableau de bord est utile pour examiner les données plus en détail. Elle permet de sélectionner de manière interactive des éléments spécifiques d'une synthèse et d'afficher des données détaillées sur ceux-ci. Concentrez-vous sur l'élément qui vous intéresse en allant des informations de synthèse aux informations les plus détaillées sur celui-ci. En règle générale, vous pouvez descendre de plusieurs niveaux dans la hiérarchie.

Il existe quatre types de descentes dans la hiérarchie :

- Affichez des **informations détaillées** : nom de l'ordinateur et description, nom du groupe statique, etc. Permet d'afficher les données d'origine (non agrégées) de la ligne qui a fait l'objet d'un clic.
- Affichez **uniquement la « *valeur* »** : informations, informations critiques, risque de sécurité, notification de sécurité, etc.
- **Développez la colonne « *valeur* »** : elle affiche les informations agrégées (généralement pour un nombre ou une somme). Par exemple, si la colonne contient uniquement un nombre et si vous cliquez sur **Développer la colonne Ordinateur**, elle affiche tous les détails sur les ordinateurs.
- Affichez **Dans la page Ordinateurs (tous)** : vous redirige vers la page Ordinateurs (affiche un résultat comprenant 100 éléments uniquement).

REMARQUE : les résultats que vous obtenez lorsque vous descendez dans la hiérarchie d'autres rapports affichent les 1 000 premiers éléments uniquement.

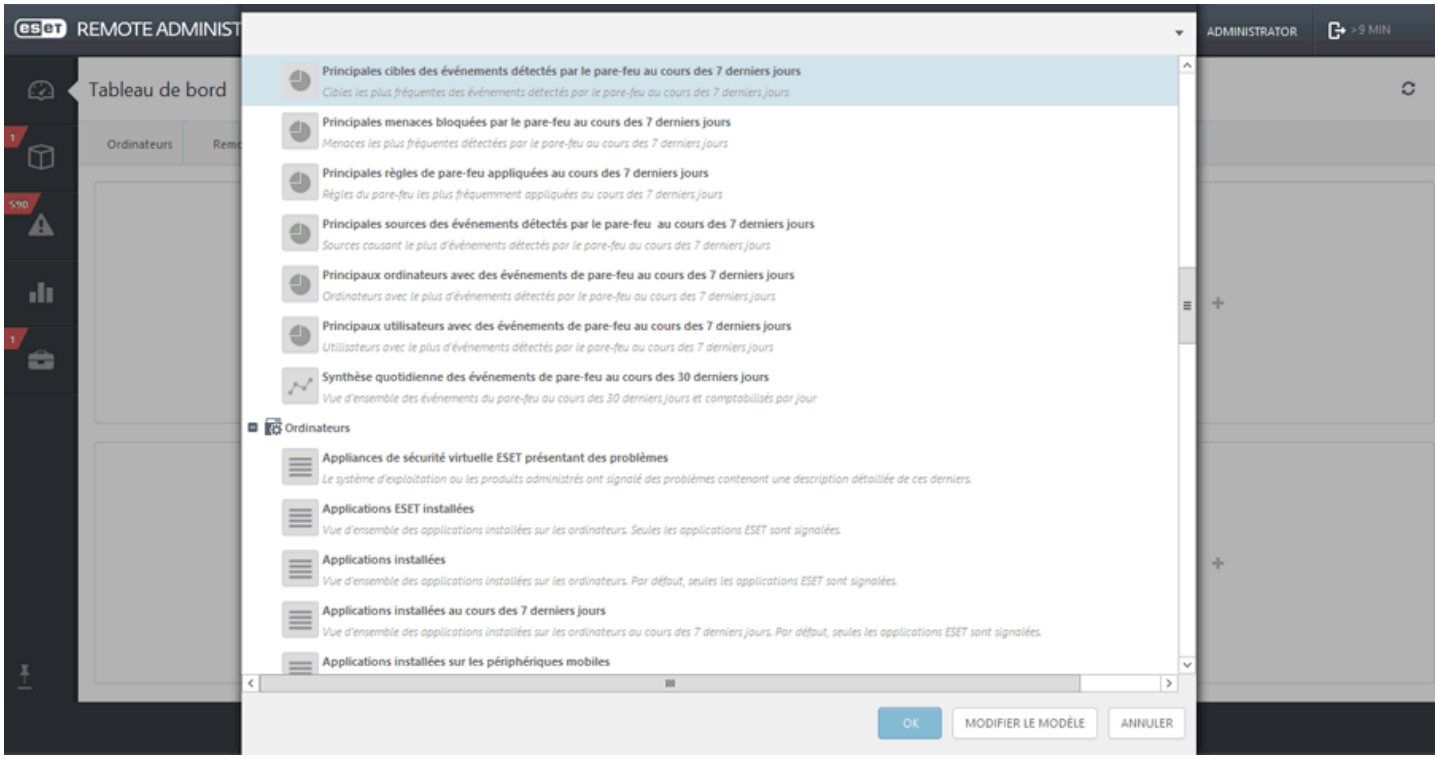




2.8.3 Modifier le modèle de rapport

Cette section décrit comment modifier des modèles de rapport existants (pour plus d'informations sur la création d'un modèle de rapport, cliquez ici).

Cliquez sur un **cadre vide** dans le nouveau tableau de bord. La fenêtre Ajouter un rapport s'affiche. Sélectionnez des applications installées, puis cliquez sur **Ajouter** ou Modifier le modèle.

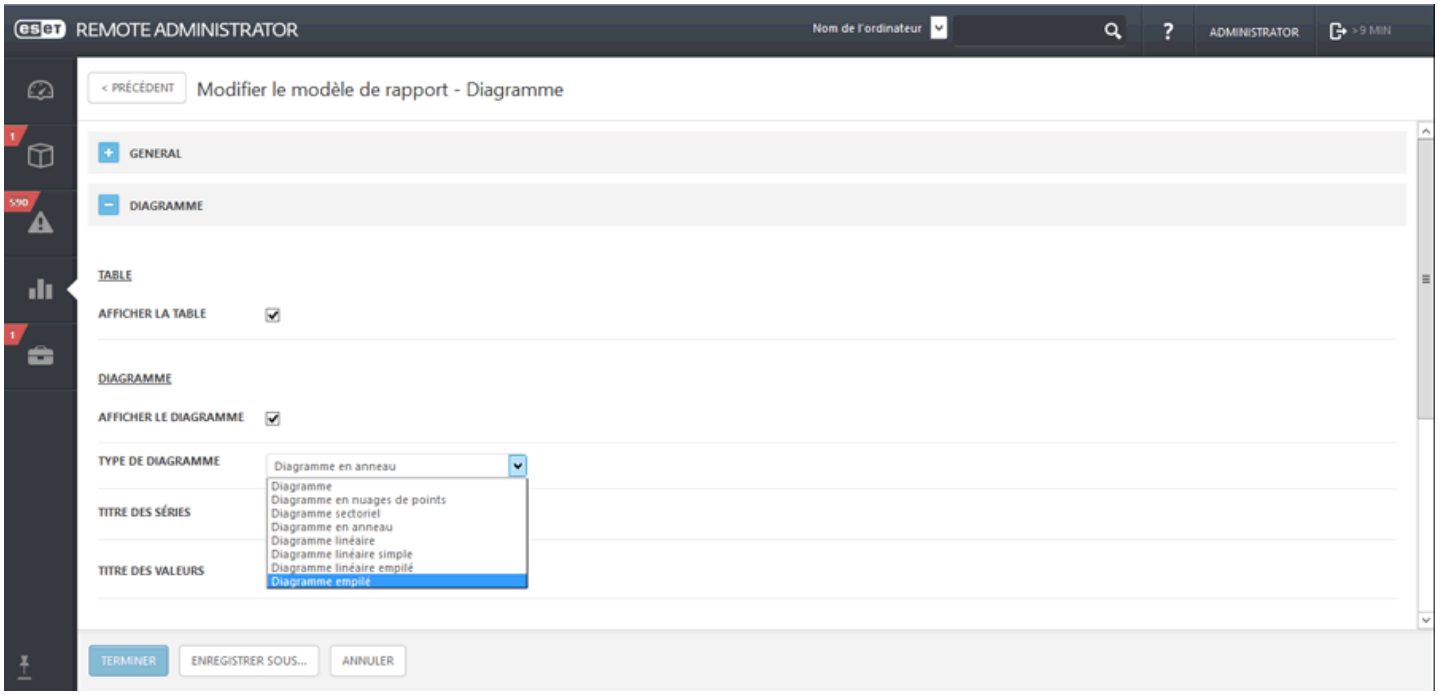


General

Modifiez les informations de **base** sur le modèle. Conservez ou modifiez le **nom**, la **description** et la **catégorie**. Ces informations sont prédéfinies selon le type de **rapport** sélectionné.

Diagramme

Dans la section **Diagramme**, sélectionnez le type de **rapport**. Dans cet exemple, l'option **Afficher la table** n'est pas sélectionnée, tandis que l'option **Afficher le diagramme** l'est.

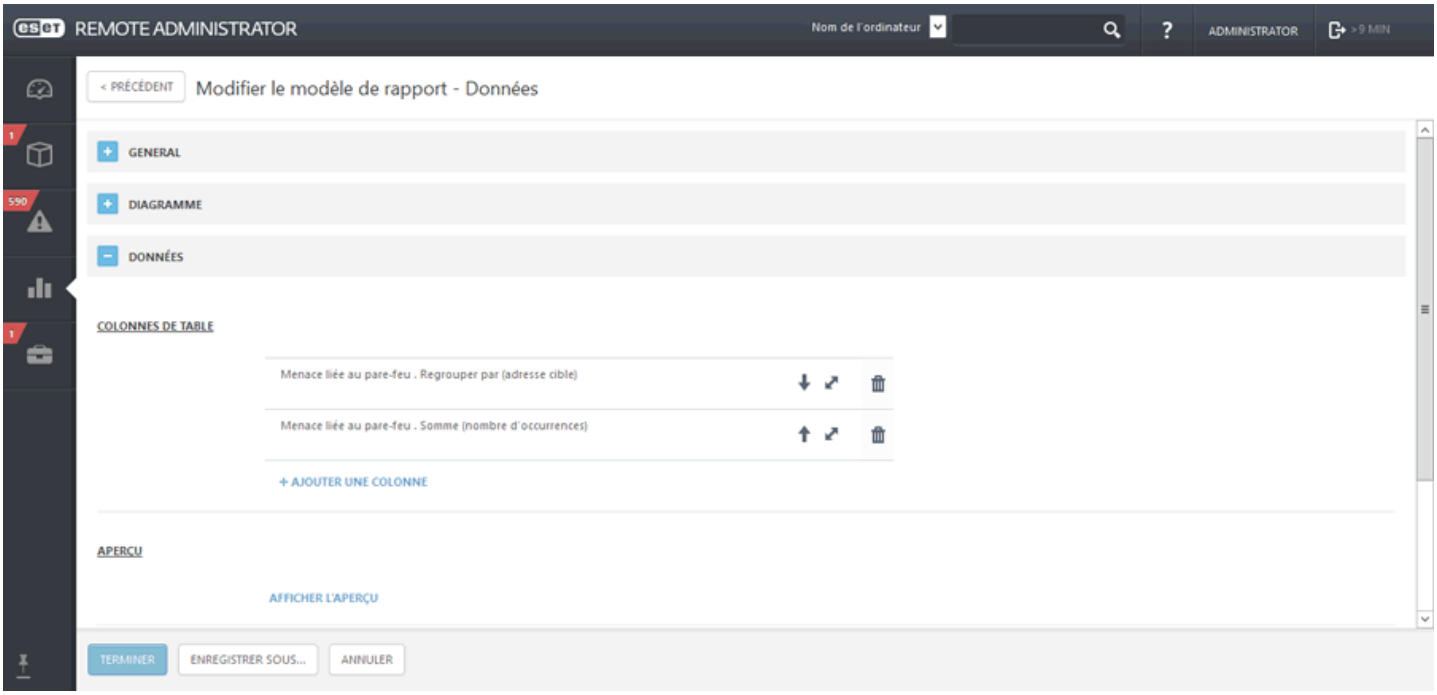


REMARQUE : chaque type de diagramme sélectionné s'affiche dans la section **Aperçu**. Vous pouvez ainsi déterminer l'aspect du rapport en temps réel.

Lorsque vous sélectionnez un **diagramme**, vous disposez de plusieurs options. Pour une meilleure vue d'ensemble, le **type Diagramme linéaire empilé** est sélectionné. Ce type de diagramme est utilisé pour analyser des données avec des unités de mesure différentes.

Vous pouvez éventuellement saisir un titre pour les axes **X** et **Y** du diagramme pour en faciliter la lecture et détecter des tendances.

Données

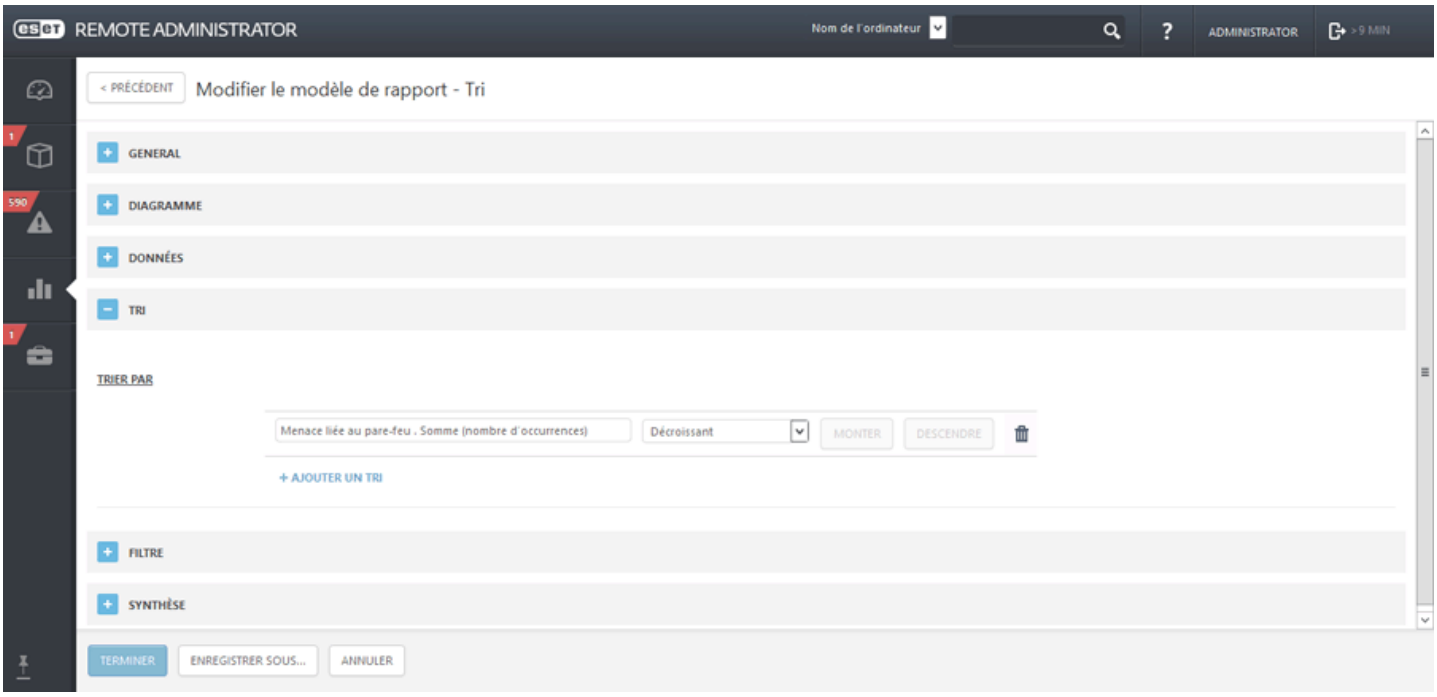


La section **Données** contient les informations saisies à afficher sur les axes **X** et **Y** du diagramme. Lorsque vous cliquez sur l'un des symboles, la fenêtre correspondante s'affiche pour proposer des options. Les options disponibles pour l'axe **Y** dépendent toujours des informations sélectionnées pour l'axe **X**, et inversement. Comme le diagramme affiche leur relation, les données doivent être compatibles.

Pour l'axe **X**, sélectionnez **Ordinateur** > **Nom de l'ordinateur** pour déterminer quels ordinateurs envoient du courrier indésirable. Le **format** est défini sur **Valeur** > **Absolue**. La couleur est les icônes sont définies par l'administrateur.

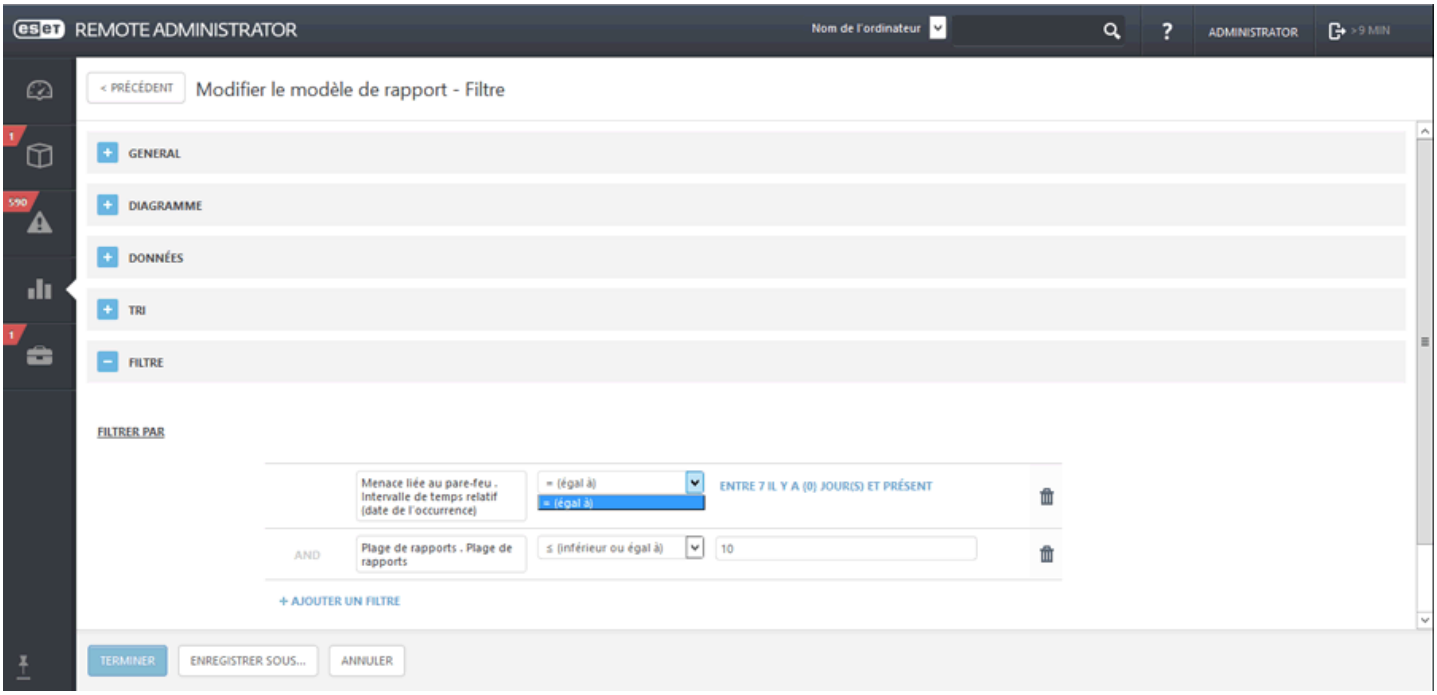
Pour l'axe **Y**, sélectionnez **Logiciel installé** > **Taille en Mo** pour déterminer le nombre absolu de messages indésirables. Le **format** est défini sur **Valeur** > **Absolue**. La couleur est les icônes sont définies par l'administrateur.

Tri



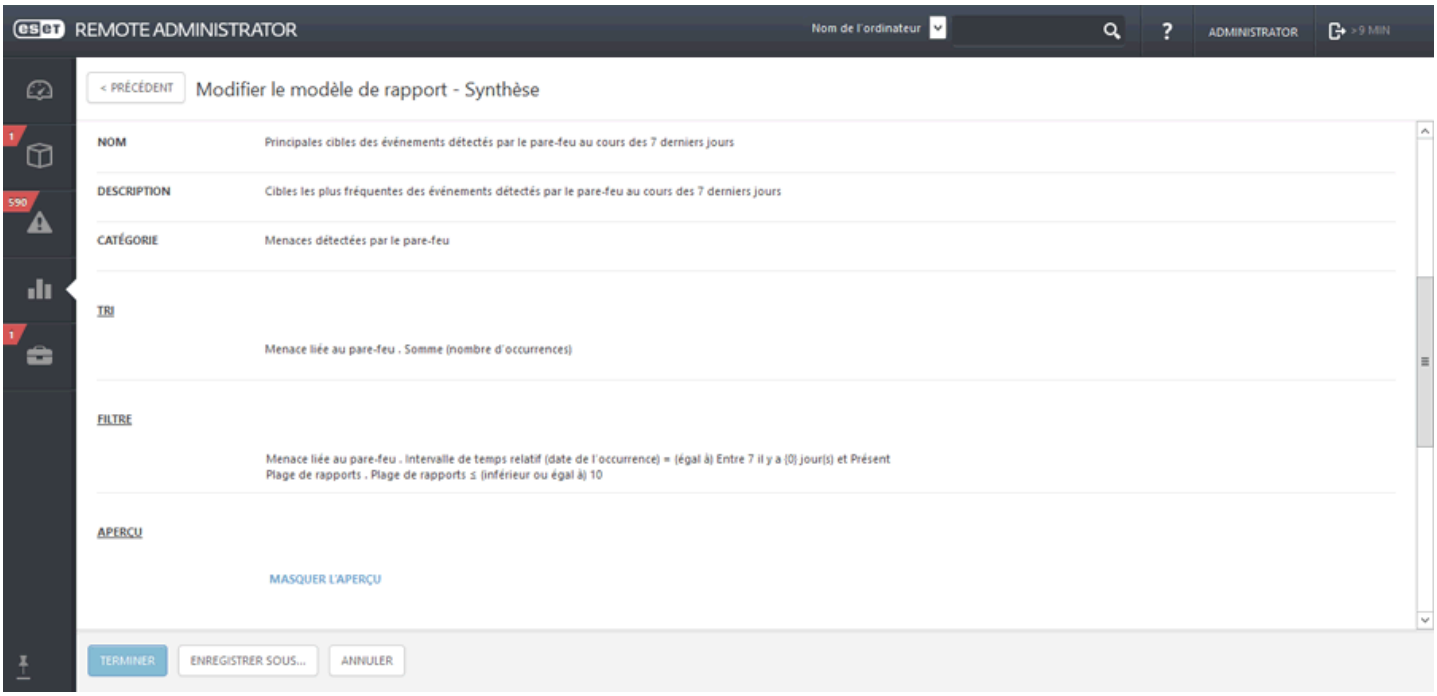
Utilisez l'option Ajouter un tri pour définir la relation entre les données sélectionnées. Sélectionnez les informations de début et la méthode de tri (**Croissant** ou **Décroissant**). Il est également possible de trier les données à l'aide des deux options (voir ci-dessus).

Filtre



Les options affichées dans cette section dépendent des paramètres précédemment configurés (informations pour les axes X et Y). Sélectionnez une option et une fonction mathématique pour déterminer le filtrage des données. Dans cet exemple, les options et fonctions suivantes ont été sélectionnées : **Logiciel installé** et **Nom de l'application** > **est égal à** > **ESS** et **Logiciel installé**. **Taille en Mo** > **est supérieur à** > **50**.

Résumé

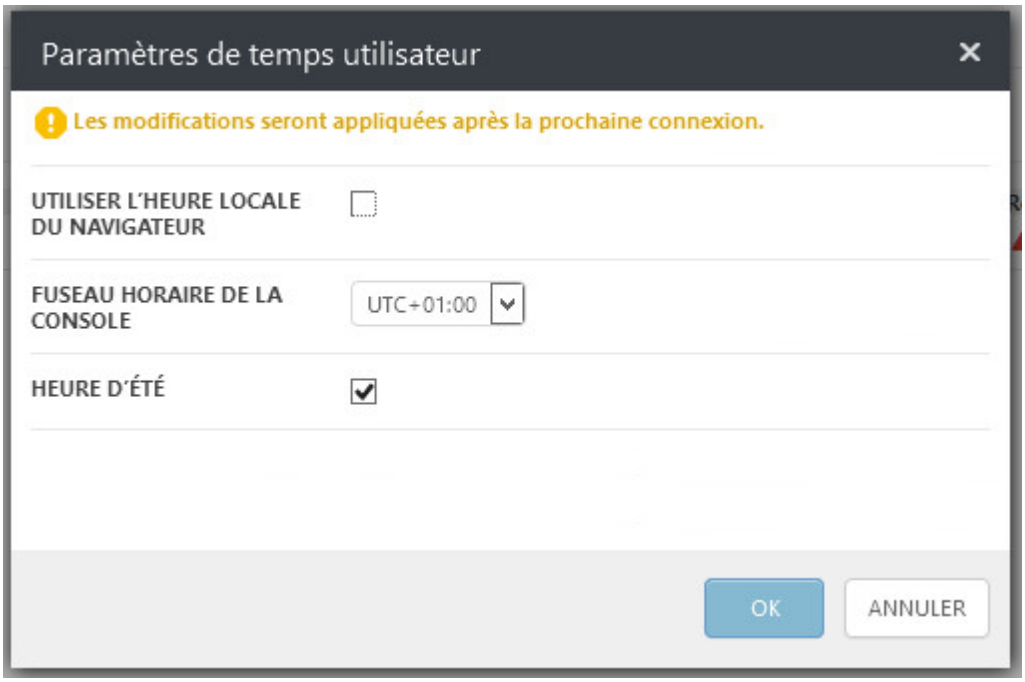


Dans la section **Résumé**, passez en revue les options sélectionnées et les informations. Si elles vous conviennent, cliquez sur **Terminer** pour créer un **modèle de rapport**.

2.8.4 Fuseau horaire

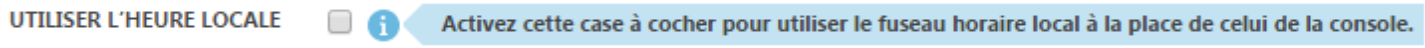
Toutes les informations sont stockées en interne dans ESET Remote Administrator à l'aide de la norme UTC (Coordinated Universal Time, temps universel coordonné). L'heure UTC est automatiquement convertie dans le fuseau horaire utilisé par ERA Web Console (en tenant compte du changement d'heure hiver/été). ERA Web Console affiche l'heure locale du système sur lequel la console est exécutée (et non pas l'heure UTC interne). Vous pouvez remplacer ce paramètre pour définir manuellement l'heure dans ERA Web Console.

Pour modifier les **paramètres de temps utilisateur**, cliquez sur votre nom d'utilisateur situé dans le coin supérieur droit d'ERA Web Console. Décochez la case située en regard de l'option **Utiliser l'heure locale du navigateur**pour remplacer le paramètre par défaut. Vous pouvez alors spécifier le **fuseau horaire de la console manuellement** et choisir d'utiliser ou non l'option **Heure d'été**.



REMARQUE : ce paramètre s'applique uniquement à l'utilisateur actuellement connecté. Chaque utilisateur peut posséder ses paramètres d'heure préférés pour ERA Web Console. Les paramètres d'heure propres à l'utilisateur sont appliqués quel que soit l'emplacement d'accès à ERA Web Console.

IMPORTANT : dans certains cas, l'option permettant d'utiliser un autre fuseau horaire (l'heure locale d'un client sur lequel s'exécute ERA, par exemple) devient disponible. Ce paramètre peut s'avérer particulièrement utile lors de la configuration de déclencheurs. Lorsque cette option est disponible, cela est indiqué dans ERA Web Console. Vous avez alors la possibilité d'**utiliser l'heure locale** ou non.



2.9 Ordinateurs

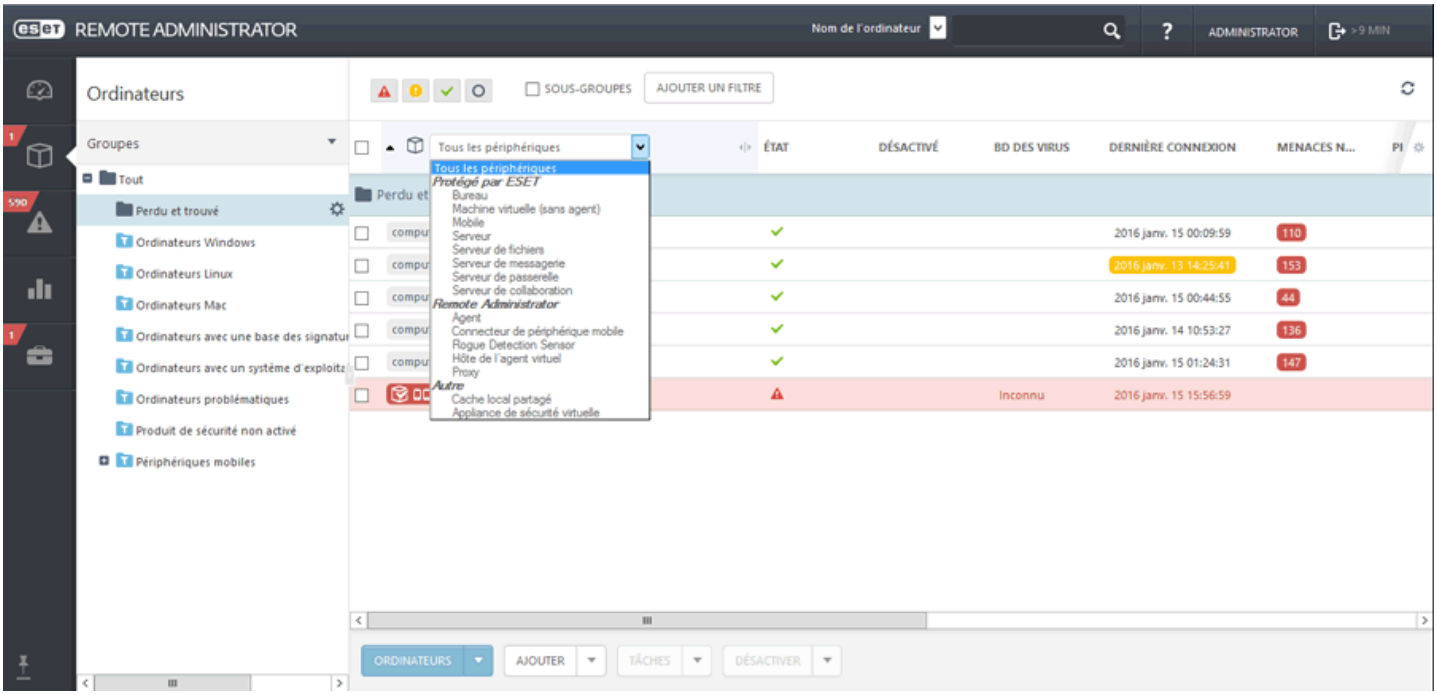
Tous les ordinateurs clients ayant été ajoutés à ESET Remote Administrator sont affichés dans cette section. Ils sont répartis dans des groupes. Lorsque vous cliquez sur un groupe dans la liste (à gauche), les membres (clients) de ce dernier sont affichés dans le volet droit. Vous pouvez filtrer les clients à l'aide des filtres situés dans la partie supérieure de la page. Lorsque vous cliquez sur **Ajouter un filtre**, les critères de filtrage disponibles s'affichent. Il existe également quelques filtres prédéfinis qui sont rapidement accessibles :

- Quatre icônes permettant d'appliquer un filtre par gravité (rouge : **Erreurs**, jaune : **Avertissements**, verte : **Avis** et grise : ordinateurs **Non gérés**). L'icône de gravité représente l'état actuel du produit ESET sur un ordinateur client spécifique. Vous pouvez utiliser une combinaison de ces icônes en les activant ou les désactivant. Pour n'afficher par exemple que les ordinateurs avec des avertissements, activez uniquement l'icône jaune (les autres icônes doivent être désactivées). Pour afficher les avertissements et les erreurs, activez uniquement les deux icônes correspondantes.
- Case à cocher **Sous-groupes** : affiche les sous-groupes du groupe actuellement sélectionné.
- Les ordinateurs **non gérés** (clients du réseau sur lesquels ERA Agent ou un produit de sécurité n'est pas installé) apparaissent généralement dans le groupe **Perdu et trouvé**.

À l'aide du menu déroulant situé sous les filtres, vous pouvez limiter l'affichage des clients (ordinateurs). Plusieurs catégories sont disponibles :

- **Tous les périphériques** dans le menu déroulant pour réafficher tous les ordinateurs clients, sans limiter (filtrer) les clients affichés. Vous pouvez utiliser une combinaison de toutes les options de filtrage ci-dessus lors de la limitation de l'affichage.
- **Protégé par ESET** (protégé par un produit ESET).
- **Remote Administrator** (composant ERA distincts, tels que l'Agent, RD Sensor, le proxy, etc.).
- **Autre** (cache local partagé, appliance virtuelle). Lorsque vous effectuez une sélection, seuls les clients correspondants sont affichés.

REMARQUE : si vous ne parvenez pas à trouver un ordinateur spécifique dans la liste alors qu'il figure dans l'infrastructure ERA, vérifiez que tous les filtres sont désactivés.



Vous pouvez utiliser le menu contextuel (icône ⚙) pour créer un groupe statique ou dynamique, une tâche ou effectuer une sélection parmi d'autres actions disponibles.

Actions du bouton **Ordinateurs** :

+ Nouveau...
Ajoutez manuellement les ordinateurs qui ne sont pas détectés ou automatiquement ajoutés.

Détails...
- **General** (Nom, Groupe parent, Périphérique, Informations sur le SE, etc.)
- **Configuration** (Configuration, Stratégies appliquées, etc.)
- **SysInspector** : affiche Visionneuse des journaux SysInspector, vous devez exécuter la tâche client demande de journal SysInspector pour voir la sortie.
- **Exécutions de tâche** (Survenance, Nom de la tâche, Type de tâche, État, etc.)
- **Applications installées** (Nom, Fournisseur, Version, L'agent prend en charge la désinstallation, etc.)
- **Alertes** (Problème, État, etc.)
- **Menaces et quarantaine** (Tous les types de menace, Désactivé, Cause, Nom de la menace, Type de menace, Nom de l'objet, Hachage, etc.)

Supprimer
Supprime le client de la liste, mais celui-ci apparaît dans le groupe Perdu et trouvé tant qu'il se trouve sur le réseau.

Déplacer...
Vous pouvez déplacer le client vers un autre groupe. Lorsque vous sélectionnez cette option, la liste des groupes disponibles s'affiche.

Renommer plusieurs éléments
Pour effectuer une modification en bloc des noms d'ordinateur affichés dans la console Web ERA. Par exemple, si le nom affiché est « jean.sg.société.com », tapez « sg\.société » dans le champ **Rechercher (Regex)** et « société » dans **Remplacer par**. Cliquez sur le bouton **Renommer** et les ordinateurs seront affichés sur la console Web ERA en tant que « jean.eset.com ».

Gérer les stratégies...
Une stratégie peut être également attribuée directement à un client (ou plusieurs clients), et pas seulement à un groupe. Sélectionnez cette option pour attribuer la stratégie aux clients sélectionnés.

Envoyer un appel de mise en éveil
ERA Server établit une communication immédiate avec ERA Agent sur un ordinateur client. Cette option s'avère utile lorsque vous ne souhaitez pas attendre l'intervalle de connexion régulier entre ERA Agent et ERA Server, quand vous souhaitez exécuter immédiatement une tâche de client sur les clients ou appliquer tout de suite une stratégie, par exemple.

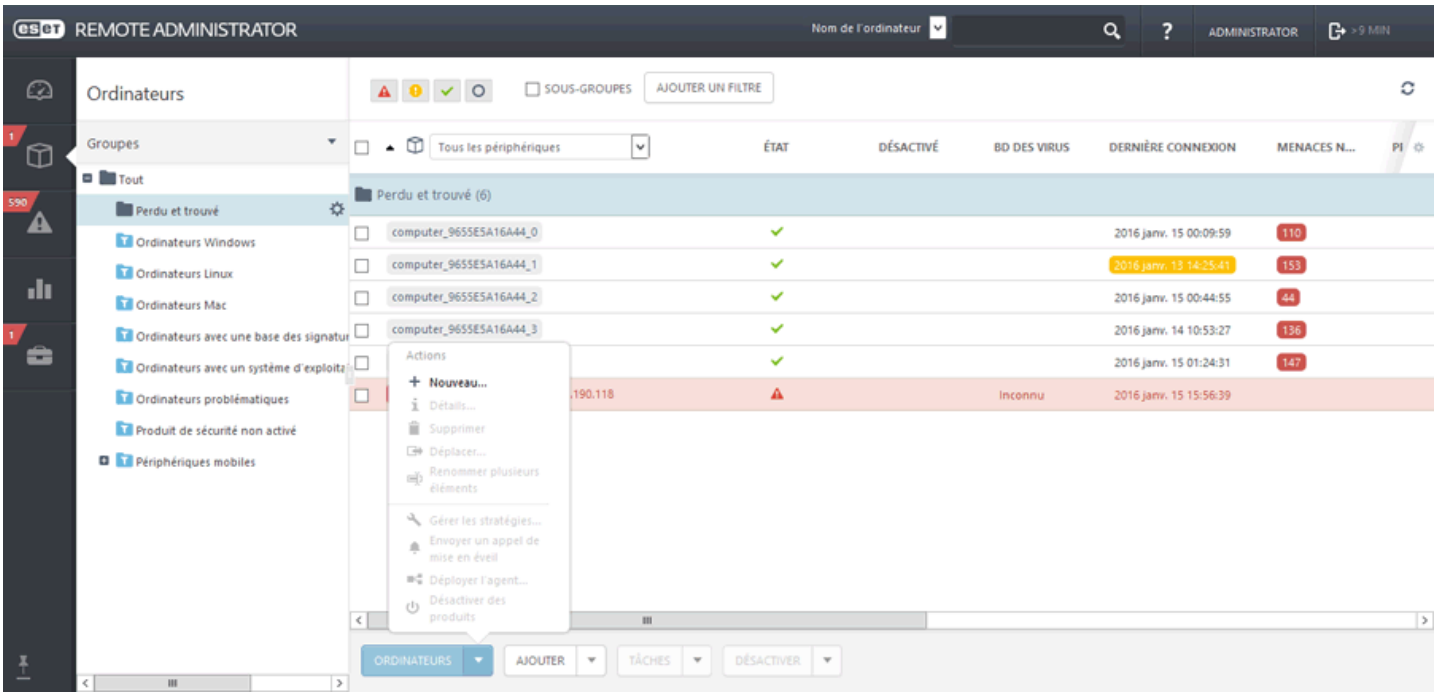
REMARQUE : lorsque vous apportez une modification que vous souhaitez appliquer, patientez environ une minute avant d'utiliser la fonction d'appel de mise en éveil.

Déployer l'agent...
À l'aide de cette option, vous pouvez créer une tâche de serveur.

Désactiver des produits
Cette option est utilisée pour désactiver une licence (pour l'ordinateur client sélectionné) dans ESET License Administrator. Le produit de sécurité ESET s'exécutant sur l'ordinateur client constatera que la licence est désactivée lors de sa prochaine connexion à Internet. Ce système vous offre l'avantage de pouvoir désactiver des licences sur des ordinateurs qui ne sont plus gérés par ERA.

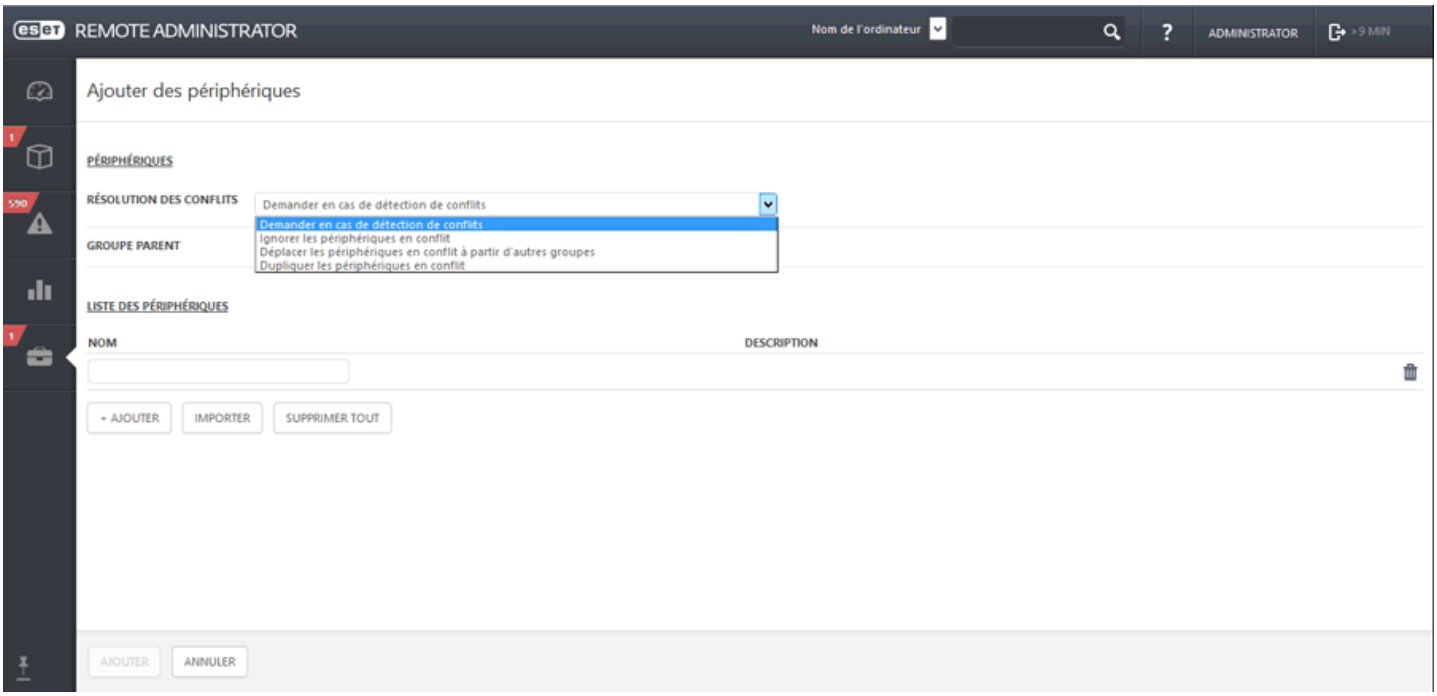
2.9.1 Ajouter des ordinateurs

Cette fonctionnalité permet d'ajouter manuellement des ordinateurs ou des périphériques mobiles qui ne sont pas détectés ou ajoutés automatiquement. Cliquez sur l'onglet **Ordinateurs**, sélectionnez un **groupe statique**, puis cliquez sur **Ajouter**, sélectionnez **Ordinateurs**.



Saisissez le nom de l'ordinateur à ajouter dans le champ **Nom**. Utilisez le menu déroulant **Résolution des conflits** pour sélectionner l'action à exécuter si un ordinateur que vous ajoutez existe déjà dans ERA :

- **Demander en cas de détection de conflits :** lorsqu'un conflit est détecté, le programme vous demande de sélectionner une action (voir les options ci-dessous).
- **Ignorer les ordinateurs en conflit :** les ordinateurs en double ne sont pas ajoutés.
- **Déplacer les ordinateurs en conflit vers d'autres groupes :** les ordinateurs en conflit sont déplacés de leur groupe d'origine vers le groupe **Tous**.
- **Dupliquer les ordinateurs en conflit :** les nouveaux ordinateurs sont ajoutés avec des noms différents.

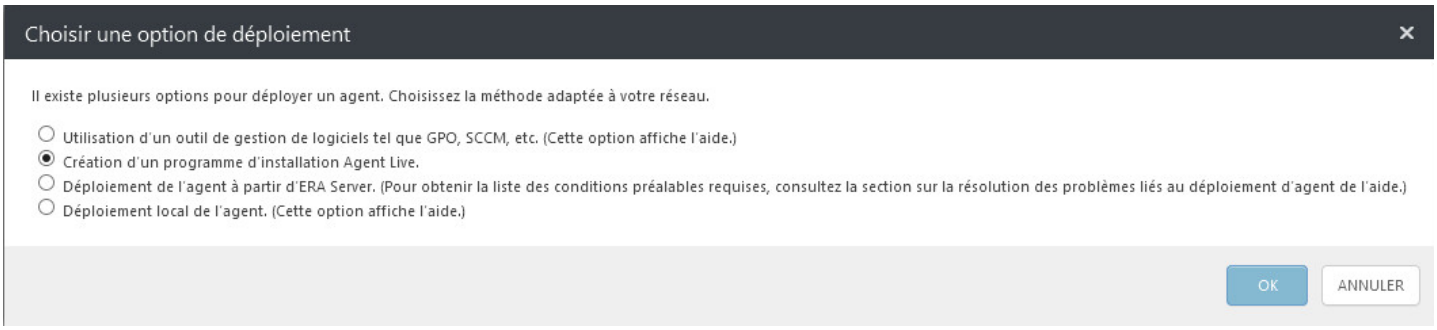


- Cliquez sur + **Ajouter** pour ajouter d'autres ordinateurs. Vous pouvez également cliquer sur **Importer** pour charger un fichier `.csv` qui contient la liste des ordinateurs à ajouter. Vous pouvez éventuellement saisir une **description** des ordinateurs. Lorsque vous avez terminé vos modifications, cliquez sur **Ajouter**.

REMARQUE : l'ajout de plusieurs ordinateurs peut prendre plus de temps. Une recherche DNS inversée peut être effectuée.

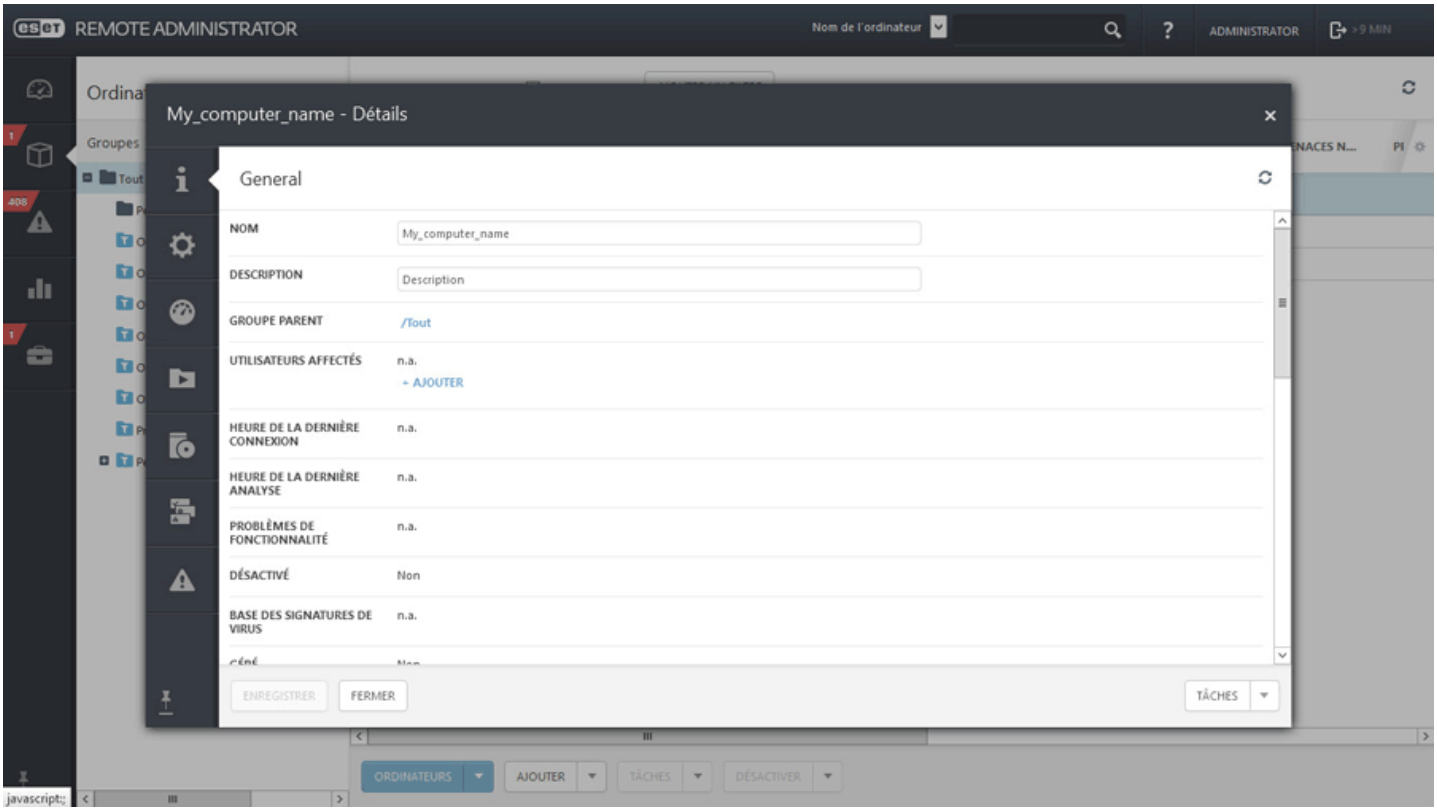
Les ordinateurs sont visibles dans la liste de droite lorsque vous sélectionnez le groupe auquel ils appartiennent. Une fois l'ordinateur ajouté, une fenêtre indépendante s'affiche avec l'option **Déployer l'agent**.

Choisissez le type de déploiement à utiliser parmi les options disponibles :



2.9.2 Détails de l'ordinateur

Sélectionnez un ordinateur dans un groupe dynamique ou statique, puis cliquez sur **Détails** pour afficher des informations supplémentaires sur celui-ci.



Le menu Détails de l'ordinateur contient les paramètres suivants :

- **General :** permet de modifier le nom, la description et le groupe parent de l'ordinateur.
- **Configuration :** affiche la configuration, la connexion et les stratégies appliquées pour cet ordinateur.
- **SysInspector** : affiche le journal/la sortie. Vous devez exécuter la tâche client Demander un rapport SysInspecto pour afficher la sortie.
- **Exécutions de tâche -** Survenance, Nom de la tâche, Type de tâche, État
- **Applications installées :** Nom, Version, Taille L'agent prend en charge la désinstallation, etc.
- **Alertes** : Problème, État, Gravité, Produit, etc.
- **Menaces et quarantaine -** Tous les types de menace, Ordinateur désactivé, Menace résolue, Cause, Nom de la menace, Type, Nom de l'objet, Hachage, etc.

Actions du bouton Tâches

Après avoir sélectionné un ordinateur ou un ensemble d'ordinateurs et cliqué sur Tâches, les options suivantes sont disponibles :

Analyser
Cette option permet d'exécuter la tâche Analyse à la demande sur le client qui a signalé la menace.

Mettre à jour la base des virus
Cette option permet d'exécuter la tâche Mise à jour de la base des signatures de virus (déclenche manuellement une mise à jour).

Mobile

- **Inscrire...** : à l'aide de cette option, vous pouvez créer une tâche de client.
- **Rechercher** : utilisez cette option si vous souhaitez obtenir les coordonnées GPS de votre périphérique.
- **Verrouiller** : le périphérique est verrouillé lorsqu'une activité suspecte est détectée ou que le périphérique est signalé comme manquant.
- **Déverrouiller** : le périphérique est déverrouillé.
- **Sirène** : déclenche à distance une sirène sonore. Celle-ci est déclenchée même si le périphérique est défini sur muet.
- **Effacer** : toutes les données stockées sur votre périphérique sont effacées de manière définitive.

Redémarrer

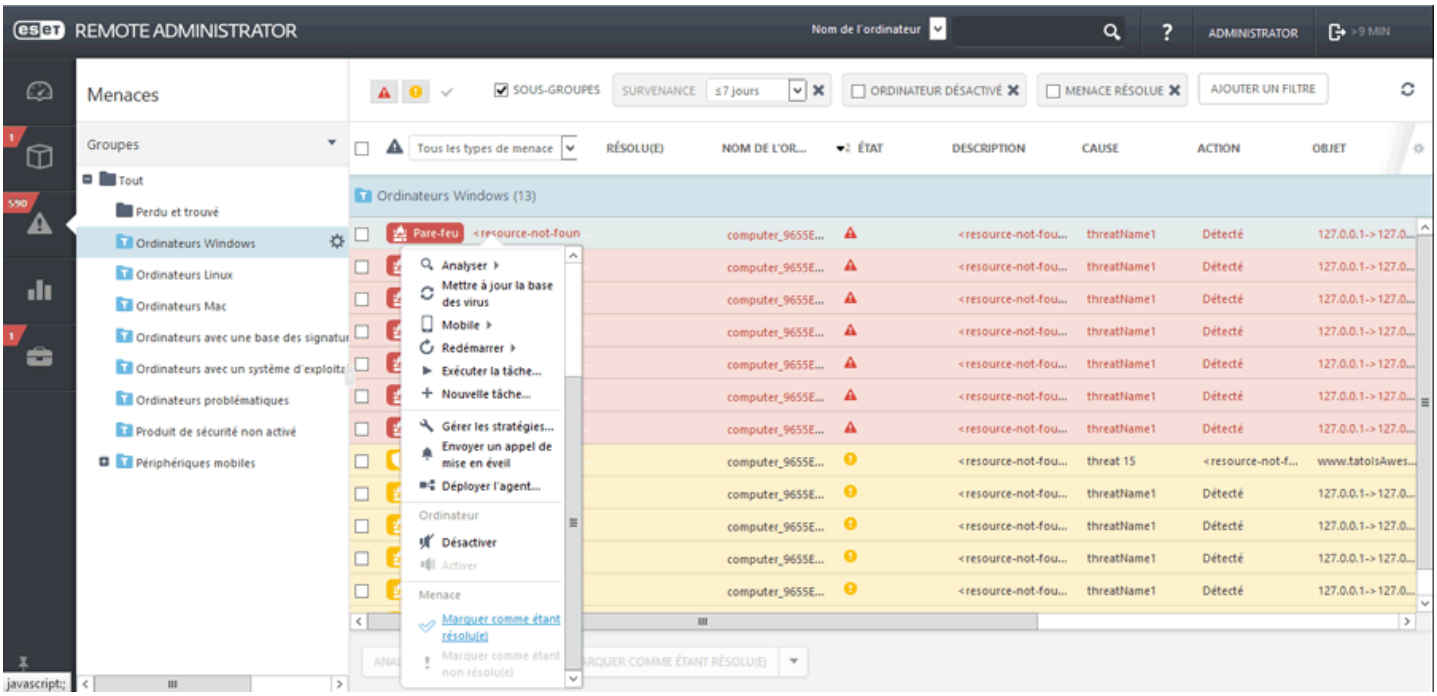
Si vous sélectionnez un ordinateur et appuyez sur **Redémarrer** ou **Arrêter**, le périphérique sera redémarré ou arrêté.

Nouvelle tâche...

Sélectionnez une tâche et configurez la limitation (facultatif) de cette dernière. La tâche est alors mise en file d'attente selon les paramètres de celle-ci.
Cette option déclenche immédiatement une tâche répertoriée dans la liste de tâches disponibles. Comme cette tâche est exécutée immédiatement, elle n'est associée à aucun déclencheur.

2.10 Menaces

La section **Menaces** vous donne une vue d'ensemble de toutes les menaces détectées sur les ordinateurs de votre réseau. La structure de groupes est affichée à gauche. Vous pouvez y parcourir les groupes et afficher les menaces détectées sur les membres d'un groupe donné. Sélectionnez le groupe **Tous** et utilisez le filtre **Tous les types de menace** pour afficher toutes les menaces détectées sur les clients de tous les groupes.



Filtrage des menaces

Par défaut, tous les types de menaces des 7 derniers jours sont affichés. Pour ajouter plusieurs critères de filtrage, cliquez sur **Ajouter un filtre**, puis sélectionnez un élément dans la liste. Vous pouvez filtrer les résultats par **Ordinateur désactivé, Menace résolue, Nom** (nom de la menace), par **Cause** (cause de la menace) ou selon l'adresse **IPv4/IPv6** du client qui a signalé cette menace. Par défaut, tous les types de menaces sont affichés. Vous pouvez toutefois appliquer un filtre par menaces **virales, liées au pare-feu** et au système **HIPS** pour obtenir une vue plus spécifique.

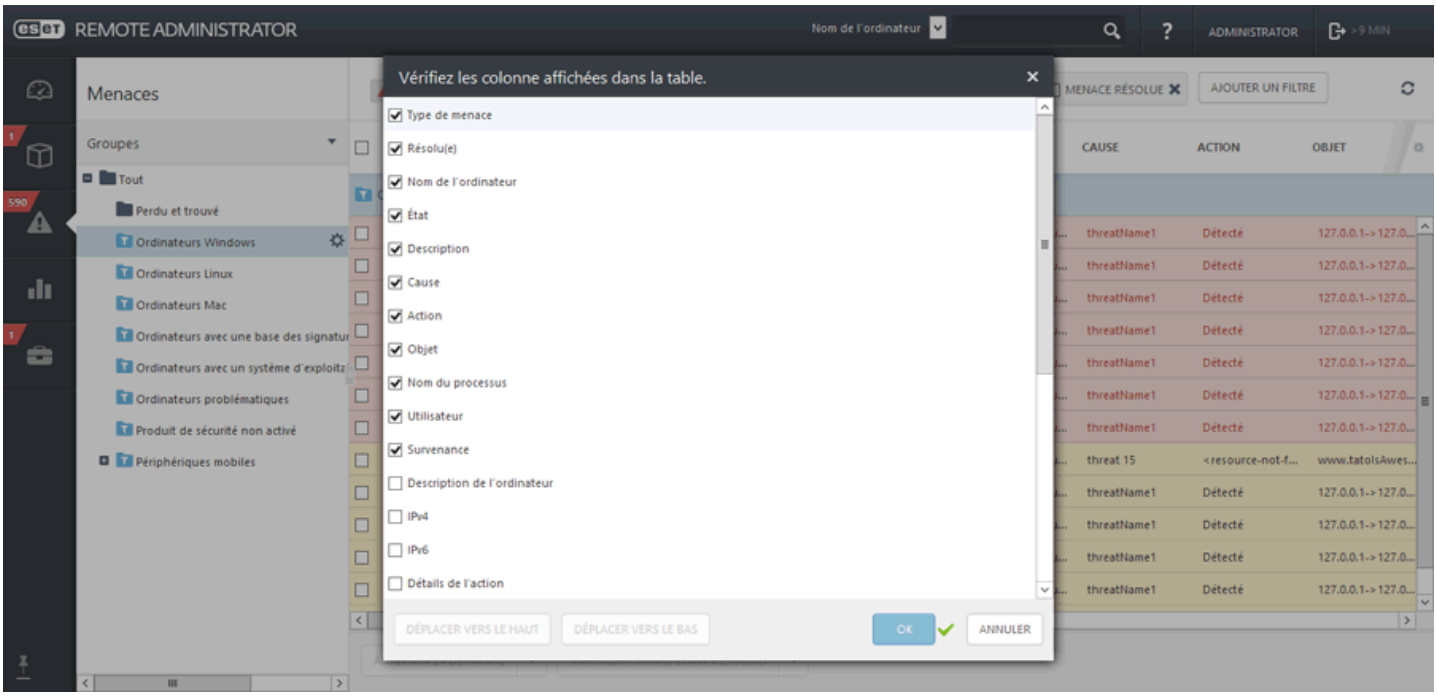
Analyse à la demande

Cette option permet d'exécuter la tâche Analyse à la demande sur le client qui a signalé la menace.

Marquer comme étant résolu(e)/Marquer comme étant non résolu(e)
Les menaces peuvent désormais être marquées comme étant résolues dans la section Menaces ou sous les détails d'un client spécifique.

Désactiver
Lorsque vous sélectionnez Désactiver pour une menace spécifique, cette menace est désactivée (et non le client). Ce rapport ne sera plus affiché comme étant actif. Vous pouvez également choisir de désactiver le client (sélectionnez **Désactiver** dans le menu déroulant de la menace) qui a signalé cette menace.

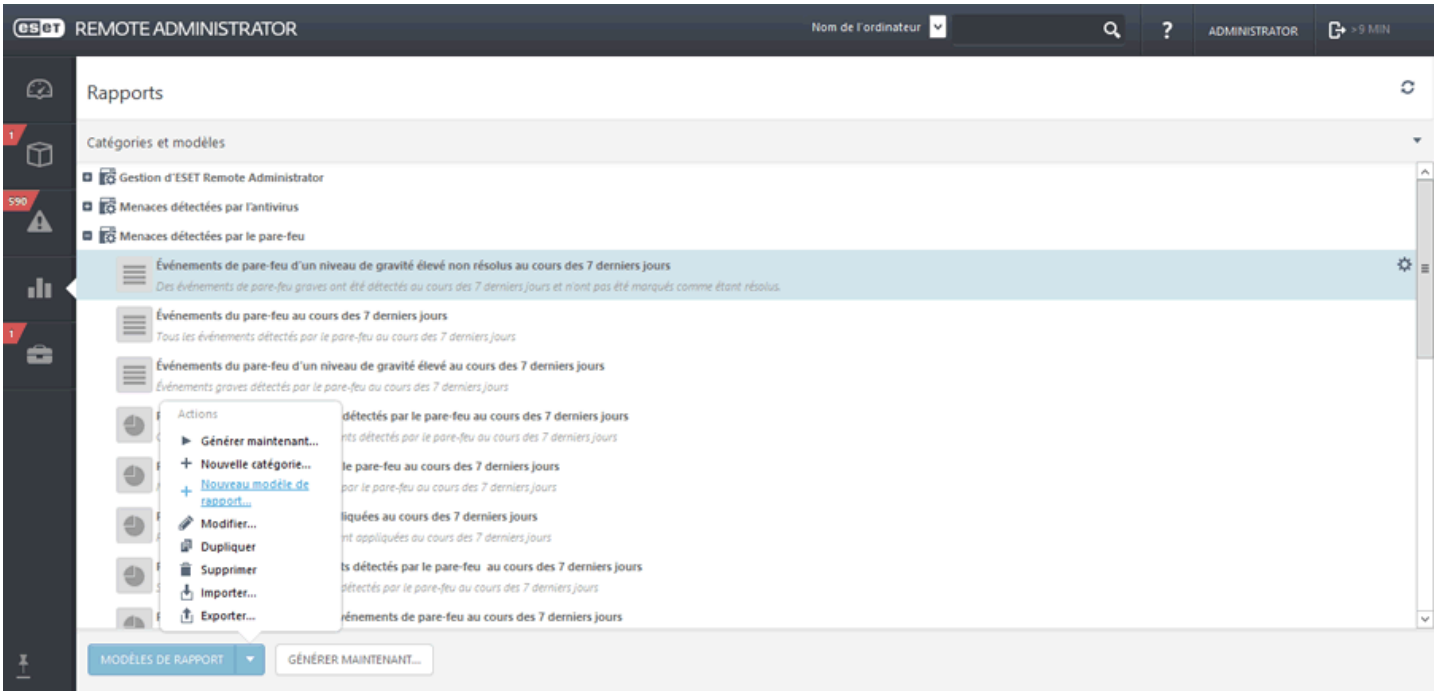
Colonnes de table :
Résolu, Objet, Nom du processus, Description, Utilisateur, Description de l'ordinateur, Détails de l'action, Redémarrage requis, Analyseur, Type d'objet, Circonstances, Nombre d'occurrences, Adresse source, Port source, Adresse cible, etc.



2.11 Rapports

Les rapports permettent d'accéder de manière efficace aux données de la base de données et de les filtrer. Les rapports sont classés dans des catégories. Chaque catégorie contient une brève description du rapport. Cliquez sur **Générer maintenant** dans la partie inférieure de la page pour créer un rapport basé sur un modèle sélectionné et l'afficher.

Vous pouvez utiliser des modèles de rapport prédéfinis de la liste **Catégories et modèles** ou créer un modèle de rapport avec des paramètres personnalisés. Cliquez sur Créer un modèle de rapport pour afficher en détail les paramètres de chaque rapport et spécifier des paramètres personnalisés pour un nouveau rapport.



Lorsque vous sélectionnez un rapport, le menu contextuel **Actions** s'affiche après avoir cliqué sur **Modèles de rapport** dans la partie inférieure de la page. Les options disponibles sont les suivantes :

Générer maintenant...
Sélectionnez un rapport dans la liste, puis accédez à **Modèles de rapport** > **Générer maintenant...** ou cliquez sur **Générer maintenant...**. Le rapport est alors généré et vous pouvez examiner les données de sortie.

Nouvelle catégorie...
Saisissez un **nom** et une **description** pour créer une catégorie de modèles de rapport.

Nouveau modèle de rapport...
Créez un modèle de rapport personnalisé.

Modifier...
Modifiez un modèle de rapport existant. Les mêmes paramètres et options que ceux utilisés lors de la création d'un modèle de rapport s'appliquent.

Dupliquer
Cette option permet de créer un nouveau rapport selon le rapport sélectionné. Un nouveau nom est requis pour le rapport en double.

Supprimer
Supprime entièrement le modèle de rapport sélectionné.

Importer...
Sélectionnez un modèle de rapport dans la liste, cliquez sur **Modèles de rapport** > **Importer**, puis sur **Sélectionner un fichier**, et recherchez le fichier à **importer**.

Exporter...
Sélectionnez le ou les modèles de rapport à exporter à partir de la liste, puis cliquez sur **Modèles de rapport** > **Exporter.** Le ou les modèles de rapport seront exportés dans un fichier *.dat*. Pour exporter plusieurs modèles de rapport, changez le mode de sélection, voir les **Modes** ci-dessous. Vous pouvez également exporter toute la catégorie Modèle en englobant tous les modèles de rapport.

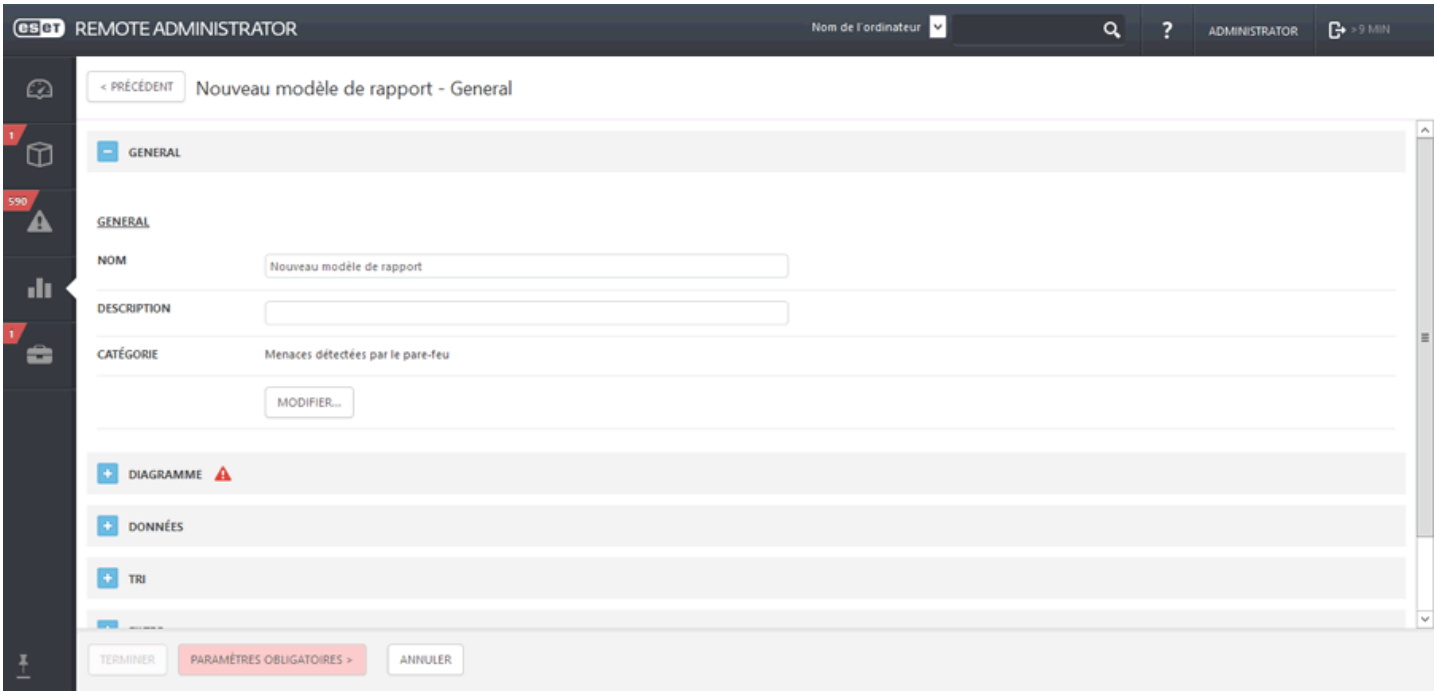
Vous pouvez utiliser l'option **Modes** pour modifier le mode de sélection (unique ou multiple). Cliquez sur la flèche dans le coin supérieur droit et sélectionnez l'une des options suivantes dans le menu contextuel :
Mode de sélection unique : vous pouvez sélectionner un seul élément.
Mode de sélection multiple : permet d'utiliser les cases à cocher pour sélectionner plusieurs éléments.
Rafraîchir : recharge/actualise les informations affichées.

REMARQUE : La fonctionnalité **Exporter...** exporte le ou les modèles de rapport sélectionnés, qui peuvent ensuite être importés sur un autre ERA Server à l'aide de **Importer**. Cela s'avère pratique, par exemple, lorsque vous souhaitez migrer vos modèles de rapport personnalisés sur un autre ERA Server.

IMPORTANT : La fonctionnalité **Importer** / **Exporter** est conçue pour l'importation et l'exportation de modèles de rapport uniquement, et non d'un rapport généré contenant des données.

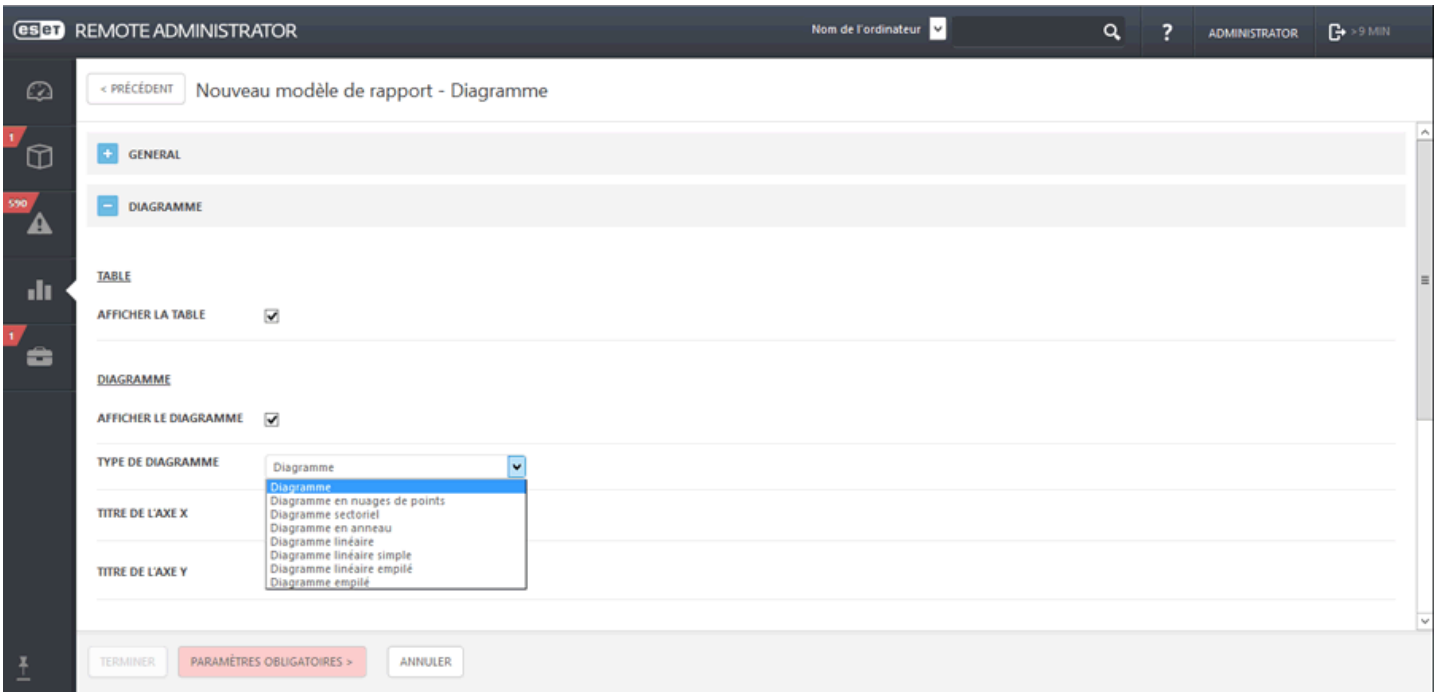
2.11.1 Créer un modèle de rapport

Accédez à **Rapports**, puis cliquez sur **Modèles de rapport** sous **Catégories et modèles** à gauche. Dans la fenêtre indépendante, sélectionnez **Nouveau modèles de rapport...**.



General

Modifiez les informations de base sur le modèle. Saisissez un **nom**, une **description** et une **catégorie**. Il peut s'agir d'une catégorie prédéfinie ou d'une catégorie que vous créez (utilisez l'option Nouvelle catégorie décrite dans le chapitre précédent).



Diagramme

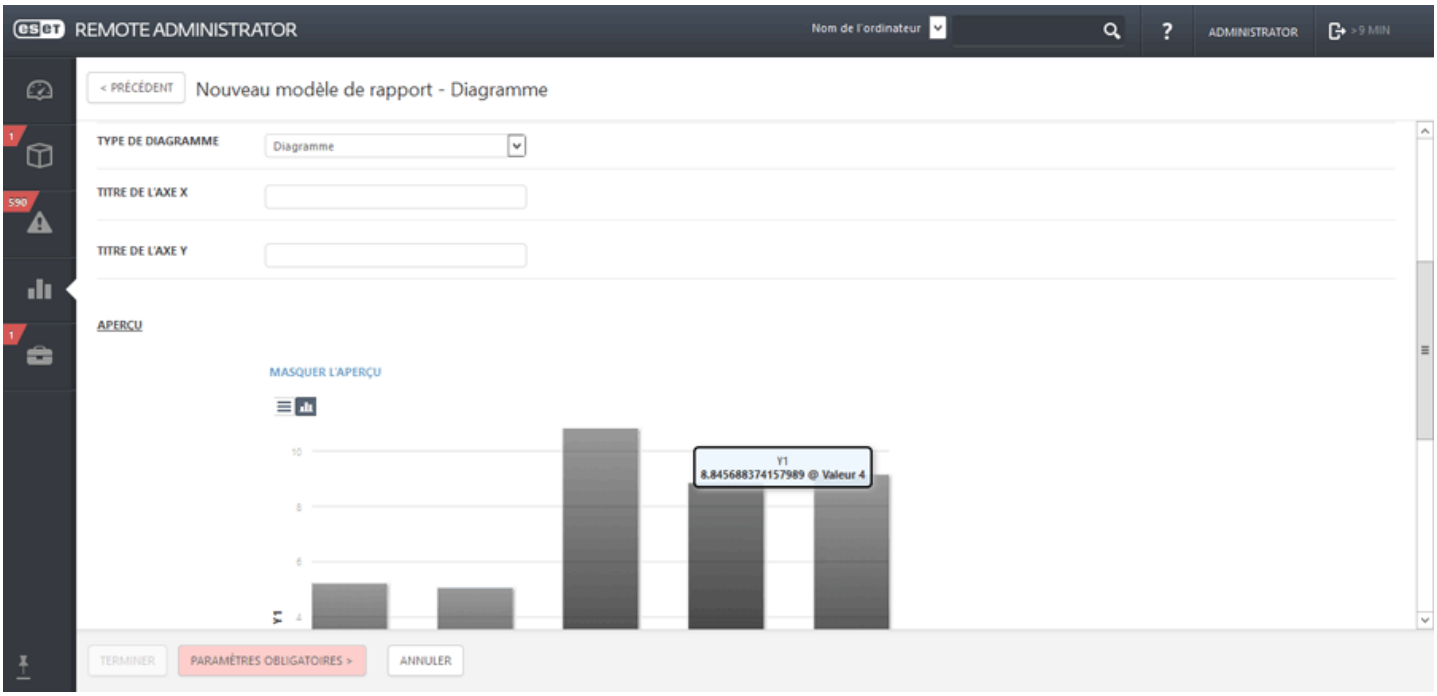
Dans la section **Diagramme**, sélectionnez le type de **rapport**. Il peut s'agir d'une **table**, dans laquelle les informations sont triées dans des lignes et des colonnes, ou d'un **diagramme** qui représente les données à l'aide d'axes X et Y.

REMARQUE : le type de diagramme sélectionné s'affiche dans la section **Aperçu**. Vous pouvez ainsi déterminer l'aspect du rapport en temps réel.

Lorsque vous sélectionnez un **diagramme**, vous avez plusieurs options :

- **Diagramme** : diagramme avec des barres rectangulaires proportionnelles aux valeurs qu'elles représentent.
- **Diagramme en nuages de points** : dans ce diagramme, des points sont utilisés pour afficher des valeurs quantitatives (similaire à un diagramme).
- **Diagramme sectoriel** : il s'agit d'un diagramme circulaire divisé en secteurs proportionnels représentant des valeurs.
- **Diagramme en anneau** : similaire à un diagramme sectoriel, il contient toutefois plusieurs types de données.
- **Diagramme linéaire** : affiche les informations sous la forme d'une série de points de données reliés par des segments de ligne droite.
- **Diagramme linéaire simple** : affiche les informations sous la forme d'une ligne reposant sur les valeurs sans points de données visibles.
- **Diagramme linéaire empilé** : ce type de diagramme est utilisé pour analyser des données avec des unités de mesure différentes.
- **Diagramme empilé** : similaire à un diagramme simple, il contient toutefois plusieurs types de données avec des unités de mesure différentes représentées par des barres empilées.

Vous pouvez éventuellement saisir un titre pour les axes **X** et **Y** du diagramme pour en faciliter la lecture et détecter des tendances.



Données

Dans la section **Données**, sélectionnez les informations à afficher :

a. **Colonnes de table** : les informations de la table sont automatiquement ajoutées en fonction du type de rapport sélectionné. Vous pouvez personnaliser le **nom**, l'**étiquette** et le **format** (voir ci-dessus).

b. **Axes de diagramme** : sélectionnez les données pour les axes **X** et **Y**. Lorsque vous cliquez sur l'un des symboles, la fenêtre correspondante s'affiche pour proposer des options. Les options disponibles pour l'axe **Y** dépendent toujours des informations sélectionnées pour l'axe **X**, et inversement. Comme le diagramme affiche leur relation, les données doivent être compatibles. Sélectionnez les informations souhaitées, puis cliquez sur **OK**.

Vous pouvez remplacer le **format** sous lequel les données s'affichent par l'un des formats suivants :

- **Barre de données** (uniquement pour les diagrammes) / **Valeur** / **Couleur** / **Icônes**

Tri

Utilisez l'option **Ajouter un tri** pour définir la relation entre les données sélectionnées. Sélectionnez les informations de début (valeur de tri) et la méthode de tri (**Croissant** ou **Décroissant**. Ces options définissent le résultat affiché dans le diagramme.

Filtre

Définissez ensuite la méthode de filtrage. Dans la liste, sélectionnez la valeur de filtrage et sa valeur. Les informations affichées dans le diagramme sont ainsi définies.

Résumé

Dans la section **Résumé**, passez en revue les options sélectionnées et les informations. Si elles vous conviennent, cliquez sur **Terminer** pour créer un modèle de rapport.

Dans le tableau de bord, chaque rapport dispose d'options de personnalisation. Pour les afficher, cliquez sur le symbole de roue situé dans le coin supérieur droit. Vous pouvez **rafraîchir** les informations affichées, **remplacer** le rapport par un autre, **modifier** le modèle de rapport (voir les options ci-dessus), définir un nouvel intervalle de **rafraîchissement** qui définit la fréquence d'actualisation des données du rapport ou **renommer/supprimer** le rapport. À l'aide des flèches dans le symbole ci-dessous, vous pouvez personnaliser la taille du rapport. Vous pouvez agrandir les rapports les plus pertinents et rendre plus petits les rapports les moins pertinents. Cliquez sur **Basculer le mode plein écran** pour afficher un rapport en mode plein écran.

2.11.2 Générer un rapport

Deux méthodes permettent de créer ou modifier un modèle :

1. Accédez à **Admin** > **Tâches** > **Tâches serveur**. Sélectionnez **Nouveau...** pour créer une tâche Générer un rapport.
2. Sélectionnez un modèle de rapport à partir duquel générer un rapport. Vous pouvez utiliser un modèle de rapport prédéfini et le **modifier** ou créer un modèle de rapport.

- Vous pouvez envoyer ce rapport par courrier électronique (dans un format de fichier défini dans cette section) ou l'enregistrer directement dans un fichier. Lorsque vous cliquez sur l'une des options, les paramètres correspondants s'affichent.
- Configurez les paramètres (comme décrit dans la tâche Générer un rapport), puis cliquez sur **Terminer**.
- La tâche est créée et affichée dans la liste **Types de tâche**. Sélectionnez la tâche et cliquez sur **Exécuter maintenant** dans la partie inférieure de la page. La tâche est immédiatement exécutée.
- Vous pouvez utiliser **Enregistrer** ou **Actualiser** générer un rapport.

2.11.3 Planifier un rapport

1. Accédez à **Admin** > **Tâches** > **Tâches serveur**. Sélectionnez **Nouveau** pour créer une tâche **Générer un rapport**.
2. Sélectionnez un modèle de rapport à partir duquel générer un rapport. Vous pouvez utiliser un modèle de rapport prédéfini et le modifier ou créer un modèle de rapport.

- Vous pouvez envoyer ce rapport par courrier électronique (dans un format de fichier défini dans cette section) ou l'enregistrer dans un fichier. Lorsque vous cliquez sur l'une des options, les paramètres correspondants s'affichent.
- Configurez les paramètres (comme décrit dans la tâche Générer un rapport). Cette fois, un **déclencheur de serveur** est créé pour la tâche.
- Dans la section **Déclencheur**, accédez à **Paramètres**. Sélectionnez **Déclencheur planifié** et la date/heure d'exécution de la tâche.
- Cliquez sur **Terminer**. La tâche est créée. Elle s'exécutera à la période (une fois ou de manière répétée) définie ici.

2.11.4 Applications obsolètes

Pour déterminer quels sont les composants ERA qui ne sont pas à jour, utilisez le rapport appelé **Applications obsolètes**.

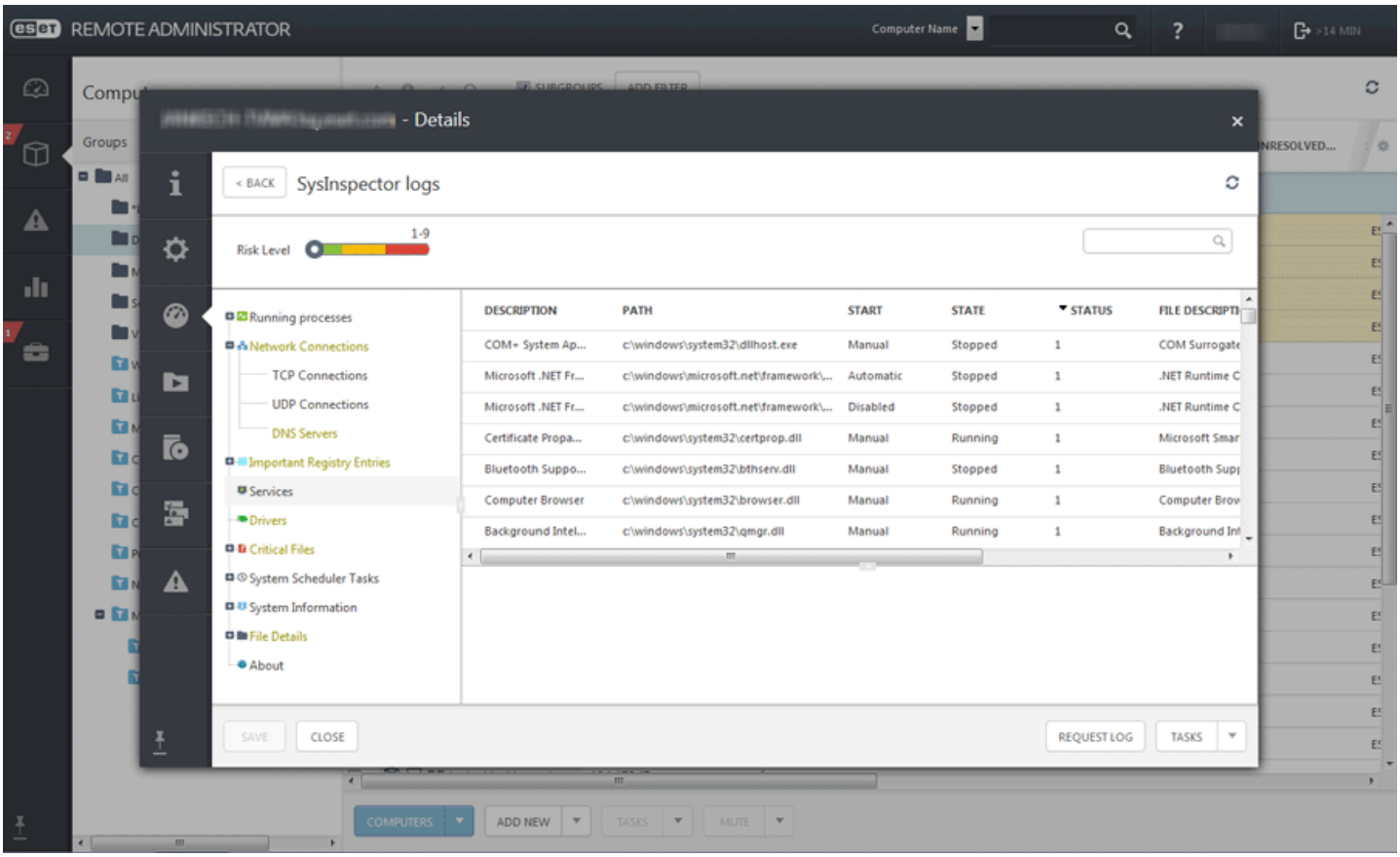
Vous pouvez procéder de deux manières différentes :

1. Ajoutez un nouveau tableau de bord, puis cliquez sur l'une des mosaïques pour afficher un écran indépendant répertoriant la liste des **modèles de rapport**. Sélectionnez le rapport **Applications obsolètes** dans la liste, puis cliquez sur **Ajouter**.
2. Accédez à **Rapports**, puis à la catégorie **Ordinateurs**. Sélectionnez le modèle **Applications obsolètes** dans la liste, puis cliquez sur le bouton **Générer maintenant...** situé dans la partie inférieure. Le rapport est alors généré et vous pouvez examiner les données de sortie.

Pour mettre les composants à niveau, utilisez la tâche de client Mettre à jour les composants d'ESET Remote Administrator.

2.11.5 Visionneuse des journaux SysInspector

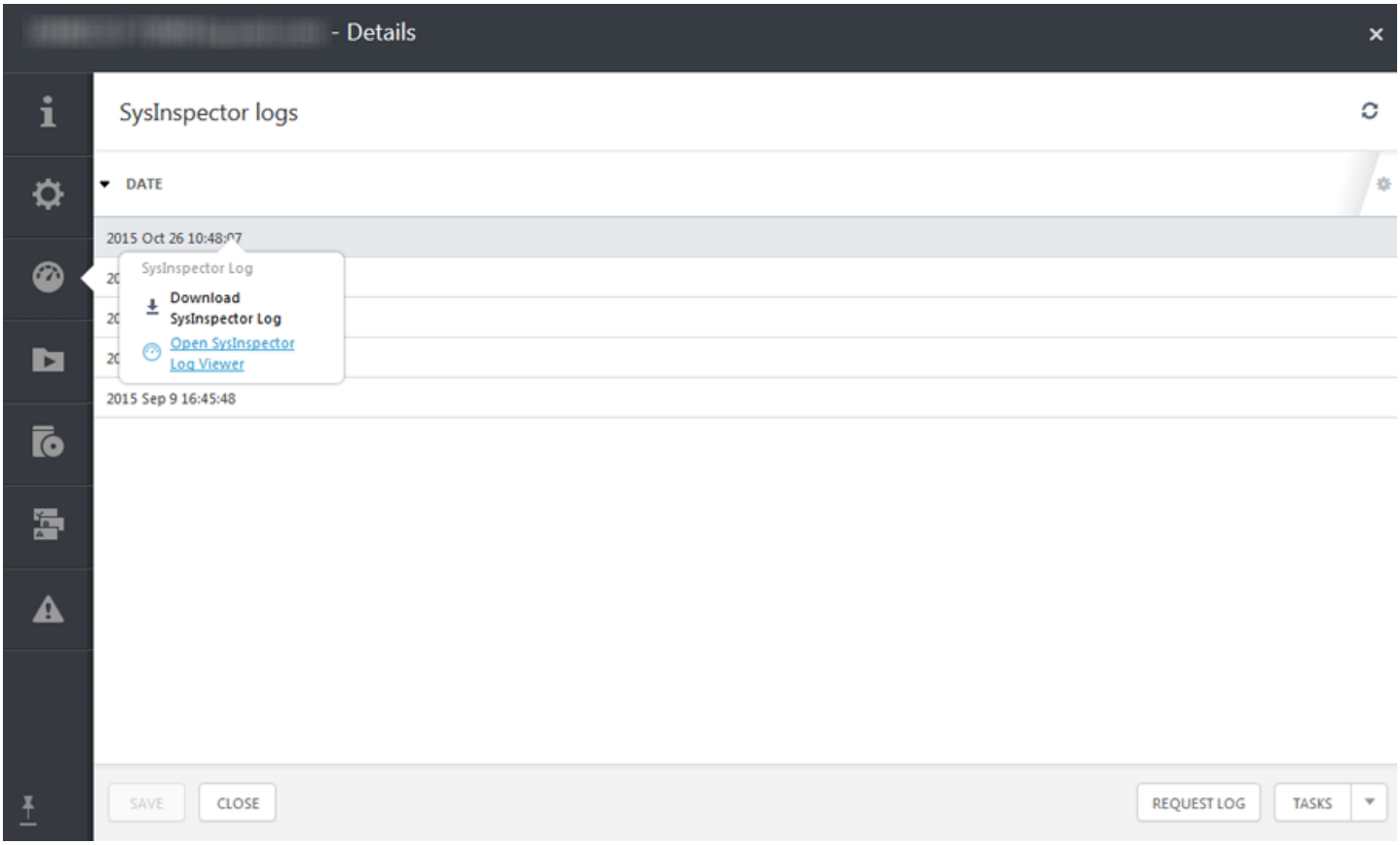
La visionneuse des journaux SysInspector permet de consulter les journaux de SysInspector après son exécution sur un ordinateur client. Vous pouvez également ouvrir les journaux SysInspector directement à partir d'une tâche de demande de rapport SysInspector après la réussite de son exécution.



Pour ce faire, procédez comme suit :

1. Ajoutez un nouveau tableau de bord, puis cliquez sur l'une des mosaïques pour afficher un écran indépendant répertoriant la liste des **modèles de rapport**.
2. Accédez à Rapports, accédez à la catégorie **Automatisation**, sélectionnez le modèle **Historique des rapports SysInspector au cours des 30 derniers jours** dans la liste et **Générer maintenant...** Le rapport est alors généré et vous pouvez examiner les données de sortie.

3. Sélectionnez un ordinateur dans un groupe dynamique ou statique, puis cliquez sur **Détails**, cliquez sur l'onglet SysInspector et sélectionnez **Ouvrir la visionneuse des journaux SysInspector**.



3. Mobile Device Management

Pour profiter de la fonctionnalité Mobile Device Management feature dans ESET Remote Administrator, respectez les étapes suivantes pour installer, inscrire, configurer et appliquer des stratégies.

1. Installez **Mobile Device Connector** (MDC) à l'aide du programme d'installation tout en un ou de l'installation de composants pour Windows ou Linux. Veillez à remplir les conditions préalables requises avant l'installation.

REMARQUE : Si vous installez MDC à l'aide du programme d'installation tout en un, vous n'avez pas besoin de certificat HTTPS tiers. Si vous installez le composant MDC par lui-même, vous aurez besoin d'une chaîne de certificats HTTPS tiers. Si vous voulez installer ERA avec le programme d'installation tout en un et utiliser un certificat HTTPS tiers, installez ESET Remote Administrator d'abord, puis remplacez votre certificat HTTPS à l'aide de Stratégie (dans la section **Général**, cliquez sur **Modifier le certificat** > **Certificat personnalisé**).

2. Activez ERA MDC à l'aide d'une tâche client Activation de produit. La procédure est la même que lors de l'activation d'un produit de sécurité ESET sur un ordinateur client (aucune unité de licence ne sera utilisée).

REMARQUE : Si vous ne comptez gérer que des périphériques Android (aucun périphérique iOS), vous pouvez passer à l'étape 6.

3. Exécutez une tâche serveur Synchronisation utilisateur (recommandé). Cela vous permet de synchroniser automatiquement des utilisateurs avec Active Directory ou LDAP pour la Gestion des utilisateurs.
4. Créez un certificat APN. Ce certificat est utilisé par ERA MDM pour l'inscription de périphériques iOS.
5. Créez une stratégie pour le Connecteur de périphérique mobile ESET afin d'activer APNS.
6. Inscrivez les périphériques mobiles à l'aide d'une tâche client Inscription de périphérique. Configurez la tâche pour inscrire des périphériques pour Android ou iOS. Cela peut également être effectué à partir des Groupes en cliquant sur **Ajouter** > **Périphériques mobiles**.
7. Activez les périphériques mobiles à l'aide d'une tâche client Activation de produit : utilisez une licence ESET Endpoint Security. Une unité de licence sera utilisée pour chaque périphérique mobile.
8. Vous pouvez modifier les utilisateurs afin de configurer des attributs personnalisés et d'attribuer un ou plusieurs périphériques mobiles.
9. Vous pouvez alors commencer à appliquer des stratégies et à gérer des périphériques mobiles. Par exemple, vous pouvez Créer une stratégie pour MDM iOS - Compte Exchange ActiveSync qui configurera automatiquement un compte Mail, les Contacts et le Calendrier sur les périphériques iOS. Vous pouvez également appliquer des restrictions sur un périphérique iOS et/ou ajouter une connexion Wi-Fi.

3.1 Profil de configuration MDM

Vous pouvez configurer le profil pour imposer des stratégies et des restrictions sur le périphérique mobile géré.

Nom du profil	Brève description
Code secret	Impose aux utilisateurs finaux de protéger leurs périphériques à l'aide de codes secrets chaque fois qu'ils quittent l'état inactif. Cela garantit le maintien de la protection des informations confidentielles de l'entreprise sur les périphériques gérés. Si plusieurs profils définissent des codes secrets sur un même périphérique, c'est la stratégie la plus restrictive qui est appliquée.
Restrictions	Les profils de restriction limitent les fonctionnalités disponibles pour les utilisateurs de périphériques gérés en restreignant l'utilisation d'autorisations spécifiques liées aux fonctionnalités et aux applications du périphérique, à iCloud, à la sécurité et la confidentialité.
Liste des connexions Wi-Fi	Les profils Wi-Fi pousse des paramètres Wi-Fi de l'entreprise directement vers des périphériques gérés pour accès instantané.

Liste des connexions VPN	Les profile VPN poussent des paramètres de réseau privé virtuel de l'entreprise directement vers des périphériques gérés pour que les utilisateurs puissent accéder en toute sécurité à l'infrastructure de l'entreprise à partir de sites distants. **Nom de la connexion** : consultez le nom de la connexion affiché sur le périphérique. **Type de connexion** : choisissez le type de connexion activé par ce profil. Chaque type de connexion active différentes fonctionnalités. **Serveur** : saisissez le nom d'hôte ou l'adresse IP du serveur avec lequel la connexion est établie.
Comptes de messagerie	Permet à l'administrateur de configurer des comptes de messagerie IMAP/POP3.
Comptes Exchange ActiveSync	Les profils Exchange ActiveSync permettent aux utilisateurs finaux d'accéder à l'infrastructure de messagerie push de l'entreprise. Il convient de noter que quelques champs sont préremplis et des options qui ne s'appliquent qu'à iOS 5+ .
CalDAV - Comptes de calendrier	CalDAV offre des options de configuration permettant aux utilisateurs finaux d'effectuer une synchronisation sans fil avec le serveur CalDAV de l'entreprise.
CardDAV - Comptes de contacts	Cette section permet la configuration spécifique de services CardDAV.
Comptes de calendrier avec abonnement	Les calendriers avec abonnement permettent la configuration des calendriers.

4. Admin

La section **Admin** est le composant de configuration principal d'ESET Remote Administrator. Elle contient tous les outils qu'un administrateur peut utiliser pour gérer les solutions de sécurité des clients et les paramètres d'ERA Server. Vous pouvez utiliser les outils d'administration pour configurer votre environnement réseau de sorte qu'il nécessite peu de maintenance. Vous pouvez également configurer des notifications et des tableaux de bord qui vous maintiendront informé de l'état de votre réseau.

Contenu de cette section

4.1 Groupes

Les groupes vous permettent de gérer et classer les ordinateurs. Vous pouvez ensuite facilement appliquer des paramètres, des tâches ou des restrictions différentes aux ordinateurs clients en fonction de leur présence dans un groupe spécifique. Vous pouvez utiliser des modèles de groupe et des groupes prédéfinis ou en créer de nouveaux.

Il existe deux types de groupes de clients :

Groupes statiques

Les groupes statiques sont des groupes d'ordinateurs clients sélectionnés (membres). Les membres de ces groupes sont statiques et ne peuvent être ajoutés/supprimés que manuellement, et non selon des critères dynamiques. Un ordinateur ne peut figurer que dans un seul groupe statique.

Groupes dynamiques

Les groupes dynamiques sont des groupes de clients dont l'appartenance est déterminée par des critères spécifiques. Si un client ne répond pas à ces critères, il est supprimé du groupe. Les ordinateurs qui remplissent les critères sont automatiquement ajoutés au groupe.

La fenêtre **Groupes** est divisée en trois sections :

1. Une liste de tous les groupes et leurs sous-groupes est affichée à gauche. Vous pouvez sélectionner un groupe et une action pour celui-ci dans le menu contextuel ( situé en regard du nom du groupe). Les options disponibles sont identiques à celles décrites ci-dessous (actions du bouton Groupe).
2. Les informations détaillées sur le groupe sélectionné sont affichées dans le volet droit (vous pouvez passer d'un onglet à un autre) :

- **Ordinateurs** membres du groupe
- **Stratégies** attribuées à ce groupe
- **Tâches** attribuées à ce groupe
- **Résumé** de la description de base du groupe.

3. Les boutons de menu **Groupes** et **Ordinateurs** vous permettent d'effectuer toutes les actions suivantes :

Bouton Actions du groupe :

+ Nouveau groupe statique...
Cette option devient disponible lorsque vous cliquez sur un **groupe** dans la liste de gauche. Ce groupe devient le groupe parent par défaut, mais vous pouvez modifier ce dernier lorsque vous créez un groupe statique.

+ Nouveau groupe dynamique...
Cette option devient disponible lorsque vous cliquez sur un **groupe** dans la liste de gauche. Ce groupe devient le groupe parent par défaut, mais vous pouvez modifier ce dernier lorsque vous créez un groupe dynamique.

Modifier...
Cette option permet de modifier le groupe sélectionné. Les paramètres sont identiques à ceux de la création d'un groupe (statique or dynamique).

Déplacer...
Vous pouvez sélectionner un groupe et le déplacer comme sous-groupe d'un autre groupe.

Supprimer
Supprime entièrement le groupe sélectionné.

Importer...
Vous pouvez importer une liste (généralement un fichier texte) d'ordinateurs en tant que membres du groupe sélectionné. Si les ordinateurs existent déjà en tant que membres de ce groupe, le conflit est résolu selon l'action sélectionnée :

- **Ignorer les ordinateurs en conflit** (les ordinateurs en conflit ne sont pas ajoutés)
- **Déplacer les ordinateurs en conflit vers d'autres groupes** (les ordinateurs en conflit sont déplacés vers cet emplacement à partir d'autres groupes auxquels ils appartiennent)
- **Dupliquer les ordinateurs en conflit** (les ordinateurs en conflit sont ajoutés avec des noms différents).

Exporter...
Exportez les membres du groupe (et des sous-groupes, s'ils sont sélectionnés) dans une liste (fichier *.txt*). Cette liste peut être révisée ou importée ultérieurement.

+ Ajouter...
À l'aide de cette option, vous pouvez ajouter un nouveau périphérique.

Analyser
Cette option permet d'exécuter la tâche Analyse à la demande sur le client qui a signalé la menace.

Mettre à jour la base des virus
Cette option permet d'exécuter la tâche Mise à jour de la base des signatures de virus (déclenche manuellement une mise à jour).

Mobile

- **Inscrire...** : à l'aide de cette option, vous pouvez créer une tâche de client.
- **Rechercher** : utilisez cette option si vous souhaitez obtenir les coordonnées GPS de votre périphérique.
- **Verrouiller** : le périphérique est verrouillé lorsqu'une activité suspecte est détectée ou que le périphérique est signalé comme manquant.
- **Déverrouiller** : le périphérique est déverrouillé.
- **Sirène** : déclenche à distance une sirène sonore. Celle-ci est déclenchée même si le périphérique est défini sur muet.
- **Effacer** : toutes les données stockées sur votre périphérique sont effacées de manière définitive.

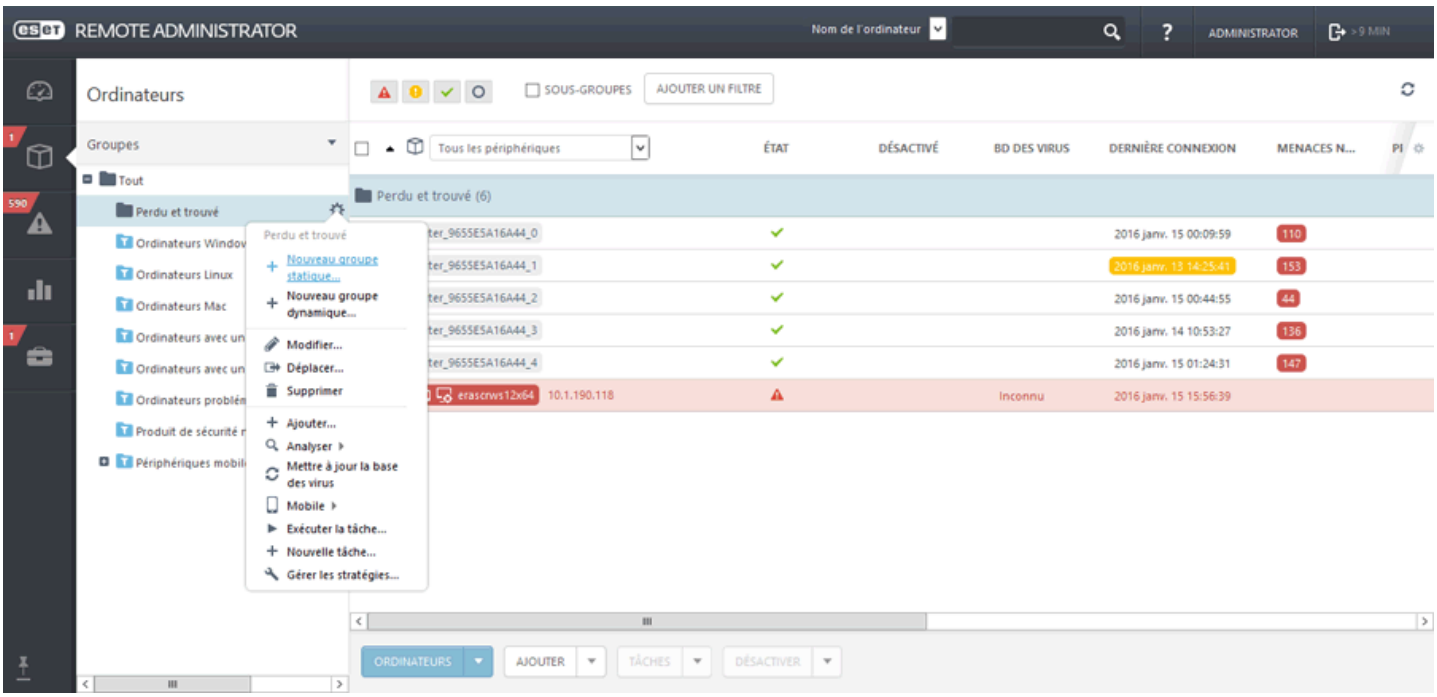
+ Nouvelle tâche...
Vous pouvez créer une tâche de client. Sélectionnez une tâche et configurez la limitation (facultatif) de cette dernière. La tâche est alors mise en file d'attente selon les paramètres de celle-ci.
Cette option déclenche immédiatement une tâche existante sélectionnée dans une liste de tâches disponibles. Comme cette tâche est exécutée immédiatement, elle n'est associée à aucun déclencheur.

Gérer les stratégies...
Attribuez une stratégie au groupe sélectionné.

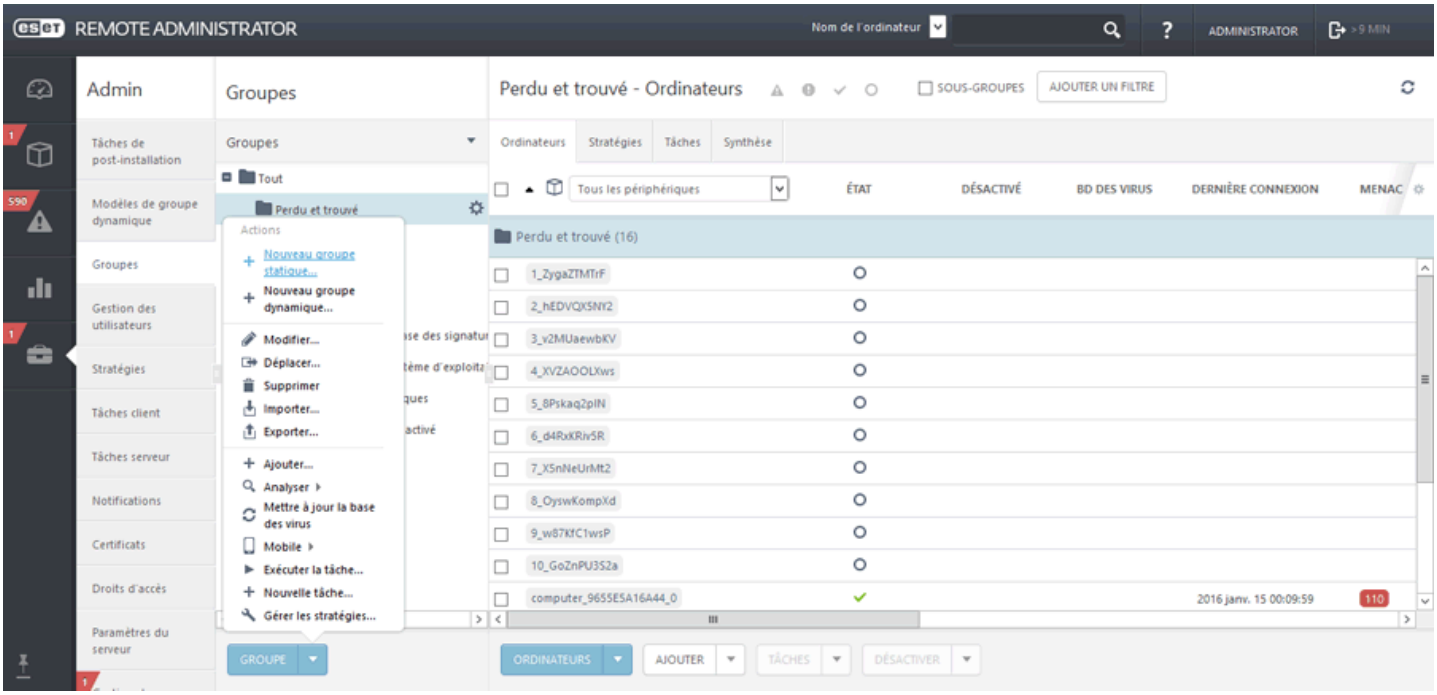
4.1.1 Créer un groupe statique

Trois méthodes permettent de créer un groupe statique :

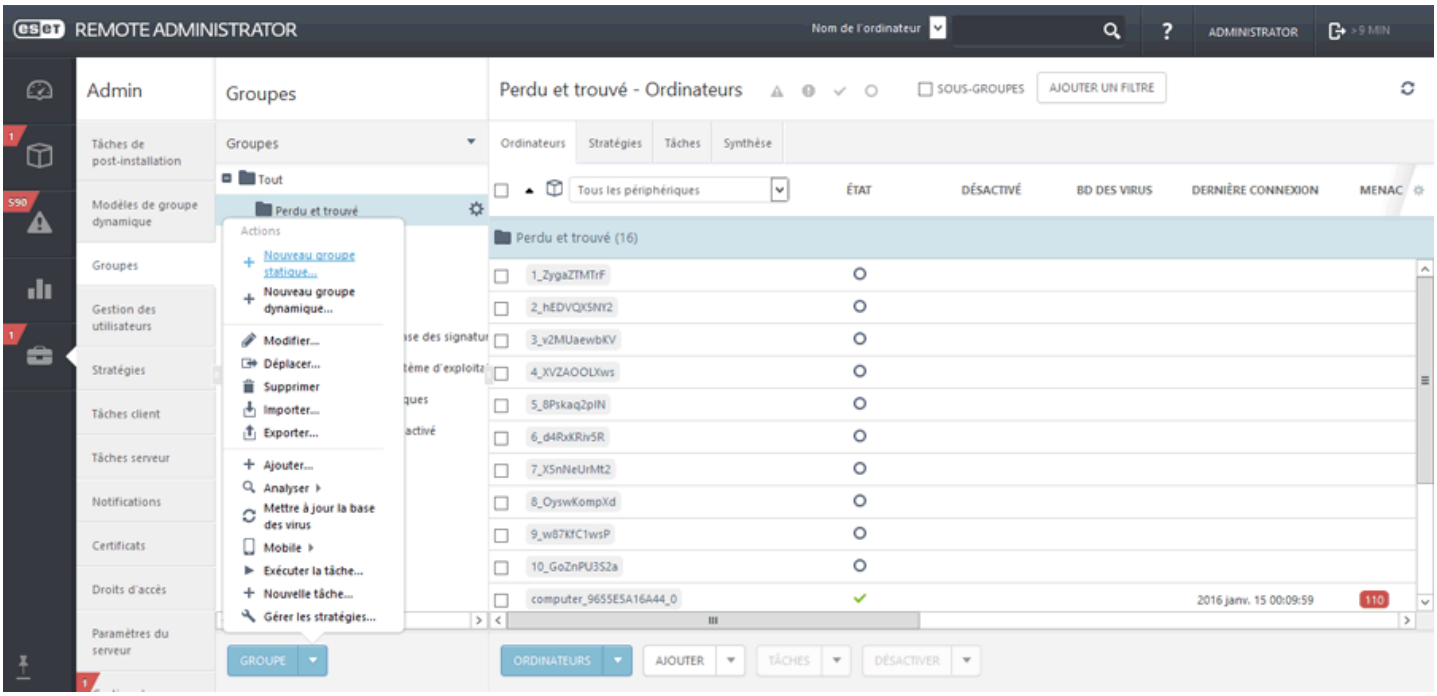
1. Cliquez sur **Ordinateurs** > **Groupes** > ⚙, puis sélectionnez **Nouveau groupe statique...**.



2. Cliquez sur **Admin** > **Groupes** > ⚙ > **Nouveau groupe statique...**.

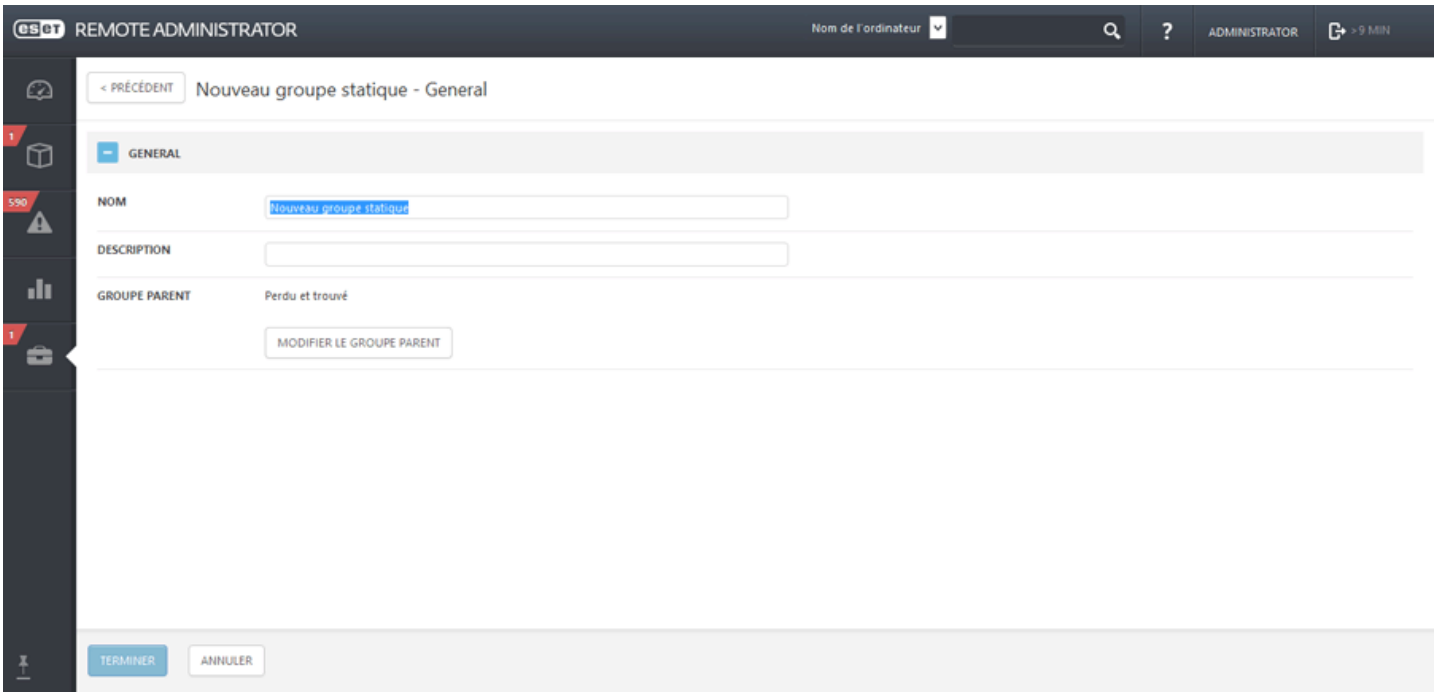


3. Cliquez sur **Admin** > **Groupes**, sélectionnez un groupe statique, puis cliquez sur **Groupe**.



General

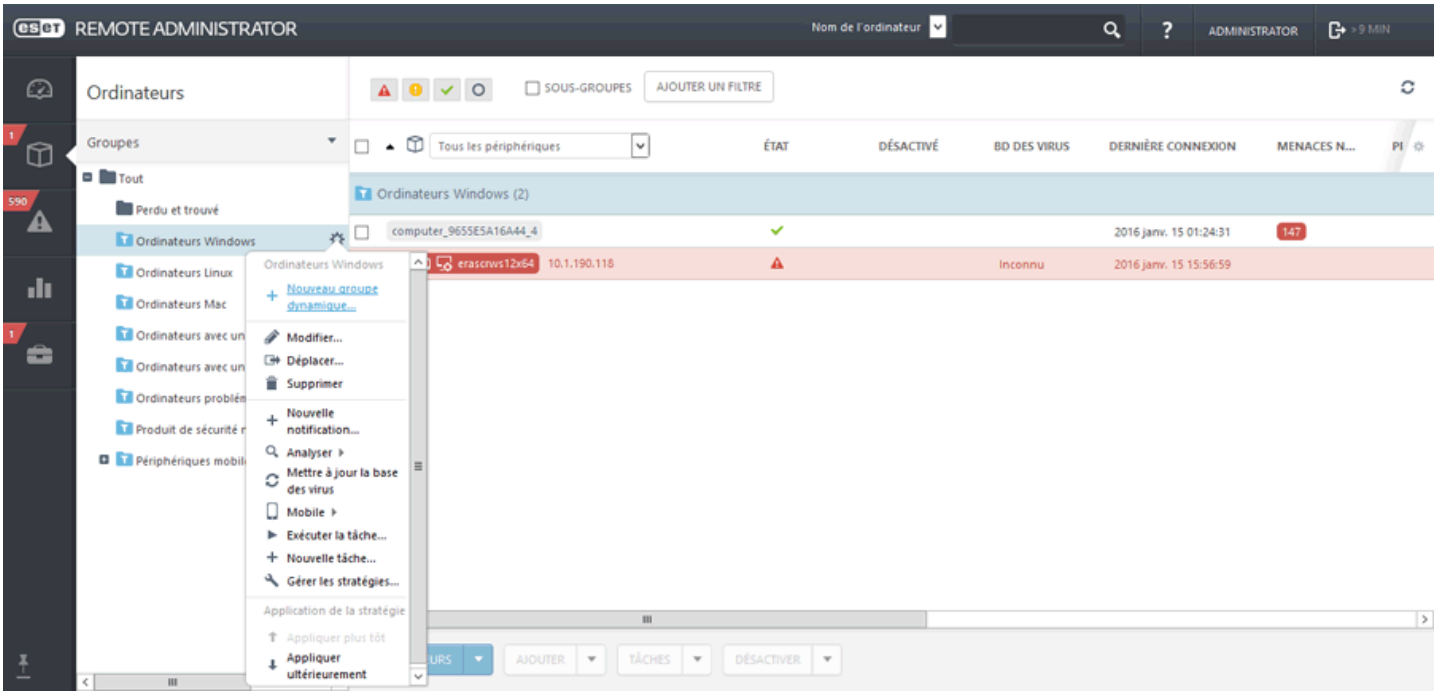
Saisissez un **nom** et une **description** (facultatif) pour le nouveau groupe statique. Par défaut, le groupe parent correspond au groupe que vous avez sélectionné lorsque vous avez commencé à créer le groupe statique. Si vous souhaitez modifier le groupe parent, cliquez sur **Modifier le groupe parent**, puis sélectionnez-en un autre dans l'arborescence. Le parent du nouveau groupe statique doit être un groupe statique, car un groupe dynamique ne peut pas comporter de groupes statiques. Cliquez sur **Terminer** pour créer le groupe statique.



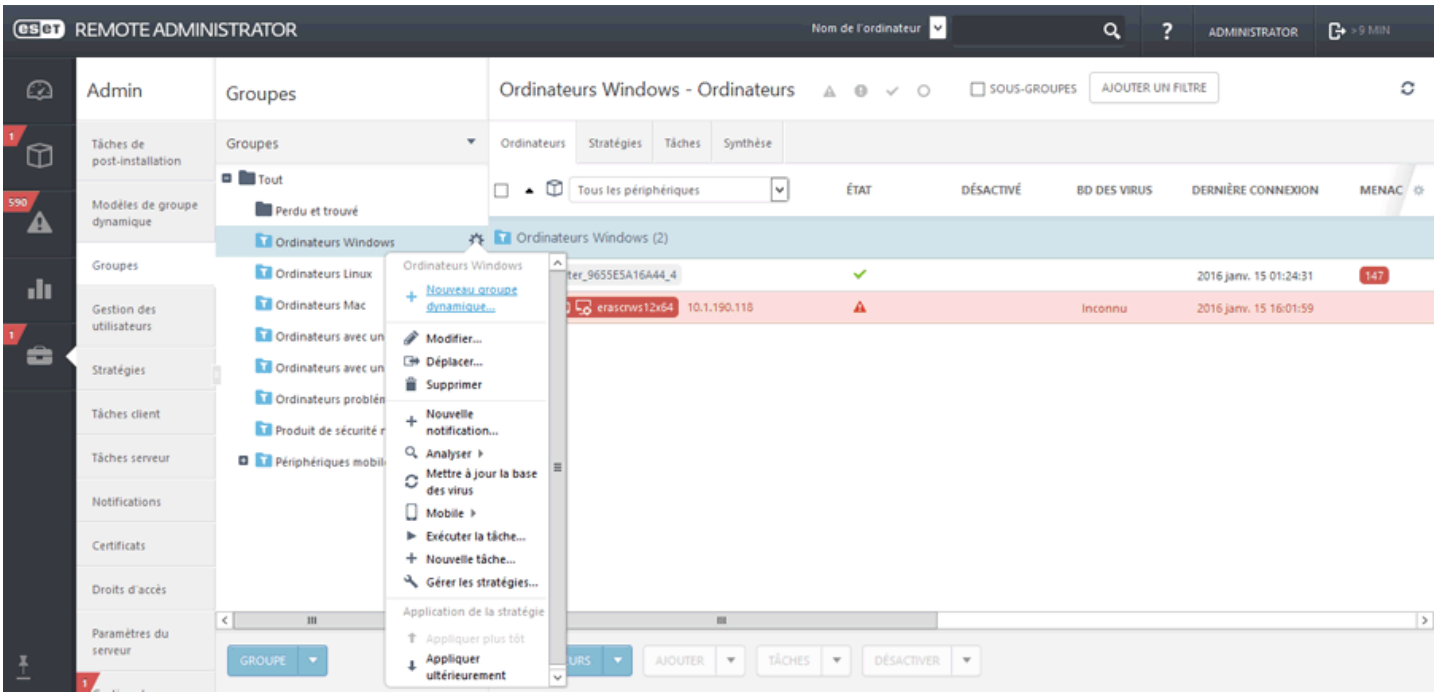
4.1.2 Créer un groupe dynamique

Trois méthodes permettent de créer un groupe dynamique :

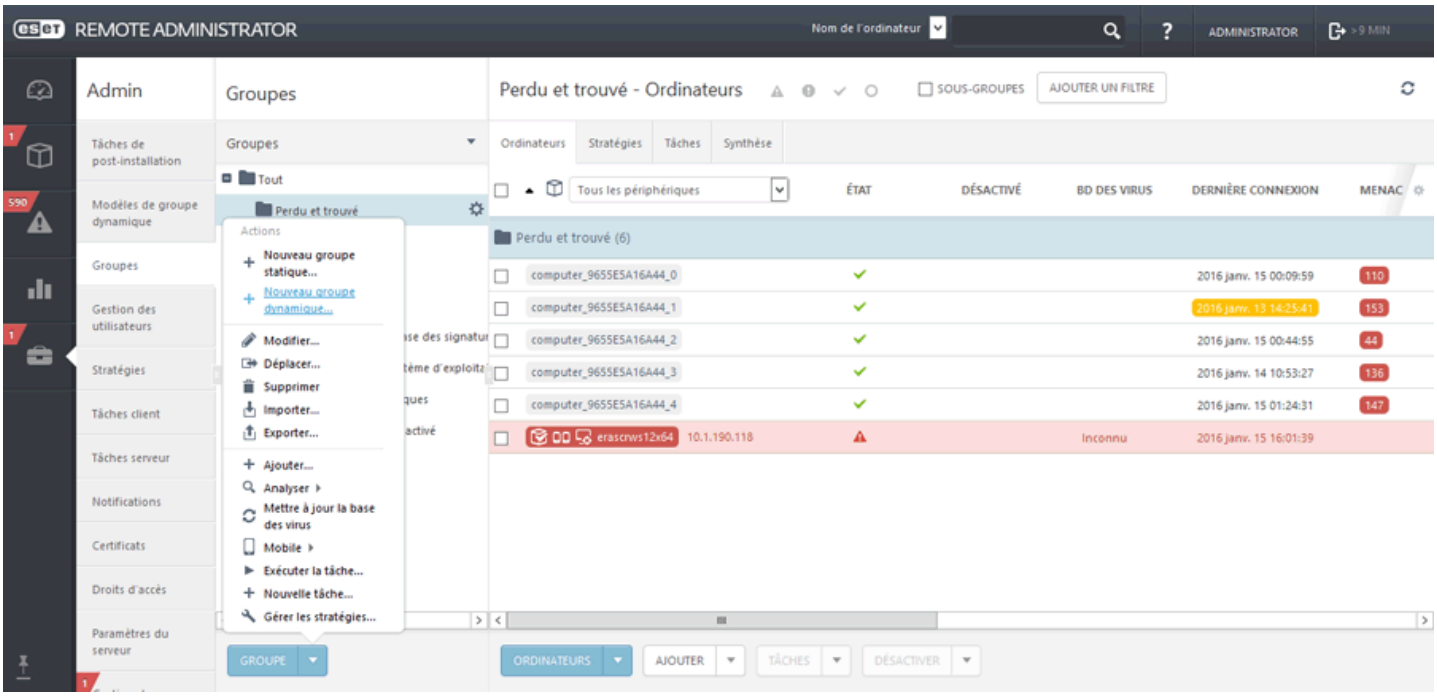
1. Cliquez sur **Ordinateurs** > **Groupes** > ⚙, puis sélectionnez **Nouveau groupe dynamique...**.



2. Cliquez sur **Admin** > **Groupes** > ⚙ > **Nouveau groupe dynamique...**.



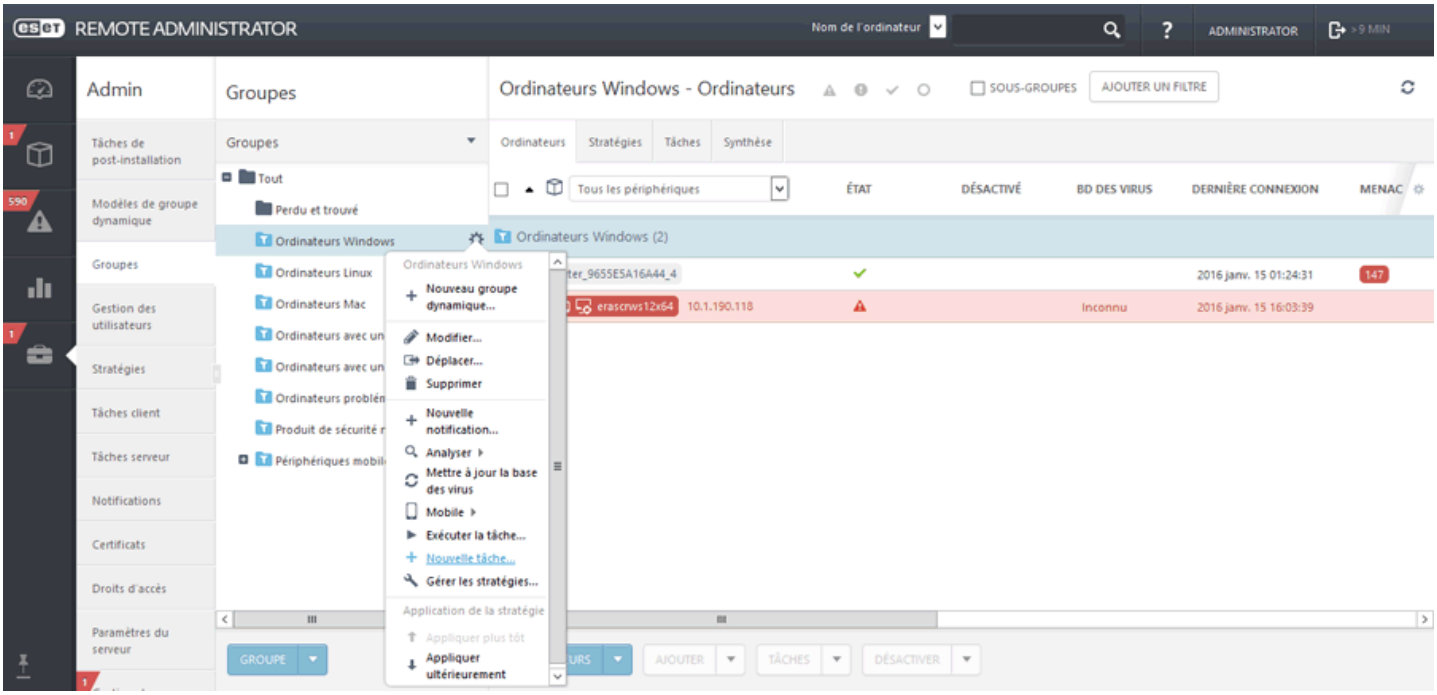
3. Cliquez sur **Admin** > **Groupes**, sur le bouton **Groupe**, puis sur **Nouveau groupe dynamique...**.



L'Assistant Nouveau groupe dynamique s'affiche. Pour obtenir d'autres cas d'utilisation sur la création d'un groupe dynamique avec des règles pour un modèle de groupe dynamique.

4.1.3 Attribuer une tâche à un groupe

Cliquez sur **Admin** > **Groupes**, sélectionnez **Groupe statique** ou **Groupe dynamique**, cliquez sur ⚙ en regard du groupe sélectionné ou sur **Groupe**, puis sur + **Nouvelle tâche**.

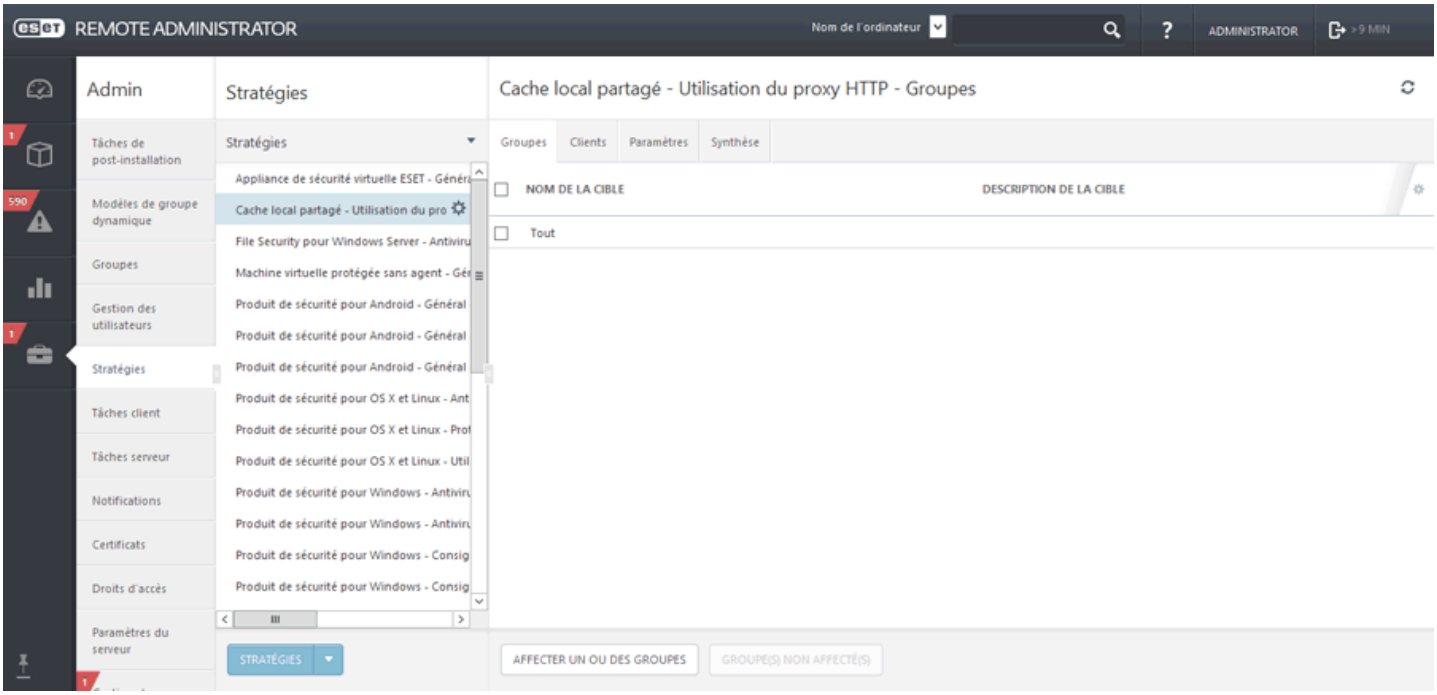


Vous pouvez également cliquer sur **Ordinateurs**, sélectionner **Statique** ou **Dynamique**, puis cliquer sur ⚙ > + **Nouvelle tâche**. La fenêtre Assistant Nouvelle tâche client s'ouvre.

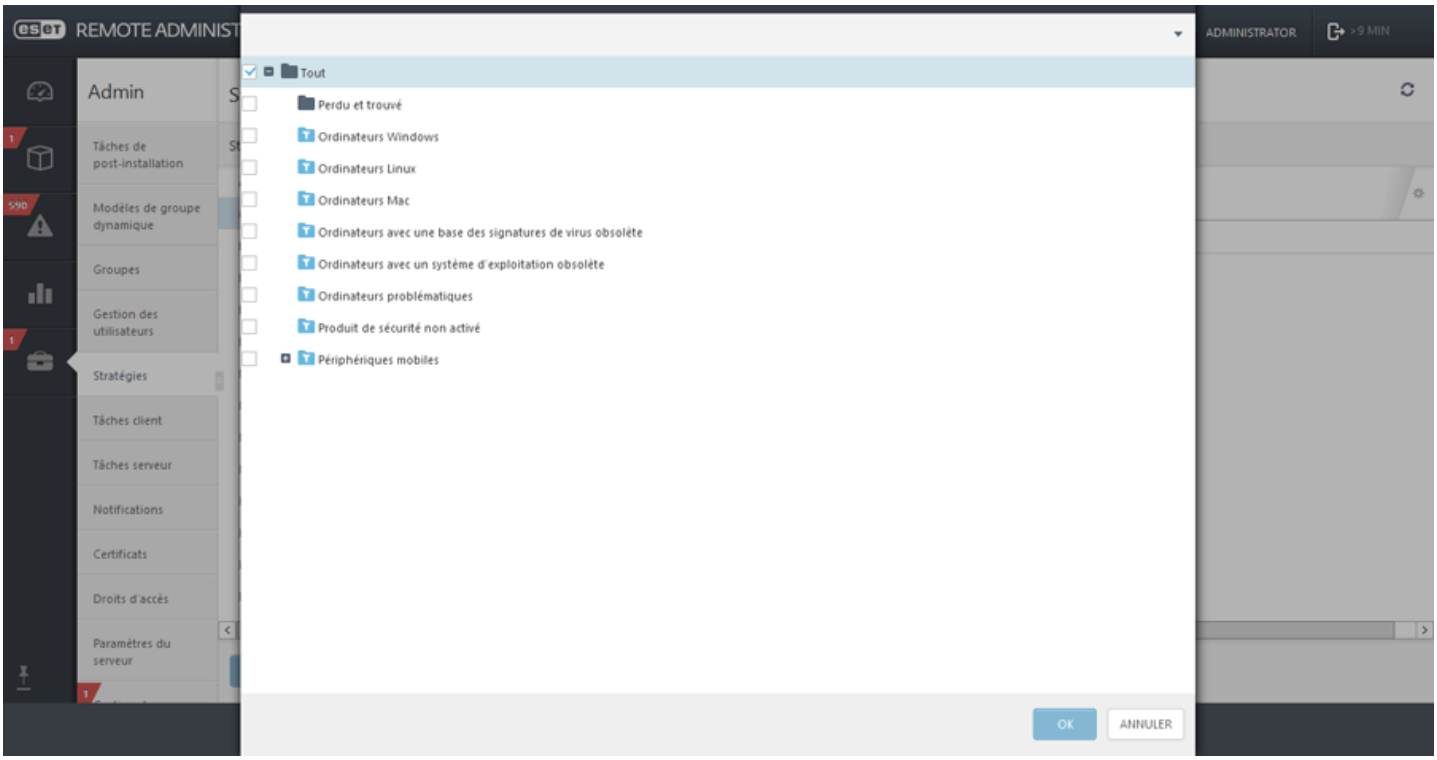
4.1.4 Attribuer une stratégie à un groupe

Une fois une stratégie créée, vous pouvez l'attribuer à un **groupe statique** ou **dynamique**. Il existe deux méthodes pour attribuer une stratégie :

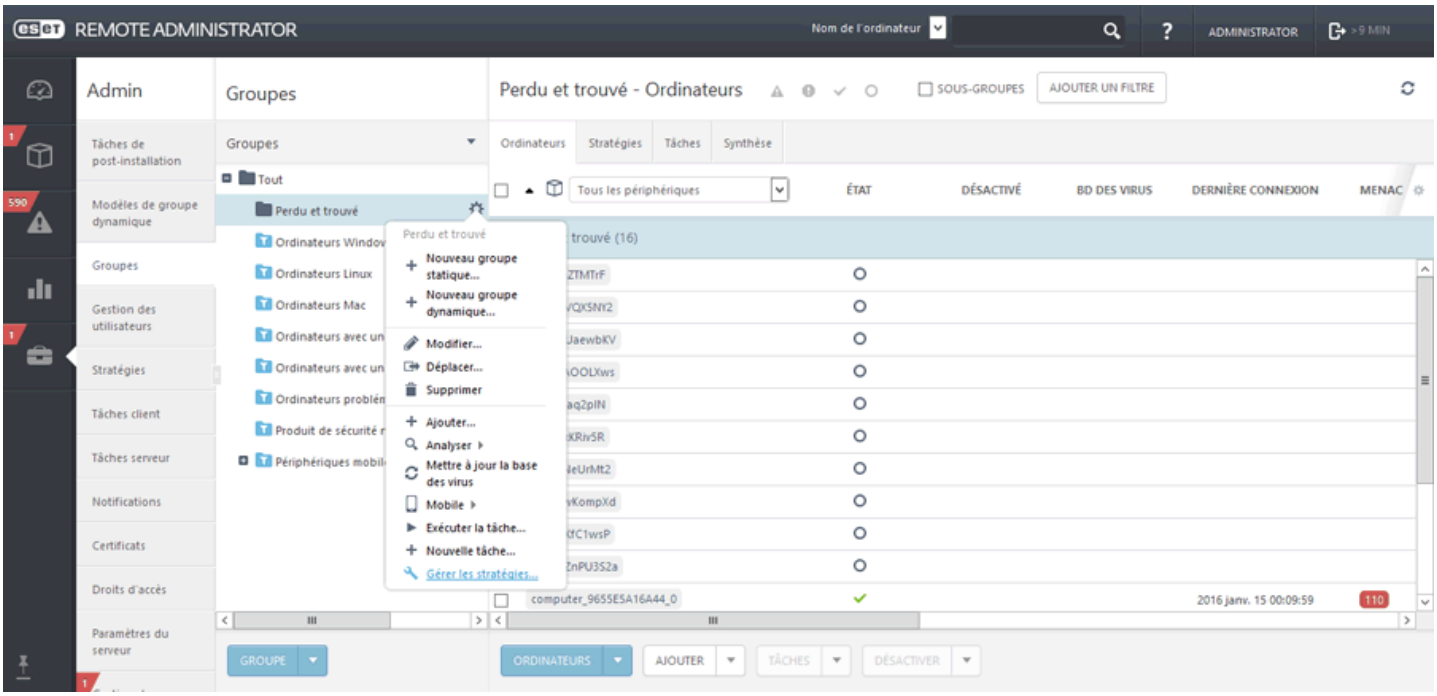
1. Sous **Admin** > **Stratégies**, sélectionnez une stratégie, puis cliquez sur **Affecter un ou des groupes**. Sélectionnez un groupe statique ou dynamique, puis cliquez sur **OK**.



Dans la liste, sélectionnez **Groupe**.



2. Cliquez sur **Admin** > **Groupes** > **Groupe** ou sur l'icône ⚙ située en regard du nom du groupe, puis sélectionnez **Gérer les stratégies**.



Dans la fenêtre **Ordre d'application de la stratégie**, cliquez sur **Ajouter une stratégie**. Cochez la case située en regard de la stratégie à attribuer à ce groupe, puis cliquez sur **OK**.
Cliquez sur **Enregistrer**. Pour afficher la liste des stratégies attribuées à un groupe spécifique, sélectionnez le groupe, puis cliquez sur l'onglet **Stratégies**.

REMARQUE : pour plus d'informations sur les stratégies, reportez-vous au chapitre Stratégies.

4.1.5 Stratégies et groupes

L'appartenance d'un ordinateur à un groupe dynamique est déterminé par les stratégies appliquées à celui-ci. Elle est également déterminée par le modèle sur lequel repose le groupe dynamique.

4.1.6 Modèles de groupe dynamique

Les modèles de groupe dynamique définissent les critères que les ordinateurs doivent respecter pour être placés dans un groupe dynamique. Lorsque ces critères sont respectés par un client, il est automatiquement déplacé vers le groupe dynamique approprié.

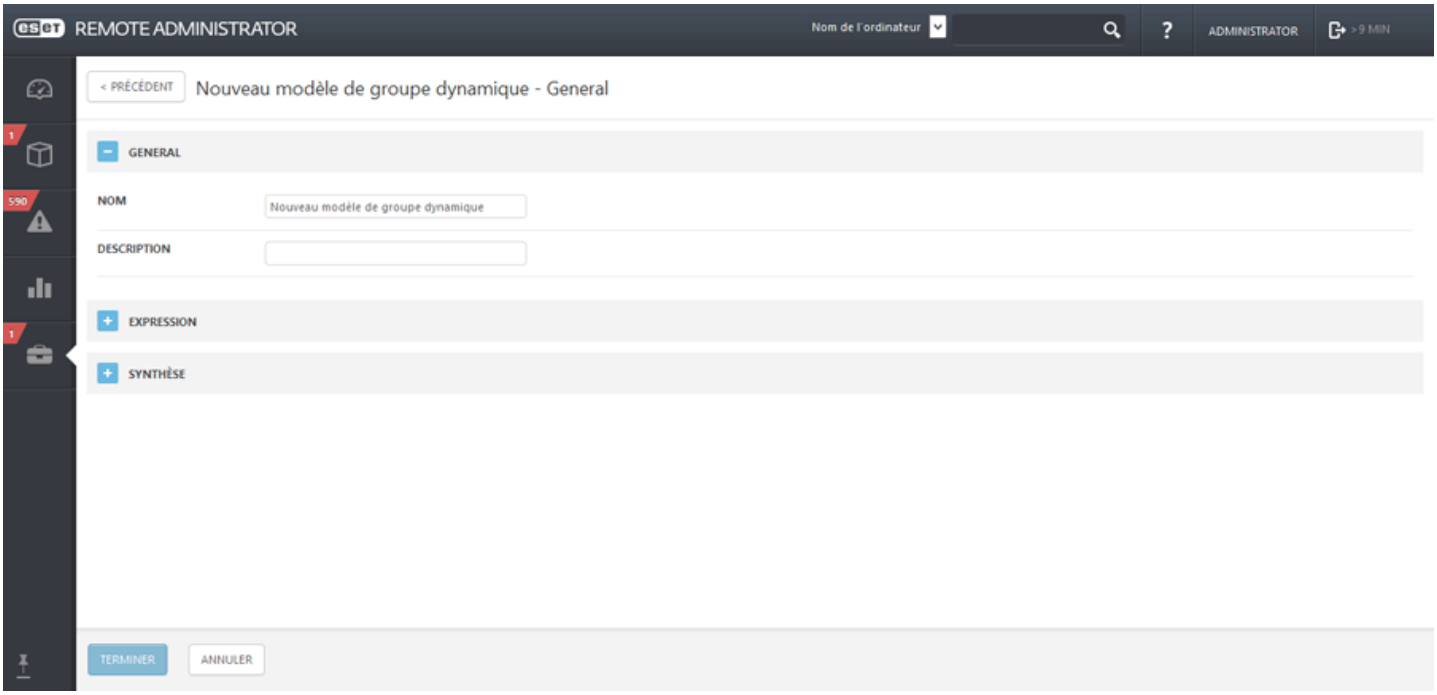
- Créer un modèle de groupe dynamique
- Gérer un modèle de groupe dynamique
- Règles pour un modèle de groupe dynamique
- Modèle de groupe dynamique : exemples

4.1.6.1 Nouveau modèle de groupe dynamique

Cliquez sur **Nouveau modèle** sous **Admin** > **Modèles de groupe dynamique**.

General

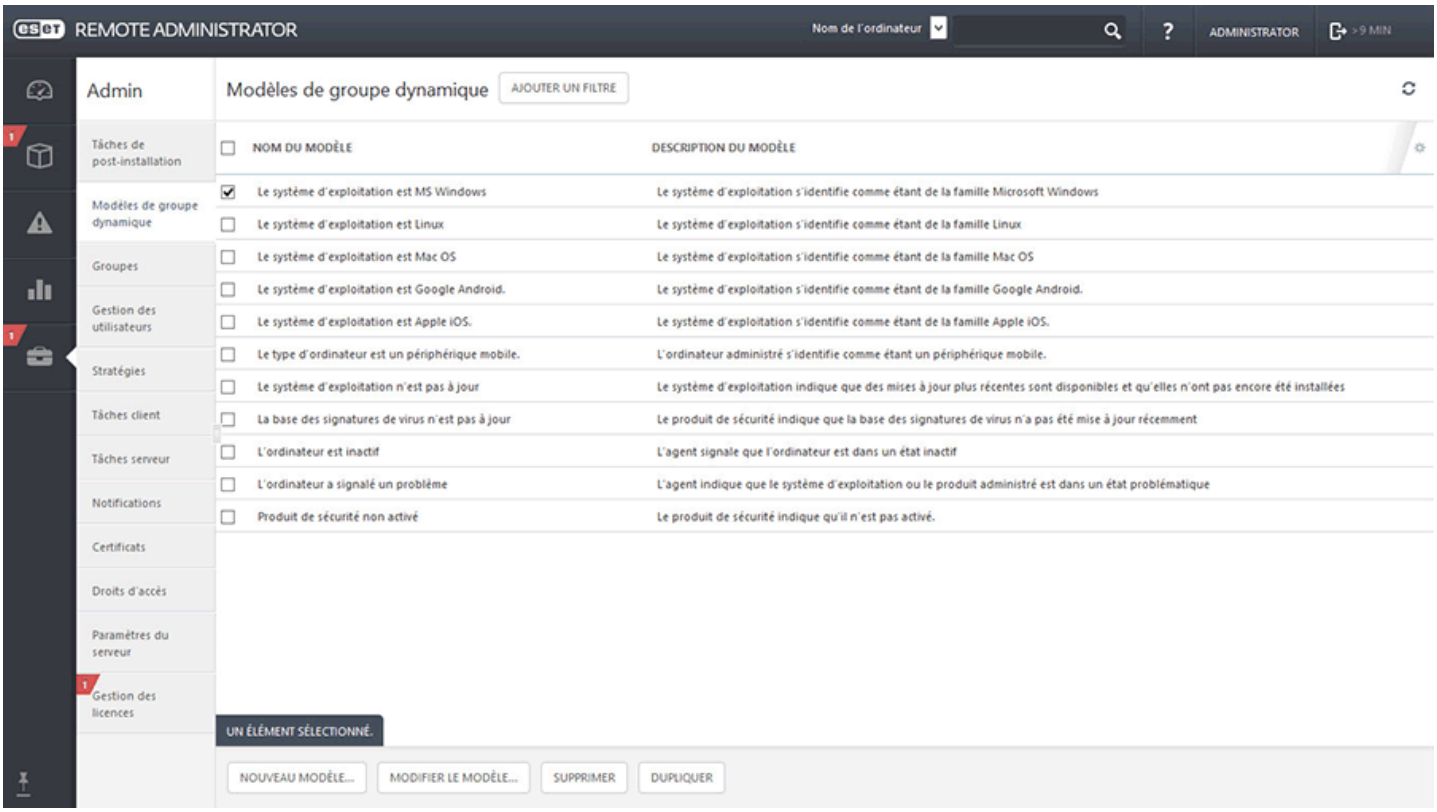
Saisissez un **nom** et une **description** pour le nouveau modèle de groupe dynamique.



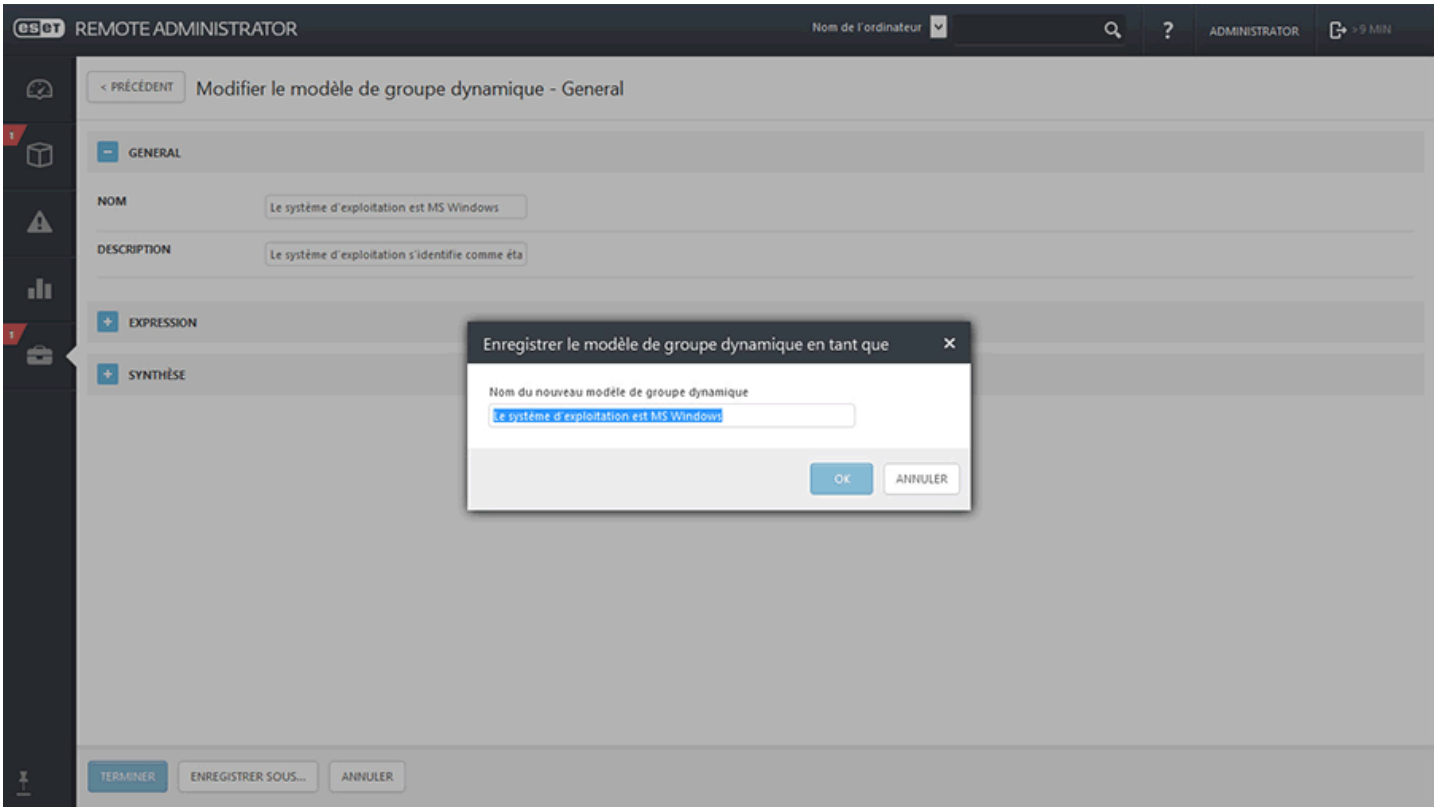
Pour découvrir comment utiliser des groupes dynamiques sur votre réseau, consultez nos exemples avec des instructions détaillées illustrées.

4.1.6.2 Gérer les modèles de groupe dynamique

Les modèles peuvent être gérés dans **Admin** > **Modèles de groupe dynamique**. Vous pouvez créer un modèle ou modifier un modèle existant. Pour modifier un modèle, sélectionnez-le et suivez l'assistant.
Vous pouvez également sélectionner un modèle en cochant la case en regard de celui-ci, puis cliquer sur **Modifier le modèle**.
Dupliquer :vous permet de créer des modèles de groupe dynamique selon les modèles sélectionnés. Un nouveau nom est requis pour la tâche en double.



Cliquez sur **Enregistrer sous** pour conserver votre modèle existant et en créer un nouveau selon le modèle en cours de modification. Donnez un nom à votre nouveau modèle.



4.1.6.3 Modèle de groupe dynamique : exemples

Les exemples de modèle de groupe dynamique de ce guide montrent comment vous pouvez utiliser des groupes dynamiques pour gérer votre réseau :

- Groupe dynamique qui détecte si un produit de sécurité est installé
- Groupe dynamique qui détecte si une version spécifique d'un logiciel est installée
- Groupe dynamique qui détecte si une version spécifique d'un logiciel n'est pas installée
- Groupe dynamique qui détecte si une version spécifique d'un logiciel n'est pas installée et si une autre version existe
- Groupe dynamique qui détecte si un ordinateur se trouve dans un sous-réseau spécifique
- Groupe dynamique qui détecte des versions de produits de sécurité serveur installées mais non activées

De nombreux autres objectifs peuvent être bien sûr atteints à l'aide de modèles de groupe dynamique avec une combinaison de règles. Les possibilités sont pratiquement infinies.

4.1.6.3.1 Groupe dynamique : un produit de sécurité est installé

Ce groupe dynamique peut être utilisé pour exécuter une tâche immédiatement après l'installation d'un produit de sécurité ESET sur un ordinateur : Activation, Analyse personnalisée, etc.

REMARQUE : il est également possible de spécifier un opérateur **pas dans** ou une opération **NON ET** pour rendre la condition négative. Comme le masque des produits administrés est un journal à une ligne, les deux fonctionnent.

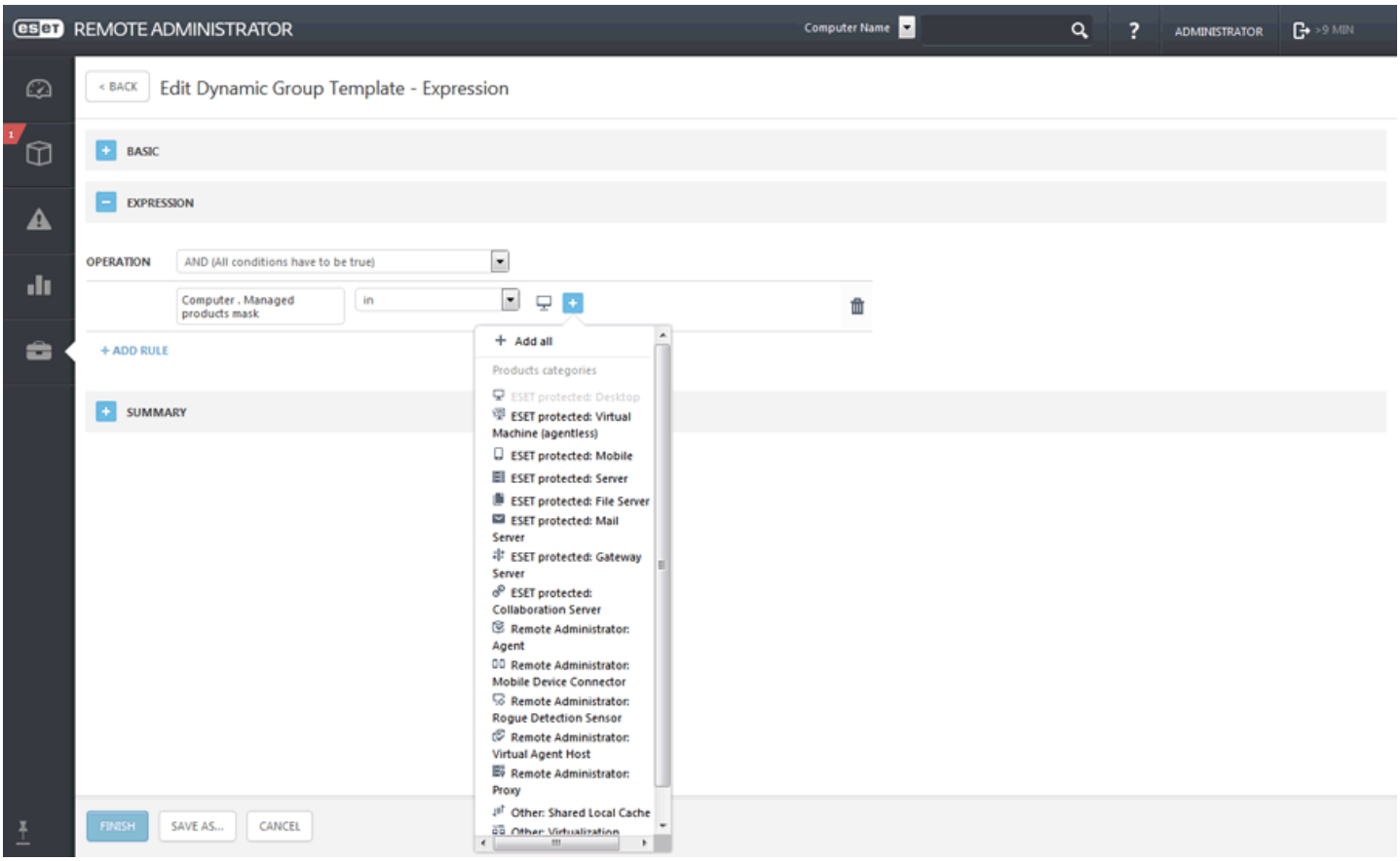
Vous pouvez créer un **modèle** sous **Admin** > **Modèles de groupe dynamique**. Vous pouvez créer un groupe dynamique avec un modèle ou un groupe dynamique à l'aide d'un modèle nouveau ou existant.

Général

Saisissez un **nom** et une **description** pour le nouveau modèle de groupe dynamique.

Expression

- Sélectionnez un opérateur logique dans le menu Opération : **ET** (Toutes les conditions doivent être vraies).
- Cliquez sur **+ Ajouter une règle**, puis sélectionnez une condition. Sélectionnez **Ordinateur** > **Masque des produits administrés** > **dans** > **Protégé par ESET : Bureau**. Vous pouvez choisir des produits ESET différents.



Résumé

Passez en revue les paramètres configurés, puis cliquez sur **Terminer** pour créer le modèle. Le nouveau modèle est ajouté à la liste de tous les modèles et peut être utilisé ultérieurement pour créer un groupe dynamique.

4.1.6.3.2 Groupe dynamique : une version de logiciel spécifique est installée

Ce groupe dynamique peut être utilisé pour détecter un logiciel de sécurité ESET sur un ordinateur. Vous pouvez ensuite exécuter une tâche de mise à niveau ou une commande personnalisée sur ces ordinateurs. Des opérateurs différents, tels que **contient** ou **contient un préfixe**, peuvent être utilisés.

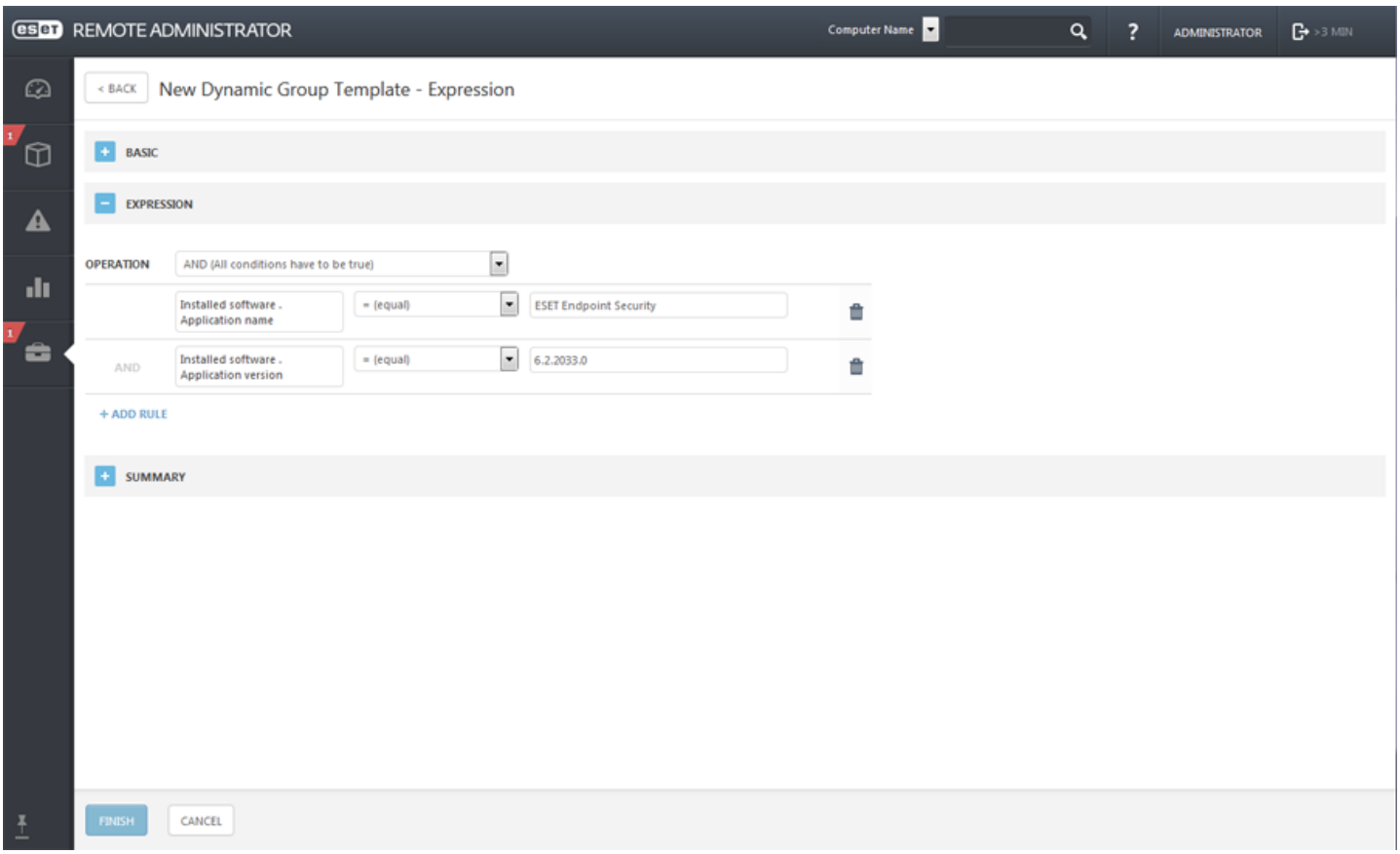
Cliquez sur **Nouveau modèle** sous **Admin** > **Modèles de groupe dynamique**.

Général

Saisissez un **nom** et une **description** pour le nouveau modèle de groupe dynamique.

Expression

- Sélectionnez un opérateur logique dans le menu Opération : **ET** (Toutes les conditions doivent être vraies).
- Cliquez sur **+ Ajouter une règle**, puis sélectionnez une condition :
  - **Logiciel installé** > **Nom de l'application** > **= (égal)** > ESET Endpoint Security
  - **Logiciel installé** > **Version de l'application** > **= (égal)** > 6.2.2033.0



Résumé

Passez en revue les paramètres configurés, puis cliquez sur **Terminer** pour créer le modèle. Le nouveau modèle est ajouté à la liste de tous les modèles et peut être utilisé ultérieurement pour créer un groupe dynamique.

4.1.6.3.3 Groupe dynamique : une version spécifique d'un logiciel n'est pas du tout installée

Ce groupe dynamique peut être utilisé pour détecter un logiciel de sécurité ESET absent d'un ordinateur. Les paramètres de cet exemple incluront des ordinateurs qui ne contiennent pas du tout le logiciel ou des ordinateurs avec des versions autres que celle spécifiée.

Ce groupe est utile car vous pouvez ensuite exécuter une tâche d'installation de logiciel sur ces ordinateurs pour effectuer une installation ou une mise à niveau. Des opérateurs différents, tels que **contient** ou **contient un préfixe**, peuvent être utilisés.

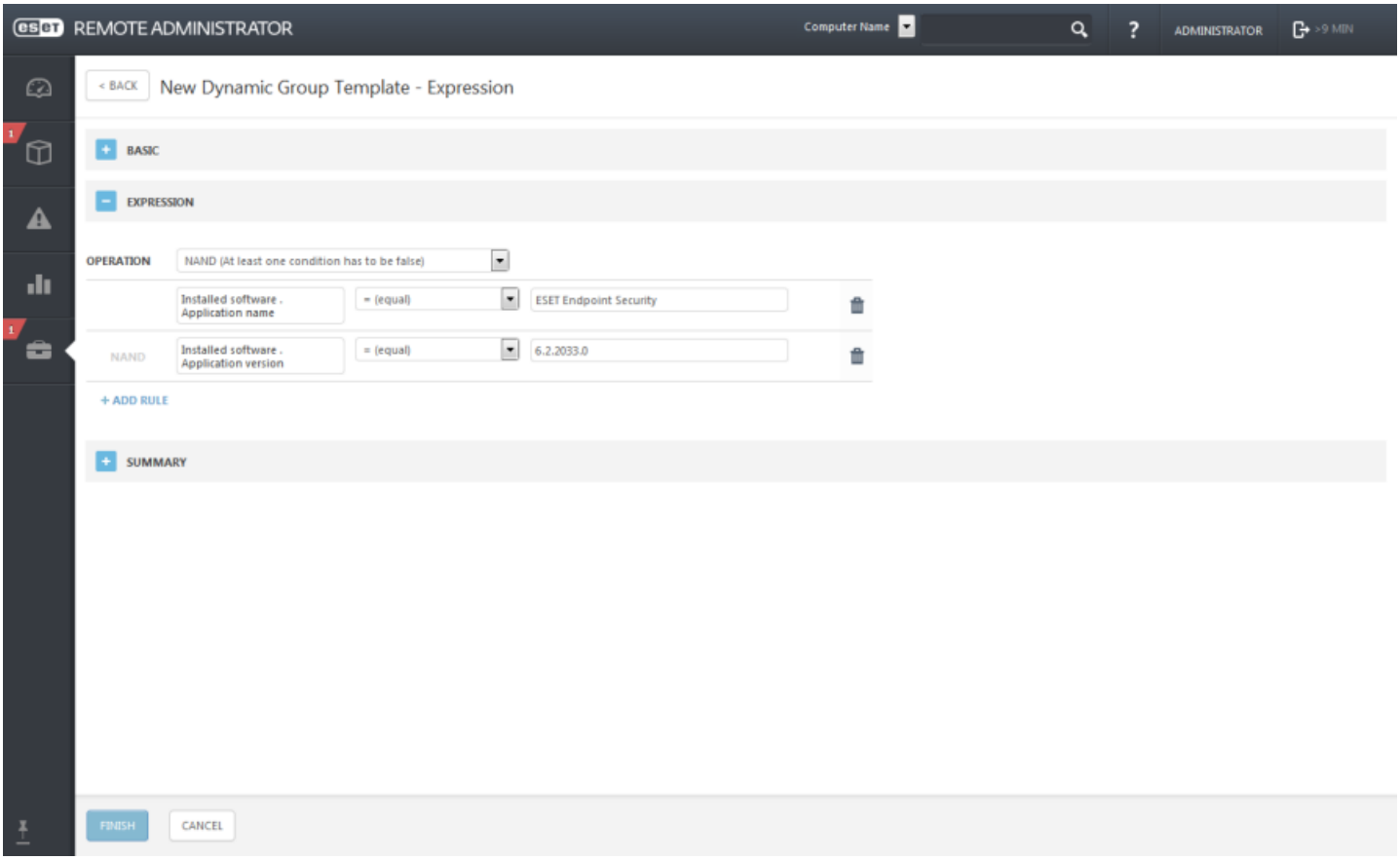
Cliquez sur **Nouveau modèle** sous **Admin** > **Modèles de groupe dynamique**.

Général

Saisissez un **nom** et une **description** pour le nouveau modèle de groupe dynamique.

Expression

- Sélectionnez un opérateur logique dans le menu Opération : **NON ET** (Au moins une des conditions doit être fausse).
- Cliquez sur **+ Ajouter une règle**, puis sélectionnez une condition :
  - **Logiciel installé** > **Nom de l'application** > **= (égal)** > « ESET Endpoint Security »
  - **Logiciel installé** > **Version de l'application** > **= (égal)** > « 6.2.2033.0 »



Résumé

Passez en revue les paramètres configurés, puis cliquez sur **Terminer** pour créer le modèle. Le nouveau modèle est ajouté à la liste de tous les modèles et peut être utilisé ultérieurement pour créer un groupe dynamique.

4.1.6.3.4 Groupe dynamique : une version spécifique d'un logiciel n'est pas installée mais une autre version existe

Ce groupe dynamique peut être utilisé pour détecter un logiciel installé mais dont la version est différente de celle demandée. Ce groupe est utile car vous pouvez ensuite exécuter des tâches de mise à niveau sur les ordinateurs sur lesquels la version demandée est absente. Des opérateurs différents peuvent être utilisés. Vérifiez toutefois que le test de la version est effectuée avec un opérateur de négation.

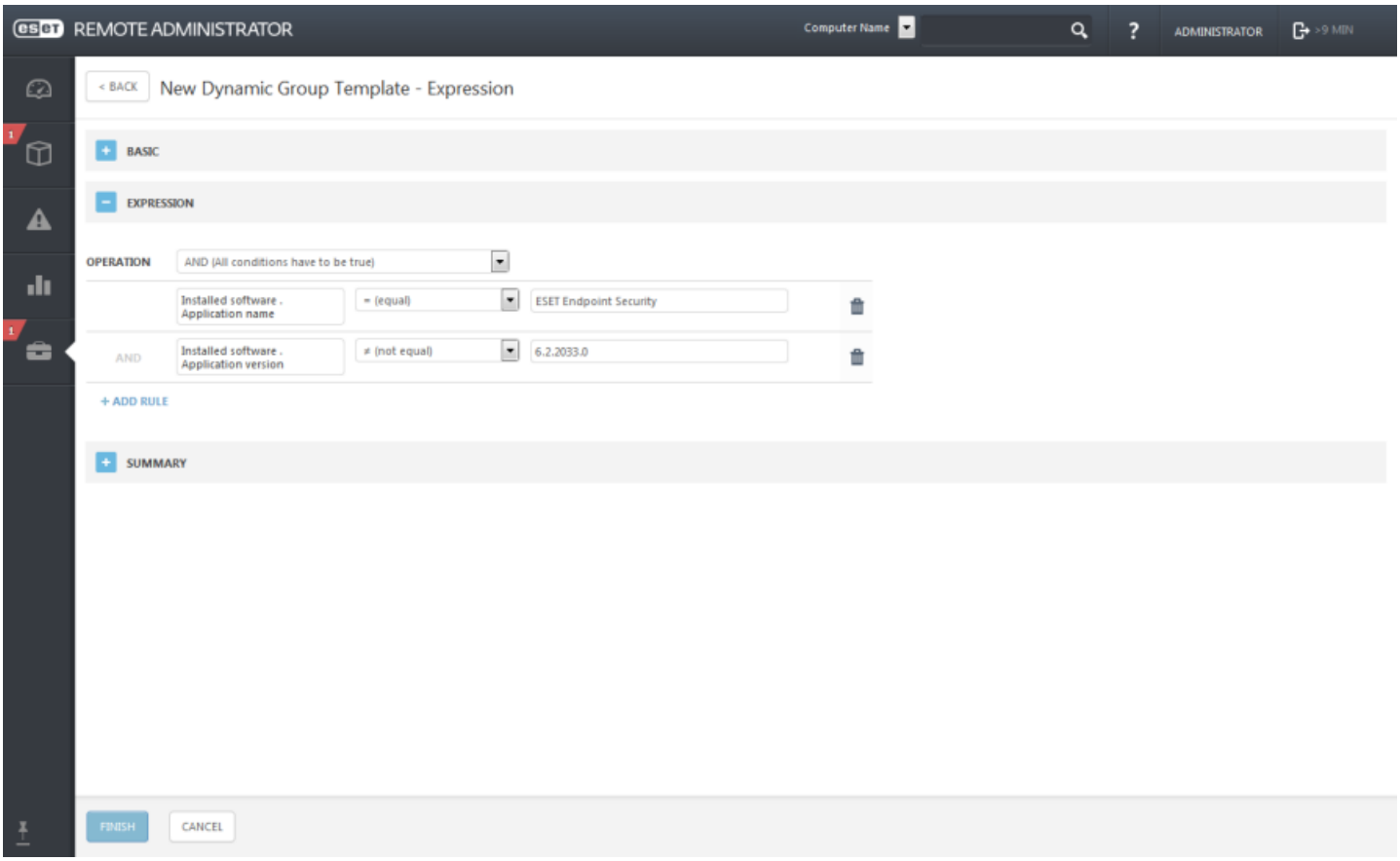
Cliquez sur **Nouveau modèle** sous **Admin** > **Modèles de groupe dynamique**.

Général

Saisissez un **nom** et une **description** pour le nouveau modèle de groupe dynamique.

Expression

- Sélectionnez un opérateur logique dans le menu Opération : **ET** (Toutes les conditions doivent être vraies).
- Cliquez sur **+ Ajouter une règle**, puis sélectionnez une condition :
  - **Logiciel installé** > **Nom de l'application** > **= (égal)** > « ESET Endpoint Security »
  - **Logiciel installé** > **Version de l'application** > **≠ (différent de)** > « 6.2.2033.0 »



Résumé

Passez en revue les paramètres configurés, puis cliquez sur **Terminer** pour créer le modèle. Le nouveau modèle est ajouté à la liste de tous les modèles et peut être utilisé ultérieurement pour créer un groupe dynamique.

4.1.6.3.5 Groupe dynamique : un ordinateur se trouve dans un sous-réseau spécifique

Ce groupe dynamique peut être utilisé pour détecter un sous-réseau spécifique. Il peut ensuite servir à appliquer une stratégie personnalisée pour une mise à jour ou le filtrage Internet. Vous pouvez spécifier différentes plages.

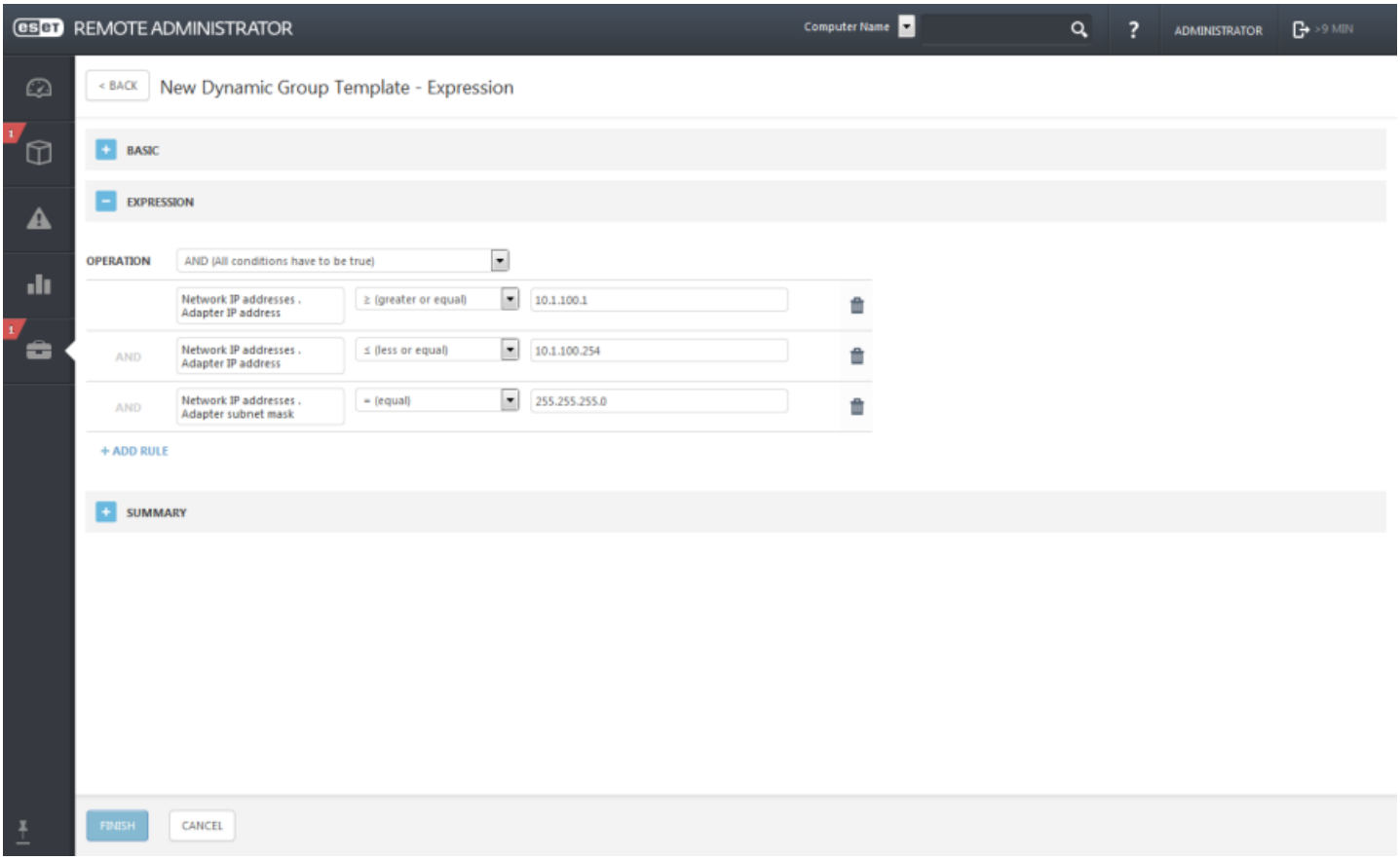
Cliquez sur **Nouveau modèle** sous **Admin** > **Modèles de groupe dynamique**.

Général

Saisissez un **nom** et une **description** pour le nouveau modèle de groupe dynamique.

Expression

- Sélectionnez un opérateur logique dans le menu Opération : **ET** (Toutes les conditions doivent être vraies).
- Cliquez sur **+ Ajouter une règle**, puis sélectionnez une condition :
  - **Adresses IP réseau** > **Adresse IP de la carte** > **≥ (supérieur ou égal)** > « 10.1.100.1 »
  - **Adresses IP réseau** > **Adresse IP de la carte** > **≤ (inférieur ou égal)** > « 10.1.100.254 »
  - **Adresses IP réseau** > **Adresse IP de la carte** > **= (égal)** > « 255.255.255.0 »



Résumé

Passez en revue les paramètres configurés, puis cliquez sur **Terminer** pour créer le modèle. Le nouveau modèle est ajouté à la liste de tous les modèles et peut être utilisé ultérieurement pour créer un groupe dynamique.

4.1.6.3.5.1 Groupe dynamique : version d'un produit de sécurité serveur installée mais non activée

Ce groupe dynamique peut être utilisé pour détecter des produits serveur inactifs. Une fois ces produits détectés, vous pouvez attribuer une tâche client à ce groupe pour activer les ordinateurs client avec la licence adéquate. Dans cet exemple, seul EMSX est spécifié, mais vous pouvez spécifier plusieurs produits.

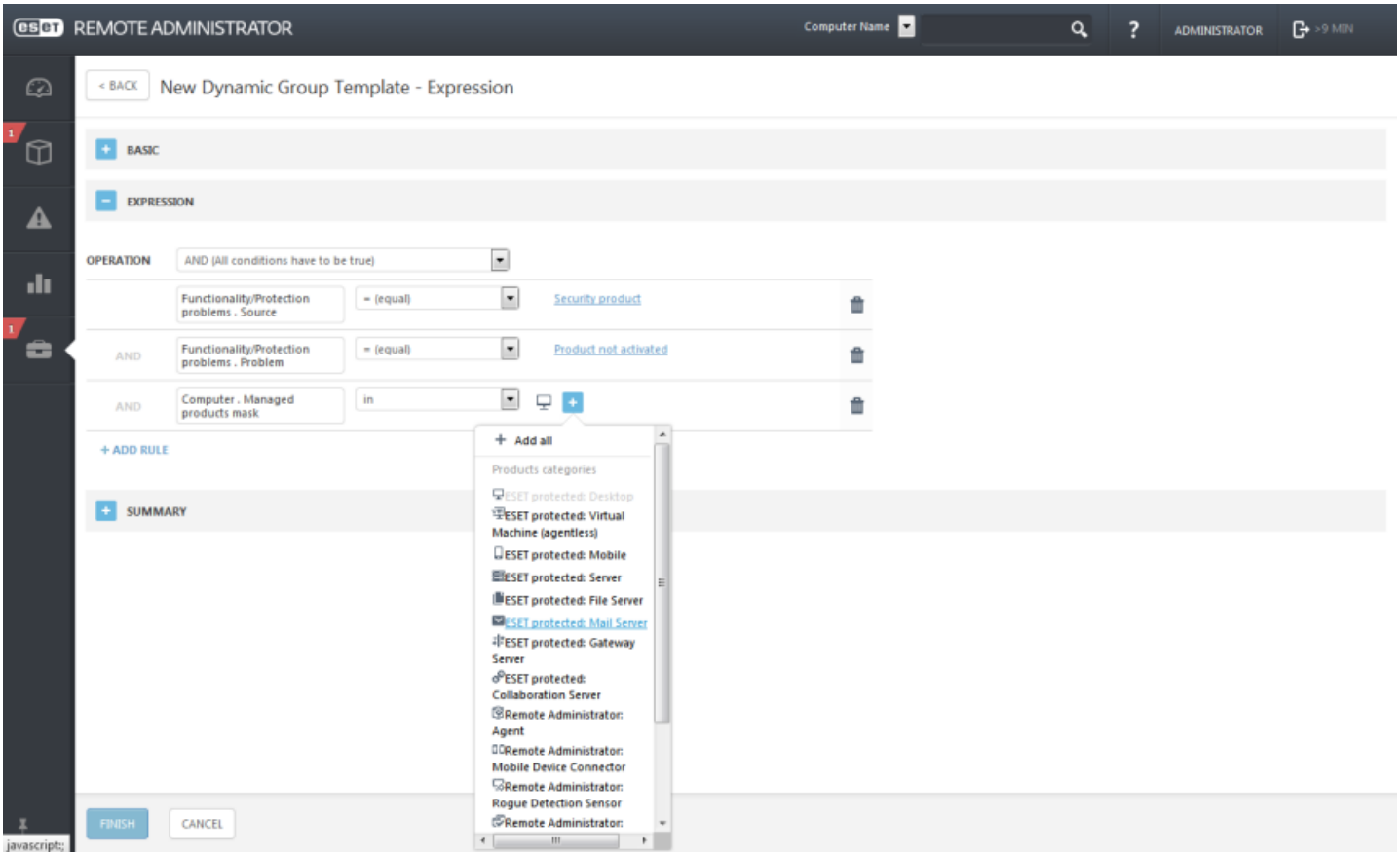
Cliquez sur **Nouveau modèle** sous **Admin** > **Modèles de groupe dynamique**.

Général

Saisissez un **nom** et une **description** pour le nouveau modèle de groupe dynamique.

Expression

- Sélectionnez un opérateur logique dans le menu Opération : **ET** (Toutes les conditions doivent être vraies).
- Cliquez sur **+ Ajouter une règle**, puis sélectionnez une condition :
  - **Ordinateur** > **Masque des produits administrés** > **dans** > « Protégé par ESET : Serveur de messagerie »
  - **Problèmes de fonctionnalité/protection** > **Source** > **= (égal)** > « Produit de sécurité »
  - **Problèmes de fonctionnalité/protection** > **Problème** > **= (égal)** > « Produit non activé »



Résumé

Passez en revue les paramètres configurés, puis cliquez sur **Terminer** pour créer le modèle. Le nouveau modèle est ajouté à la liste de tous les modèles et peut être utilisé ultérieurement pour créer un groupe dynamique.

4.1.7 Groupes statiques

Les groupes statiques servent à trier manuellement les ordinateurs clients en **groupes** et **sous-groupes**. Vous pouvez créer des groupes statiques personnalisés et déplacer les ordinateurs de votre choix vers ceux-ci.

Les groupes statiques peuvent être uniquement créés manuellement. Les ordinateurs clients peuvent ensuite être déplacés manuellement vers ces groupes. Un ordinateur ne peut appartenir qu'à un seul groupe statique.

Il existe deux groupes statiques par défaut :

- **Tous** : il s'agit d'un groupe principal pour tous les ordinateurs d'un réseau ERA Server. Il permet d'appliquer des stratégies à chaque ordinateur en tant que stratégies par défaut. Ce groupe est toujours affiché. Il n'est pas autorisé de modifier le nom des groupes en modifiant le groupe.
- **Perdu et trouvé** en tant que groupe enfant du groupe **Tous** : chaque nouvel ordinateur qui se connecte la première fois avec l'agent au serveur est automatiquement affiché dans ce groupe. Ce groupe peut être renommé et copié, mais il ne peut pas être supprimé ni déplacé.

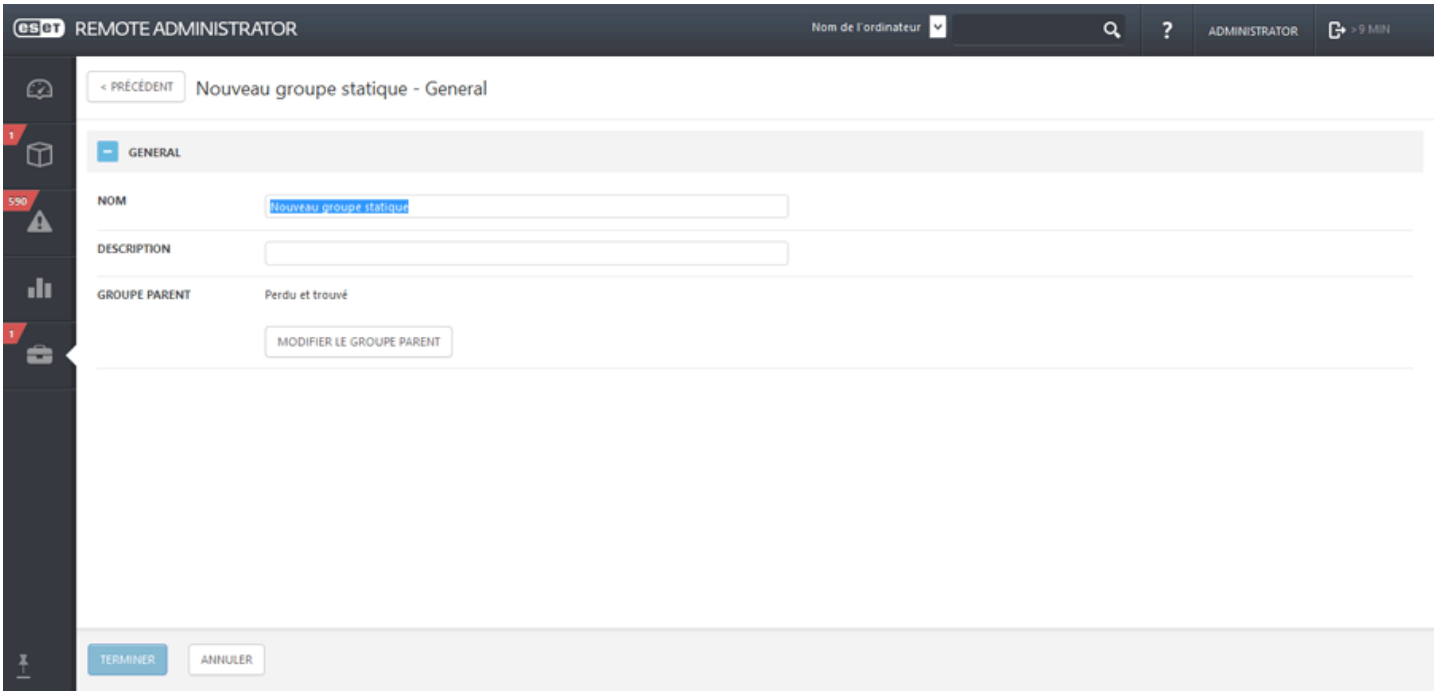
Vous pouvez créer des groupes statiques dans la section **Groupe** de l'onglet **Admin** en cliquant sur le bouton Groupes et en sélectionnant Nouveau groupe statique.

4.1.7.1 Assistant Groupe statique

Sous **Ordinateurs** > **Groupes**, sélectionnez un des groupes statiques, cliquez sur ⚙ et sélectionnez **Nouveau groupe statique**. Vous pouvez créer des groupes statiques dans la section **Groupe** de l'onglet **Admin**. Cliquez sur le bouton **Groupes** et ou sur ⚙ en regard du nom du Groupe statique.

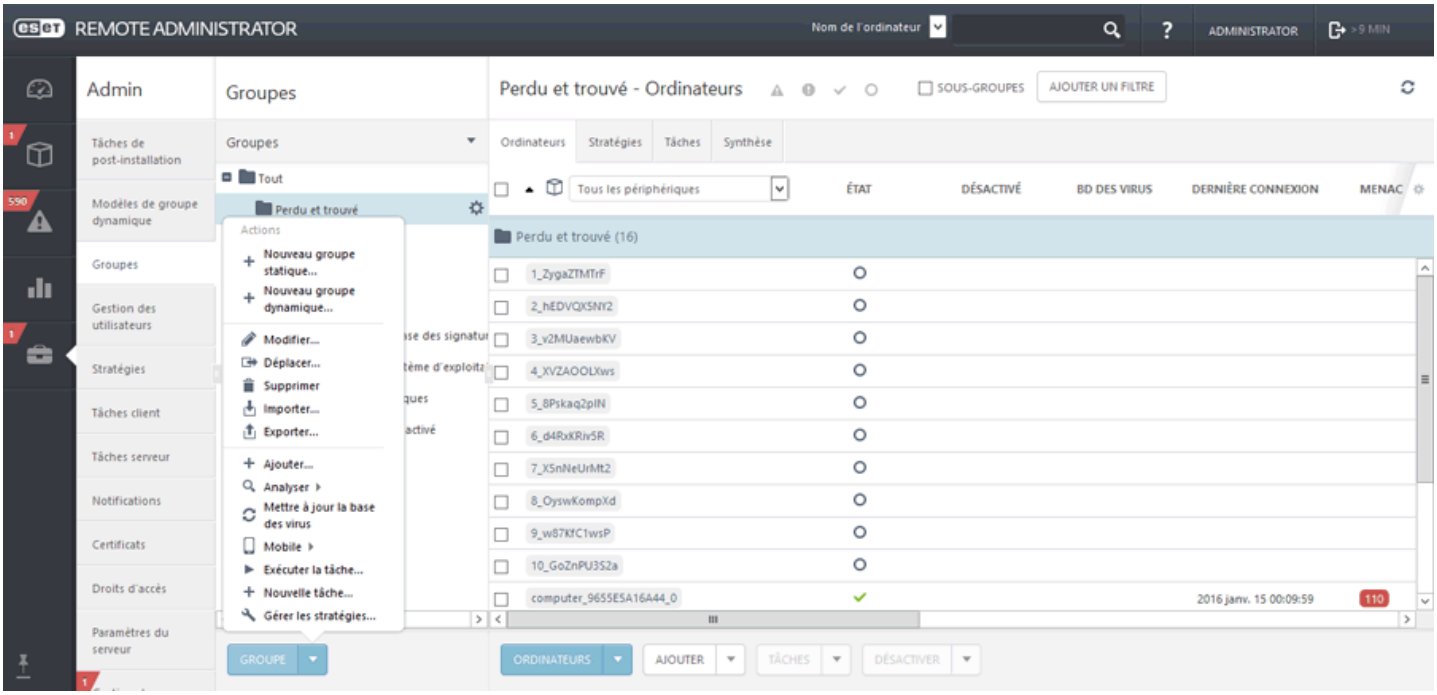
General

Saisissez un **nom** et une **description** pour le nouveau groupe. Vous pouvez éventuellement modifier le **groupe parent**. Par défaut, le groupe parent correspond au groupe que vous avez sélectionné lorsque vous avez créé le groupe statique. Cliquez sur **Terminer** pour créer le groupe statique.



4.1.7.2 Gérer les groupes statiques

Accédez à **Admin** > **Groupes**, puis sélectionnez le groupe statique à gérer. Cliquez sur le bouton **Groupe** ou sur ⚙ en regard du nom du groupe statique. Un menu déroulant apparaît avec les options suivantes :



Actions liées au groupe statique :

+ Nouveau groupe statique... : cette option devient disponible lorsque vous cliquez sur un **groupe** dans la liste de gauche. Ce groupe devient le groupe parent par défaut, mais vous pouvez modifier ce dernier lorsque vous créez un groupe statique.

+ Nouveau groupe dynamique...
Cette option devient disponible lorsque vous cliquez sur un **groupe** dans la liste de gauche. Ce groupe devient le groupe parent par défaut, mais vous pouvez modifier ce dernier lorsque vous créez un groupe dynamique.

Modifier...
Cette option permet de modifier le groupe sélectionné. Les paramètres sont identiques à ceux de la création d'un groupe (statique or dynamique).

Déplacer...
Vous pouvez sélectionner un groupe et le déplacer comme sous-groupe d'un autre groupe.

Supprimer
Supprime entièrement le groupe sélectionné.

Importer
Vous pouvez importer une liste (généralement un fichier texte) d'ordinateurs en tant que membres du groupe sélectionné.

Exporter
Exportez les membres du groupe (et des sous-groupes, s'ils sont sélectionnés) dans une liste (fichier *.txt*). Cette liste peut être révisée ou importée ultérieurement.

+ Ajouter...
Ajoute un ordinateur à un groupe statique.

Analyser
Cette option permet d'exécuter la tâche Analyse à la demande sur le client qui a signalé la menace.

Mettre à jour la base des virus
Cette option permet d'exécuter la tâche Mise à jour de la base des signatures de virus (déclenche manuellement une mise à jour).

Mobile
- **Inscrire...** : à l'aide de cette option, vous pouvez créer une tâche de client.
- **Rechercher** : utilisez cette option si vous souhaitez obtenir les coordonnées GPS de votre périphérique.
- **Verrouiller** : le périphérique est verrouillé lorsqu'une activité suspecte est détectée ou que le périphérique est signalé comme manquant.
- **Déverrouiller** : le périphérique est déverrouillé.
- **Sirène** : déclenche à distance une sirène sonore. Celle-ci est déclenchée même si le périphérique est défini sur muet.
- **Effacer** : toutes les données stockées sur votre périphérique sont effacées de manière définitive.

Nouvelle tâche...
Sélectionnez une tâche et configurez la limitation (facultatif) de cette dernière. La tâche est alors mise en file d'attente selon les paramètres de celle-ci.
Cette option déclenche immédiatement une tâche existante sélectionnée dans une liste de tâches disponibles. Comme cette tâche est exécutée immédiatement, elle n'est associée à aucun déclencheur.

Gérer les stratégies... : attribuez une stratégie au groupe sélectionné.

Nouveau groupe statique
Le groupe statique que vous avez sélectionné en cliquant sur le bouton **Groupe** ou sur est le groupe parent par défaut. Vous pouvez toutefois le modifier ultérieurement (si nécessaire) lors de la création d'un groupe statique.

Modifier le groupe
Cette option permet de modifier le groupe sélectionné. Les paramètres sont identiques à ceux de la création d'un groupe (statique ou dynamique).

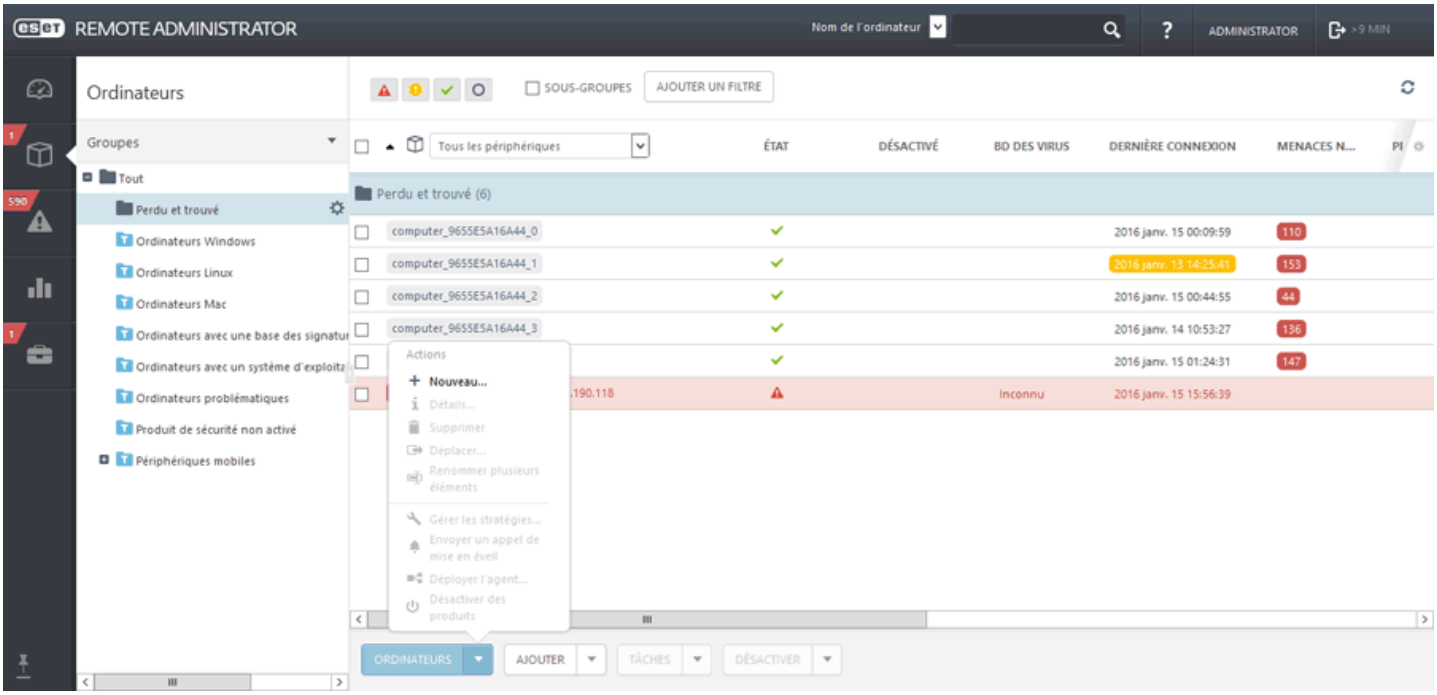
Déplacer
Cette option permet de déplacer le groupe sélectionné vers un autre groupe. Le groupe déplacé devient alors le sous-groupe de ce groupe.

Supprimer
Supprime entièrement le groupe sélectionné.

4.1.7.3 Ajouter un ordinateur client à un groupe statique

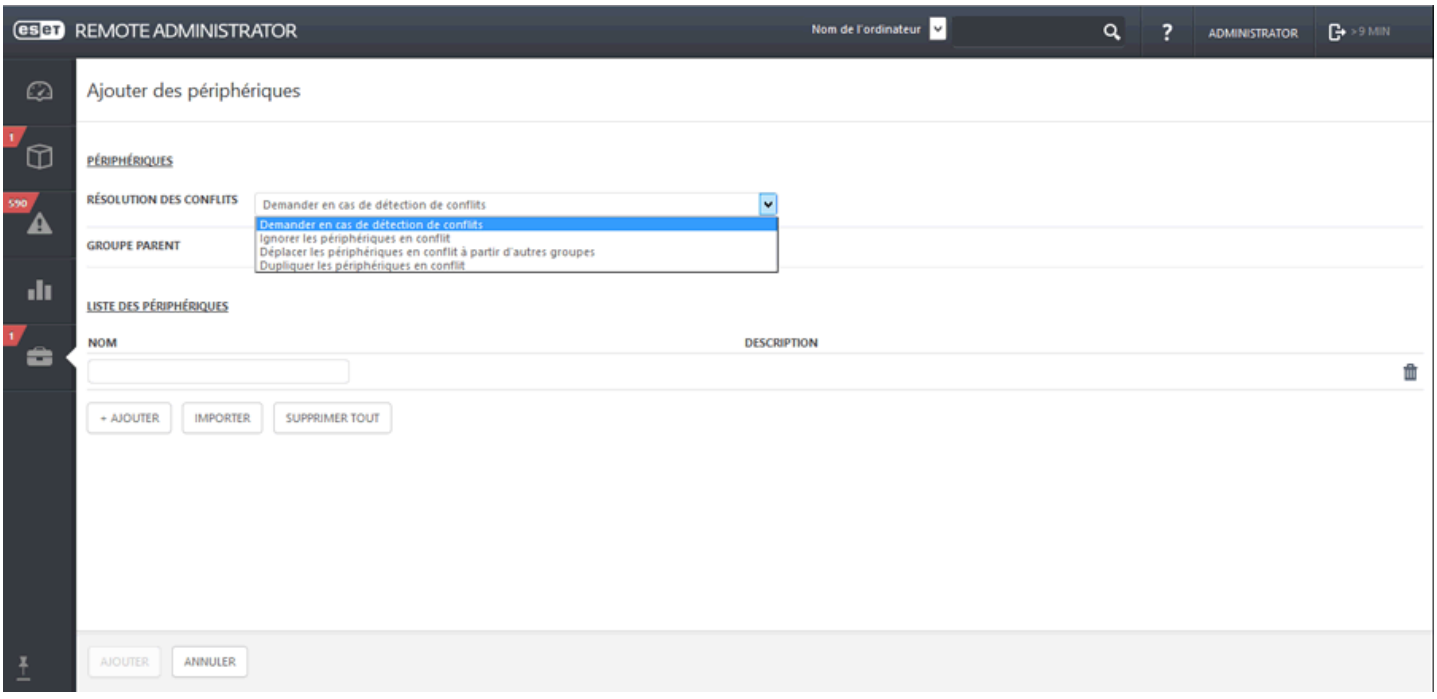
Créez des groupes statiques ou sélectionnez l'un des groupes statiques par défaut.

Cette fonctionnalité permet d'ajouter manuellement des ordinateurs ou des périphériques mobiles qui ne sont pas détectés ou ajoutés automatiquement. Cliquez sur l'onglet **Ordinateurs**, sélectionnez un **groupe statique**, puis cliquez sur **Ajouter**, sélectionnez **Ordinateurs**.



Saisissez le nom de l'ordinateur à ajouter dans le champ **Nom**. Utilisez le menu déroulant **Résolution des conflits** pour sélectionner l'action à exécuter si un ordinateur que vous ajoutez existe déjà dans ERA :

- **Demander en cas de détection de conflits :** lorsqu'un conflit est détecté, le programme vous demande de sélectionner une action (voir les options ci-dessous).
- **Ignorer les ordinateurs en conflit :** les ordinateurs en double ne sont pas ajoutés.
- **Déplacer les ordinateurs en conflit vers d'autres groupes :** les ordinateurs en conflit sont déplacés de leur groupe d'origine vers le groupe **Tous**.
- **Dupliquer les ordinateurs en conflit :** les nouveaux ordinateurs sont ajoutés avec des noms différents.

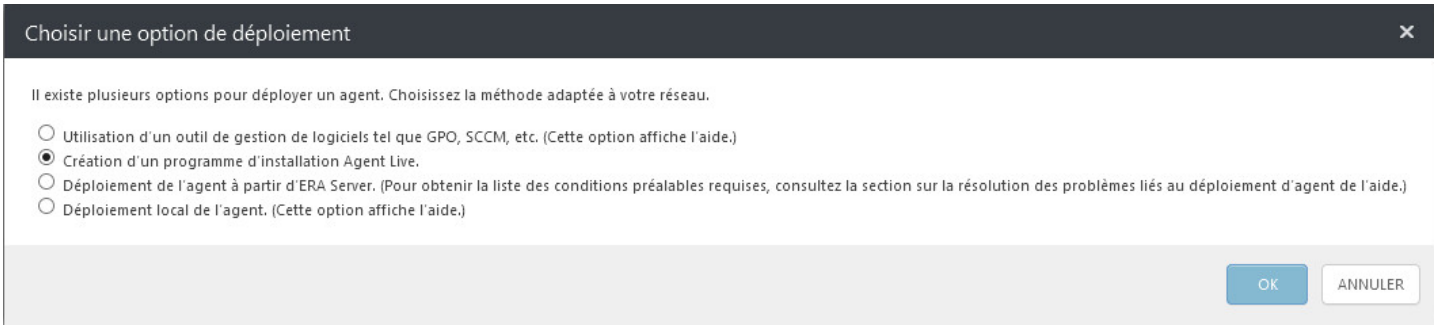


- Cliquez sur + **Ajouter** pour ajouter d'autres ordinateurs. Vous pouvez également cliquer sur **Importer** pour charger un fichier `.csv` qui contient la liste des ordinateurs à ajouter. Vous pouvez éventuellement saisir une **description** des ordinateurs. Lorsque vous avez terminé vos modifications, cliquez sur **Ajouter**.

REMARQUE : l'ajout de plusieurs ordinateurs peut prendre plus de temps. Une recherche DNS inversée peut être effectuée.

Les ordinateurs sont visibles dans la liste de droite lorsque vous sélectionnez le groupe auquel ils appartiennent. Une fois l'ordinateur ajouté, une fenêtre indépendante s'affiche avec l'option **Déployer l'agent**.

Choisissez le type de déploiement à utiliser parmi les options disponibles :



4.1.7.4 Importer des clients à partir d'Active Directory

Pour importer des clients à partir d'AD, créez une **tâche serveur** Synchronisation des groupes statiques.

Sélectionnez un groupe auquel vous souhaitez ajouter de nouveaux ordinateurs à partir d'AD. Sélectionnez également les objets d'Active Directory à partir desquels effectuer la synchronisation et l'action à exécuter sur les doublons. Saisissez les paramètres de connexion au serveur Active Directory, puis définissez le mode de synchronisation sur **Active Directory/Open Directory/LDAP**. Suivez les instructions détaillées de cet article de la base de connaissances ESET.

4.1.7.5 Attribuer une tâche à un groupe statique

Les groupes statiques et dynamiques sont traités de la même manière en ce qui concerne l'attribution de tâche. Pour obtenir des instructions pour l'attribution d'une tâche à un groupe, cliquez ici.

4.1.7.6 Attribuer une stratégie à un groupe statique

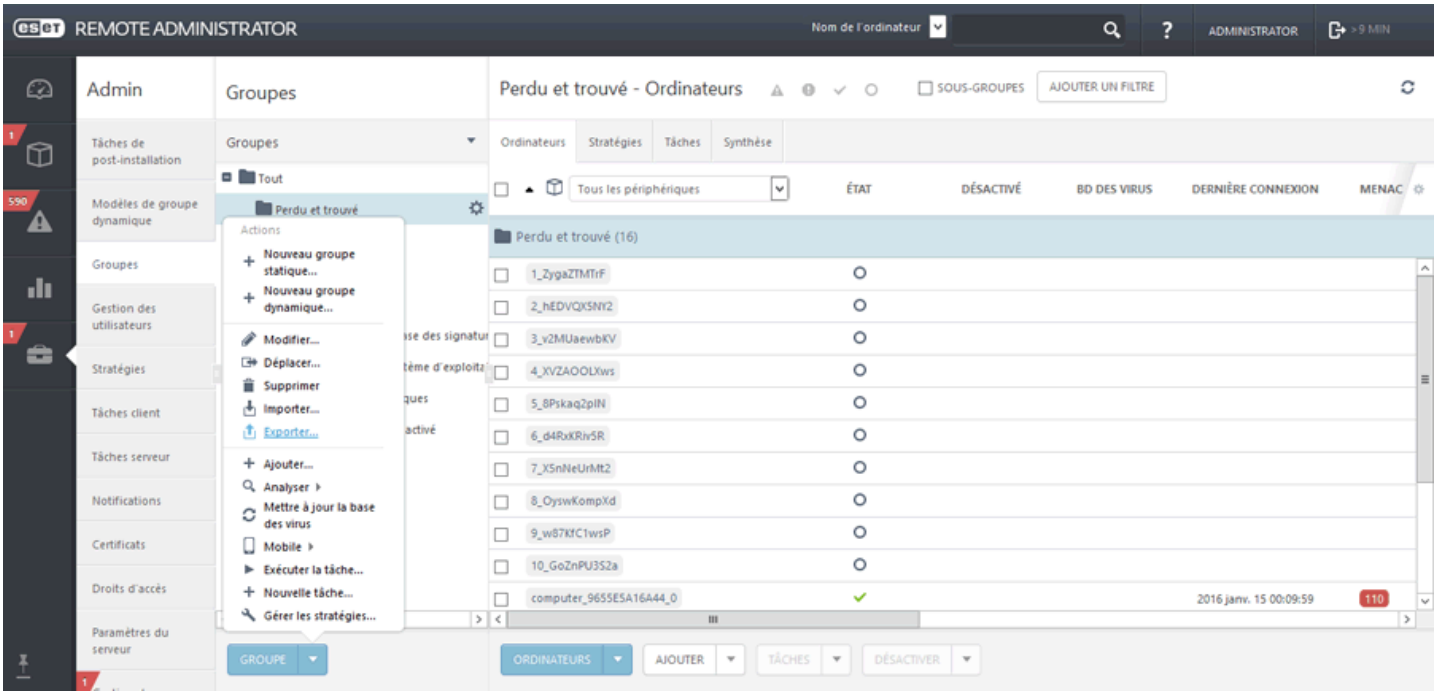
Les groupes statiques et dynamiques sont traités de la même manière en ce qui concerne l'attribution de stratégie. Pour obtenir des instructions pour l'attribution d'une stratégie à un groupe, cliquez ici.

4.1.7.7 Exporter des groupes statiques

Exporter une liste d'ordinateurs de la structure ERA est une opération simple. Vous pouvez exporter la liste et la stocker en tant que sauvegarde afin de l'importer ultérieurement (si vous souhaitez restaurer la structure de groupe, par exemple).

REMARQUE : les groupes statiques doivent contenir au moins un ordinateur. Il est impossible d'exporter des groupes vides.

1. Accédez à **Admin** > **Groupes**, puis sélectionnez le groupe statique à exporter.

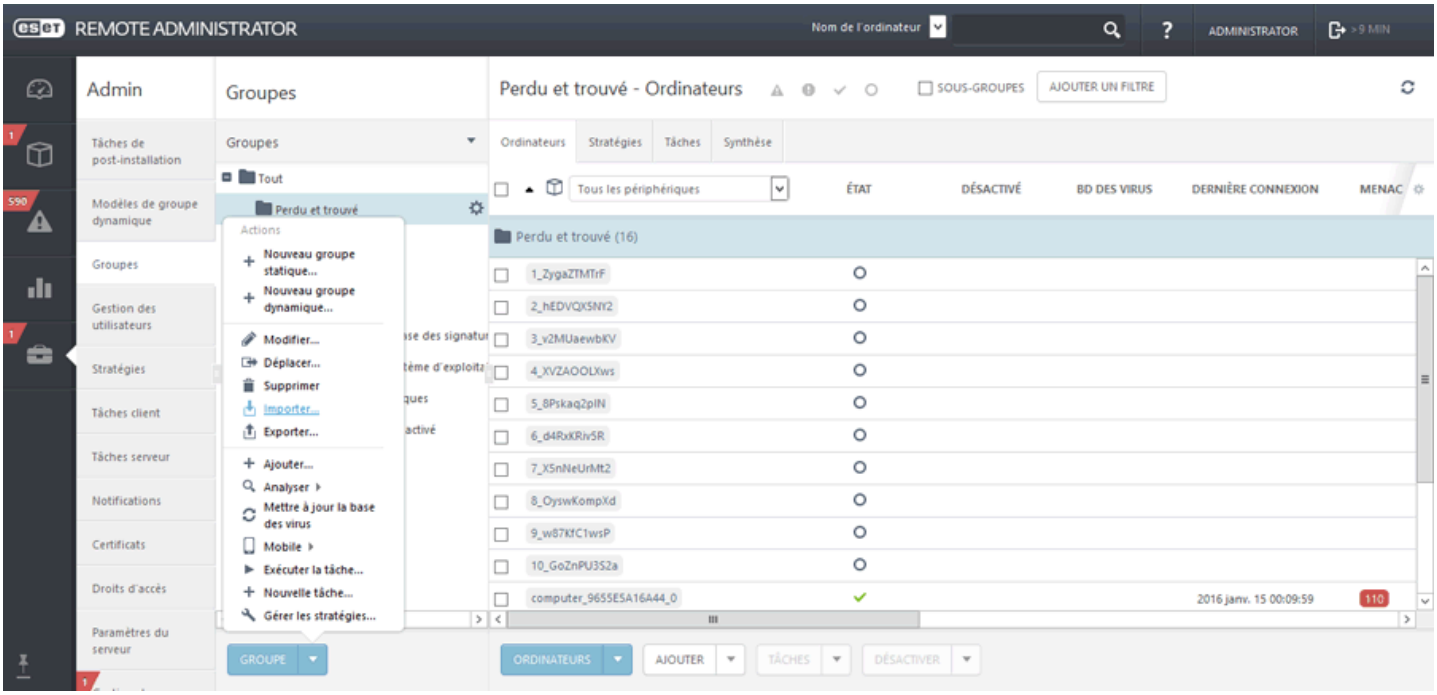


2. Cliquez sur le bouton **Groupe** situé dans la partie inférieure (un menu contextuel s'affiche).
3. Sélectionnez **Exporter.**
4. Le fichier est enregistré au format `.txt`.

REMARQUE : il n'est pas possible d'exporter les groupes dynamiques, car ce ne sont que des liens vers les ordinateurs qui sont conformes aux critères définis dans les modèles de groupe dynamique.

4.1.7.8 Importer des groupes statiques

Les fichiers exportés à partir des groupes statiques peuvent être réimportés dans ERA Web Console et inclus dans votre structure de groupe existante.



1. Cliquez sur **Groupe** (un menu contextuel s'affiche).
2. Sélectionnez **Importer**.
3. Cliquez sur **Parcourir**, puis accédez au fichier **.txt**.
4. Sélectionnez le fichier de groupe, puis cliquez sur **Ouvrir.** Le nom du fichier est affiché dans la zone de texte.
5. Sélectionnez l'une des options suivantes pour résoudre les conflits :

- **Ignorer les ordinateurs en conflit**

Si des groupes statiques existent et incluent des ordinateurs figurant dans le fichier .txt, ces ordinateurs sont ignorés et ne sont pas importés. Des informations à ce propos sont affichées.

- **Déplacer les ordinateurs en conflit vers d'autres groupes**

Si des groupes statiques existent et si des ordinateurs figurant dans le fichier .txt existent déjà dans ces groupes, il est nécessaire de déplacer ces derniers vers d'autres groupes avant de procéder à l'importation. Après l'importation, ces ordinateurs sont redéplacés vers leurs groupes d'origine à partir desquels ils ont été déplacés.

- **Dupliquer les ordinateurs en conflit**

Si des groupes statiques existent et incluent des ordinateurs figurant dans le fichier .txt, des doublons de ces ordinateurs sont créés dans les mêmes groupes statiques. L'ordinateur d'origine est affiché avec des informations complètes, tandis que le doublon n'est affiché qu'avec son nom d'ordinateur.

5. Cliquez sur **Importer**. Les groupes statiques et les ordinateurs qu'ils contiennent sont alors importés.

4.1.8 Groupes dynamiques

Les groupes dynamiques sont essentiellement des filtres personnalisés définis dans des modèles. Étant donné que les ordinateurs sont filtrés du côté de l'Agent, aucune information supplémentaire ne doit être transférée au serveur. L'Agent décide à quels groupes dynamiques appartient un client et n'envoie une notification au serveur que pour lui faire part de cette décision. Les règles des groupes dynamiques sont définies dans le modèle de groupe dynamique.

Certains groupes dynamiques prédéfinis sont proposés après l'installation d'ESET Remote Administrator. Si nécessaire, vous pouvez également créer des groupes dynamiques personnalisés. Pour ce faire, commencez par créer un modèle, puis créez un groupe dynamique.

Une autre méthode consiste à créer simultanément un groupe dynamique et un modèle.

Il est possible de créer plusieurs groupes dynamiques à partir d'un seul modèle.

Un utilisateur peut avoir recours aux groupes dynamiques dans d'autres composants d'ERA. Il est possible de leur attribuer des stratégies ou de préparer une tâche pour tous les ordinateurs qu'ils contiennent.

Les groupes dynamiques peuvent se trouver en dessous de groupes statiques ou dynamiques. Toutefois, le groupe du niveau supérieur est toujours statique.

Tous les groupes dynamiques situés en dessous d'un groupe statique donné filtrent uniquement les ordinateurs de ce dernier, indépendamment de leur niveau dans l'arborescence. De plus, dans le cas des groupes dynamiques imbriqués, un groupe dynamique de niveau inférieur filtre les résultats du groupe supérieur.

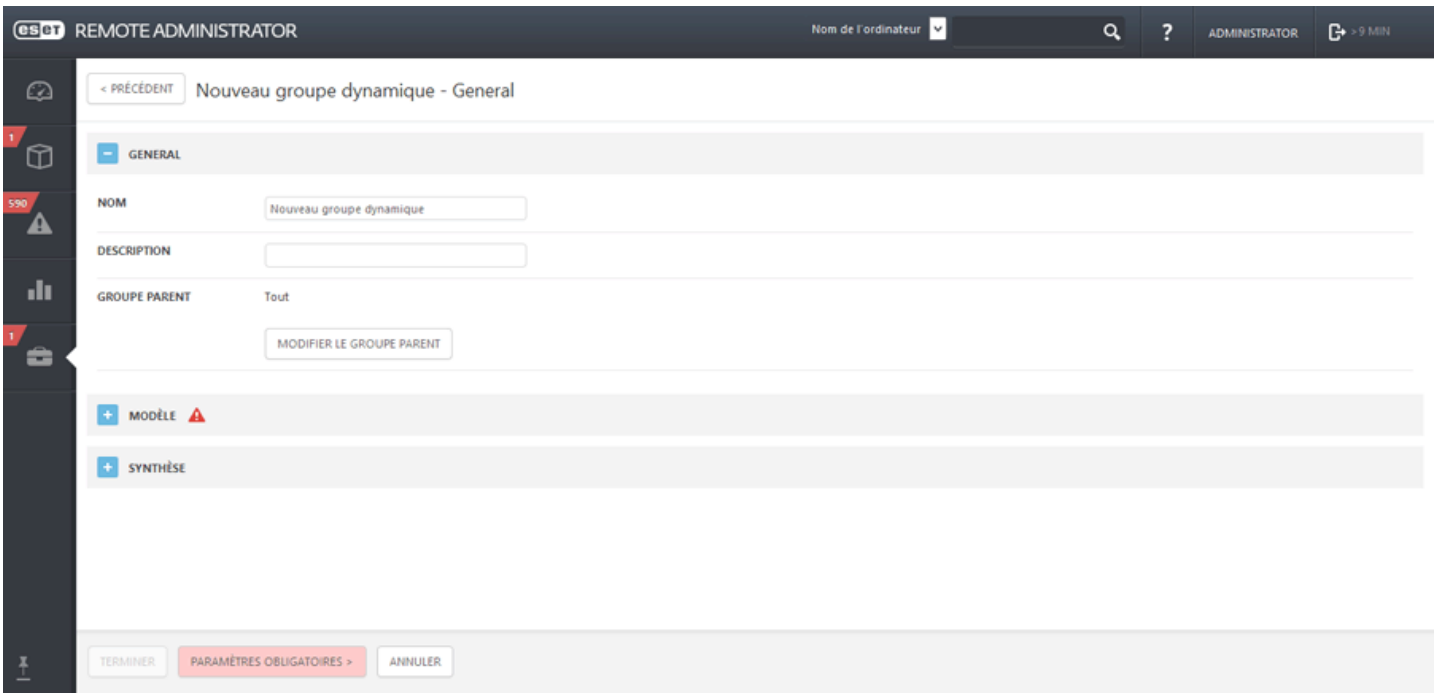
Les stratégies sont appliquées comme décrit ici. Une fois créées, elles peuvent être toutefois déplacées librement dans l'arborescence.

4.1.8.1 Assistant Groupe dynamique

Vous pouvez créer un groupe dynamique à l'aide d'un modèle existant ou d'un nouveau modèle qui sera ensuite utilisé pour ce groupe dynamique.

General

Saisissez un **nom** et une **description** (facultatif) pour le nouveau groupe dynamique. Par défaut, le groupe parent correspond au groupe que vous avez sélectionné lorsque vous avez commencé à créer le groupe statique. Si vous souhaitez modifier le groupe parent, vous pouvez cliquer sur **Modifier le groupe parent**, puis en sélectionner un autre dans l'arborescence. Le parent du nouveau groupe dynamique peut être dynamique ou statique. Cliquez sur **Terminer** pour créer le groupe dynamique.



Modèle

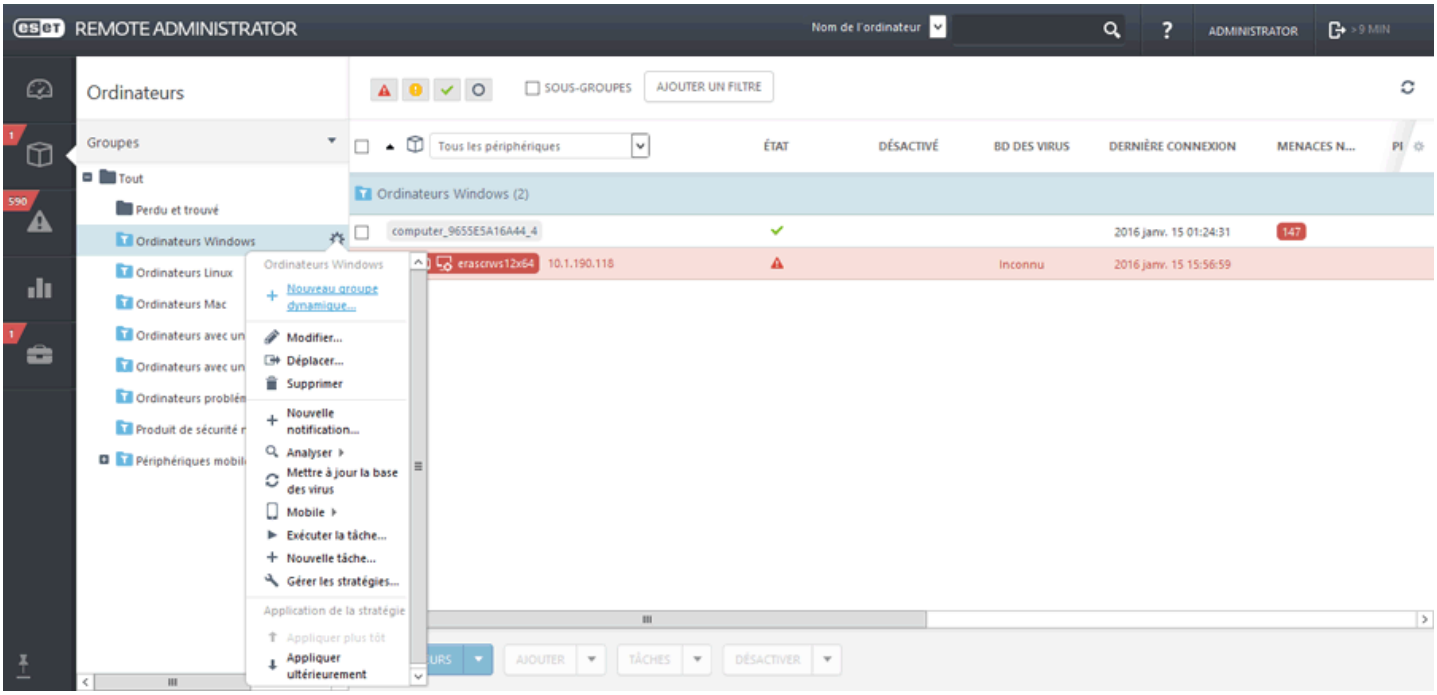
Vous pouvez sélectionner un modèle de groupe dynamique existant ou créer un modèle de groupe existant.

Résumé

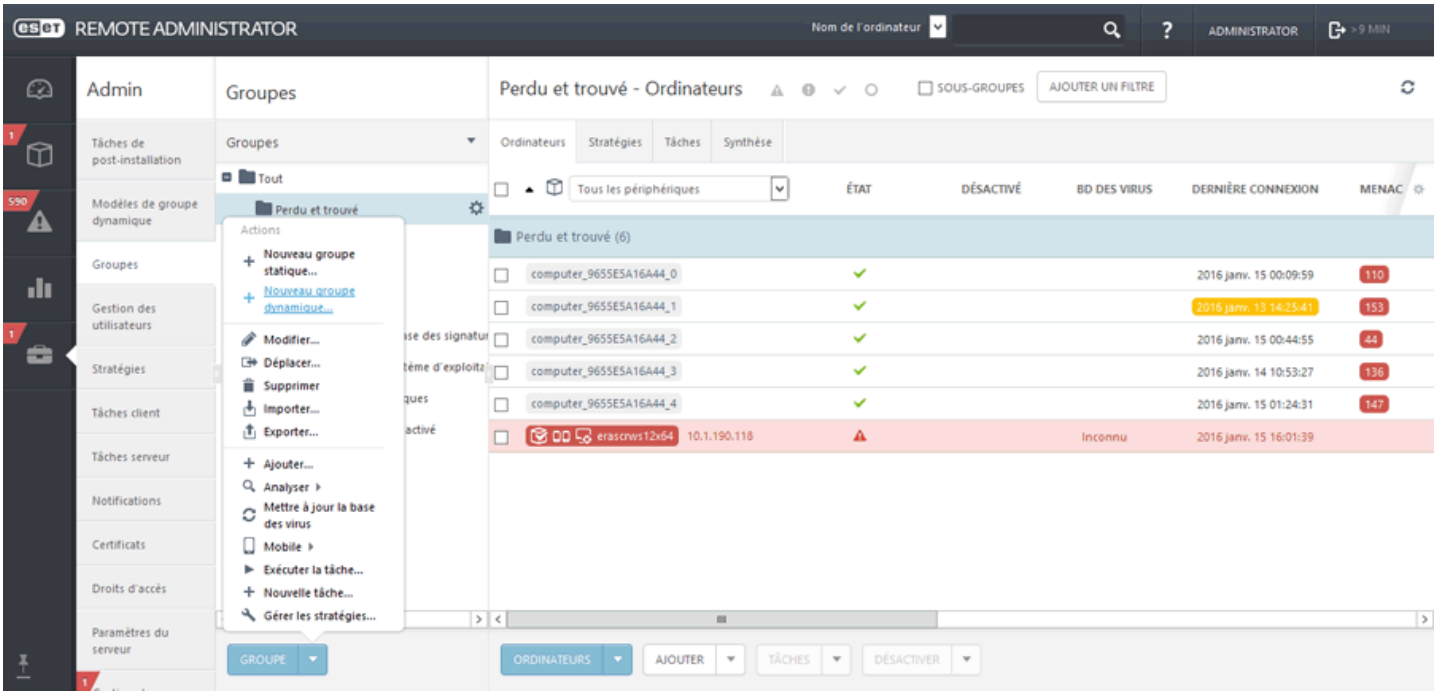
Passez en revue la configuration pour vérifier qu'elle est correcte (si vous devez effectuer des modifications, vous pouvez toujours le faire), puis cliquez sur **Terminer**.

4.1.8.2 Créer un groupe dynamique à l'aide d'un modèle existant

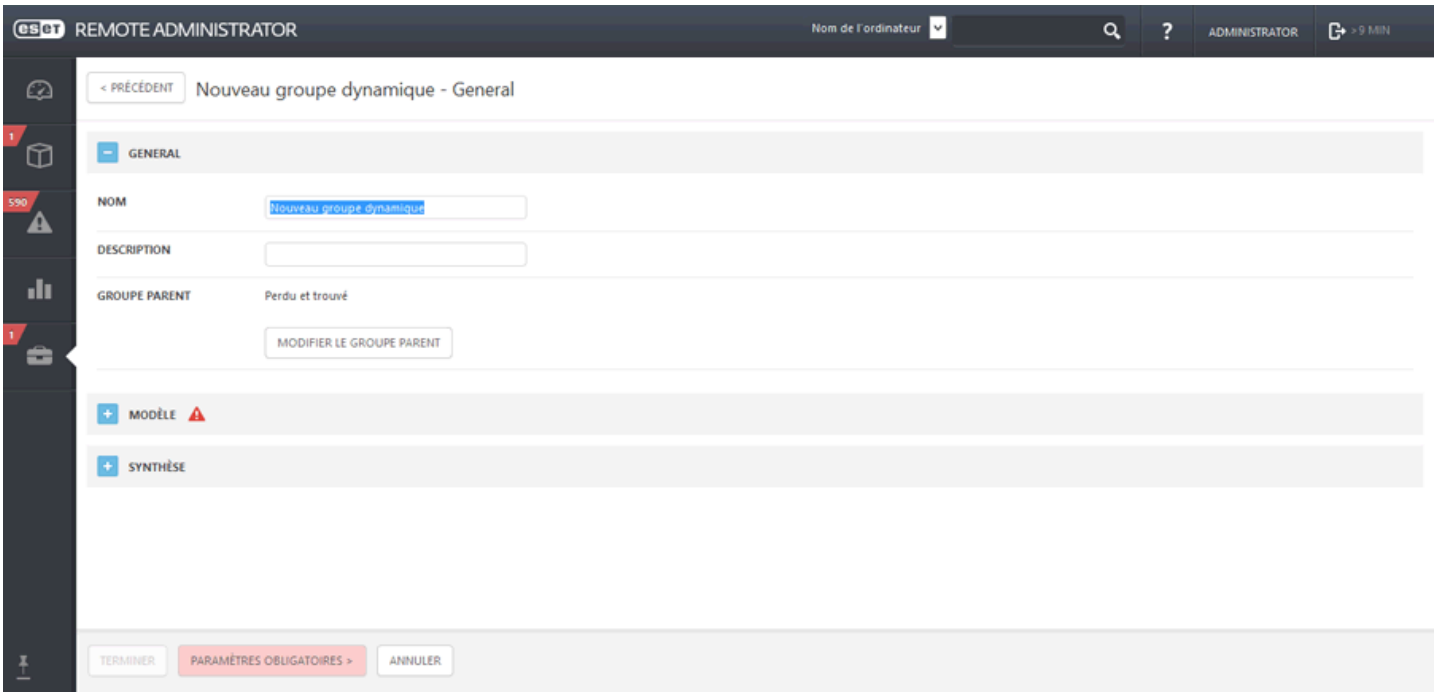
Pour créer un groupe dynamique à l'aide d'un modèle existant, cliquez sur ⚙ en regard du nom du groupe dynamique, puis sur **Nouveau groupe dynamique...**.



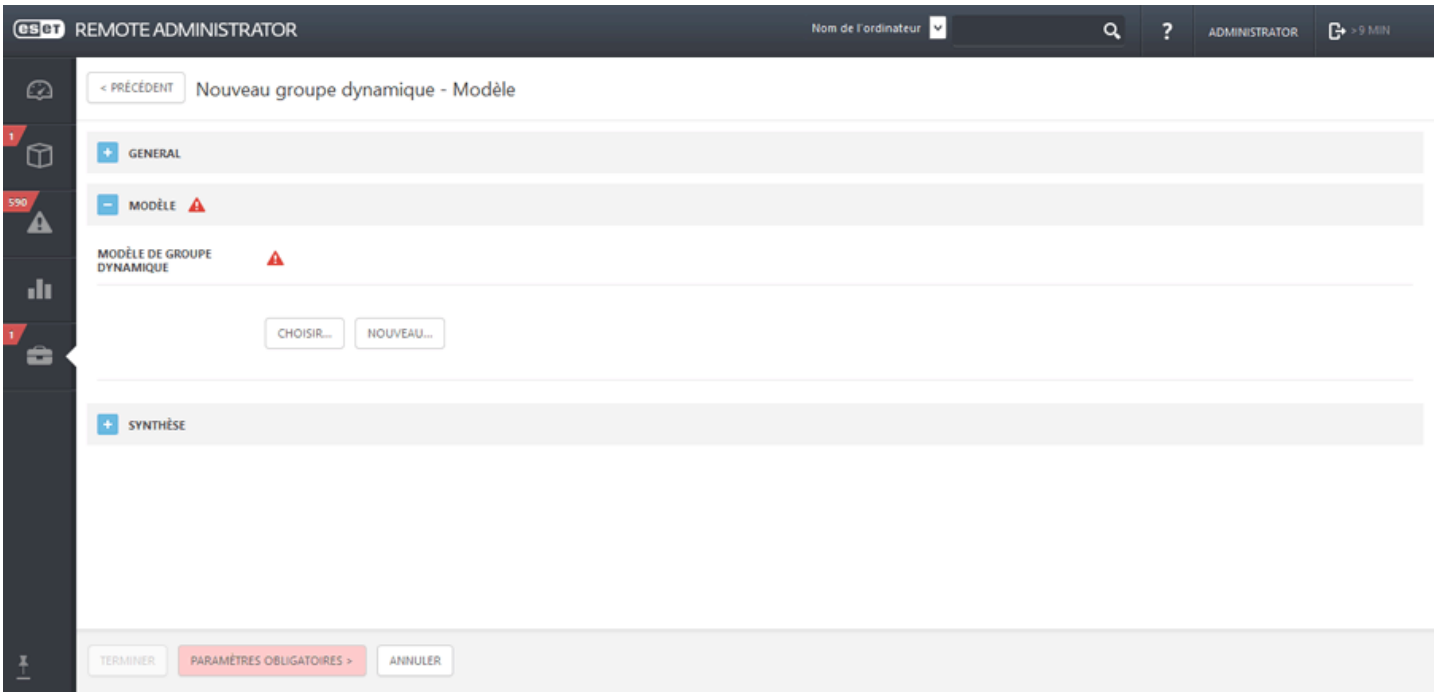
La commande **Nouveau groupe dynamique...** est également accessible depuis **Admin** > **Groupes**. Sélectionnez un groupe (dans le volet Groupes), puis cliquez sur **Groupe** dans la partie inférieure.



L'Assistant Groupe dynamique s'affiche. Saisissez un **nom** et une **description** (facultatif) pour le nouveau modèle. Les utilisateurs peuvent également modifier le groupe parent en cliquant sur le bouton **Modifier le groupe parent**.



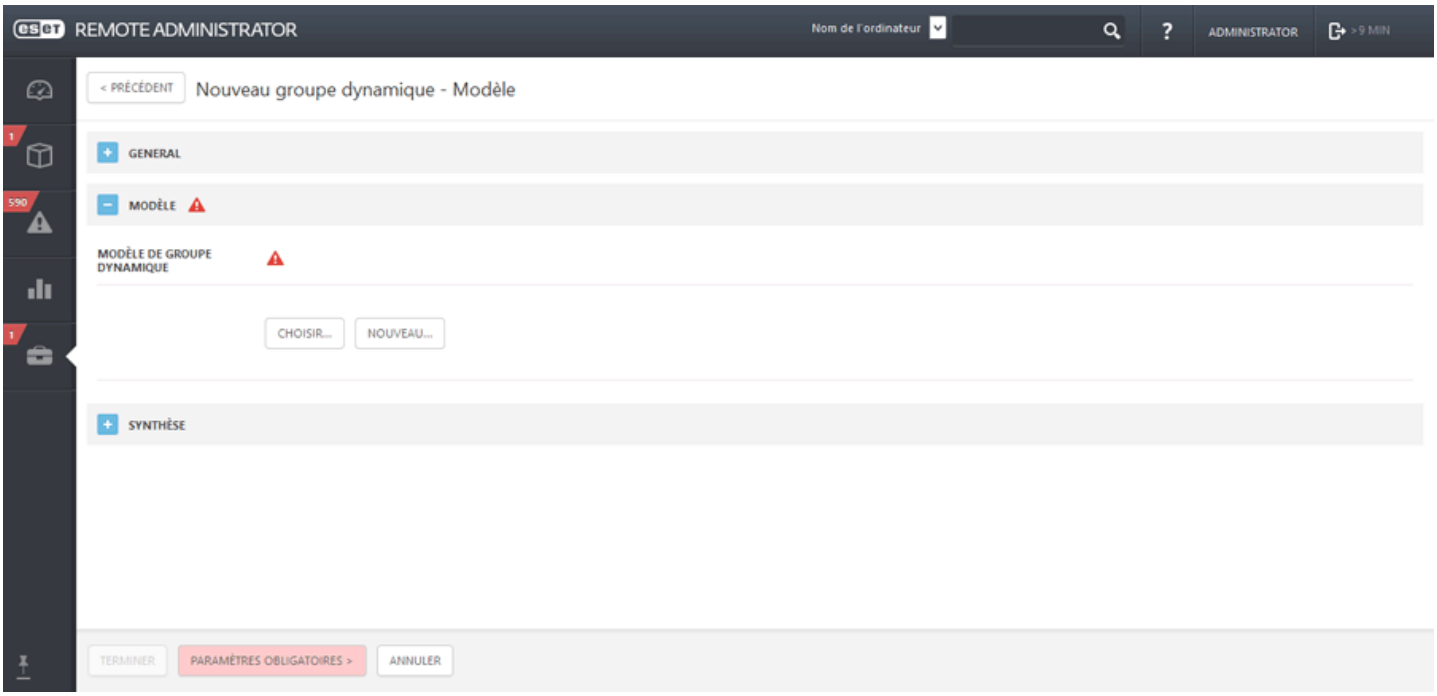
Sélectionnez un **modèle de groupe dynamique** parmi les modèles prédéfinis ou un modèle que vous avez déjà créé. Cliquez sur le bouton **Choisir**, puis sélectionnez un modèle adéquat dans la liste. Si vous n'avez pas encore créé de modèle et si aucun des modèles prédéfinis de la liste ne vous convient, cliquez sur Nouveau et suivez la procédure permettant de créer un modèle.



Le dernier écran constitue une synthèse. Le nouveau groupe apparaît sous le groupe statique parent.

4.1.8.3 Créer un groupe dynamique à l'aide d'un nouveau modèle

La procédure est identique à celle suivie lors de la création d'un groupe dynamique à l'aide d'un modèle existant jusqu'à l'étape **Modèle de groupe dynamique**, où vous devez cliquer sur Nouveau modèle de groupe dynamique pour renseigner les détails du nouveau modèle.



Une fois que vous avez terminé, le nouveau modèle est automatiquement utilisé. Celui-ci apparaît également dans la liste Modèles de groupe dynamique et peut être utilisé pour créer d'autres groupes dynamiques.

4.1.8.4 Gérer les groupes dynamiques

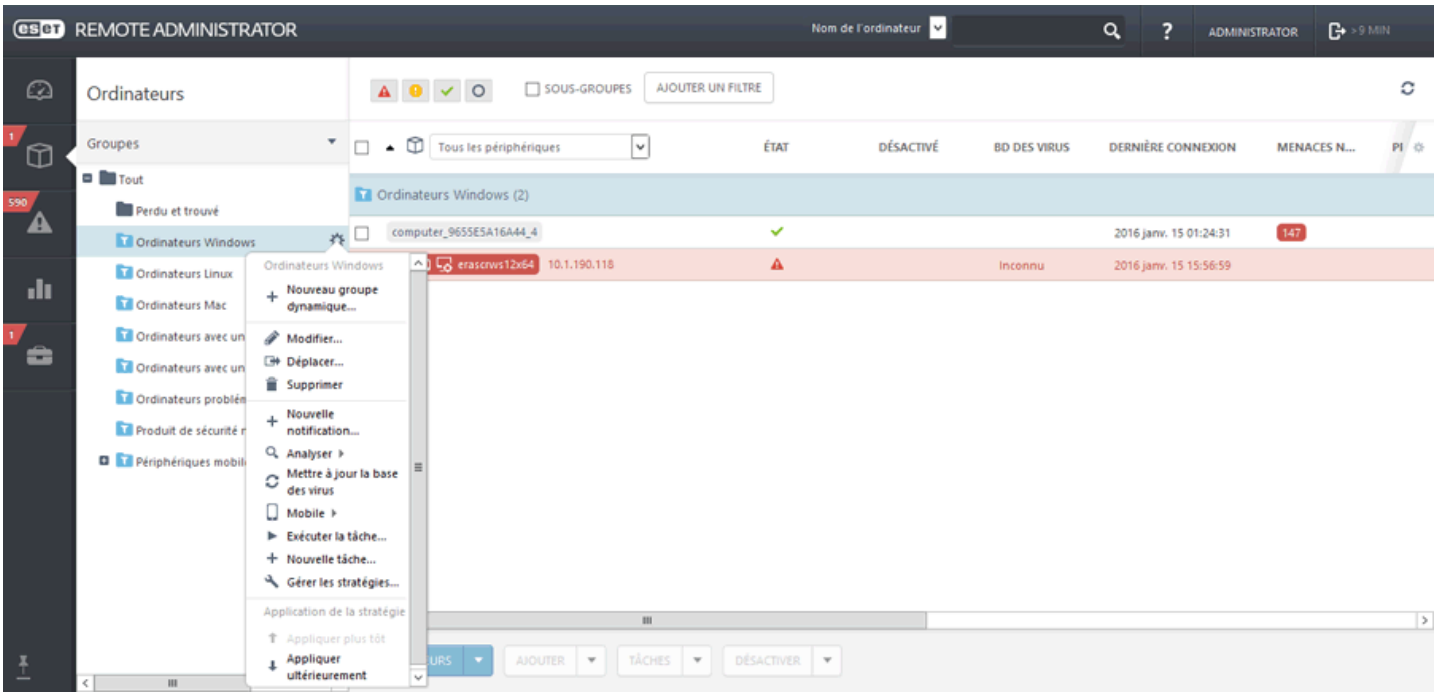
Vous pouvez créer un groupe dynamique à l'aide d'un modèle existant ou en créant un modèle qui sera utilisé pour ce groupe dynamique.

Une fois un groupe dynamique créé, vous pouvez effectuer diverses opérations sur celui-ci, notamment :

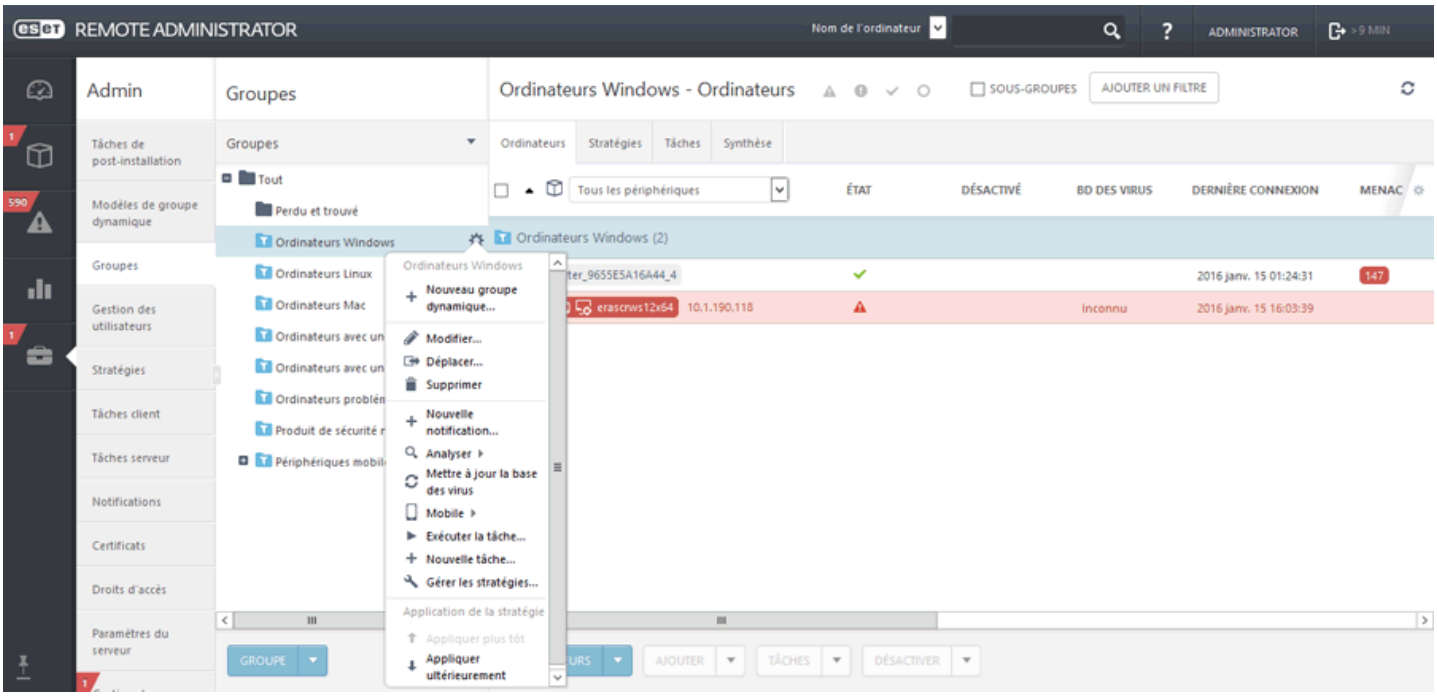
Modifier - Permet de modifier le groupe sélectionné.
Déplacer - Permet de déplacer le groupe sélectionné vers un autre groupe.
Delete - Supprime entièrement le groupe sélectionné.
Exécuter des tâches
Utiliser pour les Notifications

Vous pouvez effectuer ces opérations à partir de trois emplacements :

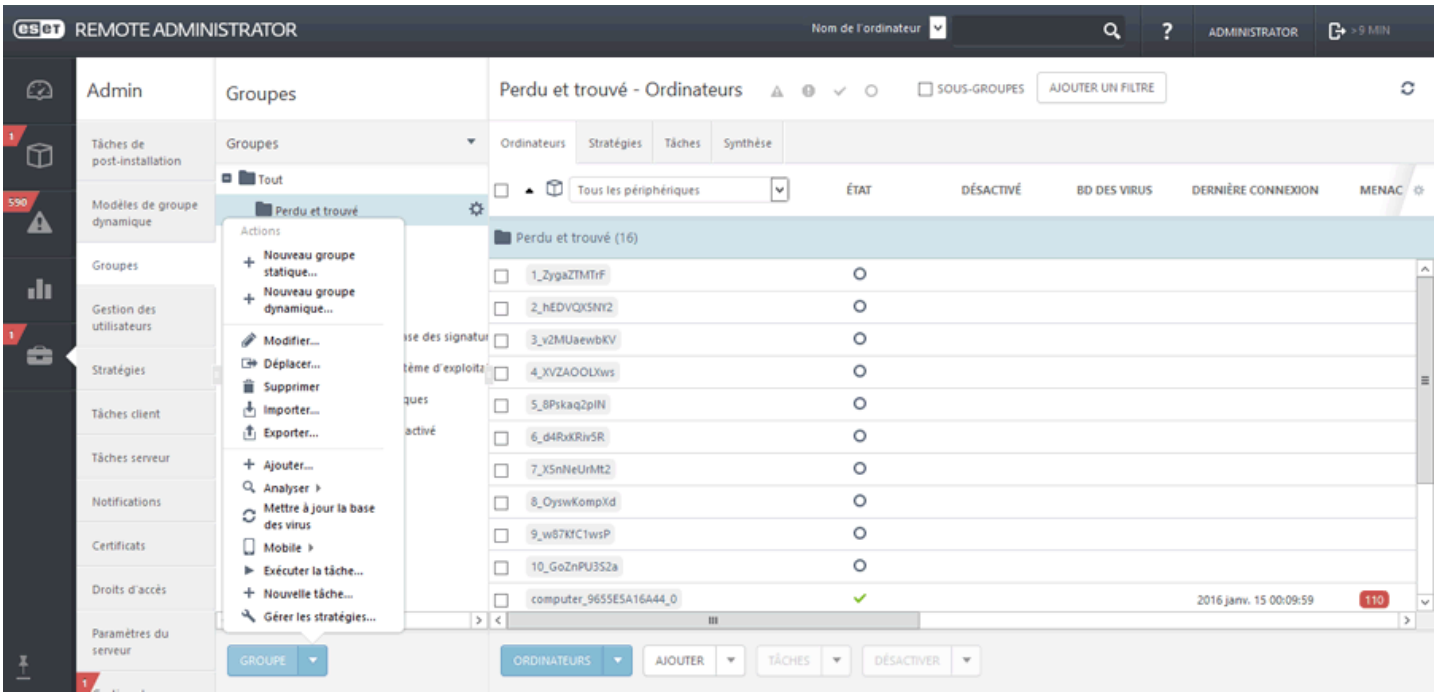
1. **Ordinateur** > **Groupes** > . et sélectionner



2. **Admin** > **Groupes** > icône ⚙.



3. **Admin** > **Groupes**, sélectionnez les groupes dynamiques à gérer, puis cliquez sur **Groupe**.



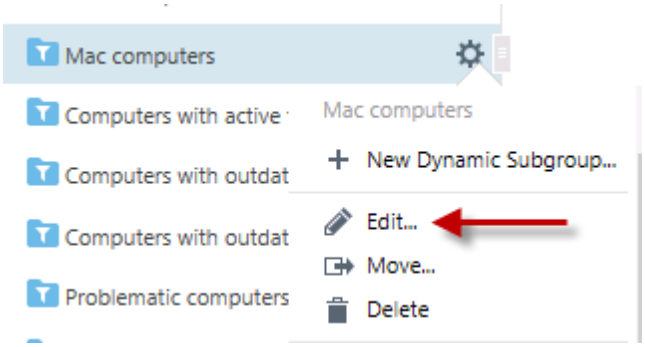
4.1.8.5 Déplacer un groupe dynamique

Cliquez sur le symbole ⚙ situé en regard du nom du groupe, puis sélectionnez **Déplacer**. Une fenêtre contextuelle s'affiche. Elle contient l'arborescence des groupes. Sélectionnez le groupe (statique ou dynamique) cible vers lequel vous souhaitez déplacer le groupe sélectionné. Le groupe cible devient un groupe parent. Vous pouvez également déplacer des groupes en les faisant glisser et en les déposant dans le groupe cible de votre choix.

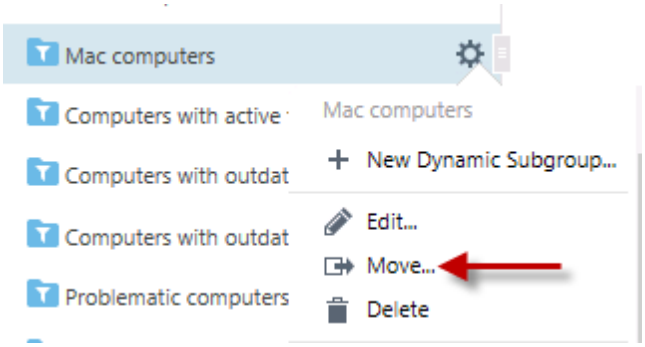
Vous devez tenir compte de quelques exceptions en ce qui concerne l'organisation des groupes. **Il n'est pas possible de déplacer un groupe statique vers un groupe dynamique**. De même, vous ne pouvez pas déplacer des groupes statiques prédéfinis (comme le groupe Perdu et trouvé) vers un autre groupe. Tous les autres groupes peuvent être déplacés librement. Un groupe dynamique peut être membre de n'importe quel autre groupe, y compris de groupes statiques.

Vous pouvez employer les méthodes suivantes pour déplacer des groupes :

Cliquez sur ⚙ > **Modifier** > **Modifier le groupe parent**.



Cliquez sur ⚙ > **Déplacer**, sélectionnez un nouveau groupe parent dans la liste, puis cliquez sur **OK**.



REMARQUE : un groupe dynamique dans un nouvel emplacement commence à filtrer les ordinateurs (selon le modèle) sans tenir compte de son emplacement précédent.

4.1.8.6 Attribuer une stratégie à un groupe dynamique

Les groupes statiques et dynamiques sont traités de la même manière en ce qui concerne l'attribution de stratégie. Pour obtenir des instructions pour l'attribution d'une stratégie à un groupe, cliquez ici.

4.1.8.7 Attribuer une tâche à un groupe dynamique

Les groupes statiques et dynamiques sont traités de la même manière en ce qui concerne l'attribution de tâche. Pour obtenir des instructions pour l'attribution d'une tâche à un groupe, cliquez ici.

4.1.8.8 Règles d'un modèle de groupe dynamique

Lorsque vous définissez des règles pour un modèle de groupe dynamique, vous pouvez utiliser des opérateurs différents pour différentes conditions.

- À quel moment un ordinateur devient-il membre d'un groupe dynamique ?
- Règles et opérateurs logiques
- Type d'opération
- Cas d'utilisation : créer un modèle de groupe dynamique spécifique
- Évaluation des règles de modèle

4.1.8.8.1 Quand un ordinateur figure-t-il dans un groupe dynamique ?

Pour qu'un ordinateur devienne membre d'un groupe dynamique spécifique, il doit satisfaire à certaines conditions. Celles-ci sont définies dans un modèle de groupe dynamique. Chaque modèle est composé d'une ou de plusieurs règles. Vous pouvez spécifier ces règles lors de la création d'un modèle.

- Certaines informations concernant la condition actuelle d'un ordinateur client sont stockées par l'Agent. La condition de l'ordinateur est évaluée par l'Agent selon les règles du modèle.
- Le jeu de conditions requis pour qu'un client puisse rejoindre un groupe dynamique est défini dans vos modèles de groupe dynamique ; les clients sont évalués en vue de leur inclusion à des groupes dynamiques chaque fois qu'ils entrent dans ESET Remote Administrator. Si le client satisfait aux valeurs spécifiées dans le modèle de groupe dynamique, il est automatiquement assigné à ce groupe.
- Les groupes dynamiques peuvent être comparés à des filtres basés sur l'état de l'ordinateur. Un ordinateur peut correspondre à plusieurs filtres et être donc attribué à plusieurs groupes dynamiques. C'est ce qui distingue les groupes dynamiques des groupes statiques, puisqu'un même client ne peut pas appartenir à plusieurs groupes statiques.

4.1.8.8.2 Description des opérations

Si vous spécifiez plusieurs règles (conditions), vous devez sélectionner l'opération qui doit être utilisée pour les associer. Selon le résultat, un ordinateur client est ou n'est pas ajouté à un groupe dynamique qui utilise le modèle donné.

ET : toutes les conditions doivent être vraies.
Vérifie si toutes les conditions sont évaluées de manière positive. L'ordinateur doit satisfaire tous les paramètres requis.

OU : au moins une des conditions doit être vraie.
Vérifie si l'une des conditions est évaluée de manière positive. L'ordinateur doit satisfaire l'un des paramètres requis.

NON ET : au moins une des conditions doit être fausse.
Vérifie si l'une des conditions ne peut pas être évaluée de manière positive. L'ordinateur ne doit pas satisfaire au moins un paramètre.

NI : toutes les conditions doivent être fausses.
Vérifie si toutes les conditions ne peuvent pas être évaluées de manière positive. L'ordinateur ne satisfait pas tous les paramètres requis.

REMARQUE : il n'est pas possible de combiner des opérations. Une seule opération est utilisée par modèle de groupe dynamique et s'applique à toutes ses règles.

4.1.8.8.3 Règles et connecteurs logiques

Une règle est composée d'un élément, d'un opérateur logique et d'une valeur définie.

Lorsque vous cliquez sur **+ Ajouter** une règle, une fenêtre indépendante s'ouvre. Elle contient une liste d'éléments divisés en catégorie. Par exemple :

Logiciel installé > **Nom de l'application**
Cartes réseau > **Adresse MAC**
Édition du SE > **Nom du SE**

Pour créer une règle, sélectionnez un élément, choisissez un opérateur logique et spécifiez une valeur. La règle est évaluée selon la valeur spécifiée et l'opérateur logique utilisé.

Les types de valeurs acceptées sont les suivants : nombre(s), chaîne(s), énumération(s), adresse(s) IP, masques de produit et ID d'ordinateur. Chaque type de valeur est associé à des opérateurs logiques différents. ERA Web Console n'affiche automatiquement que les opérateurs pris en charge.

- **= (égal)** : les valeurs du symbole et du modèle doivent correspondre. Les chaînes sont comparées sans tenir compte de la casse.
- **≠ (différent de)** : les valeurs du symbole et du modèle ne doivent pas correspondre. Les chaînes sont comparées sans tenir compte de la casse.
- **> (supérieur à)** : la valeur du symbole doit être supérieure à celle du modèle. Cet opérateur peut être également utilisé pour créer une comparaison de plages pour les symboles d'adresse IP.
- **≥ (supérieur ou égal à)** : la valeur du symbole doit être supérieure ou égale à celle du modèle. Cet opérateur peut être également utilisé pour créer une comparaison de plages pour les symboles d'adresse IP.
- **< (inférieur à)** : la valeur du symbole doit être inférieure à celle du modèle. Cet opérateur peut être également utilisé pour créer une comparaison de plages pour les symboles d'adresse IP.
- **≤ (inférieur ou égal à)** : la valeur du symbole doit être inférieure ou égale à celle du modèle. Cet opérateur peut être également utilisé pour créer une comparaison de plages pour les symboles d'adresse IP.
- **contient** : la valeur du symbole contient celle du modèle. La recherche ne respecte pas la casse.
- **contient un préfixe** : la valeur du symbole contient le même préfixe de texte que la valeur du modèle. Les chaînes sont comparées sans tenir compte de la casse. Définit les premiers caractères de la chaîne de recherche ; par exemple, pour "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", le préfixe est "Micros", "Micr", "Microsof", etc.
- **contient un suffixe** : la valeur du symbole contient le même suffixe de texte que la valeur du modèle. Les chaînes sont comparées sans tenir compte de la casse. Définit les premiers caractères de la chaîne de recherche ; par exemple, pour "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", le suffixe est "319" ou "0.30319", etc.
- **contient un masque** : la valeur du symbole doit correspondre à un masque défini dans un modèle. La mise en forme du masque autorise n'importe quel caractère, les symboles spéciaux « * » (zéro, un ou plusieurs caractères) et « ? » (un caractère uniquement, par exemple : "6.2.*" ou "6.2.2033.?".
- **"regex"** : la valeur du symbole doit correspondre à l'expression régulière (regex) d'un modèle. L'expression régulière doit être écrite au format **Perl**.
- **dans** : la valeur du symbole doit correspondre à n'importe quelle valeur d'une liste d'un modèle. Les chaînes sont comparées sans tenir compte de la casse.
- **dans (masque de chaîne)** : la valeur du symbole doit correspondre à n'importe quel masque d'une liste d'un modèle.

Règles négatives :

IMPORTANT : les opérateurs de négation doivent être utilisés avec précaution, car en cas de journaux à plusieurs lignes, comme « application installée », toutes les lignes sont testées par rapport à ces conditions. Examinez les exemples inclus pour déterminer comment les opérateurs et les opérations de négation doivent être utilisés pour obtenir les résultats escomptés.

- **ne contient pas** : la valeur du symbole ne contient pas la valeur du modèle. La recherche ne respecte pas la casse.
- **"n'a pas de préfixe"** : la valeur du symbole ne contient pas le même préfixe de texte comme la valeur du modèle. Les chaînes sont comparées sans tenir compte de la casse.
- **"n'a pas de suffixe"** : la valeur du symbole ne contient pas de suffixe de texte comme la valeur du modèle. Les chaînes sont comparées sans tenir compte de la casse.
- **n'a pas de masque** : la valeur du symbole ne doit pas correspondre à un masque défini dans un modèle.
- **"n'est pas une expression regex"** : la valeur du symbole ne doit pas correspondre à une expression régulière (regex) d'un modèle. L'expression régulière doit être écrite au format Perl. L'opération de négation est fournie à titre d'exemple pour éviter toute réécriture.
- **"n'est pas dans"** : la valeur du symbole ne doit pas correspondre à n'importe quelle valeur de la liste d'un modèle. Les chaînes sont comparées sans tenir compte de la casse.
- **n'est pas dans (masque de chaîne)** : la valeur du symbole ne doit pas correspondre à n'importe quel masque d'une liste d'un modèle.

4.1.8.8.4 Évaluation des règles de modèle

L'évaluation des règles de modèle est gérée par ERA Agent, et non par ERA Server (seul le résultat est envoyé à ERA Server). Le processus d'évaluation s'effectue selon les règles configurées dans un modèle. La section qui suit explique le processus d'évaluation à l'aide de quelques exemples.

L'état est un ensemble d'informations diverses. Certaines sources fournissent plusieurs états dimensionnels par ordinateur (système d'exploitation, taille de la RAM, etc.). D'autres sources donnent des informations d'état multidimensionnelles (adresse IP, application installée, etc.).

Vous trouverez ci-dessous une représentation visuelle de l'état d'un client :

Cartes réseau : adresse IP	Cartes réseau : adresse MAC	Nom du SE	Version du SE	Matériel : taille de la RAM en Mo	Application installée
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Entreprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Lecteur de fichiers PDF
124.256.25.25	52-FB-E5-74-35-73				Suite Office
					Prévisions météorologiques

L'état est composé de groupes d'informations. Un groupe de données fournit toujours des informations cohérentes organisées en lignes. Le nombre de lignes par groupe peut varier.

Les conditions sont évaluées par groupe et par ligne. S'il existe plus de conditions concernant les colonnes d'un groupe, seules les valeurs de la même ligne sont prises en compte.

Exemple 1 :

Pour cet exemple, prenez en compte la condition suivante :

```
Cartes réseau.Adresse IP = 10.1.1.11 ET Cartes réseau.Adresse MAC = 4A-64-3F-10-FC-75
```

Cette règle ne correspond à aucun ordinateur, car il n'existe aucune ligne dans laquelle les deux conditions sont vraies.

Cartes réseau : adresse IP	Cartes réseau : adresse MAC	Nom du SE	Version du SE	Matériel : taille de la RAM en Mo	Application installée
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Entreprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Lecteur de fichiers PDF
124.256.25.25	52-FB-E5-74-35-73				Suite Office
					Prévisions météorologiques

Exemple 2 :

Pour cet exemple, prenez en compte la condition suivante :

```
Cartes réseau.Adresse IP = 192.168.1.2 ET Cartes réseau.Adresse MAC = 4A-64-3F-10-FC-75
```

Cette fois, les deux conditions correspondent à des cellules d'une même ligne. La règle dans son ensemble est donc évaluée comme VRAIE. Un ordinateur est sélectionné.

Cartes réseau : adresse IP	Cartes réseau : adresse MAC	Nom du SE	Version du SE	Matériel : taille de la RAM en Mo	Application installée
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Entreprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Lecteur de fichiers PDF
124.256.25.25	52-FB-E5-74-35-73				Suite Office
					Prévisions météorologiques

Exemple 3 :

Pour les conditions avec l'opérateur OU (au moins une condition doit être VRAIE), telles que :

```
Cartes réseau.Adresse IP = 10.1.1.11 OU Cartes réseau.Adresse MAC = 4A-64-3F-10-FC-75
```

La règle est VRAIE pour deux lignes, dans la mesure ou une condition sur les deux doit être remplie. Un ordinateur est sélectionné.

Cartes réseau : adresse IP	Cartes réseau : adresse MAC	Nom du SE	Version du SE	Matériel : taille de la RAM en Mo	Application installée
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Entreprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Lecteur de fichiers PDF
124.256.25.25	52-FB-E5-74-35-73				Suite Office
					Prévisions météorologiques

4.1.8.8.5 Comment automatiser ESET Remote Administrator

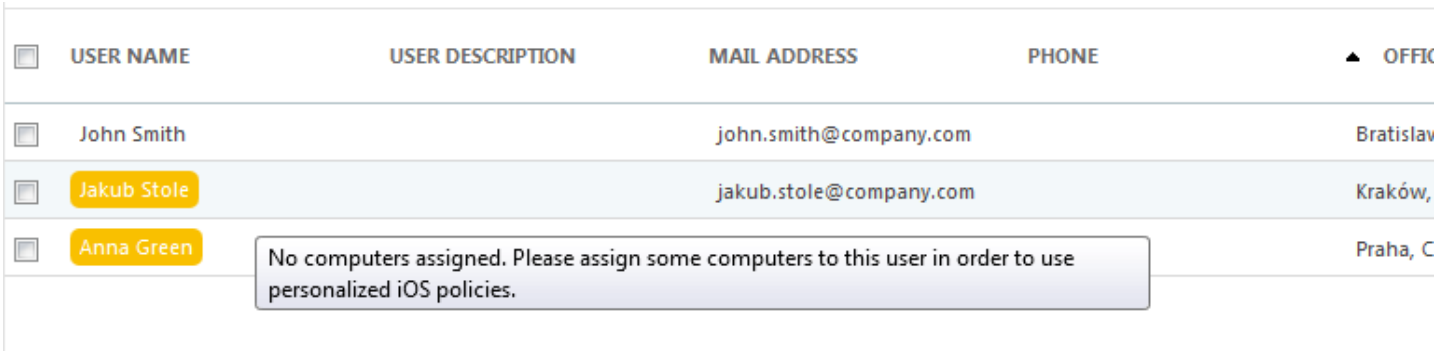
1. Créez un groupe dynamique, par exemple : « Ordinateurs infectés ».
2. Créez une tâche, pour une analyse approfondie, et attribuez-la au groupe dynamique Ordinateurs infectés (la tâche est déclenchée lorsque des clients deviennent membres du groupe dynamique).
3. Créez une stratégie spécifique (dans le cas présent, une « stratégie d'isolement »). Lorsqu'un produit de sécurité ESET est installé, créez une règle de pare-feu qui bloque tout le trafic, à l'exception des connexions à ESET Remote Administrator.
4. Créez un modèle de notification pour les ordinateurs infectés (vous pouvez spécifier diverses conditions). Une notification est déclenchée pour vous avertir de la propagation d'une menace.

À l'aide de la même technique, vous pouvez automatiser les mises à jour de produit et de système d'exploitation, les analyses, les activations automatiques des produits nouvellement ajoutés avec une licence présélectionnée et d'autres tâches.

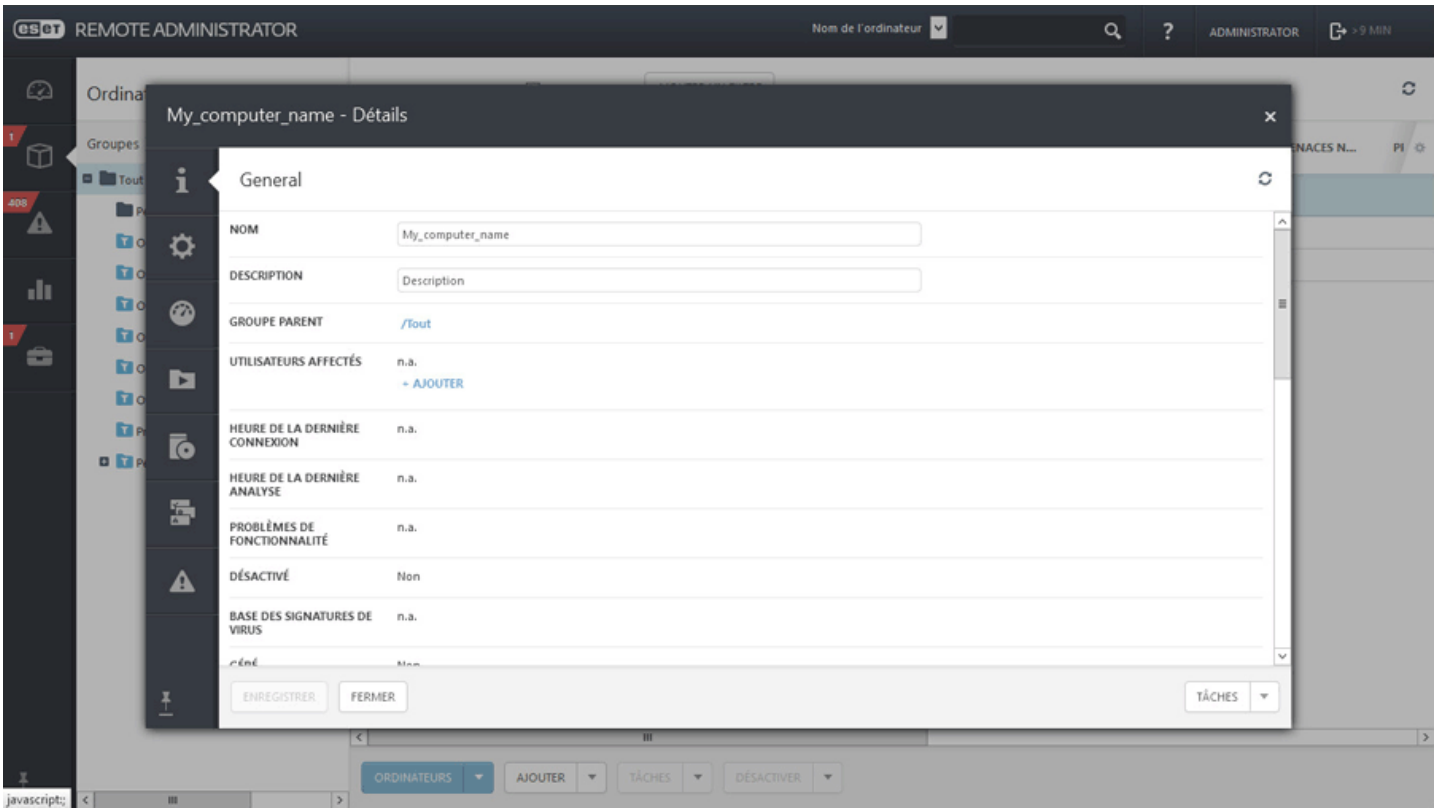
4.2 Gestion des utilisateurs

Cette section vous permet de gérer les utilisateurs et les groupes d'utilisateurs pour la gestion des périphériques mobiles iOS. La gestion des périphériques mobiles s'effectue en utilisant des stratégies attribuées à des périphériques iOS. Nous vous recommandons toutefois de synchroniser les utilisateurs avec Active Directory au préalable. Vous pourrez ensuite modifier des utilisateurs ou ajouter des attributs personnalisés.

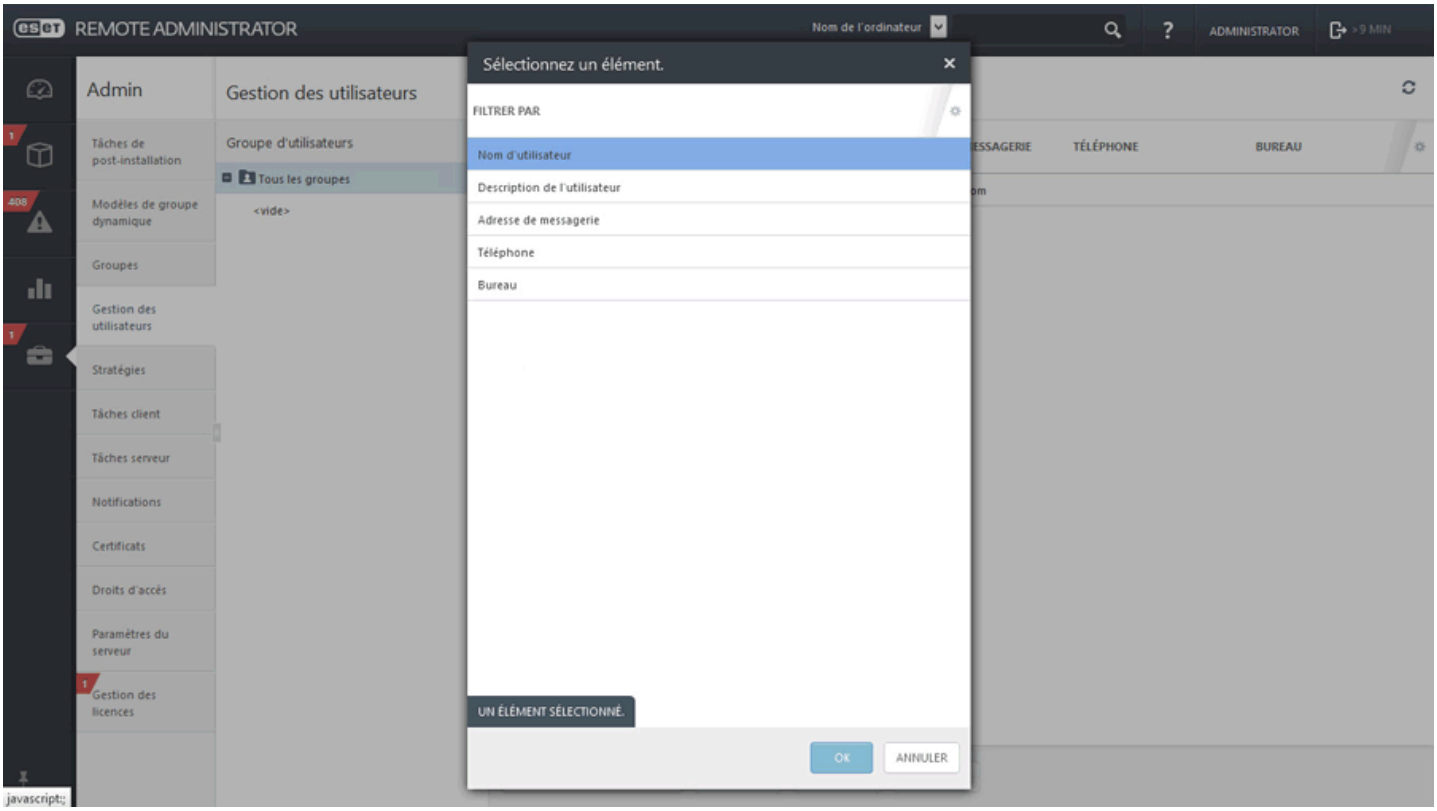
- Un utilisateur surligné en orange n'a aucun périphérique attribué. Cliquez sur l'utilisateur, sélectionnez Modifier..., puis cliquez sur **Ordinateurs attribués** pour afficher les détails de cet utilisateur. Cliquez sur **Ajouter des ordinateurs** pour attribuer des ordinateurs ou un ou des périphériques à cet utilisateur.



- Vous pouvez également ajouter ou supprimer des **utilisateurs attribués** depuis Détails de l'ordinateur. Lorsque vous êtes dans Ordinateurs ou Groupes, sélectionnez un ordinateur ou un périphérique mobile, puis cliquez sur **Détails**. L'utilisateur peut être attribué à plusieurs ordinateurs/périphériques mobiles.

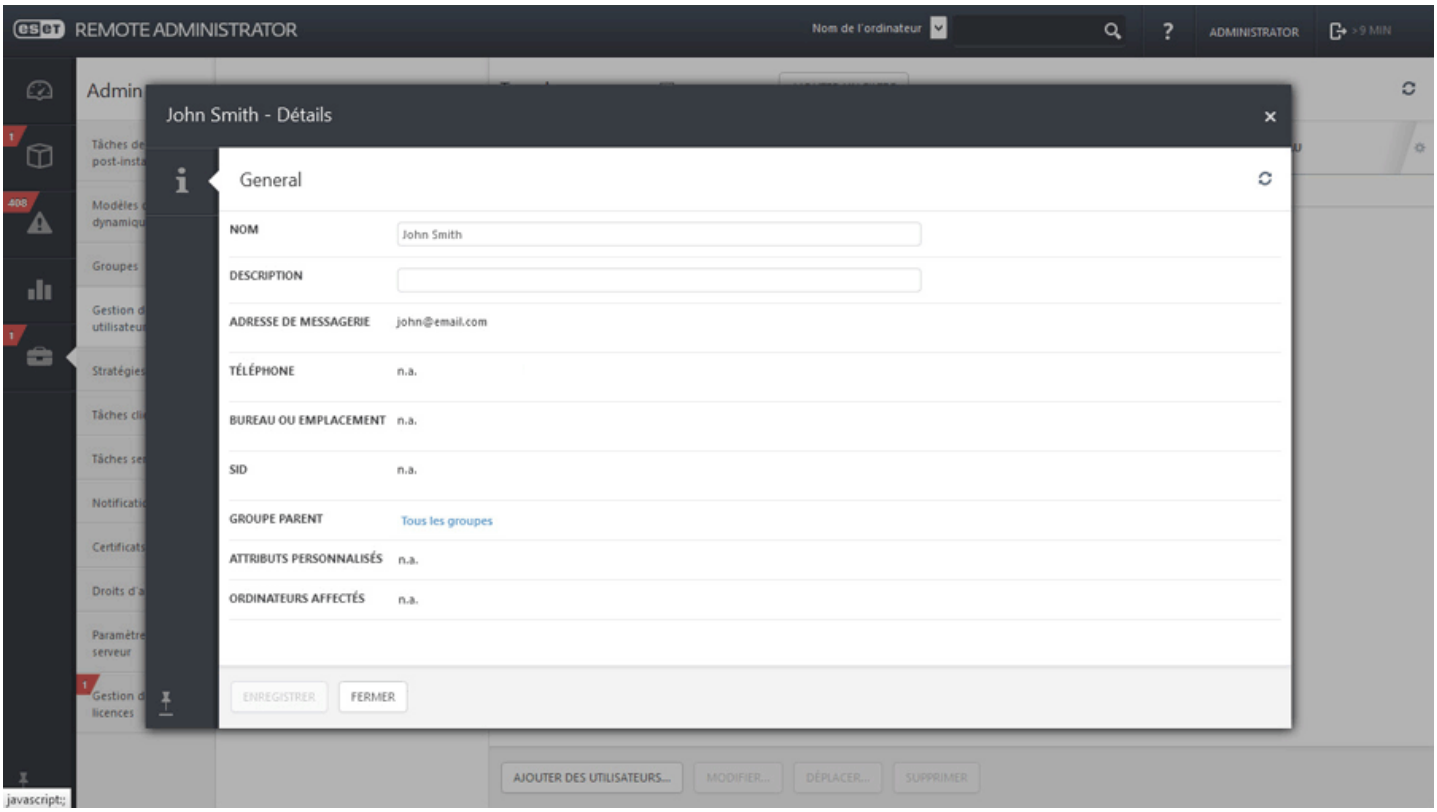


- Vous pouvez filtrer les utilisateurs à l'aide des filtres situés dans la partie supérieure de la page. Cliquez sur **Ajouter un filtre**, puis sélectionnez un élément dans la liste.



- **Actions de gestion des utilisateurs :**

Détails....
Le menu des détails de l'utilisateur présent des informations telles que l'adresse électronique, le bureau, l'emplacement, des attributs personnalisés et les ordinateurs attribués. L'utilisateur peut avoir plusieurs ordinateurs/périphériques mobiles attribués. Vous pouvez modifier le nom, la description et le groupe parent de l'utilisateur. Les attributs personnalisés affichés ici sont ceux qui peuvent être utilisés lors de la création de stratégies.



Nouveau groupe d'utilisateurs...
Vous pouvez créer un groupe d'utilisateurs.

Ajouter des utilisateurs...
Ajoutez un nouvel utilisateur ou des nouveaux utilisateurs.

Synchroniser
Créez une tâche serveur Synchronisation utilisateur.

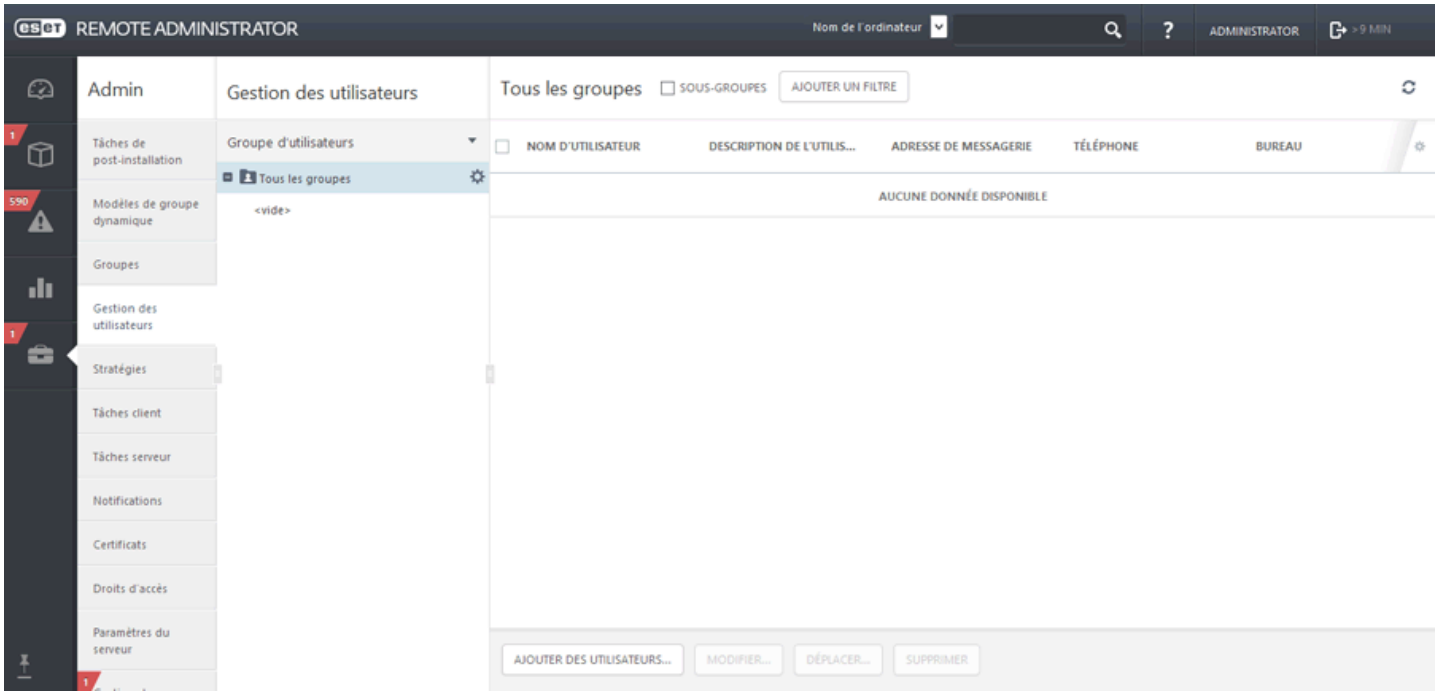
Modifier...
Cette option permet de modifier l'utilisateur ou le **groupe d'utilisateurs** sélectionné.

Déplacer...
Vous pouvez sélectionner un utilisateur ou un groupe d'utilisateurs et le déplacer comme sous-groupe d'un autre groupe d'utilisateurs.

Supprimer
Supprime complètement l'utilisateur ou le groupe d'utilisateurs sélectionné.

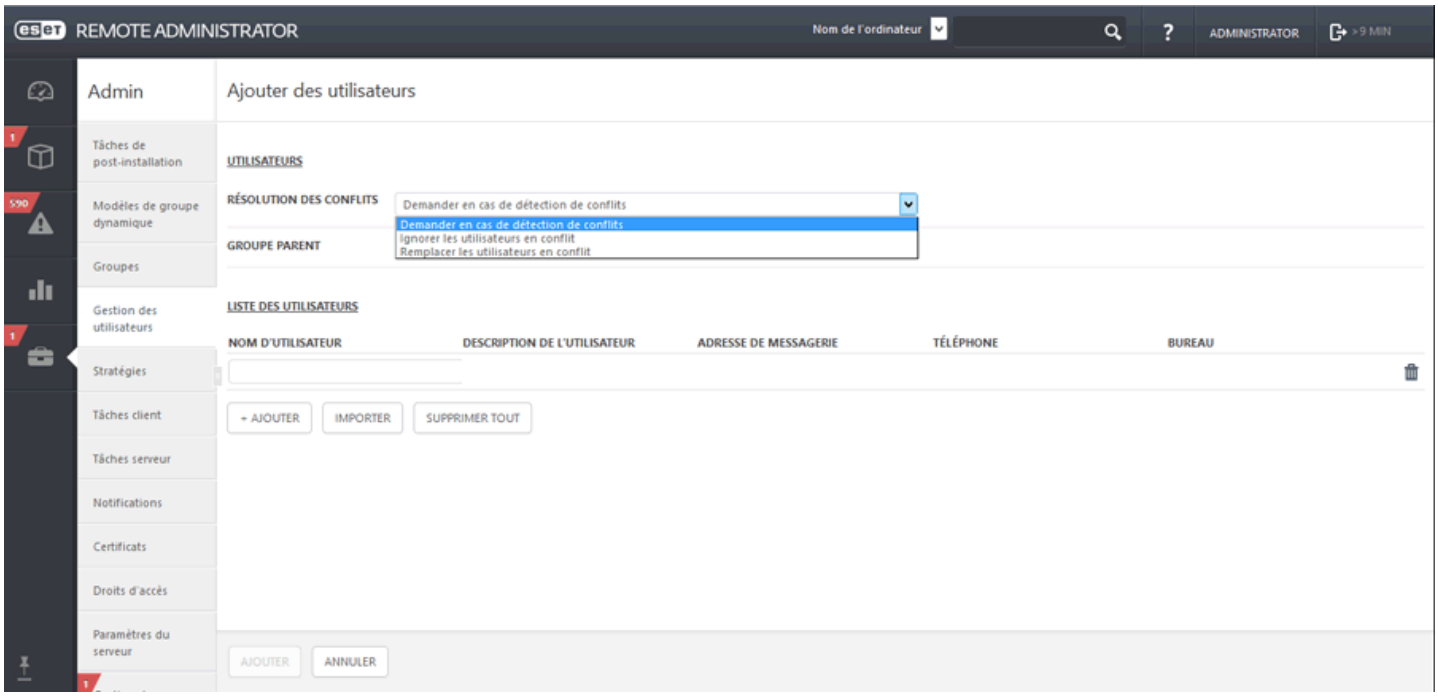
4.2.1 Ajouter de nouveaux utilisateurs

Cliquez sur **Admin** > **Gestion des utilisateurs** > **Ajouter des utilisateurs...** pour ajouter des utilisateurs qui n'ont pas été trouvés ou ajoutés automatiquement pendant la synchronisation des utilisateurs.



Saisissez le nom de l'utilisateur à ajouter dans le champ **Nom d'utilisateur**. Utilisez le menu déroulant **Résolution des conflits** pour sélectionner l'action à exécuter si un utilisateur que vous ajoutez existe déjà dans ERA :

- **Demander en cas de détection de conflits** : lorsqu'un conflit est détecté, le programme vous demande de sélectionner une action (voir les options ci-dessous).
  - **Ignorer les utilisateurs en conflit** : les utilisateurs portant le même nom ne sont pas ajoutés. Cela permet aussi de s'assurer que les attributs personnalisés de l'utilisateur existant dans ERA sont conservés (ils ne sont pas remplacés par les données d'Active Directory).
  - **Remplacer les utilisateurs en conflit :** l'utilisateur existant dans ERA est remplacé celui d'Active Directory. Si deux utilisateurs disposent du même SID, l'utilisateur existant dans ERA est supprimé de son précédent emplacement (même si l'utilisateur était dans un autre groupe).



Cliquez sur + Ajouter pour ajouter d'autres utilisateurs. Si vous souhaitez ajouter simultanément plusieurs utilisateurs, cliquez sur **Importer** pour charger un fichier `csv` qui contient la liste des utilisateurs à ajouter. Vous pouvez éventuellement saisir une **description** des utilisateurs pour simplifier leur identification.

Lorsque vous avez terminé vos modifications, cliquez sur **Ajouter**. Les utilisateurs apparaissent dans le groupe parent que vous avez spécifié.

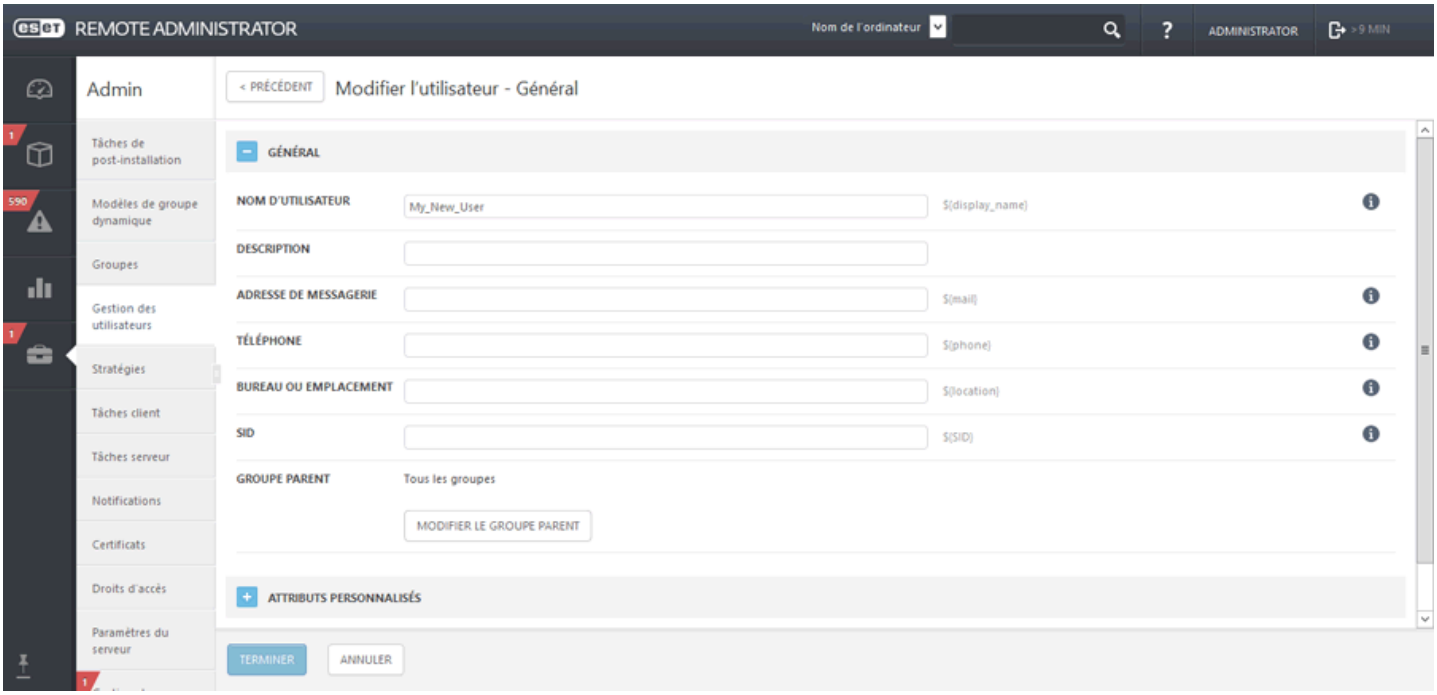
4.2.2 Modifier des utilisateurs

Vous pouvez modifier les détails d'un utilisateur, tels que les informations **de base**, les **attributs personnalisés** et les **ordinateurs attribués**.

REMARQUE : lorsque vous exécutez une tâche Synchronisation utilisateur pour les utilisateurs qui disposent d'attributs personnalisés, définissez le paramètre Gestion des collisions de création d'utilisateur sur Ignorer. Si vous ne le faites pas, les données utilisateur seront écrasées par celles provenant d'Active Directory.

Général

Si vous avez utilisé une tâche Synchronisation utilisateur pour créer l'utilisateur et si certains champs sont vides, vous pouvez, au besoin, les spécifier manuellement.

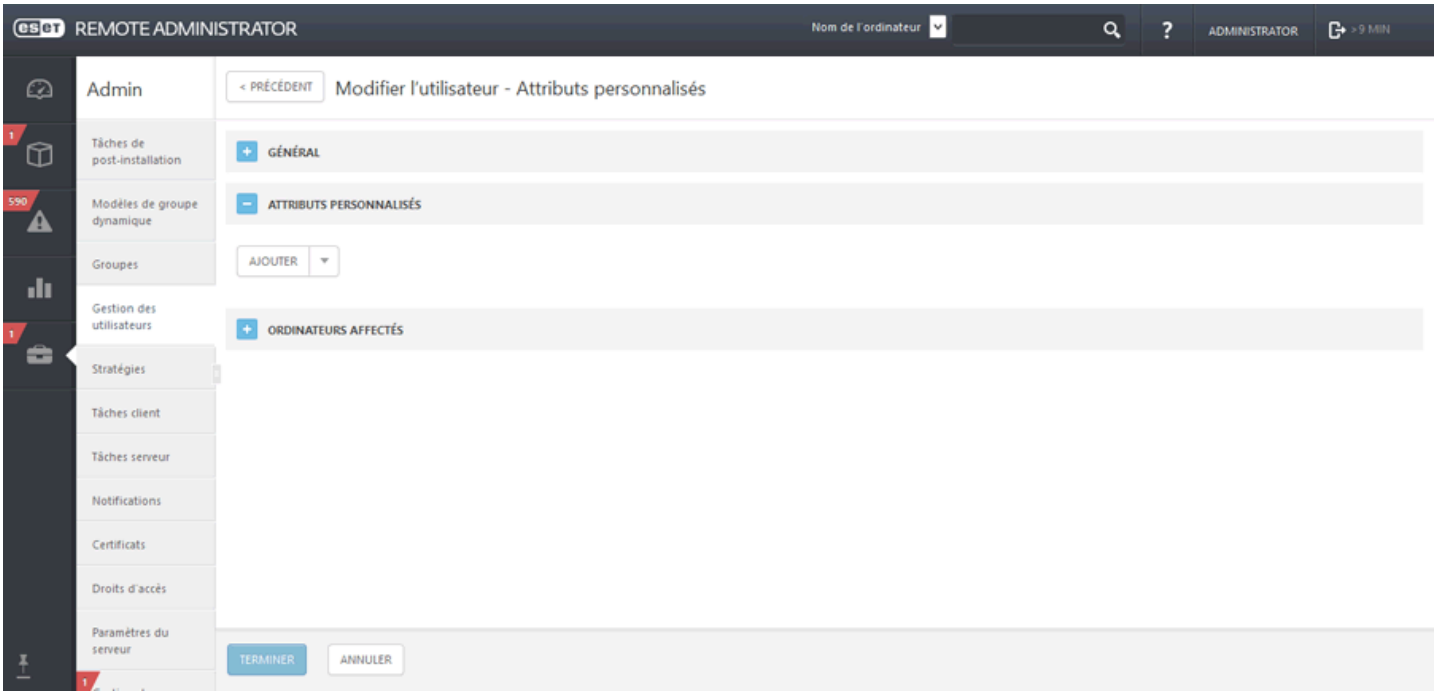


Attributs personnalisés

Vous pouvez modifier des attributs personnalisés existants ou en ajouter de nouveaux. Pour en ajouter de nouveau, cliquez sur **Ajouter** et sélectionnez dans les catégories :

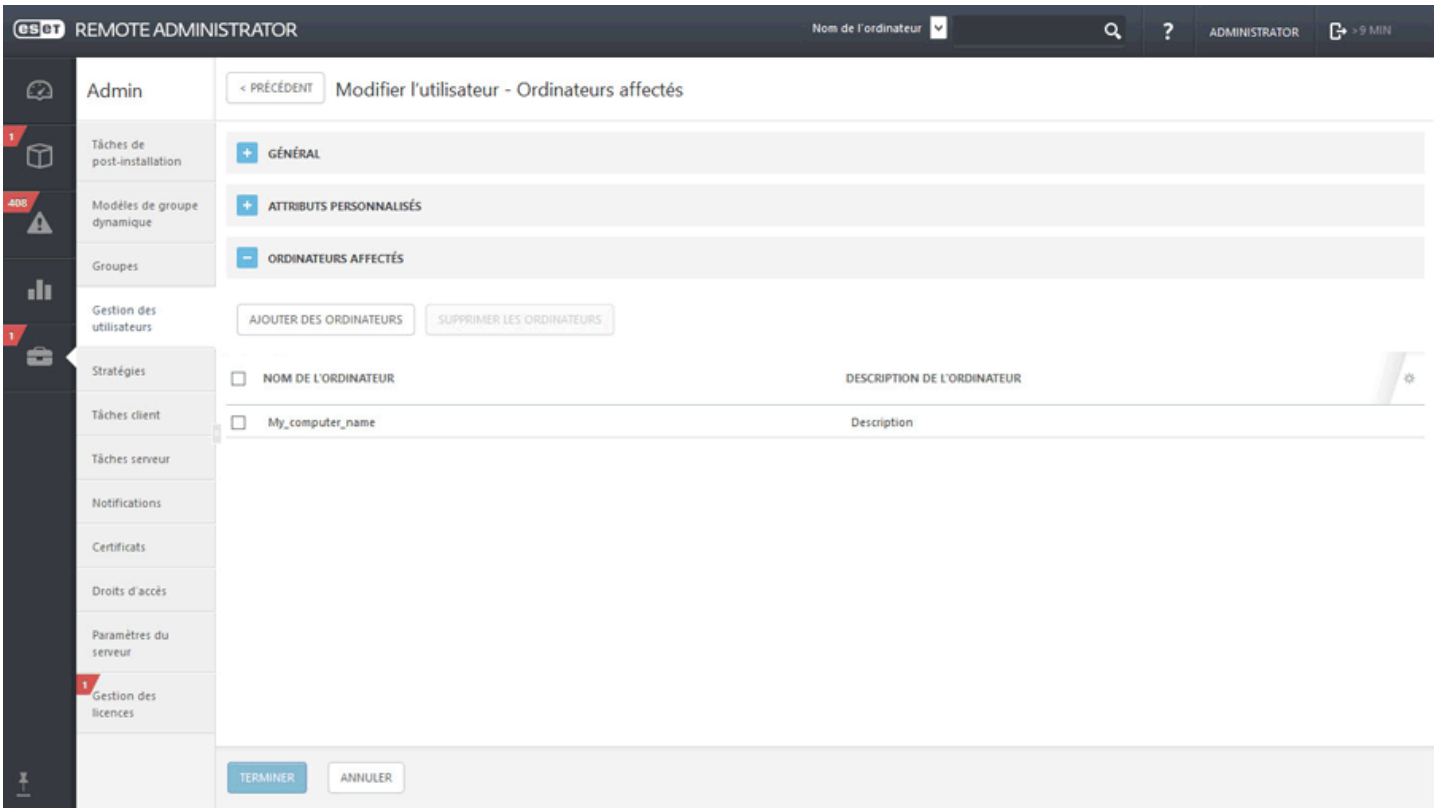
- **Comptes Wi-Fi :** Il est possible d'utiliser des profils pour pousser les paramètres Wi-Fi de l'entreprise directement vers des périphériques gérés.
- **Comptes VPN :** Vous pouvez configurer un VPN avec les informations d'identification, les certificats et autres informations requises pour que le VPN soit immédiatement accessible aux utilisateurs.
- **Comptes de messagerie** : Cette catégorie est destinée à tout compte de messagerie qui utilise les spécifications IMAP ou POP3. Si vous utilisez un serveur Exchange, choisissez les paramètres Exchange ActiveSync ci-dessous.
- **Comptes Exchange** : Si votre entreprise utilise Microsoft Exchange, vous pouvez définir tous les paramètres ici pour réduire le temps de configuration de l'accès des utilisateurs à la messagerie, au calendrier et aux contacts.
- **LDAP (alias d'attribut) :** Cela s'avère tout particulièrement pratique si votre entreprise utilise LDAP pour les contacts. Vous pouvez associer les champs des contacts aux champs iOS correspondants.
- **CalDAV :** Cette élément contient les paramètres pour tout calendrier qui utilise les spécifications CalDAV.
- **CardDAV :** Les informations peuvent être définies ici pour tous les contacts synchronisés au moyen de la spécification CardDAV.
- **Calendriers avec abonnement :** Si des calendriers CalDAV sont configurés, il est possible de configurer ici l'accès en lecture seule aux calendriers d'autres utilisateurs.

Certains des champs deviendront un attribut ensuite utilisable lors de la création d'une stratégie pour périphérique mobile iOS sous la forme d'une variable (espace réservé). Par exemple, nom de connexion `${exchange_login/exchange}` ou adresse électronique `${exchange_email/exchange}`.



Ordinateurs affectés

Vous pouvez sélectionner ici des ordinateurs/périphériques mobiles individuels. Pour ce faire, cliquez sur **Ajouter des ordinateurs -** tous les groupes statiques et dynamiques avec leurs membres seront affichés. Utilisez les cases à cocher pour effectuer votre sélection, puis cliquez sur **OK**.



Résumé

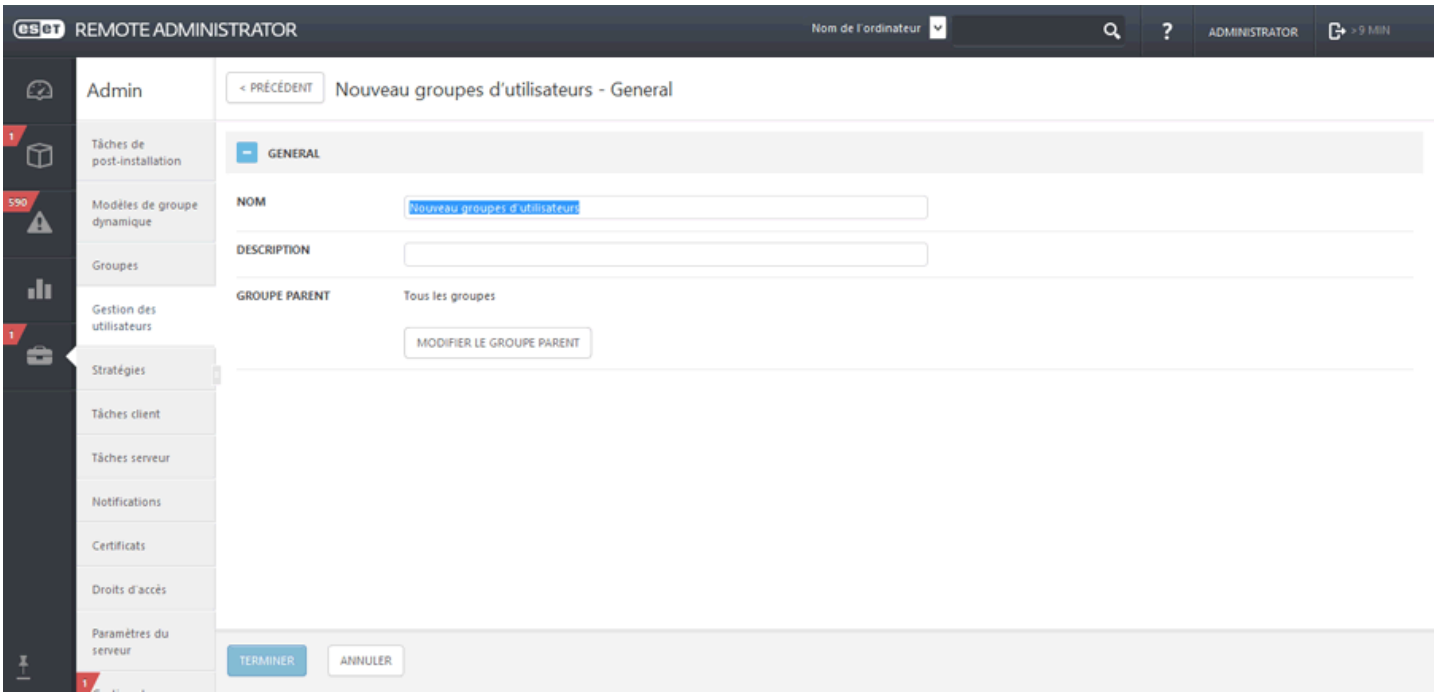
Passez en revue les paramètres de ce compte utilisateur, puis cliquez sur **Terminer**.

4.2.3 Créer un groupe d'utilisateurs

Cliquez sur Admin > **Gestion des utilisateurs** > ⚙, puis sélectionnez + **Nouveau groupe d'utilisateurs...**

Général

Saisissez un **nom** et une **description** (facultatif) pour le nouveau groupe d'utilisateurs. Par défaut, le groupe parent correspond au groupe que vous avez sélectionné lorsque vous avez commencé à créer le groupe d'utilisateurs. Si vous souhaitez modifier le groupe parent, cliquez sur **Modifier le groupe parent**, puis sélectionnez-en un autre dans l'arborescence. Cliquez sur **Terminer** pour créer le groupe d'utilisateurs.



Vous pouvez attribuer des autorisations spécifiques à ce groupe d'utilisateurs dans Droits d'accès en utilisant des jeux d'autorisations (voir la section **Groupes d'utilisateurs**). De cette manière, vous pouvez spécifier quels utilisateurs spécifiques de la Console ERA peuvent gérer quels groupes d'utilisateurs spécifiques. Vous pouvez même limiter l'accès de ces utilisateurs à d'autres fonctions ERA, si vous le souhaitez. Ces utilisateurs ne gèrent alors que des groupes d'utilisateurs.

4.3 Stratégies

Les stratégies servent à transmettre des configurations spécifiques aux produits ESET s'exécutant sur les ordinateurs clients. Vous pouvez ainsi appliquer la configuration sans avoir à configurer manuellement le produit ESET de chaque client. Une stratégie peut être appliquée directement à des ordinateurs distincts et à des groupes (statiques et dynamiques). Vous pouvez également attribuer plusieurs stratégies à un ordinateur ou à un groupe, contrairement aux versions ESET Remote Administrator 5 et antérieures dans lesquelles une seule stratégie pouvait être appliquée à un produit ou composant.

- **Application des stratégies**

Les stratégies sont appliquées dans l'ordre dans lequel les groupes statiques sont disposés. Cela n'est pas le cas pour les groupes dynamiques, où les groupes dynamiques enfants sont d'abord parcourus. Vous pouvez ainsi appliquer des stratégies avec un plus grand impact au niveau supérieur de l'arborescence des groupes et des stratégies plus spécifiques pour les sous-groupes. Grâce à des stratégies correctement configurées associées à des indicateurs, un utilisateur ERA ayant accès aux groupes situés à un niveau supérieur de l'arborescence peut remplacer les stratégies des groupes de niveau inférieur. L'algorithme est expliqué en détail dans la section Application des stratégies aux clients.

- **Fusion des stratégies**

Une stratégie appliquée à un client est généralement le résultat de plusieurs stratégies fusionnées en une seule stratégie finale.

REMARQUE : il est recommandé d'attribuer des stratégies plus génériques (des paramètres généraux tels que la mise à jour du serveur, par exemple) aux groupes dont le niveau est supérieur dans l'arborescence des groupes. Des stratégies plus spécifiques (des paramètres de contrôle de périphérique, par exemple) doivent être appliquées aux groupes de niveau inférieur. La stratégie de niveau inférieur remplace généralement les paramètres des stratégies de niveau supérieur lors de la fusion (à moins que des indicateurs de stratégie n'aient été définis).

REMARQUE : lorsqu'une stratégie est en place et que vous souhaitez la supprimer, la configuration des ordinateurs clients n'est pas rétablie une fois la stratégie supprimée. La configuration conservée est celle de la dernière stratégie appliquée aux clients. Il en est de même lorsqu'un ordinateur devient membre d'un groupe dynamique auquel une stratégie spécifique qui modifie les paramètres de l'ordinateur est appliquée. Ces paramètres sont conservés même si l'ordinateur ne figure plus dans le groupe dynamique. Pour cette raison, il est recommandé de créer une stratégie avec des paramètres par défaut et de l'appliquer au groupe racine (**Tous**) pour que les valeurs par défaut de ces paramètres soient rétablis dans une situation de ce type. Ainsi, lorsqu'un ordinateur ne figure plus dans un groupe dynamique qui a modifié ses paramètres, l'ordinateur retrouve les paramètres par défaut.

4.3.1 Assistant Stratégies

Vous pouvez utiliser des stratégies pour configurer votre produit ESET comme vous le feriez dans la fenêtre Configuration avancée de l'interface utilisateur graphique du produit. Contrairement aux stratégies d'Active Directory, les stratégies d'ERA ne peuvent pas comporter de scripts ou de séries de commandes.

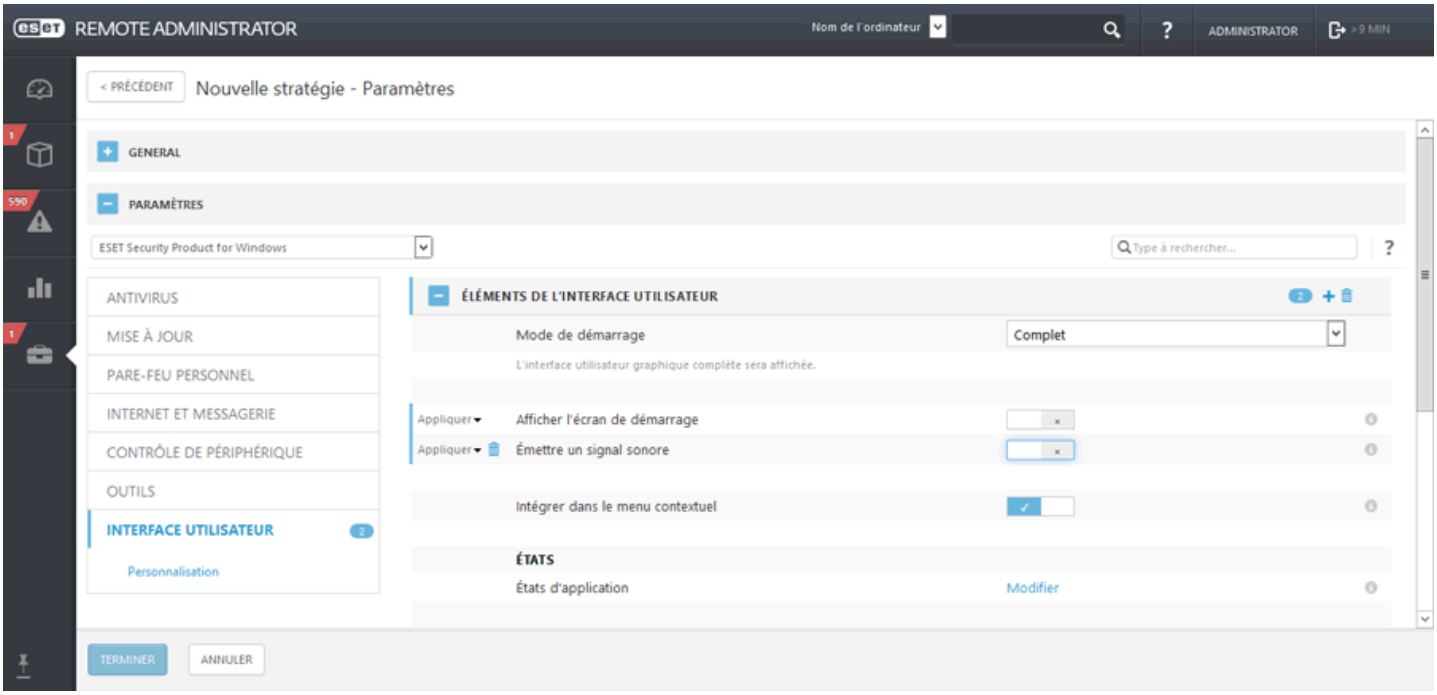
Pour créer et gérer des stratégies, cliquez sur **Admin**, puis sur l'onglet **Stratégies**. Cliquez ensuite sur **Stratégies** dans la partie inférieure, puis sélectionnez **Nouveau...**.

General

Saisissez un **nom** pour la nouvelle stratégie. Le champ **Description** est facultatif.

Paramètres

Sélectionnez votre produit dans le menu déroulant.



Sélectionnez une catégorie dans l'arborescence située à gauche. Dans le volet droit, modifiez les paramètres au besoin. Chaque paramètre est une règle pour laquelle vous pouvez définir un indicateur. Pour faciliter la navigation, toutes les règles sont comptabilisées. Le nombre de règles que vous avez définies dans une section spécifique s'affiche automatiquement. Un nombre apparaît également en regard du nom d'une catégorie dans l'arborescence de gauche. Il indique la somme des règles dans toutes ses sections. Vous pouvez ainsi rapidement déterminer l'emplacement et le nombre de paramètres/règles définis.

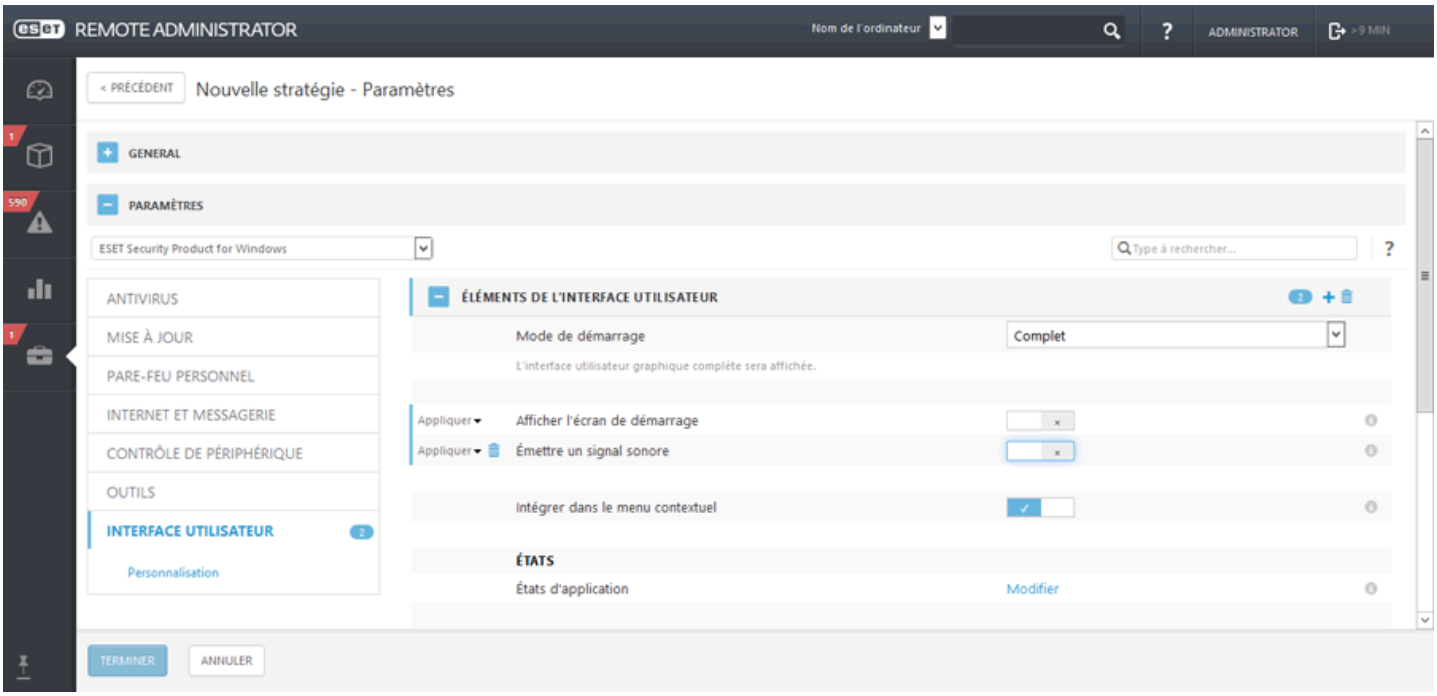
Pour faciliter la modification des stratégies, vous pouvez également suivre ces suggestions :

- utiliser + pour définir l'indicateur **Appliquer** sur tous les éléments actuels d'une section ;
- supprimer des règles à l'aide de l'icône **Corbeille**.

4.3.2 Indicateurs

Vous pouvez définir un indicateur pour chaque paramètre d'une stratégie. Il définit la façon dont le paramètre est géré par la stratégie :

- Appliquer : des paramètres associés à cet indicateur seront envoyés au client. Toutefois, en cas de fusion des stratégies, les paramètres peuvent être remplacés par une stratégie ultérieure. Lorsqu'une stratégie est appliquée à un ordinateur client et qu'un paramètre spécifique est associé à cet indicateur, ce dernier est modifié indépendamment de ce qui est configuré localement sur le client. Comme l'application de ce paramètre n'est pas forcée, il peut être modifié ultérieurement par d'autres stratégies.
- Forcer : des paramètres associés à un indicateur Forcer sont prioritaires et ne peuvent pas être remplacés par une stratégie ultérieure (même si cette stratégie ultérieure est associée à un indicateur Forcer). Il garantit que ces paramètres ne seront pas modifiés par des stratégies ultérieures lors de la fusion.



Sélectionnez une catégorie dans l'arborescence située à gauche. Dans le volet droit, modifiez les paramètres au besoin. Chaque paramètre est une règle pour laquelle vous pouvez définir un indicateur. Pour faciliter la navigation, toutes les règles sont comptabilisées. Le nombre de règles que vous avez définies dans une section spécifique s'affiche automatiquement. Un nombre apparaît également en regard du nom d'une catégorie dans l'arborescence de gauche. Il indique la somme des règles dans toutes ses sections. Vous pouvez ainsi rapidement déterminer l'emplacement et le nombre de paramètres/règles définis.

Pour faciliter la modification des stratégies, vous pouvez également suivre ces suggestions :

- utiliser + pour définir l'indicateur **Appliquer** sur tous les éléments actuels d'une section ;
- supprimer des règles à l'aide de l'icône **Corbeille**.

4.3.3 Gérer les stratégies

Accédez à **Admin** > **Stratégies**, puis sélectionnez la stratégie à gérer. Cliquez sur le bouton **Stratégies** (ou sur ⚙ en regard de la stratégie existante).

Actions que vous pouvez effectuer avec **Stratégies**:

+ Nouveau...
Utiliser cette option pour créer une stratégie.

Modifier...
Cette option permet de modifier la stratégie sélectionnée.

Dupliquer
Cette option permet de créer une nouvelle stratégie sur la base de la stratégie existante sélectionnée. Un nouveau nom est requis pour la stratégie en double.

Affecter
Cette option permet d'attribuer une stratégie à un client ou à des groupes.

Supprimer
Supprime entièrement la stratégie sélectionnée.

Importer...
Cliquez sur **Stratégies** > **Importer...**, cliquez sur **Sélectionner un fichier** et recherchez le fichier à importer. Pour sélectionner plusieurs stratégies, voir les **modes** ci-dessous.

Exporter...
Sélectionnez une stratégie à exporter dans la liste et cliquez sur le bouton **Stratégies** > sélectionnez **Exporter...** La stratégie est exportée sous forme de fichier *.dat*. Pour exporter plusieurs stratégies, voir les **modes** ci-dessous.

Vous pouvez utiliser l'option **Modes** pour modifier le mode de sélection (unique ou multiple). Cliquez sur la flèche dans le coin supérieur droit et sélectionnez l'une des options suivantes dans le menu contextuel :
Mode de sélection unique : vous pouvez sélectionner un seul élément.
Mode de sélection multiple : permet d'utiliser les cases à cocher pour sélectionner plusieurs éléments.
Rafraîchir : recharge/actualise les informations affichées.

4.3.4 Créer une stratégie pour qu'ERA Agent se connecte au nouveau serveur ERA Server

Cette stratégie permet de changer le comportement d'ERA Agent en modifiant ses paramètres. Les options suivantes s'avèrent particulièrement utiles lors de la migration des ordinateurs client vers un nouveau serveur ERA Server.

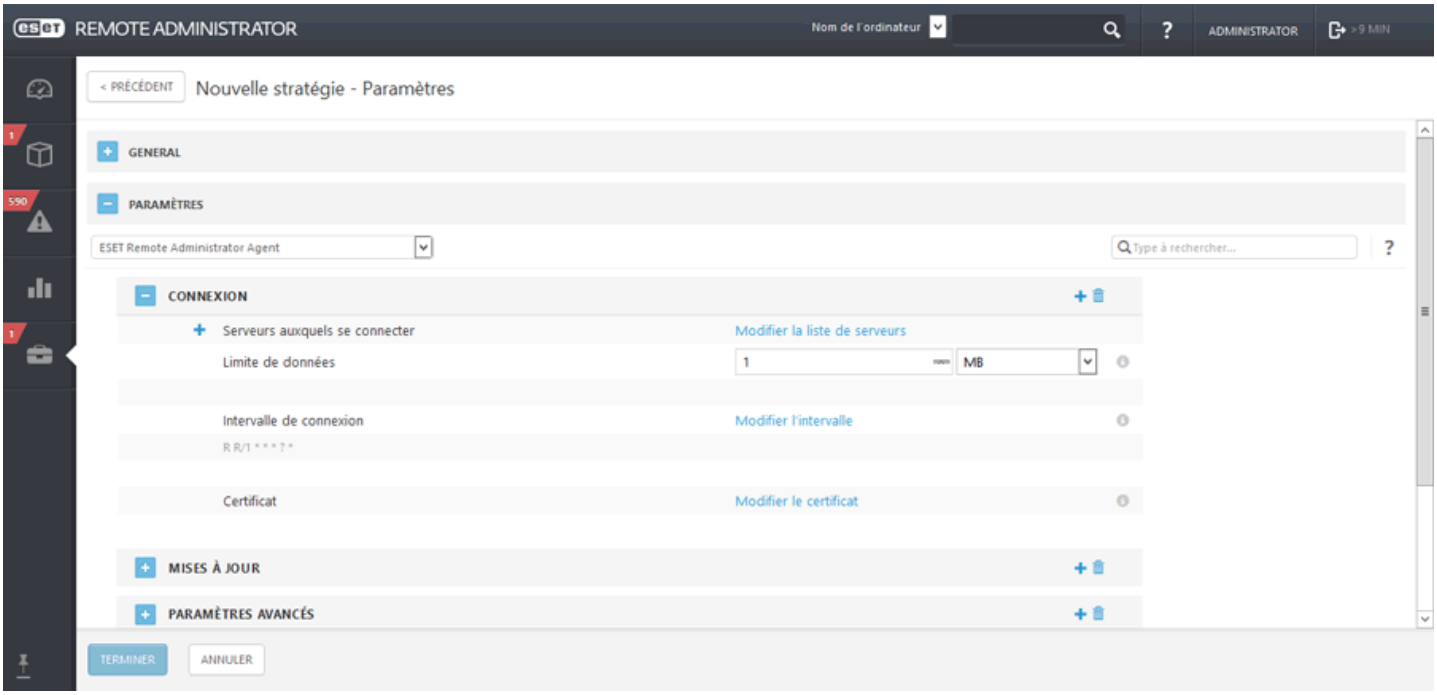
Créez une stratégie pour définir l'adresse IP du nouveau serveur ERA Server, puis attribuez la stratégie à tous les ordinateurs client. Sélectionnez **Admin** > **Stratégies** > **Nouveau**.

Général

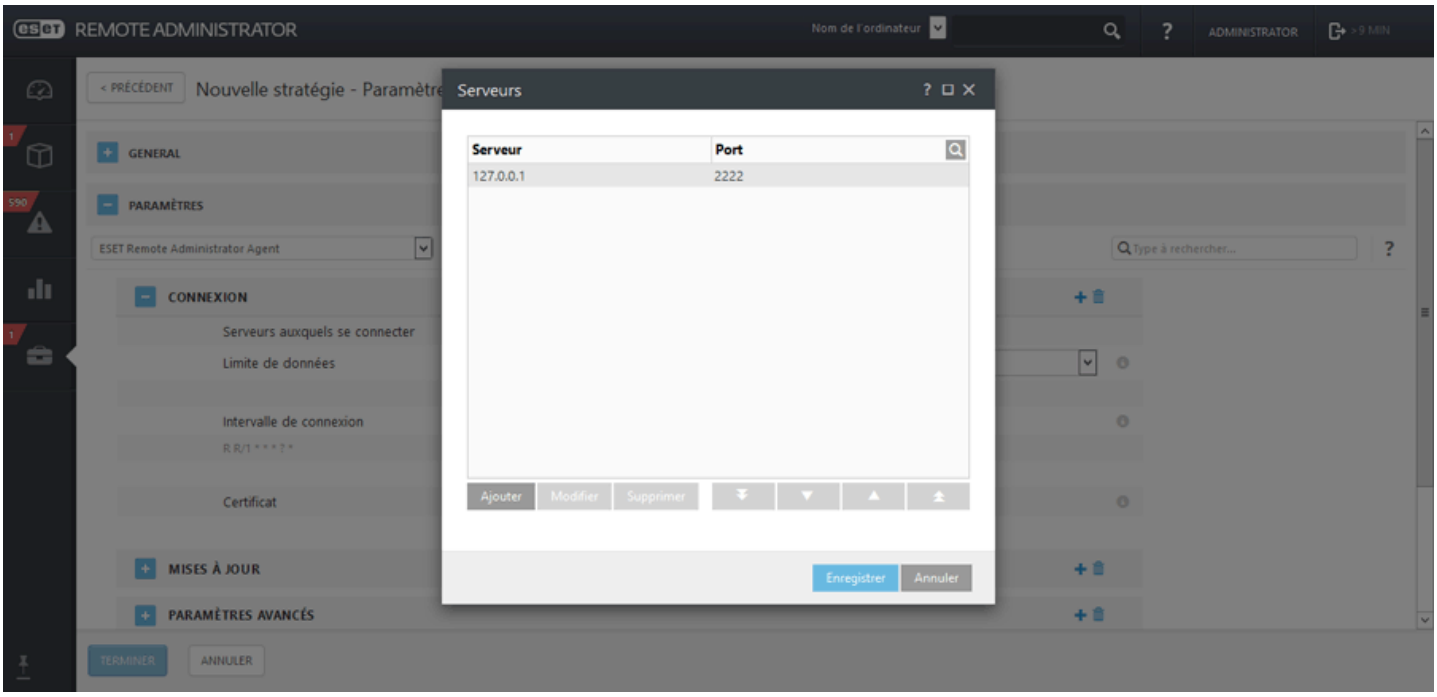
Saisissez un **nom** pour la stratégie. Le champ **Description** est facultatif.

Paramètres

Sélectionnez **ESET Remote Administrator Agent** dans le menu déroulant, développez **Connexion**, puis cliquez sur **Modifier la liste de serveurs** en regard des serveurs auxquels se connecter.



Une fenêtre s'ouvre. Elle contient la liste des serveurs ERA Server auxquels ERA Agent peut se connecter. Cliquez sur **Ajouter**, puis saisissez l'adresse IP du nouveau serveur ERA Server dans le champ **Hôte**. Si vous utilisez un autre port que le port 2222 par défaut d'ERA Server, indiquez votre numéro de port personnalisé.

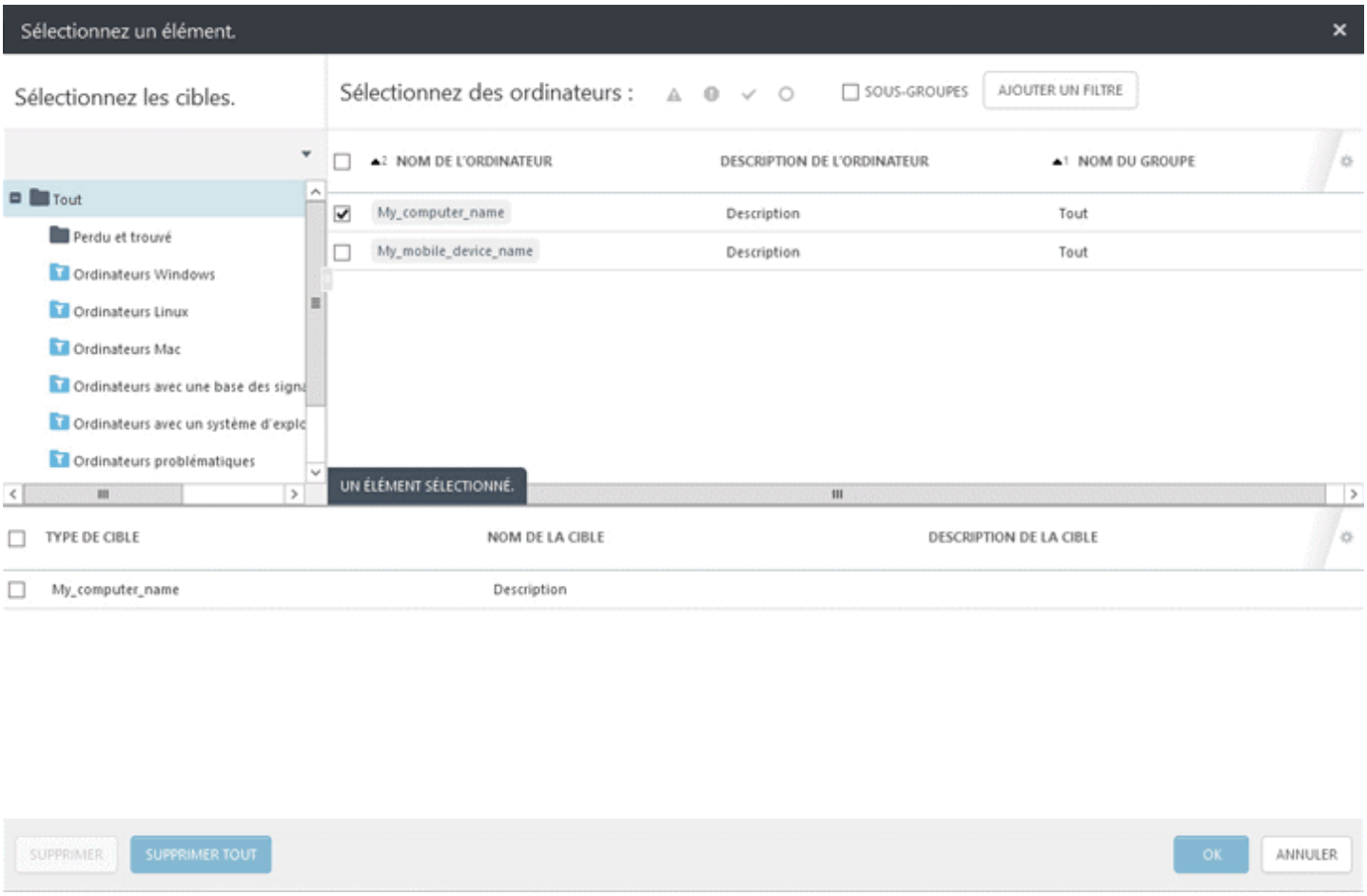


Vous pouvez utiliser les boutons représentant des flèches pour modifier la priorité des serveurs ERA Server si plusieurs entrées figurent dans la liste. Vérifiez que le nouveau serveur ERA Server se trouve en haut de la liste en cliquant sur le bouton représentant une **flèche pointant vers le haut**, puis cliquez sur **Enregistrer**.

Affecter

Cette section vous permet de spécifier les clients (ordinateurs/périphériques mobiles indépendants ou groupes) destinataires de cette stratégie.

Cliquez sur **Attribuer** pour afficher tous les groupes statiques et dynamiques et leurs membres. Sélectionnez les clients souhaités, puis cliquez sur **OK**.



Résumé

Passez en revue les paramètres de cette stratégie, puis cliquez sur **Terminer**.

4.3.5 Créer une stratégie pour activer la protection par mot de passe d'ERA Agent

Respectez la procédure suivante pour créer une stratégie qui appliquera un mot de passe pour protéger l'Agent ERA. Lorsque **Configuration protégée par mot de passe** est utilisée, l'Agent ERA ne peut pas être désinstallé ni réparé sans la fourniture d'un mot de passe. Consultez le chapitre Protection de l'agent pour plus d'informations.

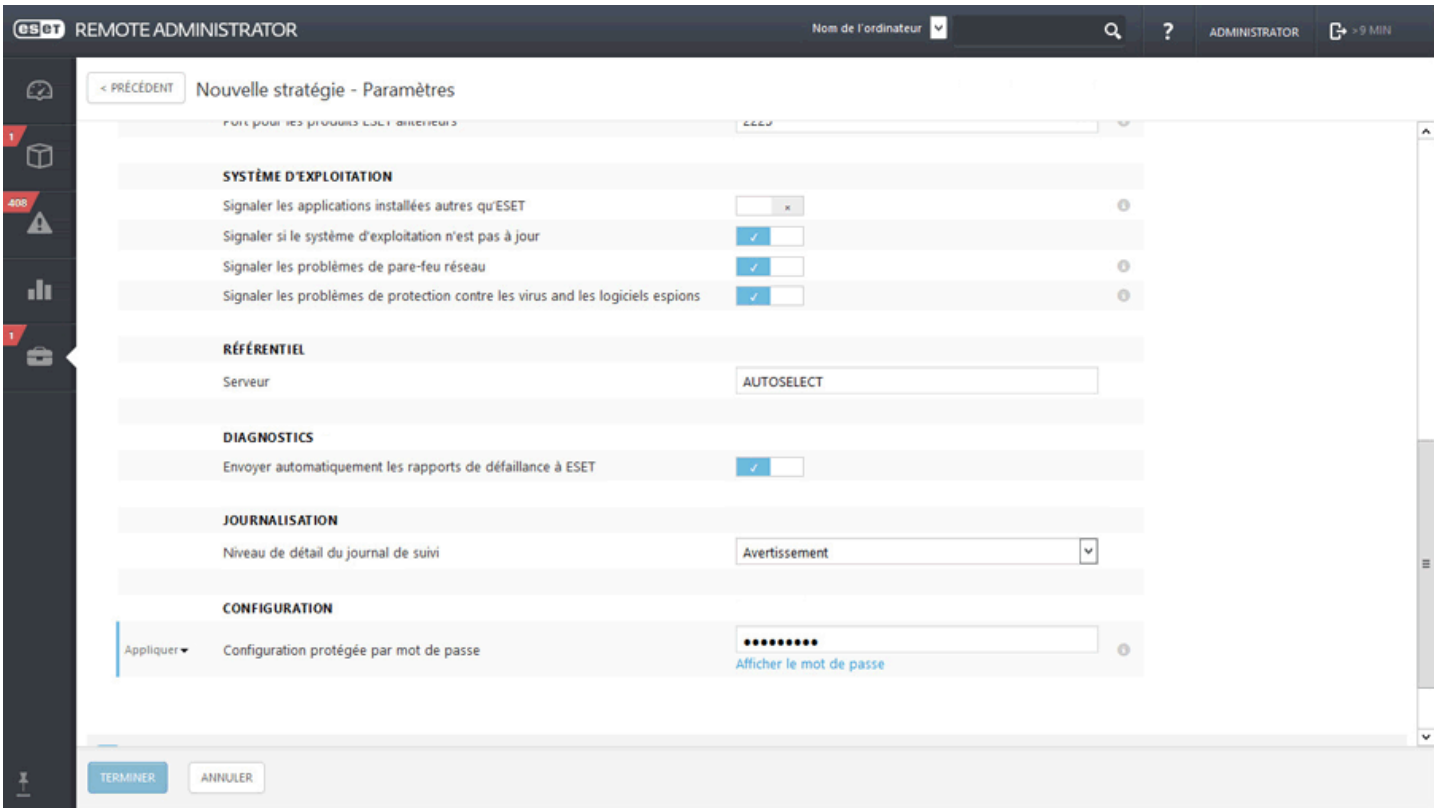
Général

Saisissez un **nom** pour cette stratégie. Le champ **Description** est facultatif.

Paramètres

Sélectionnez **ESET Remote Administrator Agent** dans la liste déroulante, développez **Paramètres avancés**, accédez à **Configuration**, puis saisissez le mot de passe dans le champ **Configuration protégée par mot de passe**. Ce mot de passe sera nécessaire si quelqu'un tente de désinstaller ou de réparer l'Agent ERA sur un ordinateur client.

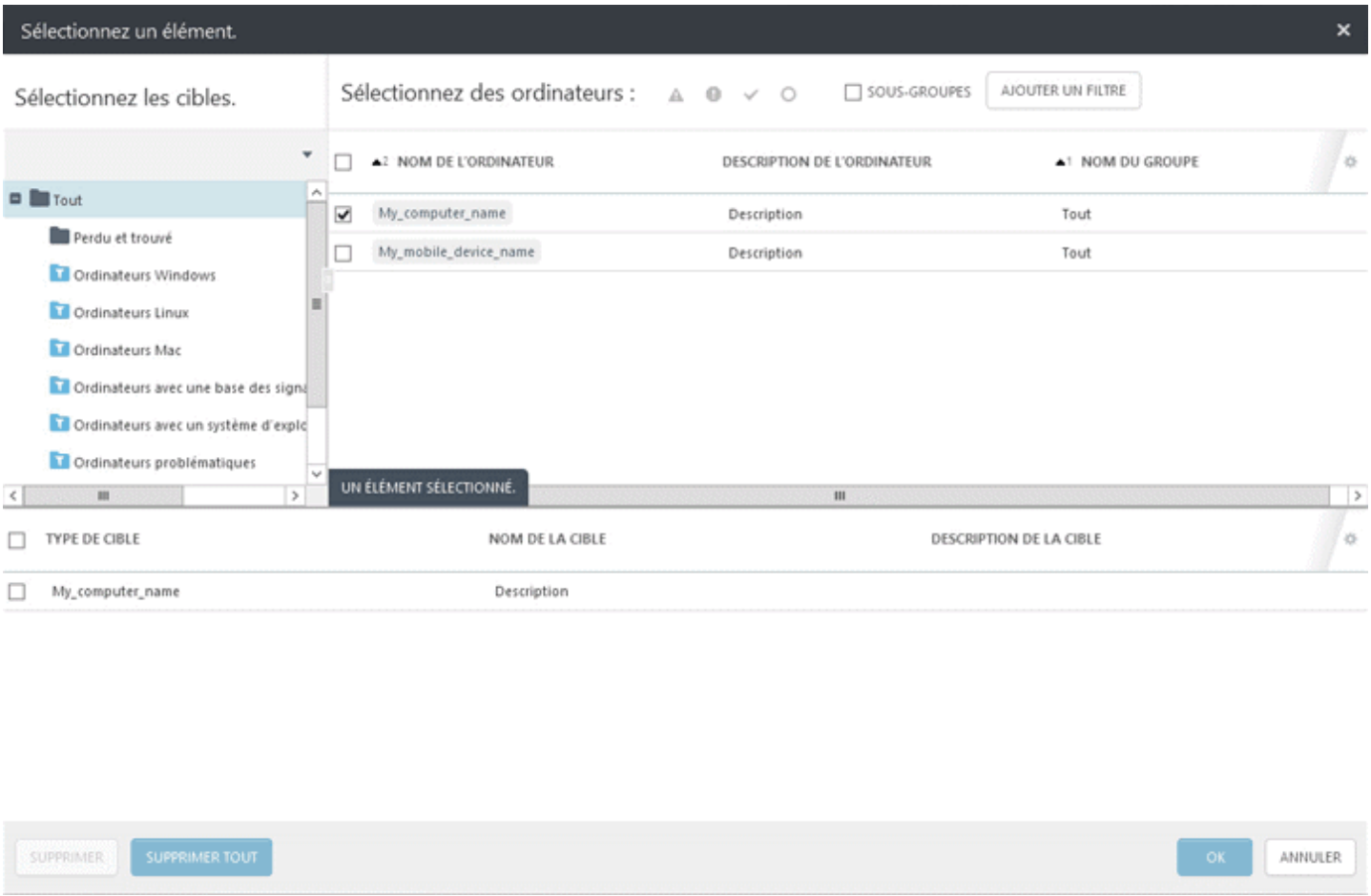
IMPORTANT : Prenez soin d'enregistrer ce mot de passe à un endroit sûr. Il est indispensable de saisir le mot de passe pour désinstaller l'Agent ERA de l'ordinateur client. Il n'existe pas d'autre manière de désinstaller l'Agent ERA sans mot de passe correct lorsque la stratégie **Configuration protégée par mot de passe** est en place.



Affecter

Cette section vous permet de spécifier les clients (ordinateurs/périphériques mobiles indépendants ou groupes) destinataires de cette stratégie.

Cliquez sur **Attribuer** pour afficher tous les groupes statiques et dynamiques et leurs membres. Sélectionnez les clients souhaités, puis cliquez sur **OK**.



Résumé

Passez en revue les paramètres de cette stratégie, puis cliquez sur **Terminer**.

4.3.6 Créer une stratégie pour MDM iOS - Compte Exchange ActiveSync

Vous pouvez utiliser cette stratégie pour configurer des Contacts, un Calendrier et un compte Mail Microsoft Exchange sur les périphériques mobiles iOS des utilisateurs. L'avantage d'une telle stratégie est qu'il vous suffit de la créer une seule fois pour l'appliquer ensuite à de nombreux périphériques mobiles iOS sans devoir les configurer un à un séparément. C'est possible à l'aide des attributs des utilisateurs d'Active Directory. Vous devez spécifier une variable, par exemple `${exchange_login/exchange}` qui sera remplacée par une valeur d'AD pour un utilisateur spécifique.

Si vous n'utilisez pas Microsoft Exchange ni Exchange ActiveSync, vous pouvez configurer manuellement chaque service (**Comptes de messagerie**, **Comptes de contacts**, **Comptes LDAP**, **Comptes de calendrier** et **Comptes de calendrier avec abonnement**).

L'exemple qui suit illustre la création et l'application d'une nouvelle stratégie pour configurer automatiquement Mail, Contacts et Calendrier pour chaque utilisateur d'un périphérique mobile iOS en utilisant le protocole Exchange ActiveSync (EAS) pour synchroniser ces services.

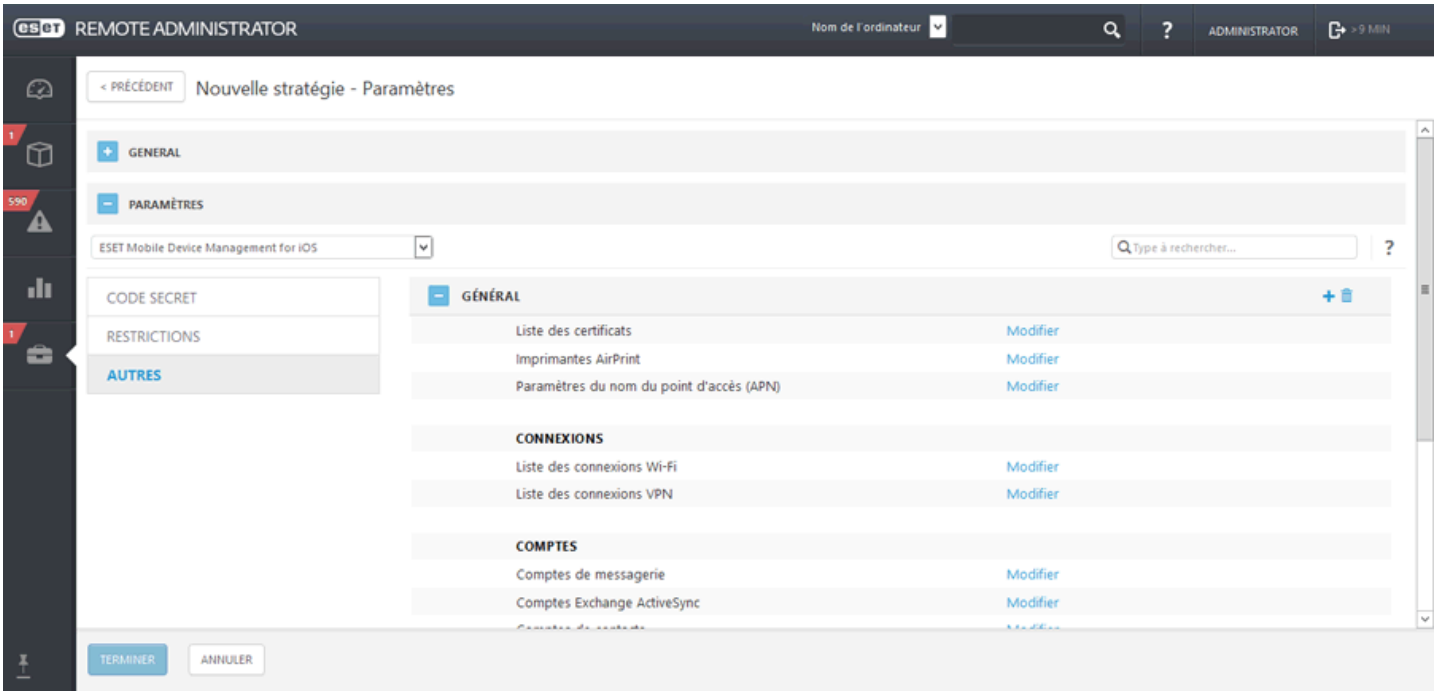
REMARQUE : Avant de définir cette stratégie, veillez à avoir effectué les étapes décrites dans Mobile Device Management.

Général

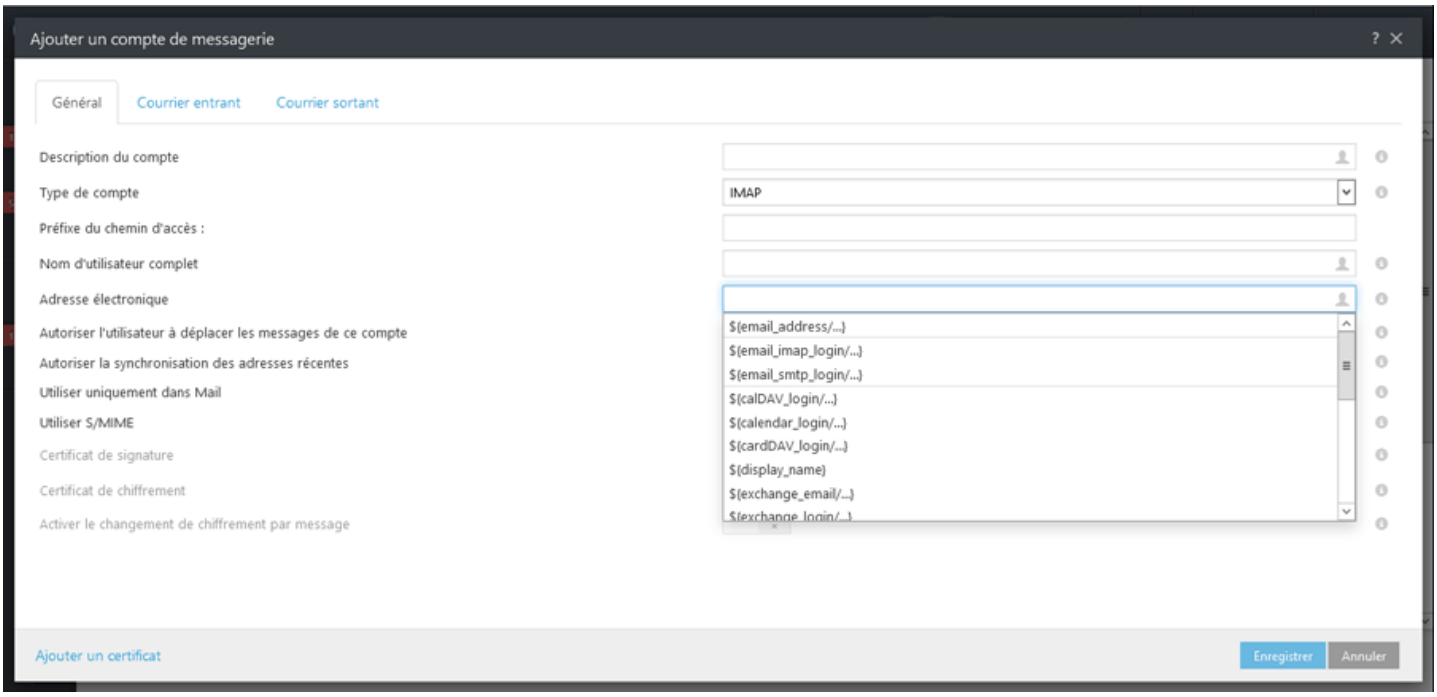
Saisissez un **nom** pour cette stratégie. Le champ **Description** est facultatif.

Paramètres

Sélectionnez **ESET Mobile Device Management pour iOS** dans la liste déroulante, cliquez sur **Autres** pour développer les catégories, puis cliquez sur **Modifier** en regard de l'option **Comptes Exchange ActiveSync**.

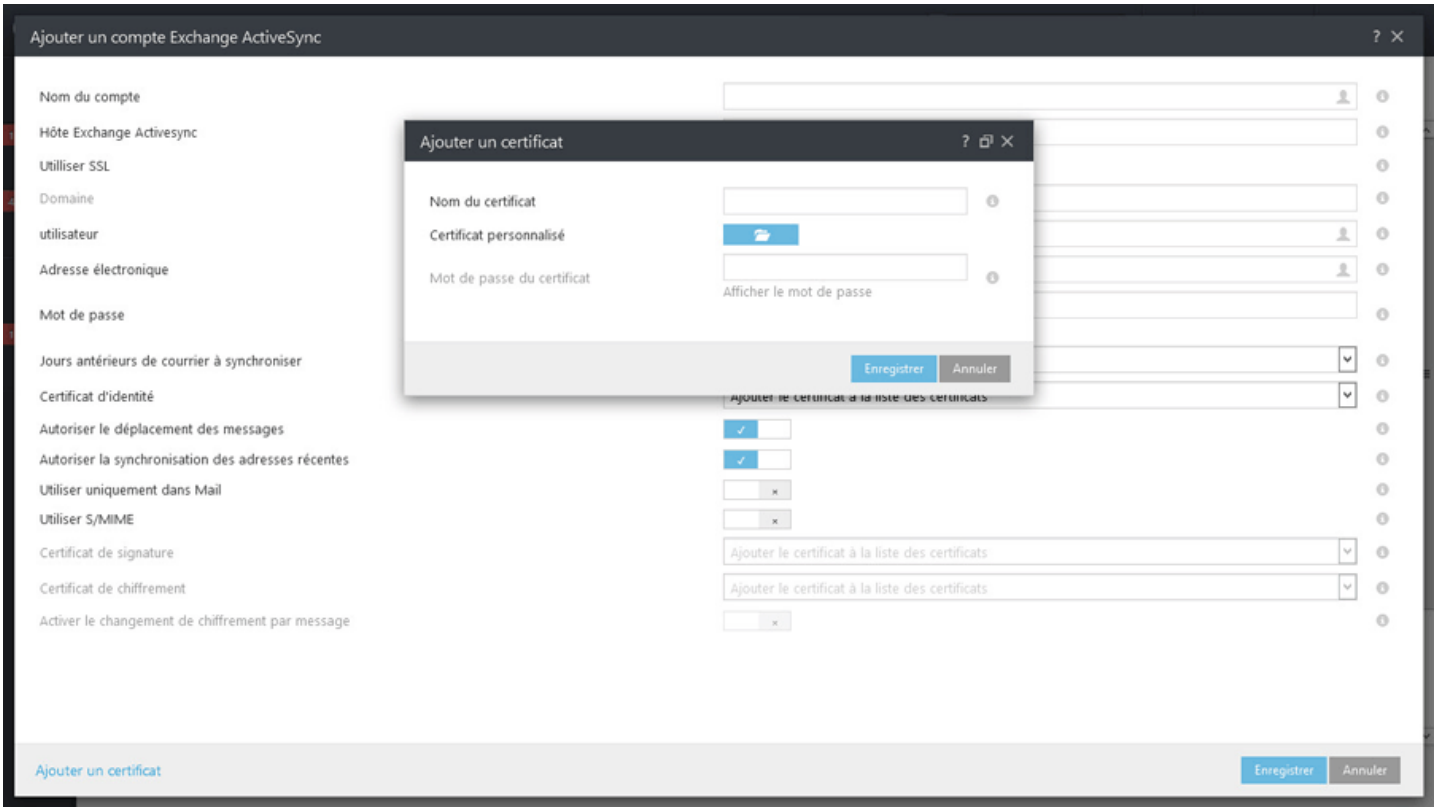


Cliquez sur **Ajouter** et spécifiez les détails de votre compte Exchange ActiveSync. Vous pouvez utiliser des variables pour certains champs (sélectionnez-les dans la liste déroulante), par exemple Utilisateur ou Adresse électronique. Elles seront remplacées par des valeurs réelles venant de Gestion des utilisateurs lors de l'application d'une stratégie.



- **Nom du compte** : saisissez le nom du compte Exchange. Cette information est destinée à permettre à l'utilisateur ou à l'administrateur d'identifier le compte Mail/Contacts/Calendrier.
- **Hôte Exchange ActiveSync** : spécifiez le nom d'hôte du serveur Exchange ou son adresse IP.
- **Utiliser SSL** : cette option est activée par défaut. Elle indique si le serveur Exchange utilise le protocole SSL (Secure Sockets Layer) pour l'authentification.
- **Domaine** : ce champ est facultatif. Vous pouvez saisir le domaine auquel ce compte appartient.
- **Utilisateur** : nom de connexion Exchange. Sélectionnez la variable appropriée dans la liste déroulante pour utiliser l'attribut de votre Active Directory pour chaque utilisateur.
- **Adresse électronique** : sélectionnez la variable appropriée dans la liste déroulante pour utiliser un attribut de votre Active Directory pour chaque utilisateur.
- **Mot de passe** : facultatif. Nous recommandons de laisser ce champ vide. S'il est vide, les utilisateurs seront invités à créer leurs propres mots de passe.
- **Jours antérieurs de courrier à synchroniser** : sélectionnez dans la liste déroulante le nombre de jours à synchroniser dans le passé.
- **Certificat d'identité** : informations d'identification pour la connexion à ActiveSync.
- **Autoriser le déplacement des messages** : si cette option est activée, les messages peuvent être déplacés d'un compte à un autre.
- **Autoriser la synchronisation des adresses récentes** : si cette option est activée, l'utilisateur est autorisé à synchroniser des adresses utilisées récemment entre périphériques.
- **Utiliser uniquement dans Mail** : activez cette option si vous ne souhaitez autoriser que l'application Mail à envoyer des messages électroniques sortants à partir de ce compte.
- **Utiliser S/MIME** : activez cette option pour utiliser le chiffrement S/MIME pour les messages électroniques sortants.
- **Certificat de signature** : informations d'identification pour la signature des données MIME.
- **Certificat de chiffrement** : informations d'identification pour le chiffrement des données MIME.
- **Activer le changement de chiffrement par message** : autoriser l'utilisateur à choisir de chiffrer ou non chaque message.

REMARQUE : Si vous ne spécifiez pas de valeur et laissez le champ vide, les utilisateurs de périphériques mobiles seront invités à entrer cette valeur. Par exemple, un **Mot de passe**.



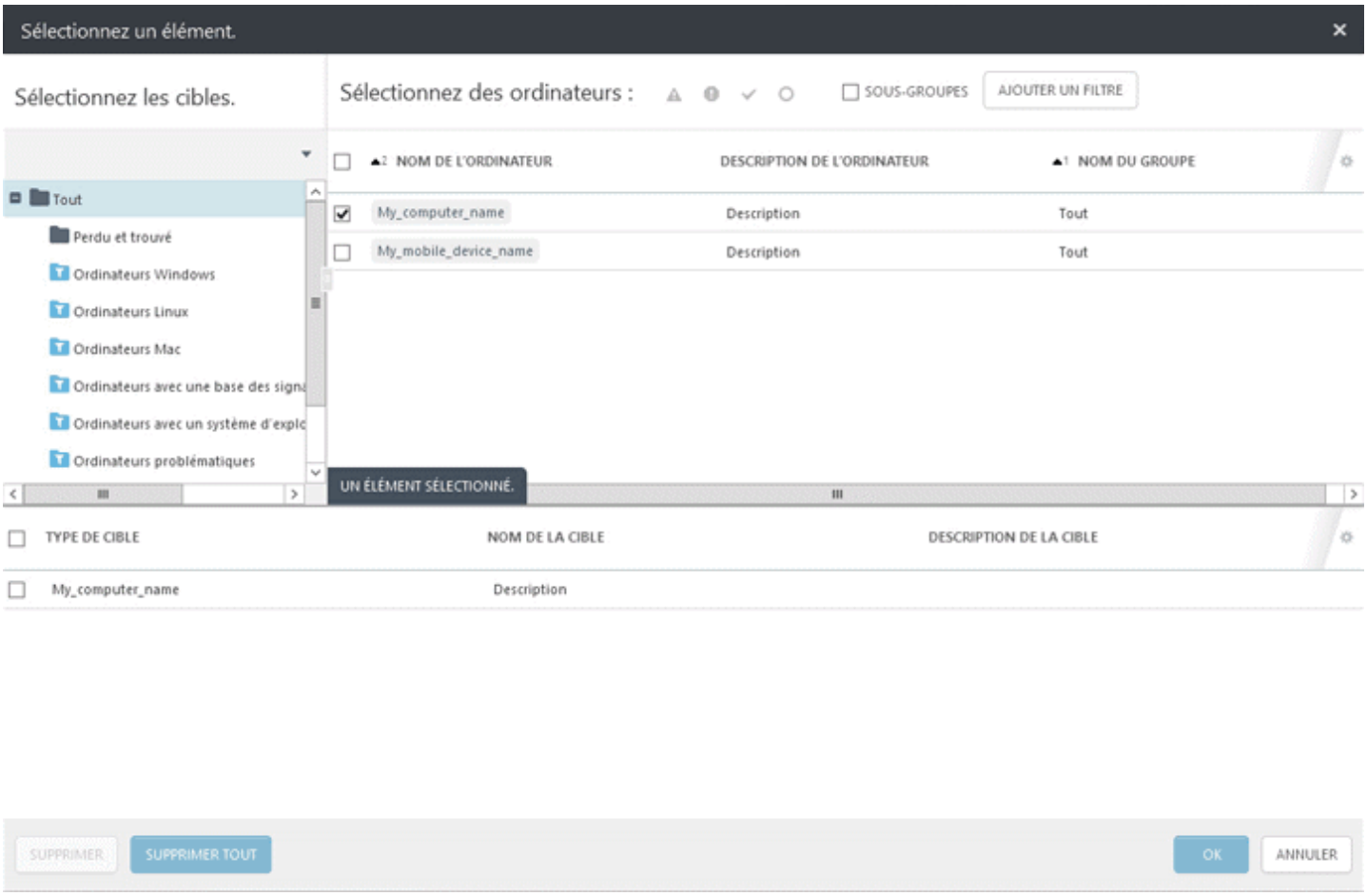
- **Ajouter un certificat** : vous pouvez ajouter des certificats Exchange spécifiques (identité utilisateur, signature numérique ou certificat de chiffrement) si nécessaire.

REMARQUE : En respectant la procédure qui précède, vous pouvez, si vous le souhaitez, ajouter plusieurs comptes Exchange ActiveSync. De cette manière, plus de comptes seront configurés sur un périphérique mobile. Au besoin, vous pouvez également modifier des comptes existants.

Affecter

Cette section vous permet de spécifier les clients (ordinateurs/périphériques mobiles indépendants ou groupes) destinataires de cette stratégie.

Cliquez sur **Attribuer** pour afficher tous les groupes statiques et dynamiques et leurs membres. Sélectionnez les clients souhaités, puis cliquez sur **OK**.



Résumé

Passez en revue les paramètres de cette stratégie, puis cliquez sur **Terminer**.

4.3.7 Créer une stratégie pour appliquer des restrictions sur iOS et ajouter une connexion Wi-Fi

Vous pouvez créer une stratégie pour périphériques mobiles iOS afin d'appliquer certaines restrictions. Il vous est également possible de définir plusieurs connexions Wi-Fi de sorte que, par exemple, les utilisateurs soient automatiquement connectés au réseau Wi-Fi de l'entreprise sur différents sites. Cela s'applique également aux connexions VPN.

Les restrictions que vous pouvez appliquer à un périphérique mobile iOS sont classées en catégories. Ainsi, il est possible de désactiver FaceTime et l'utilisation de la caméra, de désactiver certaines fonctionnalités d'iCloud, d'optimiser les options de sécurité et de confidentialité ou de désactiver des applications spécifiques.

REMARQUE : les restrictions qu'il est possible ou non d'appliquer dépendent de la version d'iOS utilisée par les périphériques clients. iOS 8.x et les versions plus récentes sont prises en charge.

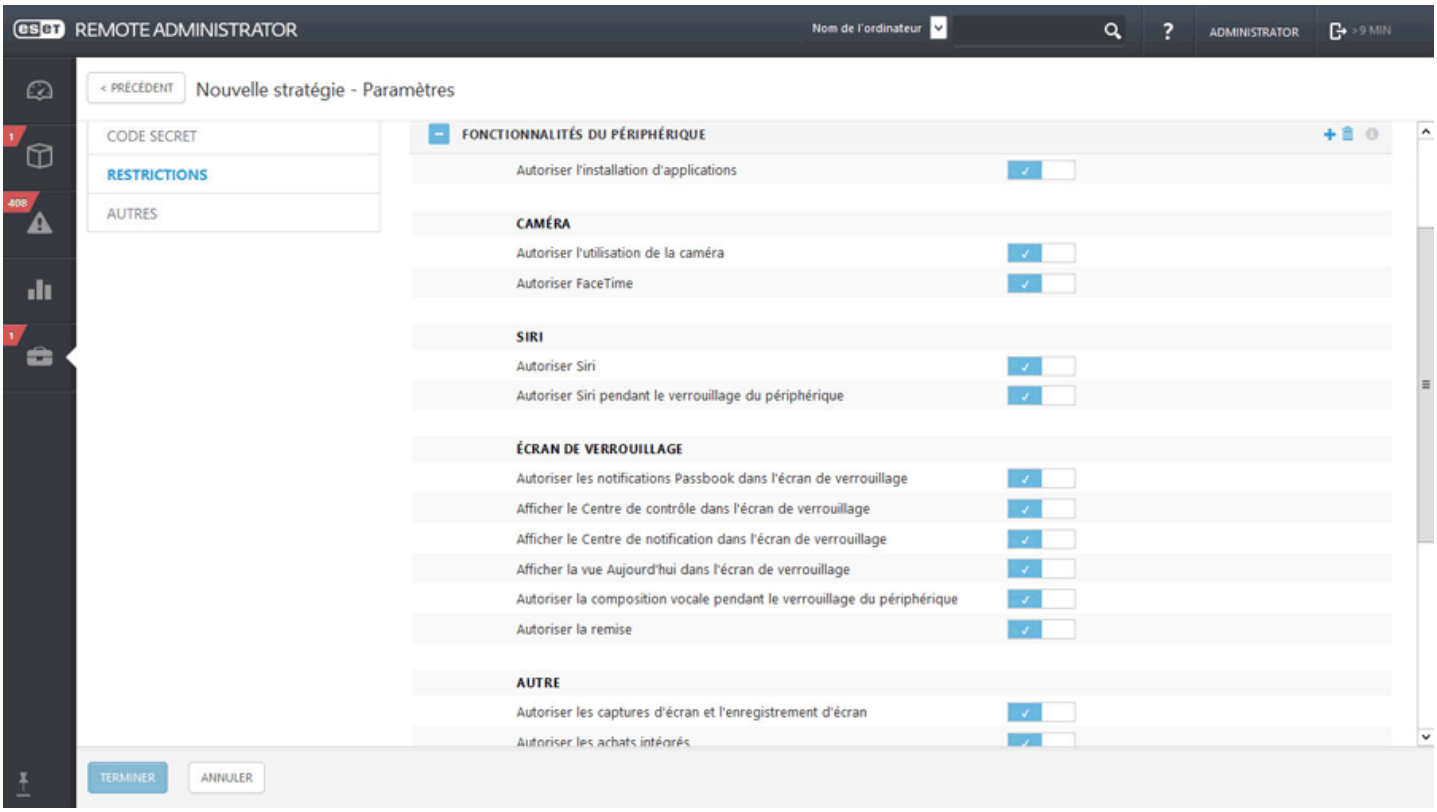
L'exemple suivante illustre la désactivation de la **caméra** et des **apps** FaceTime et l'ajout de détails de connexion Wi-Fi à la liste afin que le périphérique mobile iOS se connecte à un réseau Wi-Fi chaque fois qu'il est détecté. Si vous utilisez l'option Rejoindre automatiquement les périphériques mobiles iOS se connecteront à ce réseau par défaut. Le paramètre de la stratégie prendra le pas sur la sélection manuelle d'un réseau Wi-Fi par l'utilisateur.

Général

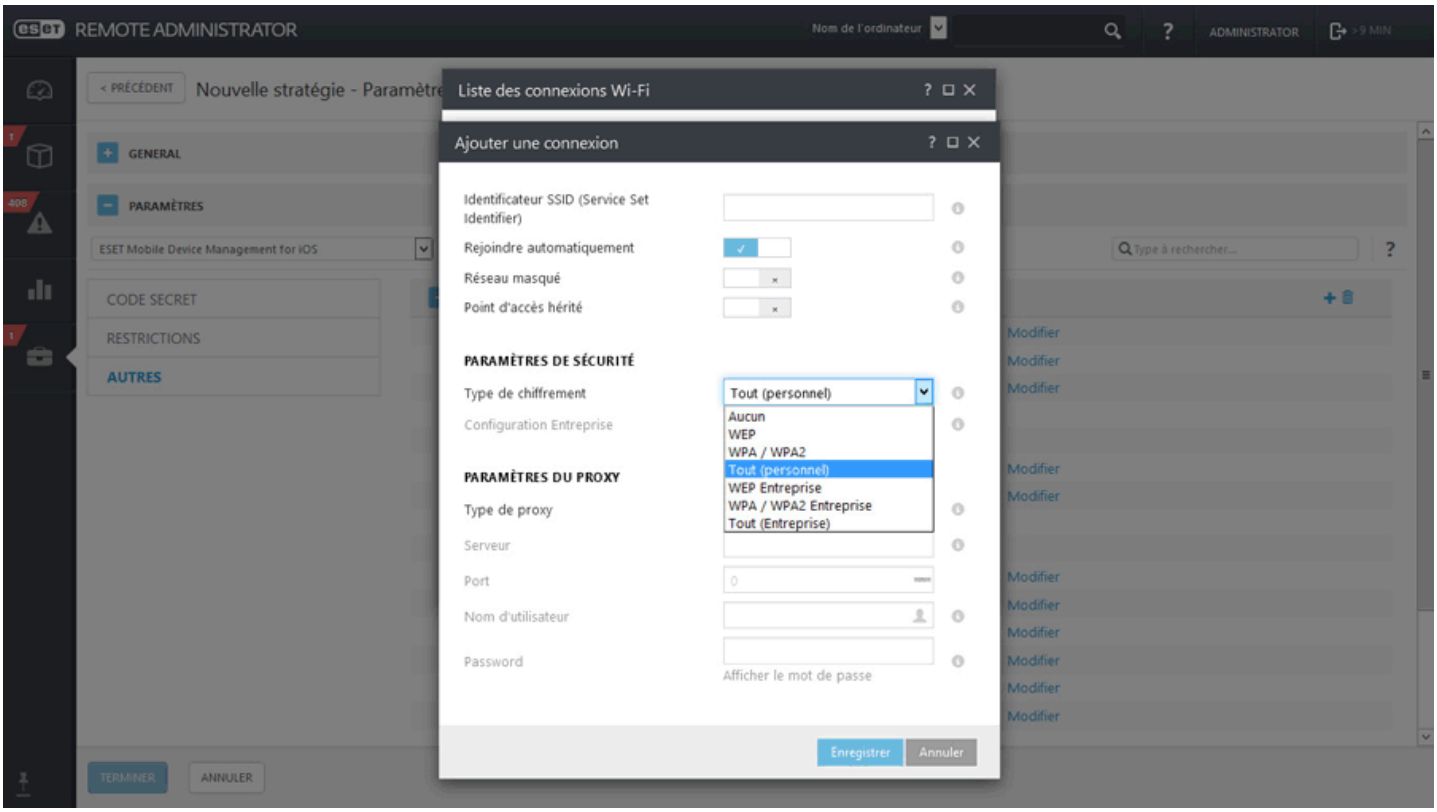
Saisissez un **nom** pour cette stratégie. Le champ **Description** est facultatif.

Paramètres

Sélectionnez **ESET Mobile Device Management pour iOS**, cliquez sur **Restrictions** pour afficher les catégories. Utilisez le bouton bascule en regard de **Autoriser l'utilisation de la caméra** pour la désactiver. La caméra étant désactivée, FaceTime le sera automatiquement aussi. Si vous ne souhaitez désactiver que FaceTime, laissez la caméra activée et utilisez le bouton bascule en regard de **Autoriser FaceTime** pour désactiver l'application.



Après avoir configuré **Restrictions**, cliquez sur **Autres**, puis sur **Modifier** en regard de **Liste des connexions Wi-Fi**. Une fenêtre s'ouvre avec la liste des connexions Wi-Fi. Cliquez sur **Ajouter** et spécifiez les détails de connexion du réseau Wi-Fi que vous souhaitez ajouter. Cliquez sur **Enregistrer**.



- **Identificateur SSID (Service Set Identifier)** : identificateur SSID du réseau Wi-FI à utiliser.
- **Rejoindre automatiquement** : facultatif (activé par défaut), le périphérique rejoint automatiquement ce réseau.

Paramètres de sécurité :

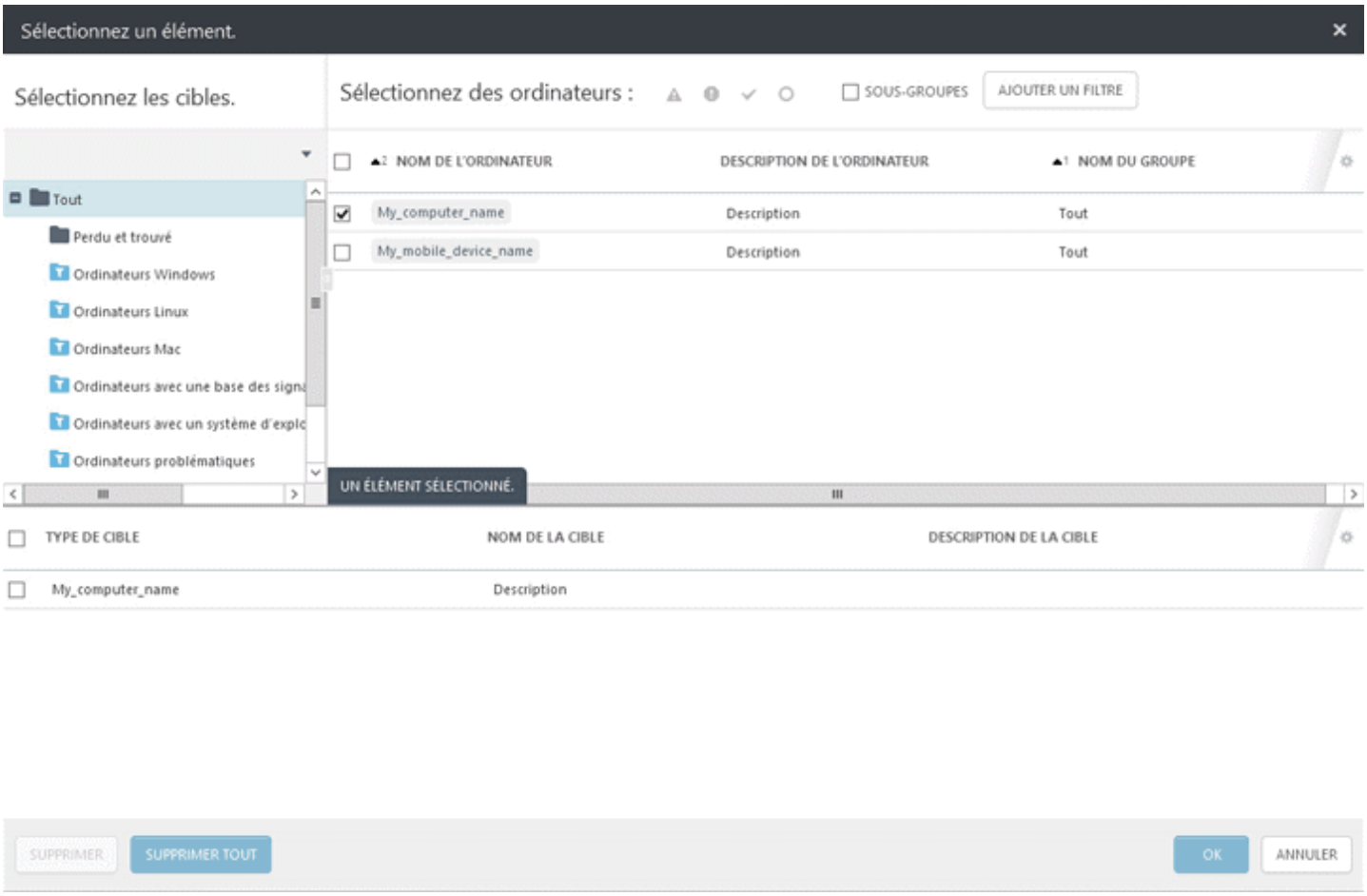
- **Type de chiffrement** : sélectionnez le chiffrement approprié dans la liste déroulante. Veillez à ce que cette valeur corresponde bien aux possibilités du réseau Wi-Fi.
- **Mot de passe** : saisissez le mot de passe qui sera utilisé pour l'authentification lors de la connexion au réseau Wi-Fi.

Paramètres du proxy : facultatif. Si votre réseau utilise un proxy, spécifiez les valeurs en conséquence.

Affecter

Cette section vous permet de spécifier les clients (ordinateurs/périphériques mobiles indépendants ou groupes) destinataires de cette stratégie.

Cliquez sur **Attribuer** pour afficher tous les groupes statiques et dynamiques et leurs membres. Sélectionnez les clients souhaités, puis cliquez sur **OK**.



Résumé

Passez en revue les paramètres de cette stratégie, puis cliquez sur **Terminer**.

4.3.8 Créer une stratégie pour MDC pour activer APNS pour l'inscription iOS

Voici un exemple de création d'une stratégie pour le Connecteur de périphérique mobile ESET destinée à activer le service APNS (Apple Push Notification Services) et la fonctionnalité d'inscription de périphériques iOS. Elle est nécessaire pour l'inscription de périphériques iOS. Avant de configurer cette stratégie, créez un certificat APN et faites-le signer par Apple sur le portail de certificats push Apple pour qu'il devienne un certificat signé ou **Certificat APNS**. Pour obtenir des instructions pas à pas sur ce processus, consultez la section Certificat APN.

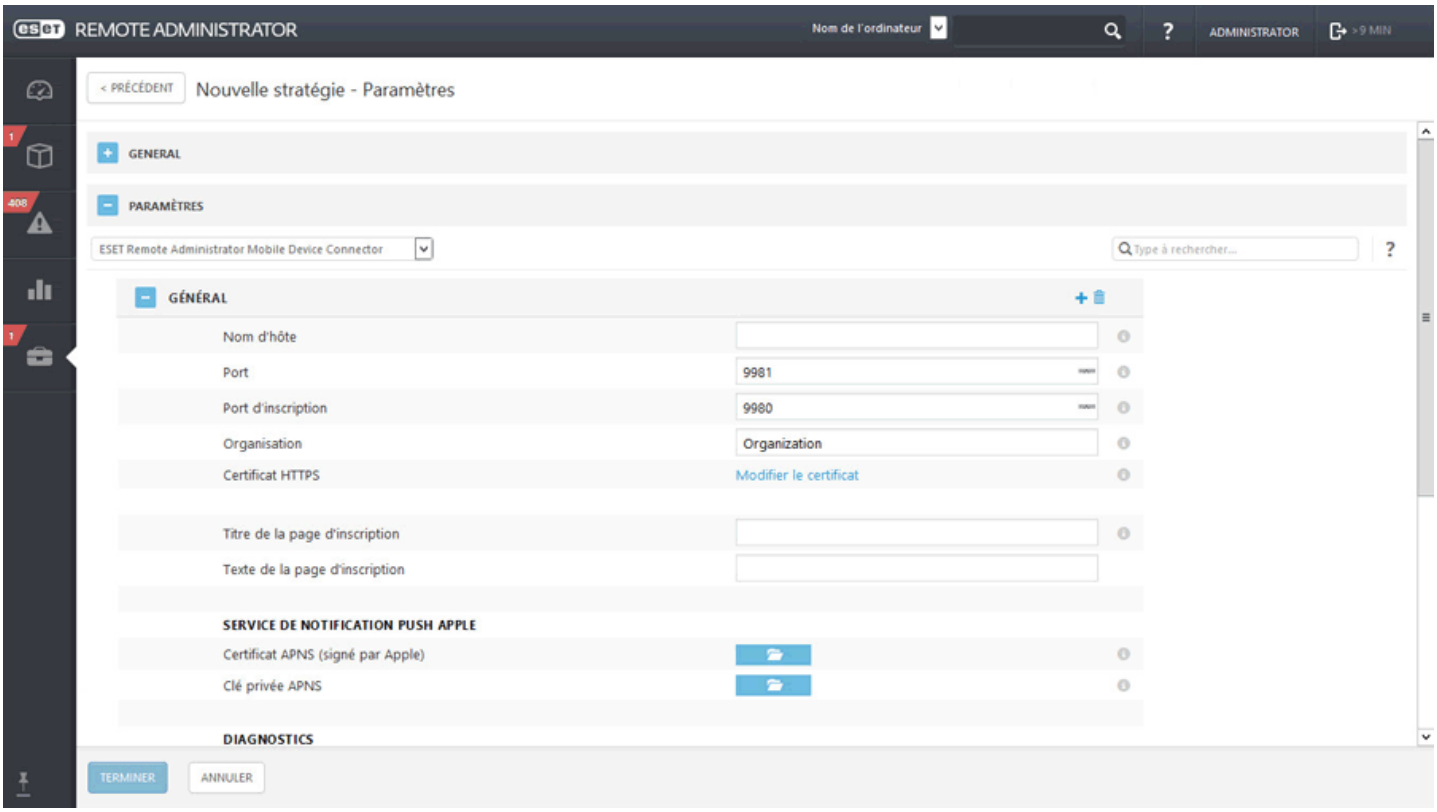
Général

Saisissez un **nom** pour cette stratégie. Le champ **Description** est facultatif.

Paramètres

Sélectionnez **Connecteur de périphérique mobile ESET Remote Administrator** dans la liste déroulante. Sous **Général**, accédez à **Service de notification Push Apple** et téléchargez le **Certificat APNS** et une **Clé privée APNS**.

REMARQUE : Remplacez la chaîne **Organization** par le nom réel de votre organisation. Ce champ est utilisé par le générateur de profil d'inscription pour inclure cette information dans le profil.



Certificat APNS (signé par Apple) : cliquez sur l'icône du dossier et recherchez le certificat APNS pour le télécharger.
Clé privée APNS : cliquez sur l'icône du dossier et recherchez la clé privée APNS pour la télécharger.

Affecter

Cette section vous permet de spécifier les clients (ordinateurs/périphériques mobiles indépendants ou groupes) destinataires de cette stratégie.

Cliquez sur **Attribuer** pour afficher tous les groupes statiques et dynamiques et leurs membres. Sélectionnez l'instance du Connecteur de périphérique mobile sur laquelle vous souhaitez appliquer un certificat APNS et cliquez sur **OK**.

Résumé

Passez en revue les paramètres de cette stratégie, puis cliquez sur **Terminer**.

4.3.9 Application des stratégies aux clients

Plusieurs stratégies peuvent être attribuées aux groupes et aux ordinateurs. En outre, un ordinateur peut figurer dans un groupe imbriqué profondément dont les parents disposent de leurs propres stratégies.

L'ordre des stratégies est l'élément le plus important lors de leur application. Il est dérivé de l'ordre des groupes et de celui des stratégies appliquées à un groupe.

Pour déterminer la stratégie active d'un client, suivez les étapes suivantes :

1. Déterminer l'ordre des groupes dans lesquels se trouve le client
2. Remplacer les groupes par les stratégies attribuées
3. Fusionner les stratégies pour obtenir des paramètres finaux

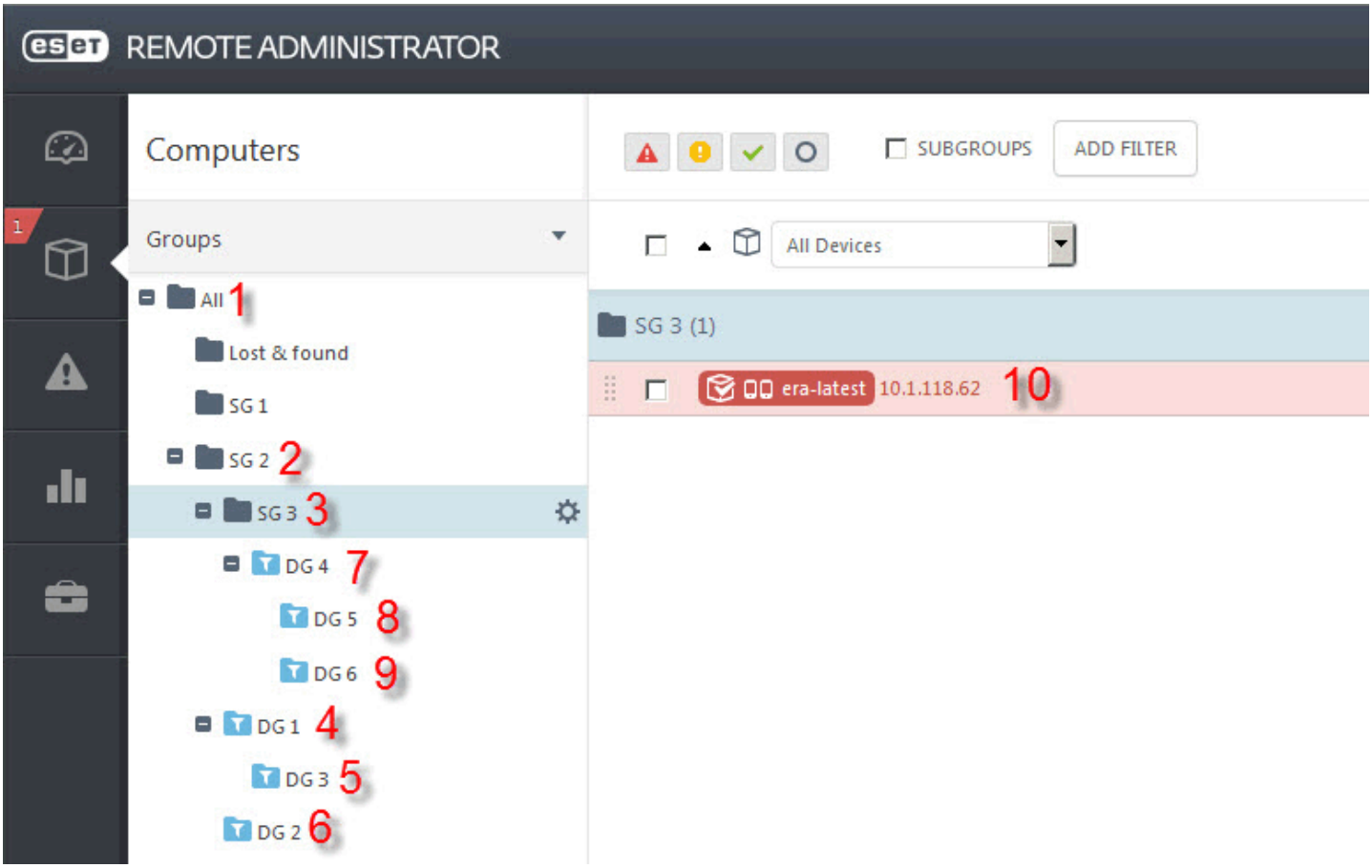
4.3.9.1 Classement des groupes

Les **stratégies** peuvent être attribuées à des **groupes** et appliquées dans un ordre spécifique.

Lors du classement des groupes dans la liste, plusieurs règles sont appliquées :

1. Les groupes statiques sont parcourus à partir du groupe statique racine Tous.
2. À chaque niveau, les groupes statiques sont d'abord parcourus dans l'ordre dans lequel ils apparaissent dans l'arborescence (recherche en largeur).
3. Une fois que tous les groupes statiques à un certain niveau figurent dans la liste, ils sont parcourus.
4. Dans chaque groupe dynamique, tous les enfants sont parcourus dans l'ordre dans lequel ils apparaissent dans la liste.
5. À n'importe quel niveau des groupes dynamiques, s'il existe un enfant, il est répertorié et ses enfants font l'objet d'une recherche. Lorsqu'il n'y a plus d'enfants, les groupes dynamiques suivants au niveau parent sont répertoriés (recherche en profondeur).
6. Le parcours se termine au niveau Ordinateur.

Dans la pratique, le parcours ressemble à celui-ci :



Comme indiqué ci-dessus, la racine (groupe statique appelé Tous) est répertoriée en tant que **Règle 1**. Comme il n'existe pas d'autres groupes au même niveau que le groupe Tous, les stratégies des groupes du niveau suivant sont ensuite évaluées.

Les groupes statiques GS 1, GS 2 et Perdu et trouvé sont ensuite évalués. L'ordinateur n'est actuellement que membre des groupes statiques Tous/GS 2/GS 3. Il n'est donc pas nécessaire de parcourir les groupes Perdu et trouvé et GS 1. GS 2 est le seul groupe de ce niveau à être évalué. Il est donc placé dans la liste, et le parcours devient plus profond.

Au troisième niveau, l'algorithme détecte les groupes GS 3, GD 1 et GD 2. Selon la **règle 2**, les groupes statiques sont répertoriés en premier. Le parcours ajoute GS 3 et, comme il s'agit du dernier groupe statique au niveau 3, passe à GD 1. Avant de passer à GD 2 au niveau 3, les enfants de GD 1 doivent être répertoriés.

GD 3 est ajouté. Comme il ne possède pas d'enfants, le parcours passe à un autre groupe.

GD 2 est répertorié. Il ne possède pas d'enfants. Au niveau 3, il ne reste plus de groupes. Le parcours passe au niveau 4.

Au niveau 4, il n'existe que le groupe dynamique GD 4 et l'ordinateur. La **règle 6** indique que l'ordinateur passe en dernier. GD 4 est donc sélectionné. GD 4 possède deux enfants qui doivent être traités avant de continuer.

GD 5 et GD 6 sont ajoutés à la liste. Comme ils ne possèdent pas d'enfants, le parcours continue. Il ajoute Ordinateur et se termine.

La liste finale est la suivante :

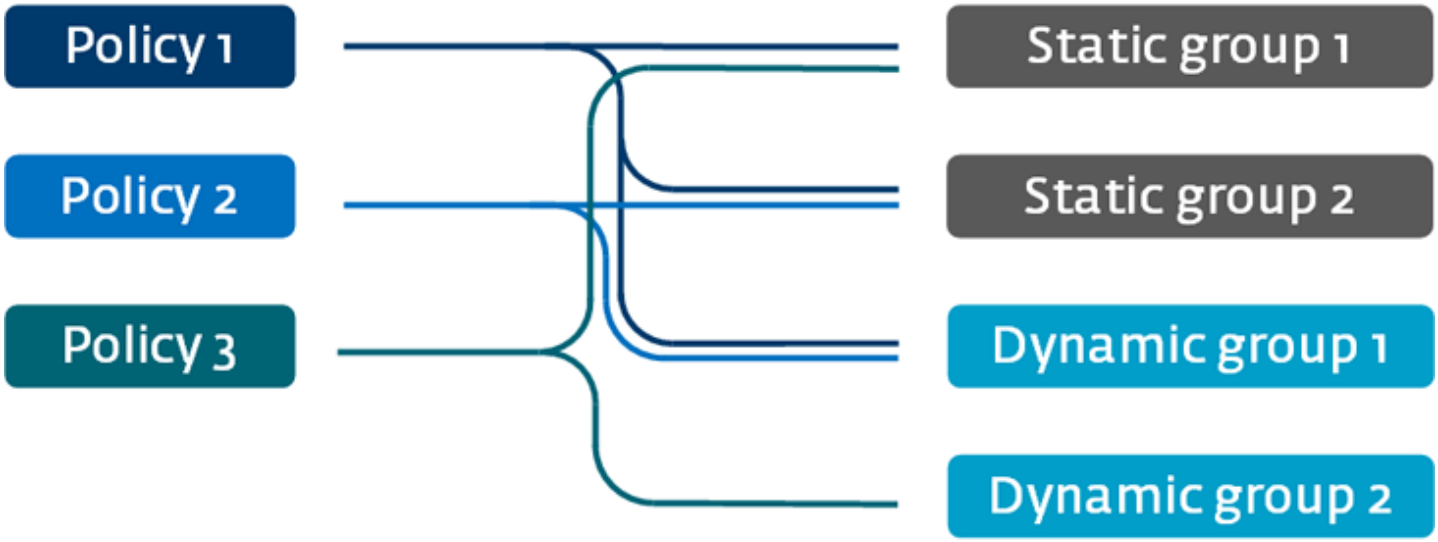
1. Tous
2. GS 2
3. GS 3
4. GD 1
5. GD 3
6. GD 2
7. GD 4
8. GD 5
9. GD 6
10. Ordinateur

Il s'agit de l'ordre dans lequel les stratégies sont appliquées.

4.3.9.2 Énumération des stratégies

Une fois que l'ordre des groupes est connu, l'étape suivante consiste à remplacer chaque groupe par les stratégies qui lui sont attribuées. Les stratégies sont répertoriées dans le même ordre que celui de leur attribution à un groupe. Un groupe sans stratégie est supprimé de la liste. Il est possible de modifier la priorité des stratégies d'un groupe auquel plusieurs stratégies sont attribuées. Chaque stratégie configure un seul produit (ERA Agent, ERA Proxy, EES, etc.)

3 stratégies sont appliquées à des groupes statiques et dynamiques (voir l'illustration ci-dessous) :



La liste de l'étape 1 serait transformée en :

1. Tous (supprimé, aucune stratégie)
2. GS 2 -> Stratégie 1, Stratégie 2
3. GS 3 (supprimé, car sans stratégie)
4. GD 1 -> Stratégie 1, Stratégie 2
5. GD 3 (supprimé, car sans stratégie)
6. GD 2 -> Stratégie 3
7. GD 4 (supprimé, car sans stratégie)
8. GD 5 (supprimé, car sans stratégie)
9. GD 6 (supprimé, car sans stratégie)
10. Ordinateur (supprimé, car sans stratégie)

La liste finale des stratégies est la suivante :

1. Stratégie 1
2. Stratégie 2
3. Stratégie 1
4. Stratégie 2
5. Stratégie 3

4.3.9.3 Fusion des stratégies

Les stratégies sont fusionnées une par une. Lors de la fusion des stratégies, la dernière stratégie remplace toujours les paramètres définis par la précédente.
Pour modifier ce comportement, vous pouvez utiliser des indicateurs de stratégie (disponibles pour chaque paramètre). Les paramètres sont fusionnés un par un.

Gardez à l'esprit que la structure des groupes (leur hiérarchie) et la séquence des stratégies déterminent la façon dont celles-ci sont fusionnées. La fusion de deux stratégies peut donner des résultats différents en fonction de leur ordre. Les groupes ont été classés et les stratégies ont été énumérées.

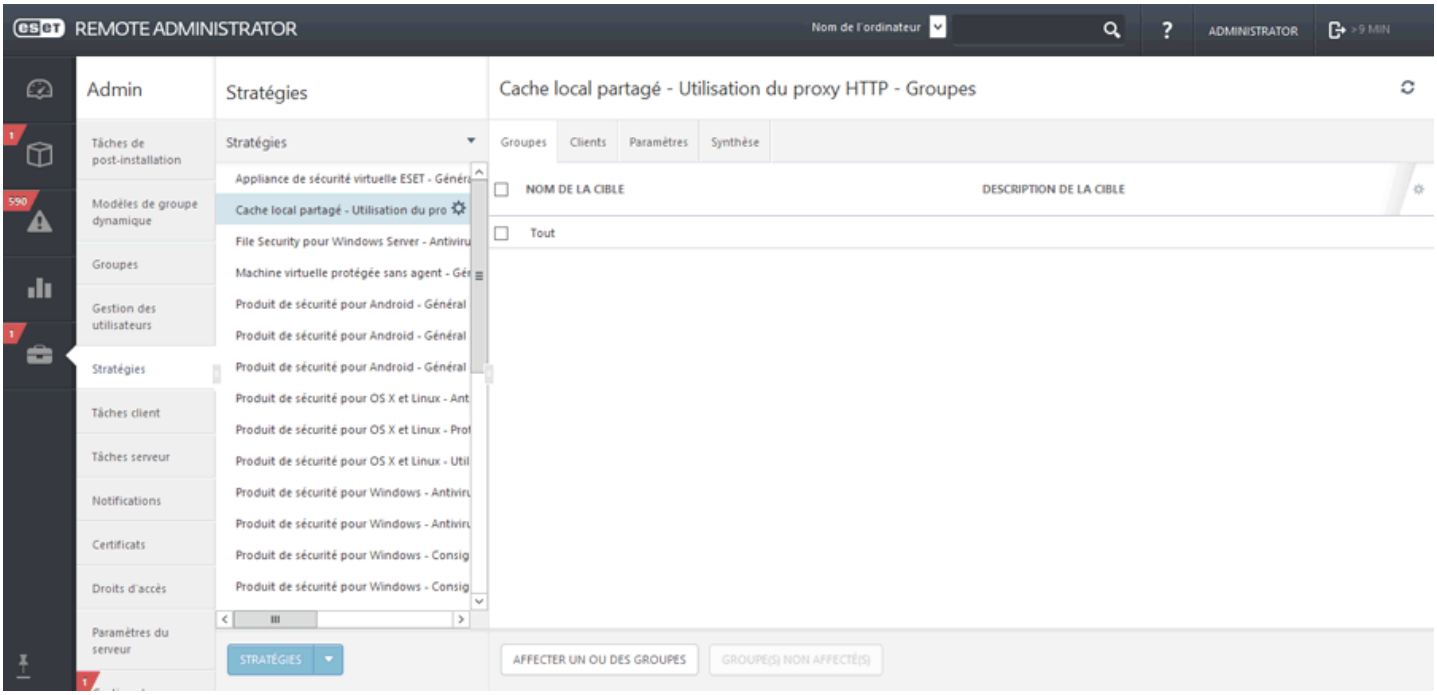
4.3.10 Configuration d'un produit à partir d'ERA

Vous pouvez utiliser des stratégies pour configurer votre produit ESET comme vous le feriez dans la fenêtre Configuration avancée de l'interface utilisateur graphique du produit. Contrairement aux stratégies d'Active Directory, les stratégies d'ERA ne peuvent pas comporter de scripts ou de séries de commandes.

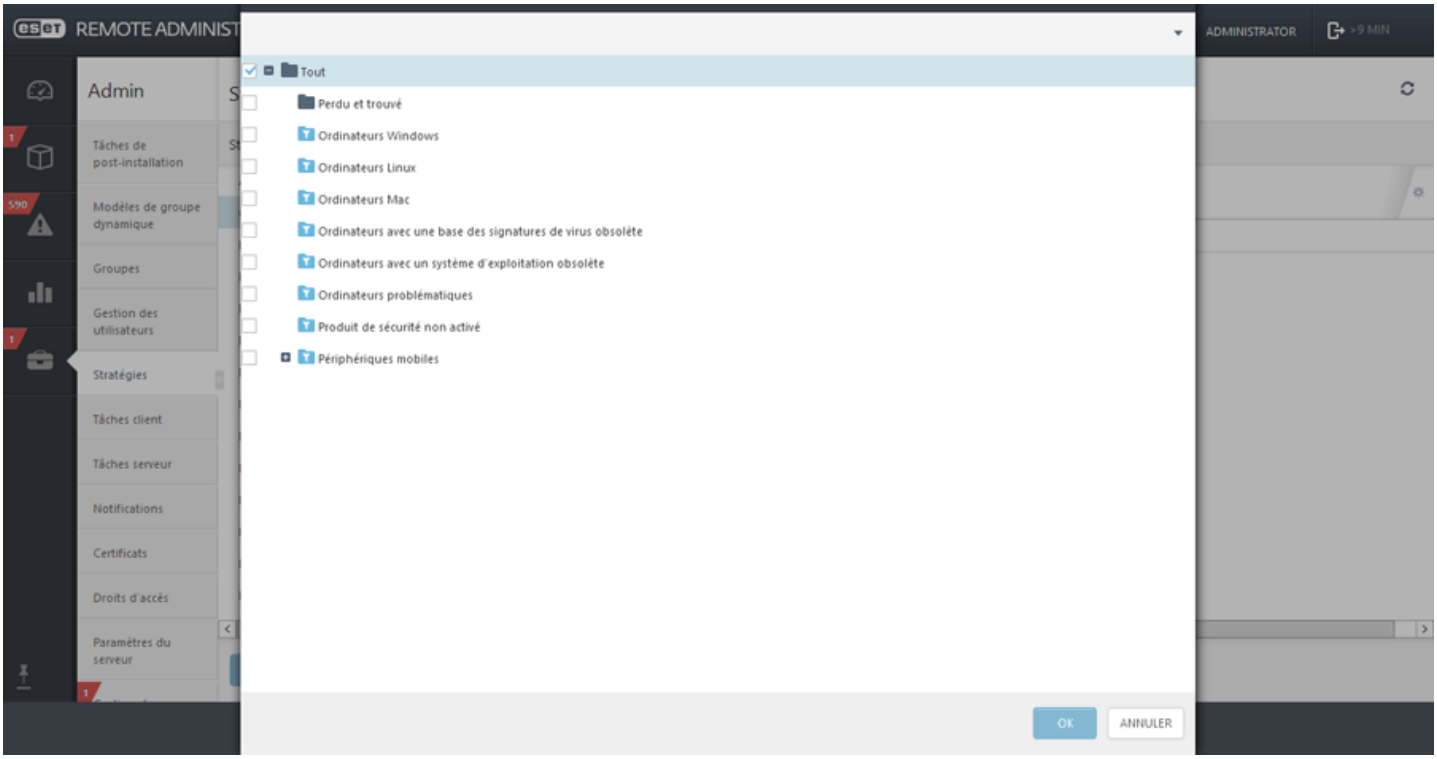
4.3.11 Attribuer une stratégie à un groupe

Une fois une stratégie créée, vous pouvez l'attribuer à un **groupe statique** ou **dynamique**. Il existe deux méthodes pour attribuer une stratégie :

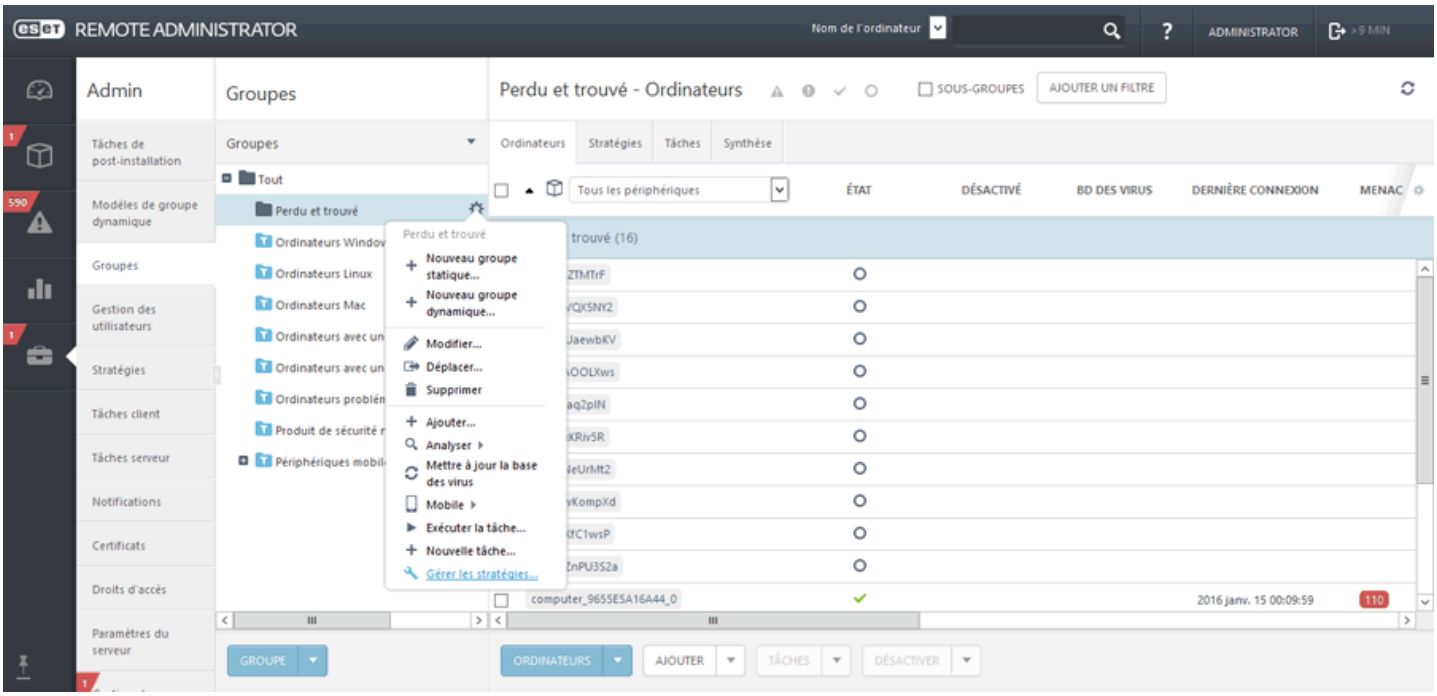
1. Sous **Admin** > **Stratégies**, sélectionnez une stratégie, puis cliquez sur **Affecter un ou des groupes**. Sélectionnez un groupe statique ou dynamique, puis cliquez sur **OK**.



Dans la liste, sélectionnez **Groupe**.



2. Cliquez sur **Admin** > **Groupes** > **Groupe** ou sur l'icône ⚙ située en regard du nom du groupe, puis sélectionnez **Gérer les stratégies**.

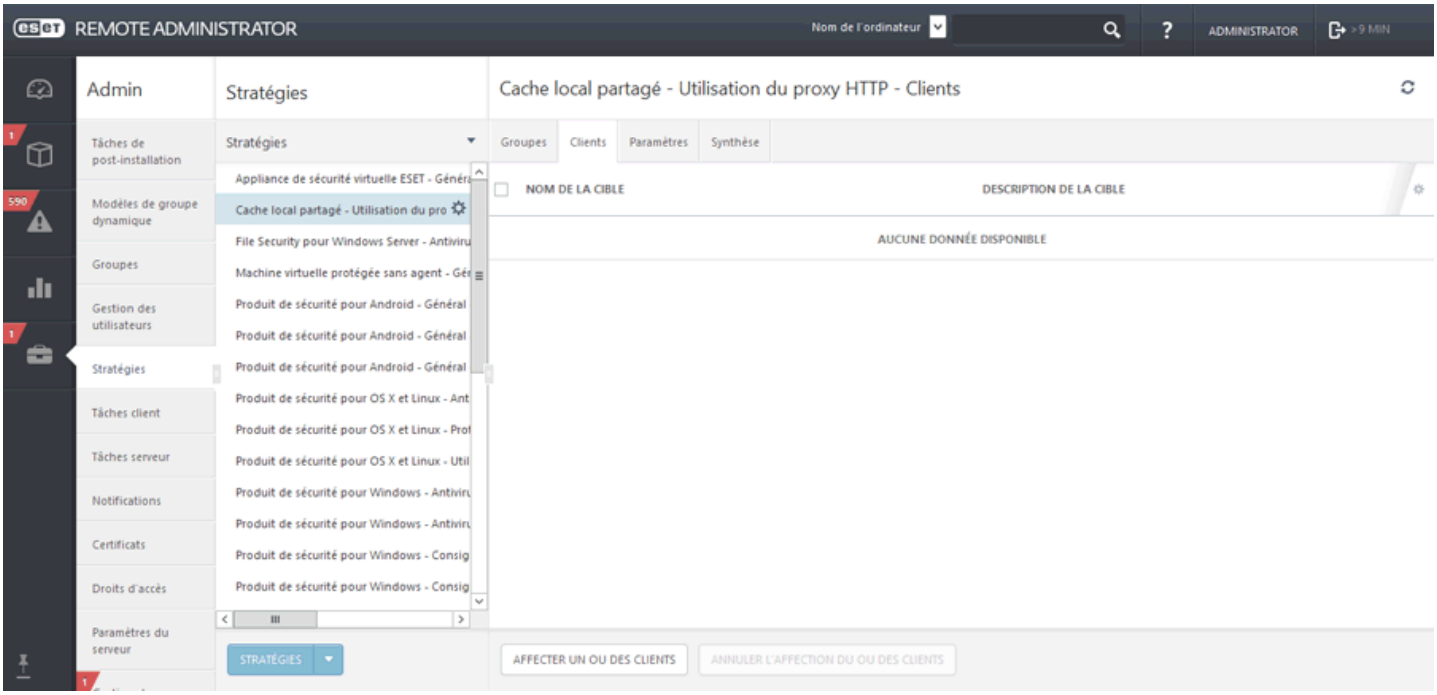


Dans la fenêtre **Ordre d'application de la stratégie**, cliquez sur **Ajouter une stratégie**. Cochez la case située en regard de la stratégie à attribuer à ce groupe, puis cliquez sur **OK**.
Cliquez sur **Enregistrer**. Pour afficher la liste des stratégies attribuées à un groupe spécifique, sélectionnez le groupe, puis cliquez sur l'onglet **Stratégies**.

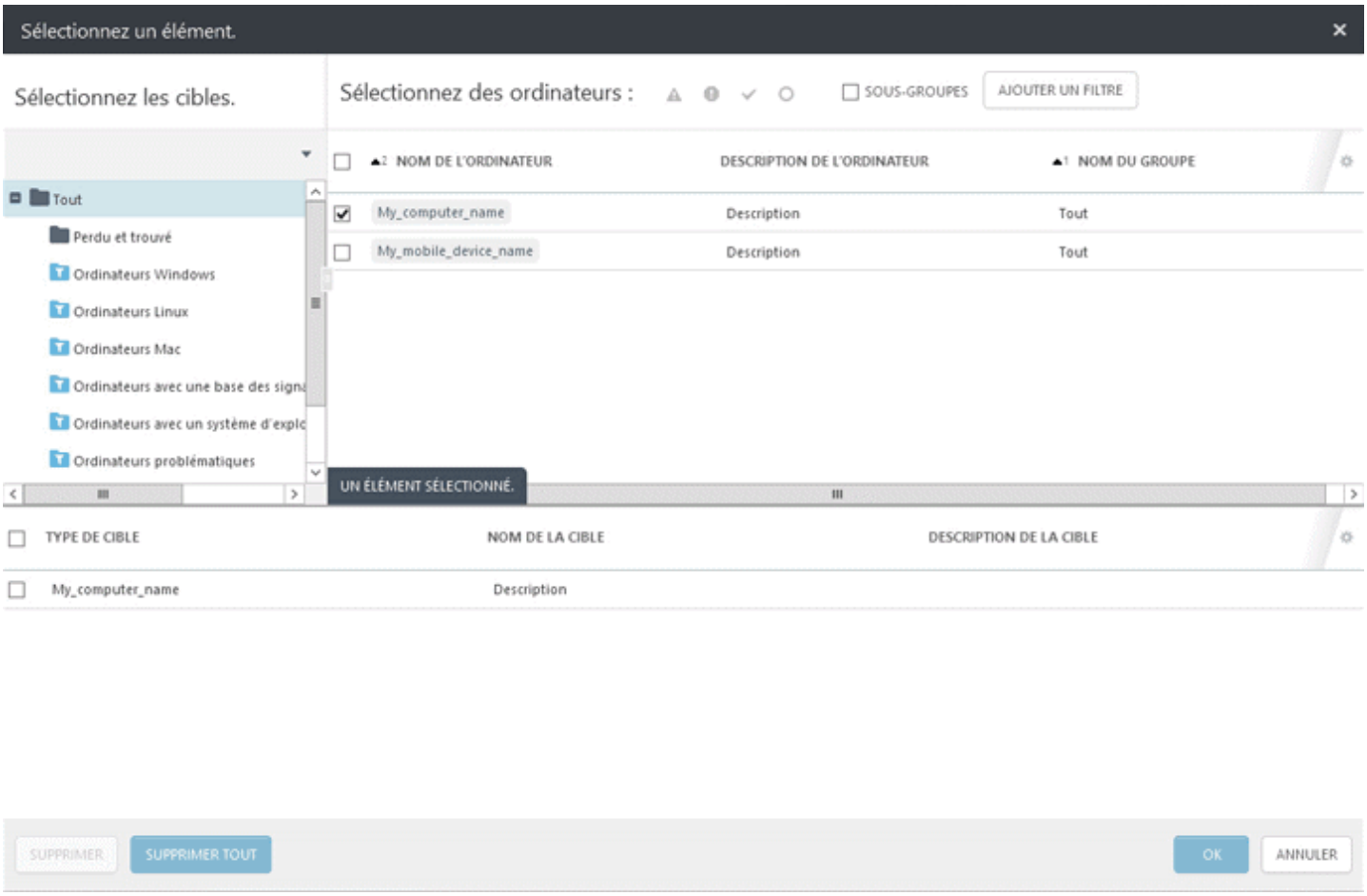
ℹ **REMARQUE** : pour plus d'informations sur les stratégies, reportez-vous au chapitre Stratégies.

4.3.12 Attribuer une stratégie à un client

Pour attribuer une stratégie à un poste de travail client, cliquez sur **Admin** > **Stratégies,** sélectionnez l'onglet **Clients**, puis cliquez sur **Affecter un ou des clients**.



Sélectionnez le ou les ordinateurs clients cibles, puis cliquez sur **OK**. La stratégie est attribuée à tous les ordinateurs sélectionnés.



4.4 Tâches client

Vous pouvez utiliser des **tâches client** pour gérer des ordinateurs clients et leurs produits de sécurité ESET. Il existe un ensemble de tâches prédéfinies qui couvrent les scénarios les plus courants. Vous pouvez également créer une tâche client personnalisée avec des paramètres spécifiques. Utilisez des tâches client pour demander une action à des ordinateurs clients.

Les tâches client peuvent être attribuées à des groupes ou des ordinateurs distincts. Une fois créée, une tâche est exécutée à l'aide d'un déclencheur. Les tâches client sont distribuées aux clients lorsque l'Agent ERA d'un client se connecte au ERA Server. De même, la communication des résultats de l'exécution des tâches vers ERA Server peut prendre également du temps. Vous pouvez gérer l'intervalle de connexion de votre Agent ERA pour réduire les durées d'exécution des tâches. Les tâches prédéfinies suivantes vous sont proposées :

Chaque **catégorie de tâche** contient des **types de tâches :**

Aoutes les tâches

- **Produit de sécurité ESET**

  Exporter la configuration des produits administrés

  Analyse à la demande

  Activation du produit

  Gestion de la quarantaine

  Exécuter un script SysInspector

  Analyse du serveur

  Installer un logiciel

Demander un rapport SysInspector

Charger un fichier mis en quarantaine

Mise à jour de la base des signatures de virus

Restauration de la mise à jour de la base des signatures de virus

ESET Remote Administrator

Mettre à jour les composants d'ESET Remote Administrator

Redéfinir l’agent cloné

Réinitialiser la base de données de Rogue Detection Sensor

Arrêter l'administration (désinstaller l'agent ERA)

Système d'exploitation

Afficher le message

Mise à jour du système d’exploitation

Exécuter une commande

Arrêter l’ordinateur

Installer un logiciel

Désinstaller un logiciel

Arrêter l'administration (désinstaller l'agent ERA)

Mobile

Actions Antivol

Inscription de périphérique

Afficher le message

Exporter la configuration des produits administrés

Analyse à la demande

Activation du produit

Installer un logiciel

Arrêter l'administration (désinstaller l'agent ERA)

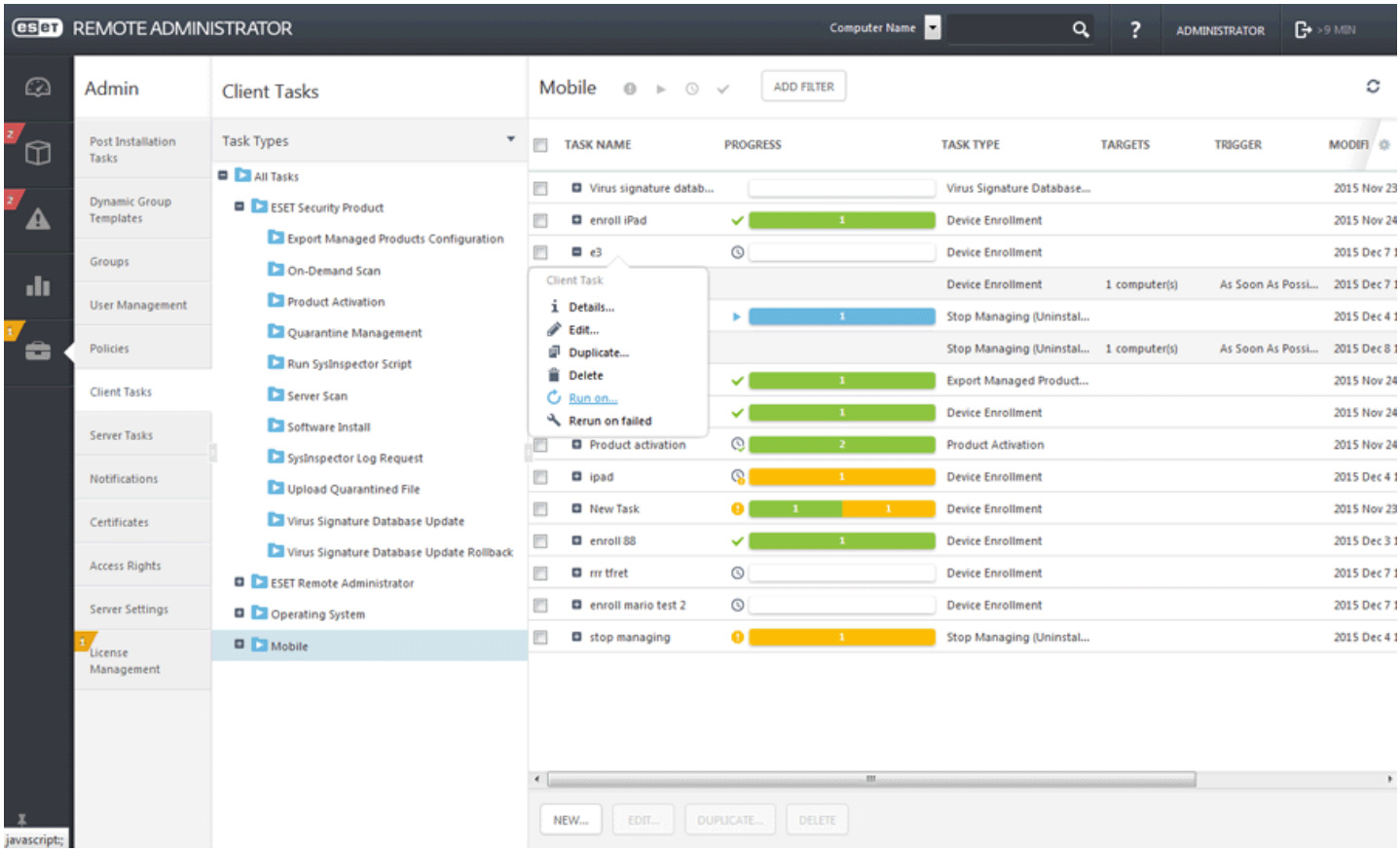
Mise à jour de la base des signatures de virus

4.4.1 Exécutions des tâches client

Il est possible de suivre l'état de chaque tâche client sous Admin > Tâches client. Pour chaque tâche, une barre d'indicateur de progression et une icône État sont affichées. Vous pouvez Descendre dans la hiérarchie pour afficher des détails supplémentaires sur une tâche client donnée et effectuer des actions supplémentaires comme Exécuter sur ou Réexécuter en cas d'échec.

IMPORTANT : Vous devez créer un déclencheur pour exécuter toutes les tâches client.

REMARQUE : de nombreuses données étant réévaluées pendant ce processus, son exécution peut donc durer plus longtemps que dans les versions précédentes (selon la tâche client, le déclencheur client et le nombre total d'ordinateurs).



- Action de la **tâche client** (cliquez sur la tâche client pour afficher le menu contextuel) :

Détails...

Les Détails de la tâche de client affichent des **informations résumées** sur la tâche. Cliquez sur l'onglet **Exécutions** pour faire passer la vue au résultat de chaque exécution. Vous pouvez Descendre dans la hiérarchie pour afficher plus de détails sur une tâche client donnée. Si les exécutions sont trop nombreuses, vous pouvez filtrer la vue pour limiter les résultats.

REMARQUE : lors de l'installation de produits ESET plus anciens, le rapport de la tâche client indiquera : La tâche a été remise au produit géré.

Modifier...

Cette option permet de modifier la tâche client sélectionnée. La modification de tâches existantes s'avère utile lorsque vous ne devez effectuer que quelques petits ajustements. Pour des tâches plus uniques, vous préférerez peut-être les créer de toutes pièces.

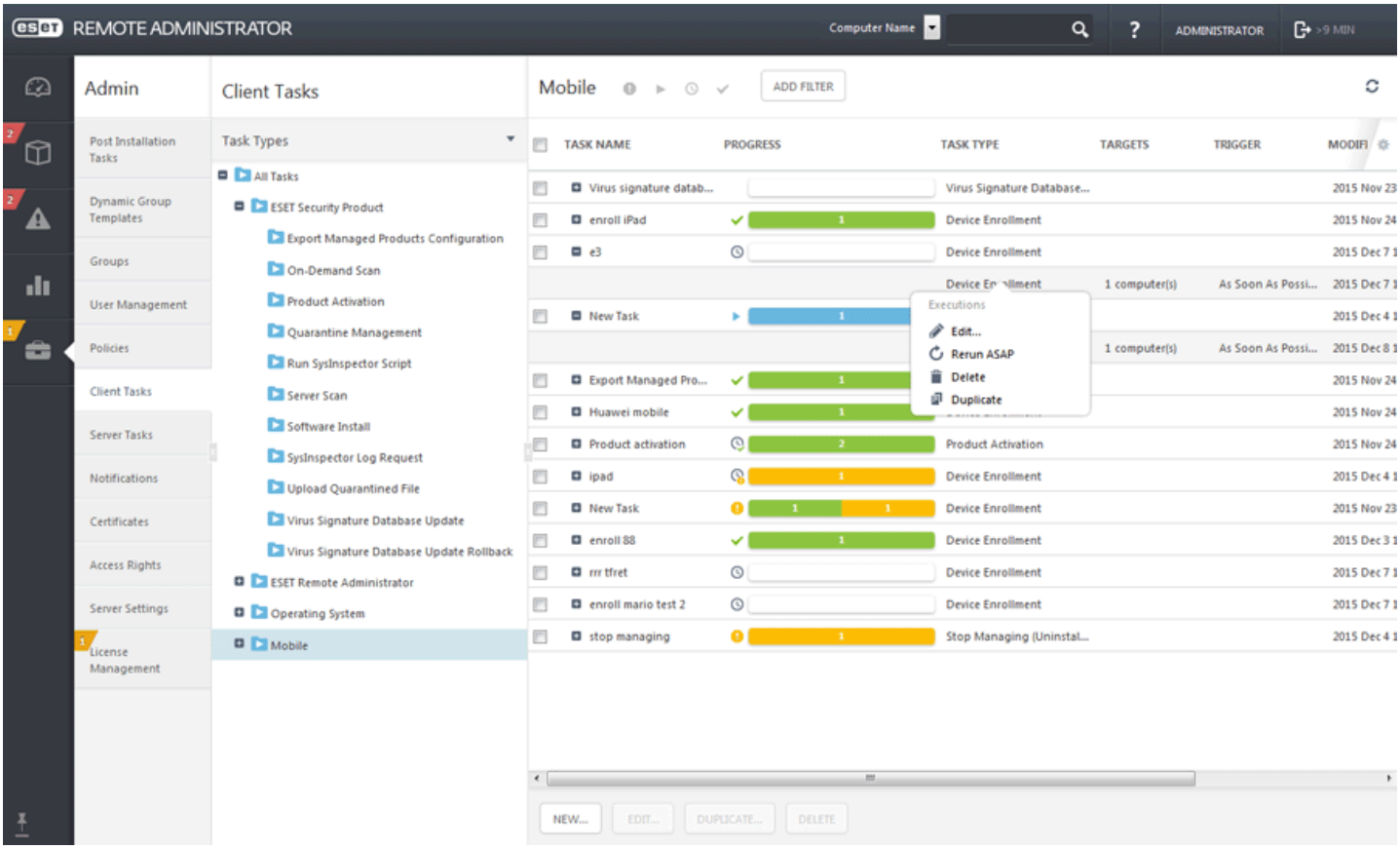
Dupliquer...

Cette option permet de créer une nouvelle tâche selon la tâche sélectionnée. Un nouveau nom est requis pour la tâche en double.

Supprimer
Supprime entièrement la ou les tâches sélectionnées.

Exécuter sur...
Ajoutez un nouveau déclencheur et sélectionnez des ordinateurs ou des groupes cibles pour cette tâche.

Réexécuter en cas d'échec
Crée un déclencheur ayant pour cibles tous les ordinateurs sur lesquels l'exécution précédente de la tâche à échoué. Vous pouvez modifier les paramètres de la tâche, si vous préférez, ou cliquer sur **Terminer** pour réexécuter la tâche inchangée.



- Action **Exécution** (utilisez le signe ⊞ pour développer la tâche client et afficher ses exécutions/déclencheurs ; cliquez sur le déclencheur pour afficher un menu contextuel) :

Modifier...
Cette option permet de modifier le déclencheur sélectionné.

Réexécuter dès que possible
Vous pouvez réexécuter la tâche client (dès que possible) en utilisant directement le déclencheur existant aucune modification.

Supprimer
Supprime entièrement le déclencheur sélectionné.

Dupliquer...
Cette option permet de créer un déclencheur sur la base de celui sélectionné. Un nouveau nom est requis pour le nouveau déclencheur.

4.4.1.1 Indicateur de progression

L'indicateur de progression est une barre de couleurs qui montre l'état de l'exécution d'une tâche client. Chaque tâche client possède son propre indicateur (affiché dans la ligne **Progression**). L'état d'exécution d'une tâche client s'affiche dans trois couleurs différentes et comprend le nombre d'ordinateurs dans cet état pour une tâche donnée :

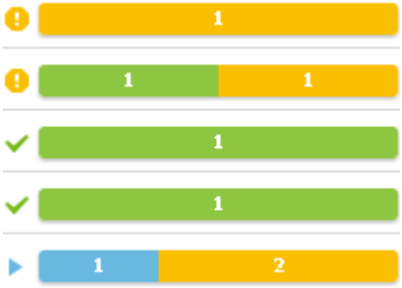
En cours (bleu)

Correctement terminé (vert)

Échec (orange)

Tâche client nouvellement créée (blanc) : il peut falloir un peu de temps pour que l'indicateur change de couleur. Le Server ERA doit recevoir une réponse de l'Agent ERA pour afficher l'état d'exécution. L'indicateur de progression sera blanc si aucun déclencheur n'est attribué.

Une combinaison de ce qui précède



Lorsque vous cliquez sur la barre de couleurs, vous pouvez sélectionner des résultats d'exécution et effectuer d'autres tâches, si nécessaire. Pour plus d'informations, voir Descendre dans la hiérarchie.

IMPORTANT : l'indicateur de progression montre l'état d'une tâche client lors de sa dernière exécution. Ces informations sont fournies par ERA Agent. L'indicateur de progression montre les informations qu'ERA Agent signale à partir des ordinateurs client.

4.4.1.2 Icône d'état

L'icône en regard de l'indicateur de progression fournit des informations supplémentaires. Elle indique si des exécutions sont planifiées pour une tâche client donnée ainsi que le résultat des exécutions terminées. Ces informations sont énumérées par ERA Server. Les états suivants sont possibles :

En cours : la tâche client est en cours d'exécution sur, au moins, une cible ; aucune exécution n'est planifiée ou n'a échoué. Cela s'applique même si la tâche client a déjà été terminée sur certaines cibles.

Réussite : - la tâche client s'est terminée sur toutes les cibles ; aucune exécution n'est planifiée ou en cours.

Erreur : la tâche client a été exécutée sur toutes les cibles, mais a échoué sur au moins une d'elles. Aucune autre exécution n'est planifiée.

Planifiée : l'exécution de la tâche client est planifiée, mais aucune exécution n'est en cours.

Planifiée/En cours : la tâche client a des exécutions planifiées (du passé ou dans le futur). Aucune exécution n'a échoué et au moins une exécution est en cours.

Planifiée/Réussite : la tâche client a encore quelques exécutions planifiées (du passé ou dans le futur), aucune exécution n'a échoué ou n'est en cours, et au moins une exécution a réussi.

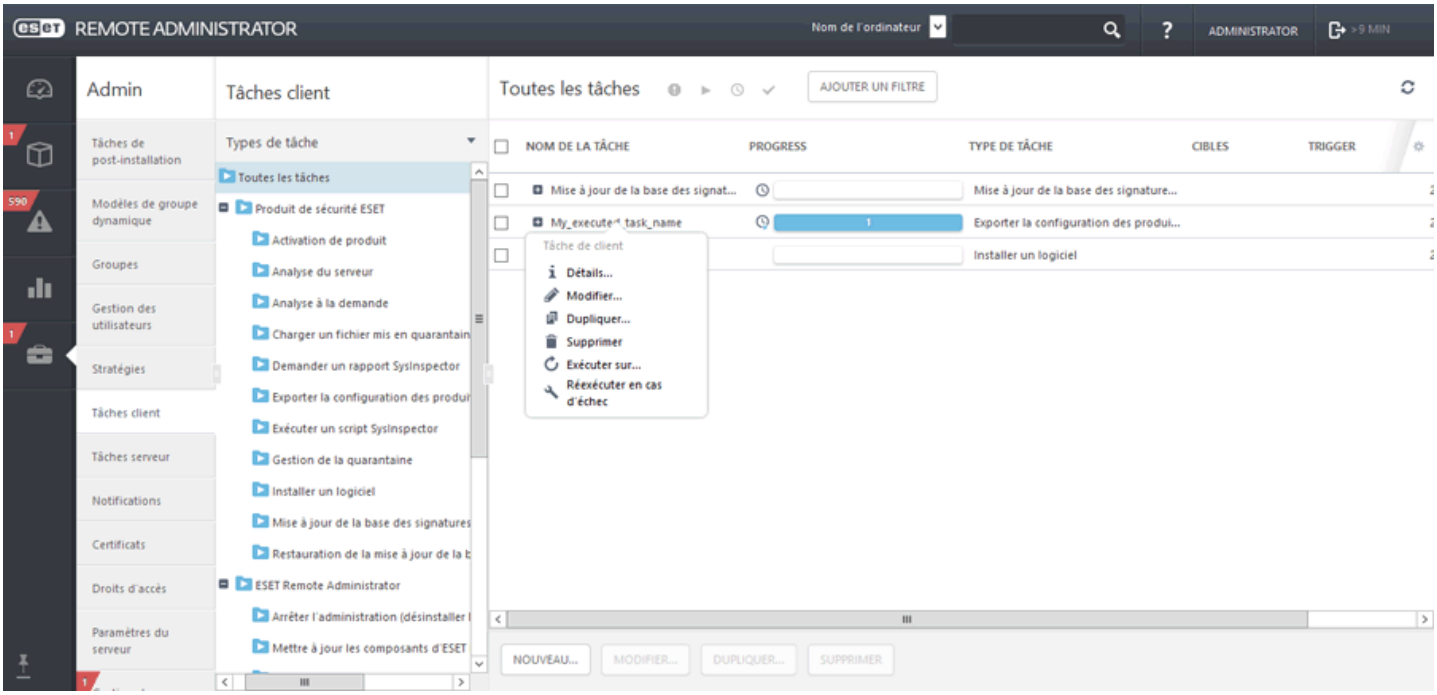
Planifiée/Erreur : la tâche client a encore quelques exécutions planifiées (du passé ou dans le futur), aucune exécution n'est en cours et au moins une exécution a échoué. Cela s'applique même si certaines exécutions se sont terminées avec succès.

4.4.1.3 Descendre dans la hiérarchie

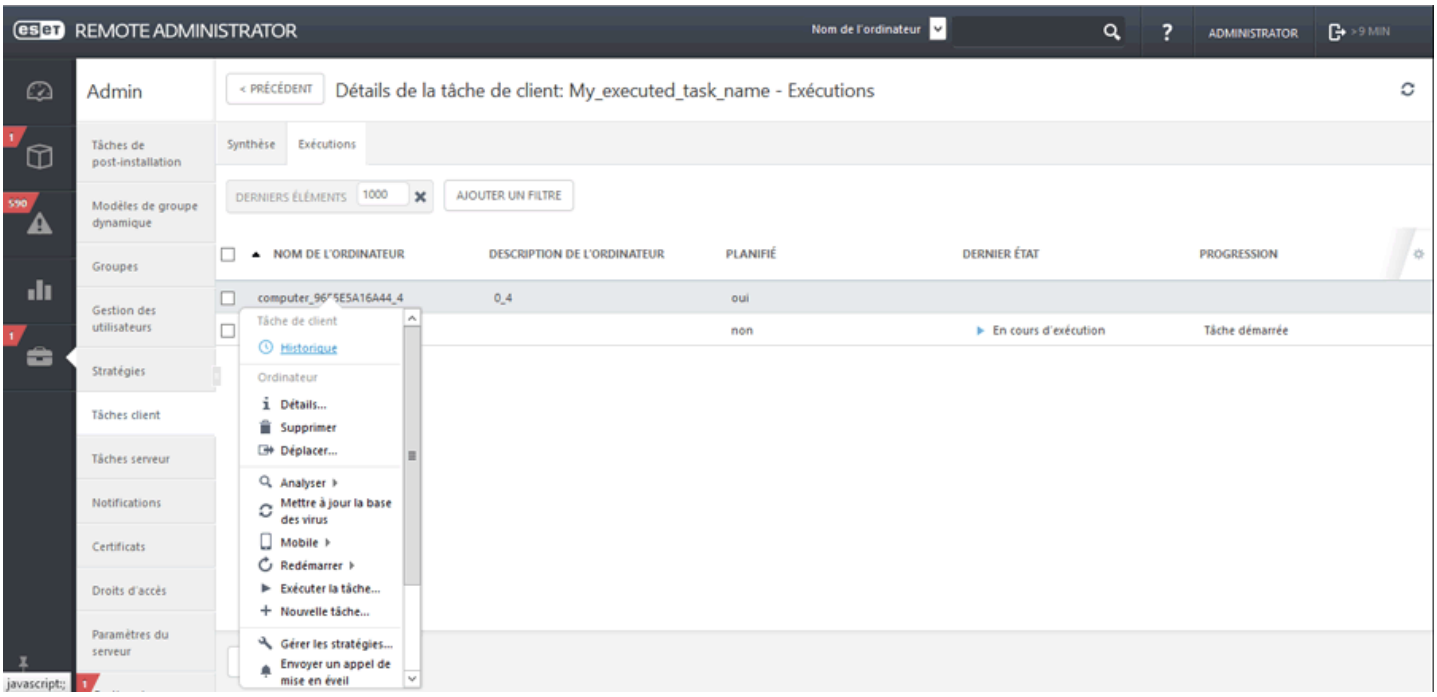
Lorsque vous cliquez sur la barre de couleurs de l'indicateur de progression, vous pouvez sélectionner l'un des résultats suivants :

- **Afficher les exécutions planifiées**
- **Afficher les exécutions en cours**
- **Afficher les réussites**
- **Afficher les échecs**

Une fenêtre Exécutions affiche la liste des ordinateurs avec le résultat sélectionné (à l'aide d'un filtre). Les ordinateurs dont le résultat est différent de celui qui a été sélectionné ne sont pas affichés. Vous pouvez modifier le filtre ou le désactiver pour afficher tous les ordinateurs indépendamment de leur dernier état.



Vous pouvez également descendre d'un autre niveau dans la hiérarchie, en sélectionnant par exemple **Historique** afin d'afficher les détails sur l'exécution de la tâche client, notamment la date d'**exécution**, l'**état** actuel, la **progression** et le **message de suivi** (le cas échéant). Vous pouvez cliquer sur **Nom de l'ordinateur** ou **Description de l'ordinateur**, puis effectuer d'autres actions, si nécessaire. Vous pouvez également afficher les détails de l'ordinateur pour un client spécifique.



REMARQUE : si le tableau de l'historique des exécutions ne contient aucune entrée, définissez le filtre **Produit** sur une durée plus longue.

4.4.1.4 Déclencheur

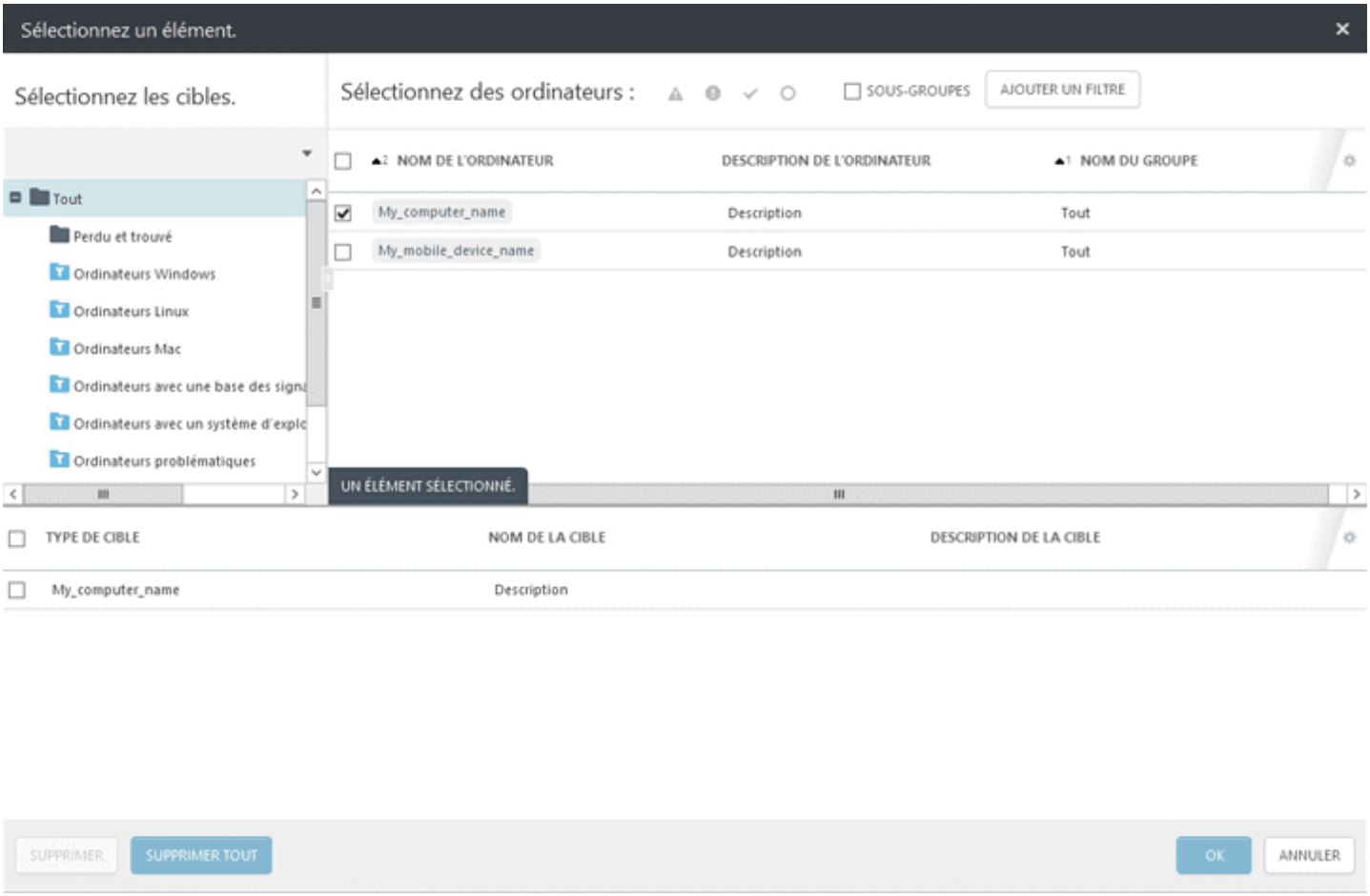
Il faut attribuer un déclencheur à une tâche client pour qu'elle soit executée. Lors de la définition d'un déclencheur, sélectionnez les ordinateurs ou les groupes **cibles** sur lesquels une tâche client doit être exécutée. Lorsque la ou les cibles sont sélectionnées, définissez les conditions du déclencheur pour exécuter la tâche à moment précisé ou lors d'un événement server. Vous pouvez également utiliser **Paramètres avancés de la limitation** pour optimiser le déclencheur, si nécessaire.

Général

Saisissez des informations de base sur le **Déclencheur** dans le cham **Description**, puis cliquez sur **Cible**.

Cible

La fenêtre **Cible** vous permet de spécifier les clients (ordinateurs ou groupes) destinataires de cette tâche. Cliquez sur **Ajouter des cibles** pour afficher tous les groupes statiques et dynamiques et leurs membres.



Sélectionnez des clients, cliquez sur **OK**, puis passez à la section Déclencheur.

Déclencheur : détermine l'événement qui déclenche la tâche.

- **Dès que possible** : exécute la tâche dès que le client se connecte à ESET Remote Administrator Server et la reçoit. Si la tâche ne peut pas être effectuée avant la **date d'expiration**, elle est retirée de la file d'attente. La tâche n'est pas supprimée, mais elle ne sera pas exécutée.
- **Déclencheur planifié** : exécute la tâche à une date sélectionnée. Vous pouvez planifier la tâche une seule fois, de manière répétée ou à l'aide d'une expression CRON.
- **Déclencheur lié au Journal des événements** : exécute la tâche selon les événements spécifiés dans cette zone. Ce déclencheur est invoqué lorsqu'un événement d'un certain type se produit dans les journaux. Définissez le **type de journal**, l'**opérateur logique** et les critères de **filtrage** qui déclencheront cette tâche.
- **Déclencheur A rejoint le groupe dynamique** : ce déclencheur exécute la tâche lorsqu'un client rejoint le groupe dynamique sélectionné dans l'option cible. Si un groupe statique ou un client a été sélectionné, cette option ne sera pas disponible.

REMARQUE : pour plus d'informations sur les déclencheurs, reportez-vous au chapitre Déclencheurs.

Paramètres avancés de la limitation : une limitation sert à limiter l'exécution d'une tâche si cette dernière est déclenchée par un événement qui se produit fréquemment, comme dans les cas **Déclencheur lié au Journal des événements** et **Déclencheur A rejoint le groupe dynamique** (voir ci-dessus). Pour plus d'informations, reportez-vous au chapitre Limitation.

Lorsque vous avez défini les destinataires et les déclencheurs de cette tâche, cliquez sur **Terminer**.

4.4.2 Arrêter l'ordinateur

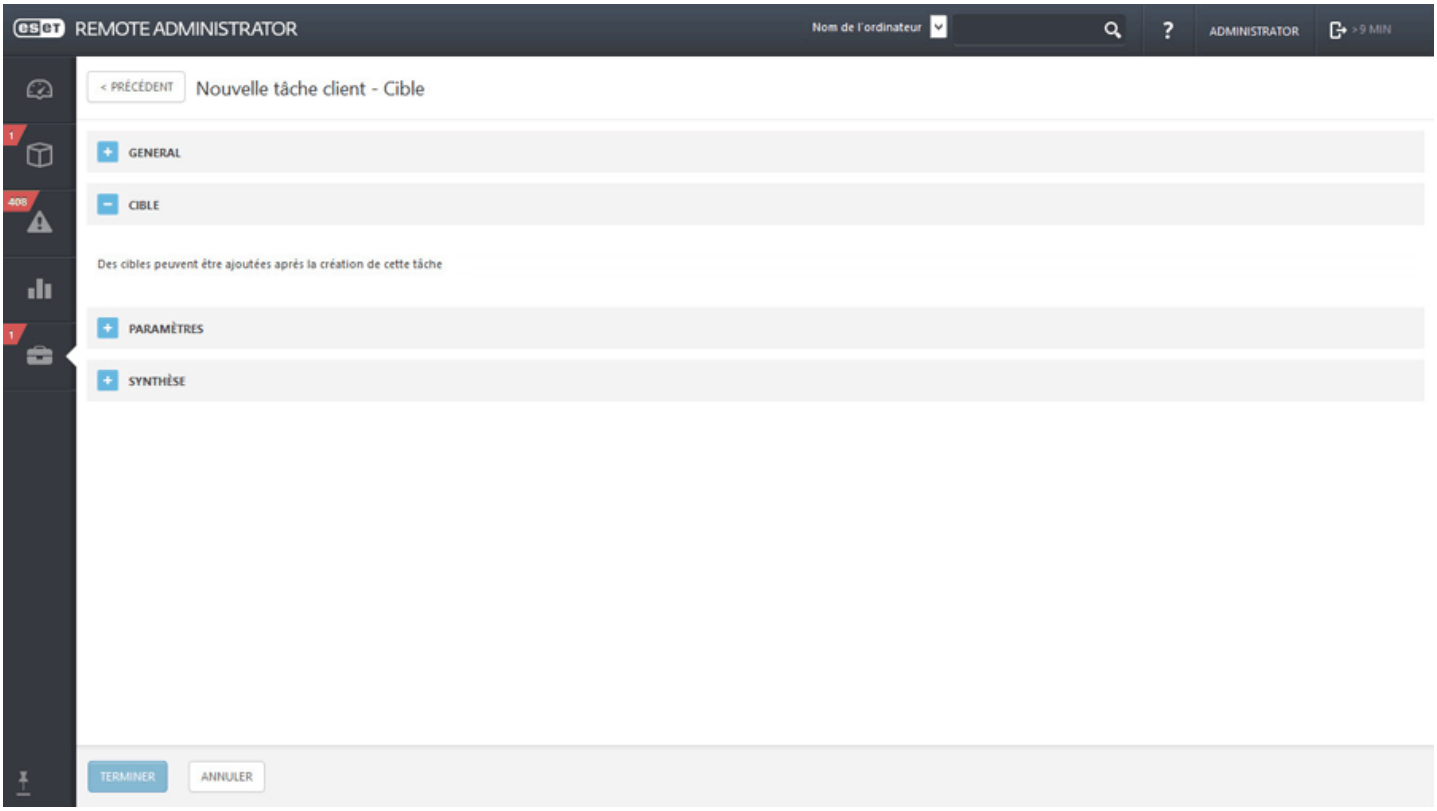
Vous pouvez utiliser la tâche **Arrêter l'ordinateur** ou redémarrer les ordinateurs clients. Cliquez sur **Nouveau...** pour commencer à configurer la nouvelle tâche.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Arrêter l'ordinateur**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.

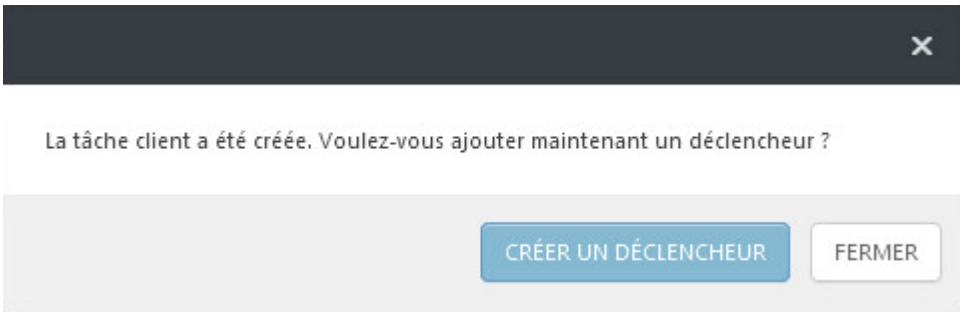


Paramètres

- **Redémarrer le ou les ordinateurs** : cochez cette case si vous voulez redémarrer après l'achèvement de la tâche. Si vous voulez arrêter le ou les ordinateurs, ne cochez pas cette case.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.3 Analyse à la demande

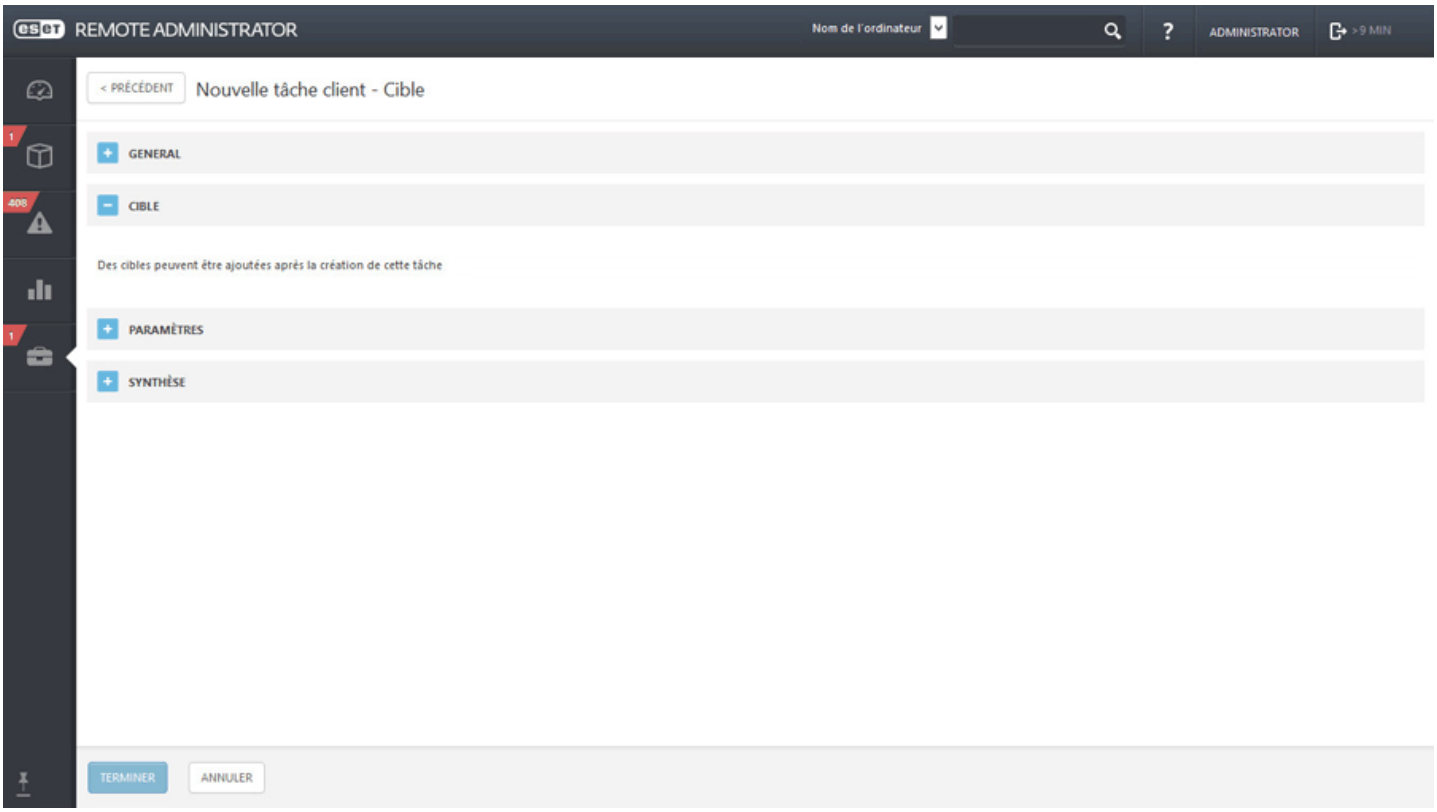
La tâche **Analyse à la demande** vous permet d'exécuter manuellement une analyse sur l'ordinateur client (en plus d'une analyse régulière planifiée). Cliquez sur **Nouveau...** pour commencer à configurer la nouvelle tâche.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Analyse à la demande**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



Paramètres

Arrêter après l'analyse : si vous cochez cette case, l'ordinateur s'arrête à la fin de l'analyse.

Profil d'analyse : vous pouvez sélectionner le profil de votre choix dans le menu déroulant :

- **Analyse approfondie** - Il s'agit d'un profil prédéfini sur le client. Il est configuré pour être le profil d'analyse le plus complet. Il vérifie l'intégralité du système mais prend le plus de temps et utilise le plus de ressources.
- **Analyse intelligente -** L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. Elle présente l'intérêt d'être facile à utiliser et de ne pas nécessiter de configuration détaillée. L'analyse intelligente vérifie tous les fichiers des disques locaux, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut.
- **Analyse à partir du menu contextuel** - Analyse un client à l'aide d'un profil d'analyse prédéfini. Il est possible de personnaliser les cibles à analyser.
- **Profil personnalisé** - L'analyse personnalisée vous permet de spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. Elle a l'avantage de permettre la configuration précise des paramètres. Les configurations peuvent être enregistrées dans des profils d'analyse définis par l'utilisateur, ce qui permet de répéter facilement une analyse avec les mêmes paramètres. Avant d'exécuter la tâche avec l'option de profil personnalisé, vous devez créer un profil. Lorsque vous sélectionnez un profil personnalisé dans le menu déroulant, saisissez le nom exact du profil dans le champ de texte **Profil personnalisé**.

Nettoyage

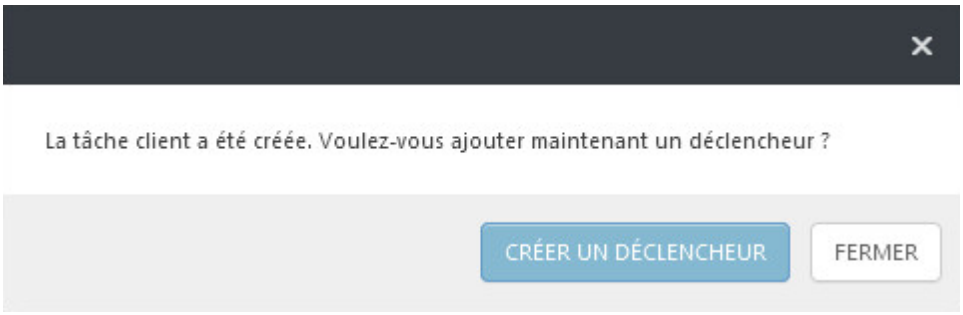
Par défaut, l'option **Analyse avec nettoyage** est sélectionnée. Cela signifie que lorsque des objets infectés sont détectés, ils sont automatiquement nettoyés. Si le nettoyage est impossible, ils sont alors mis en quarantaine.

Cibles à analyser

Cette option est également sélectionnée par défaut. À l'aide de ce paramètre, toutes les cibles spécifiées dans le profil d'analyse sont analysées. Si vous désélectionnez cette option, vous devez manuellement spécifier les cibles à analyser dans le champ **Ajouter une cible**. Saisissez la cible à analyser dans ce champ, puis cliquez sur **Ajouter**. La cible s'affiche alors dans le champ Cibles à analyser.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.4 Mise à jour du système d’exploitation

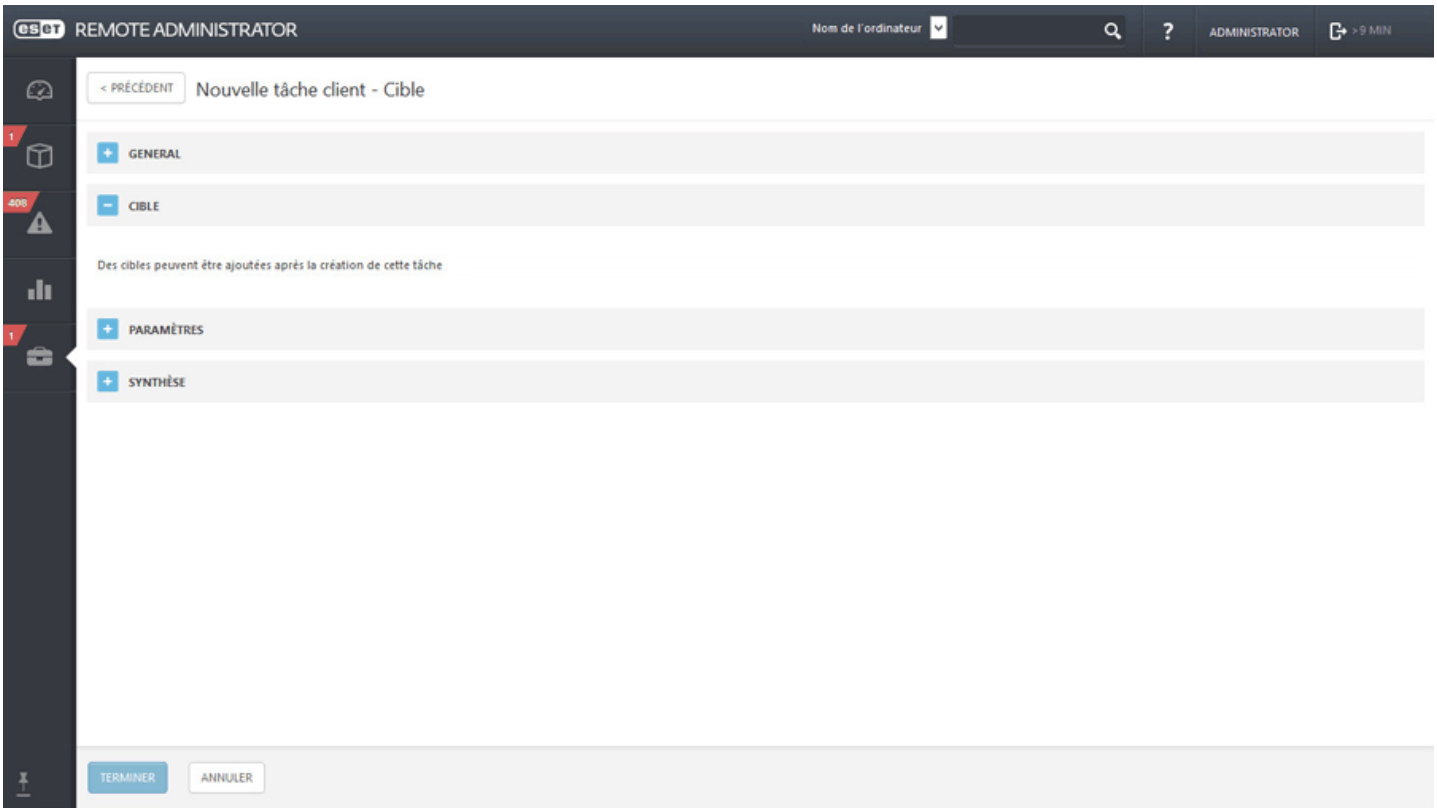
La tâche **Mise à jour du système d'exploitation** sert à mettre à jour le système d'exploitation sur l'ordinateur client. Elle peut déclencher la mise à jour du système d’exploitation sur les systèmes d’exploitation Windows, OS X et Linux.

Général

Saisissez des informations de base sur la tâche, comme un **Nom** et une **Description**, puis sélectionnez la tâche **Mettre à jour le système d’exploitation**. Le **type de tâche** (voir la liste de types de tâche client) définit les paramètres et le comportement de la tâche.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.

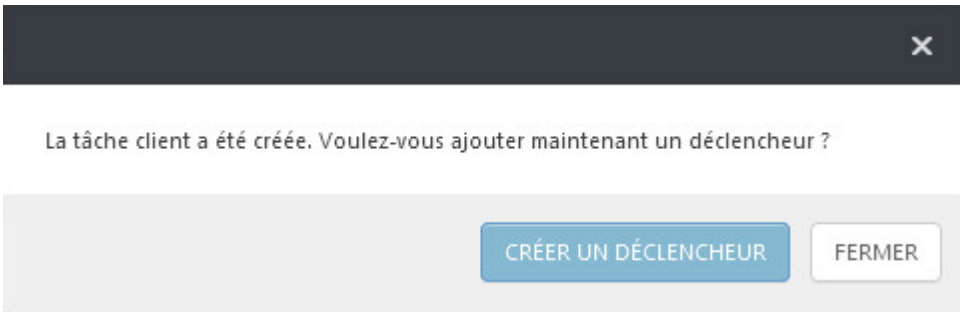


Paramètres

- **Accepter automatiquement le CLUF** : sélectionnez cette case à cocher si vous souhaitez accepter automatiquement le CLUF. Aucun texte ne sera affiché à l'utilisateur.
- **Installer les mises à jour facultatives** : cette option s'applique uniquement aux systèmes d'exploitation Windows ; les mises à jour marquées comme facultatives ne seront pas installées.
- **Autoriser le redémarrage** : cette option s'applique uniquement aux systèmes d'exploitation Windows. Elle entraîne le redémarrage de l'ordinateur client une fois les mises à jour installées.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.5 Gestion de la quarantaine

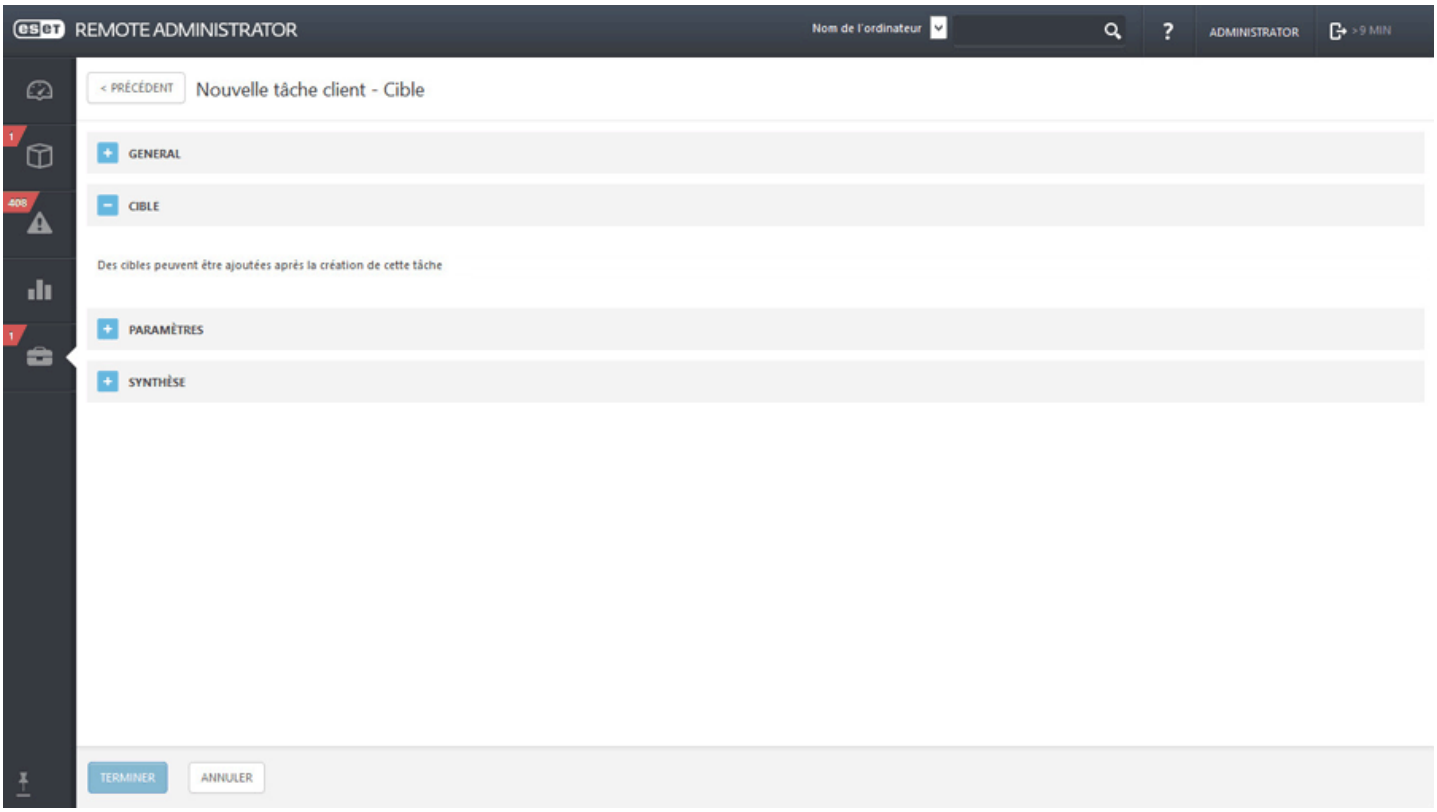
La tâche **Gestion de la quarantaine** sert à gérer les objets en quarantaine ERA Server, à savoir les objets infectés ou suspects détectés pendant l'analyse.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Gestion de la quarantaine**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



Paramètres

Paramètres de gestion de la quarantaine

Action : sélectionnez l'action à exécuter sur l'objet en quarantaine.

- **Restaurer le ou les objets** (restaure l'objet à son emplacement d'origine ; l'objet sera toutefois analysé et remis en quarantaine si les raisons de sa précédente mise en quarantaine subsistent).
- **Restaurer le ou les objets et les exclure dans le futur** (restaure l'objet à son emplacement d'origine ; il ne sera plus remis en quarantaine).
- **Supprimer le ou les objets** (supprime entièrement l'objet).

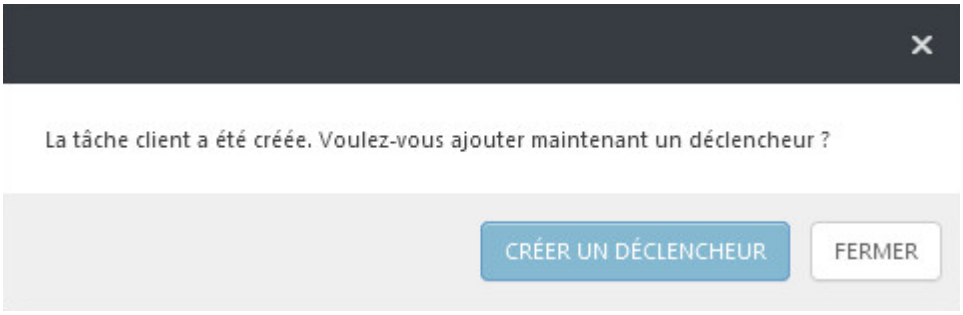
Type de filtre : permet de filtrer les objets en quarantaine selon les critères définis ci-dessous. Ces critères sont la chaîne de hachage de l'objet ou des conditions.

Paramètres de filtre conditionnel :

- **Paramètres de filtre de hachage :** ajoutez des éléments de hachage dans le champ. Seuls des objets connus (un objet ayant été déjà mis en quarantaine, par exemple) peuvent être saisis.
- **Effectué du/au** : définissez la période à laquelle l'objet a été mis en quarantaine.
- **Taille minimale/maximale (octets)** : définissez la plage de tailles de l'objet mis en quarantaine (en octets).
- **Nom de la menace** : sélectionnez une menace dans la liste des éléments mis en quarantaine.
- **Nom de l'objet** : sélectionnez un objet dans la liste des éléments mis en quarantaine.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



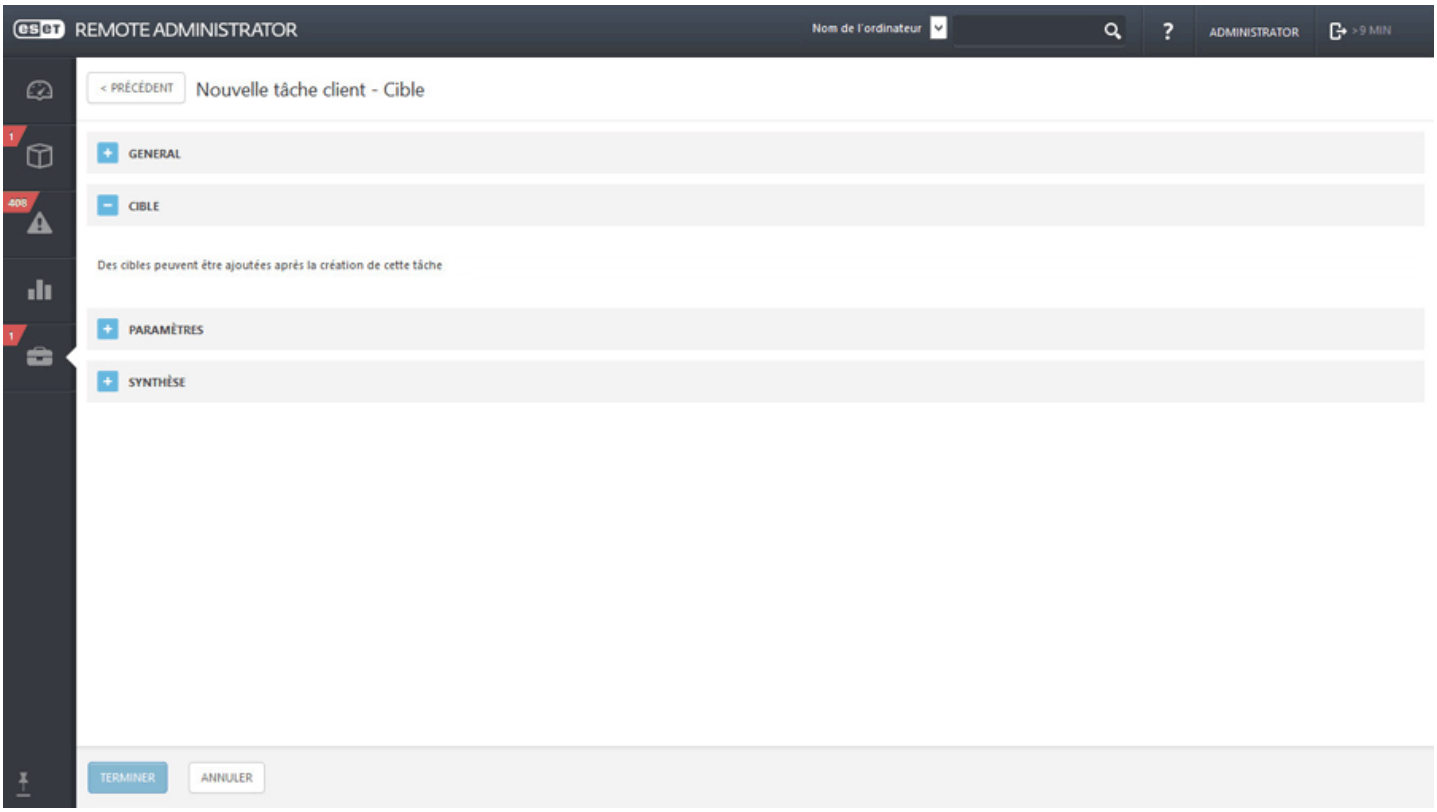
4.4.6 Réinitialiser la base de données de Rogue Detection Sensor

La tâche **Réinitialiser la base de données de Rogue Detection Sensor** sert à réinitialiser le cache de recherche RD Sensor. La tâche supprime le cache pour que les résultats de recherche puissent être de nouveau stockés. Elle ne supprime pas les ordinateurs détectés. Cette tâche s'avère utile lorsque les ordinateurs détectés figurent toujours dans le cache et ne sont pas signalés au serveur.

REMARQUE : aucun **paramètre** n'est disponible pour cette tâche.

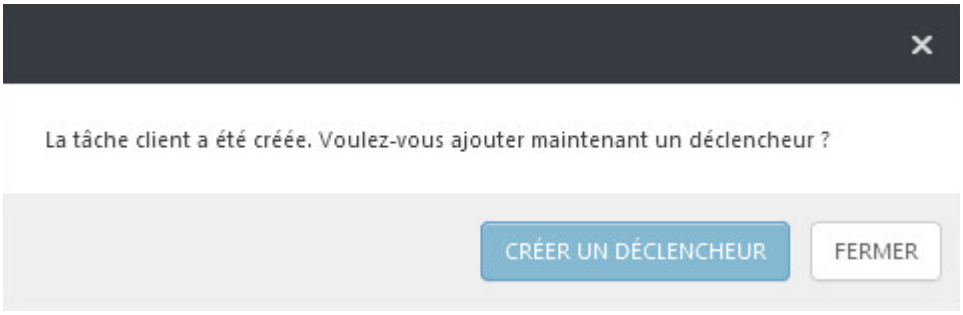
Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.7 Mettre à jour les composants d'ESET Remote Administrator

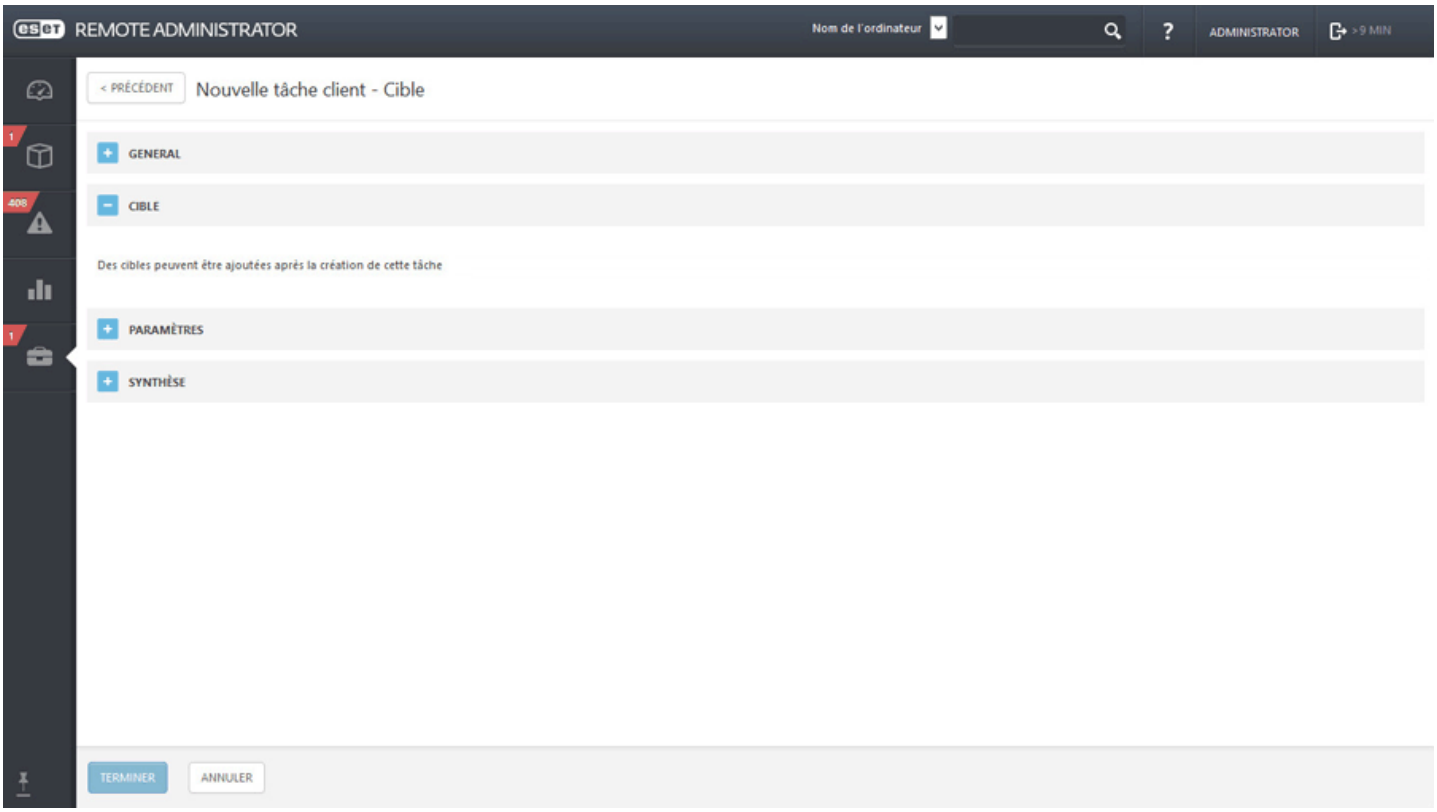
La tâche **Mettre à jour les composants d'ESET Remote Administrator** sert à mettre à niveau les composants d'ERA (ERA Agent, ERA Proxy, ERA Server et MDM). Vous pouvez l'utiliser lorsque vous souhaitez par exemple effectuer une mise à niveau d'ERA version 6.1.28.0 ou 6.1.33.0 vers ERA version 6.2.x. Pour obtenir des instructions détaillées, reportez-vous à la section Mise à niveau des composants.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Mettre à jour les composants d'ESET Remote Administrator**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



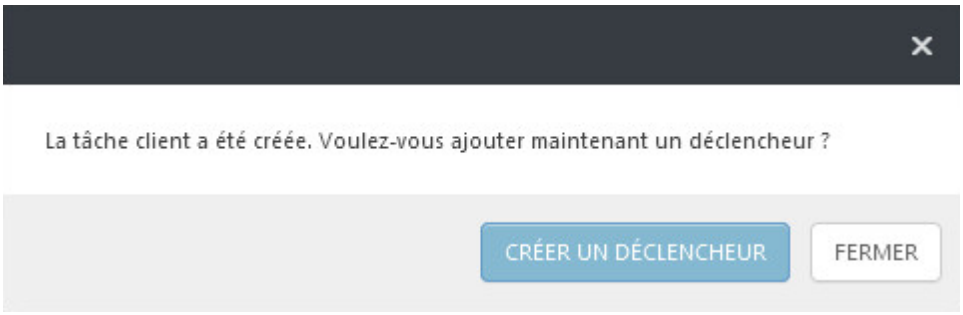
Paramètres

Cochez la case en regard de l'option **J'accepte les termes du Contrat de Licence Utilisateur Final de l'application** si vous les acceptez. Pour plus d'informations, reportez-vous à Gestion de licences ou CLUF.

- **Référencer Remote Administrator Server** : sélectionnez une version d'ERA Server dans la liste. Tous les composants ERA seront mis à niveau vers les versions compatibles avec le serveur sélectionné.
- **Redémarrage automatique si nécessaire** : vous pouvez forcer le redémarrage du système d'exploitation client si l'installation le requiert.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



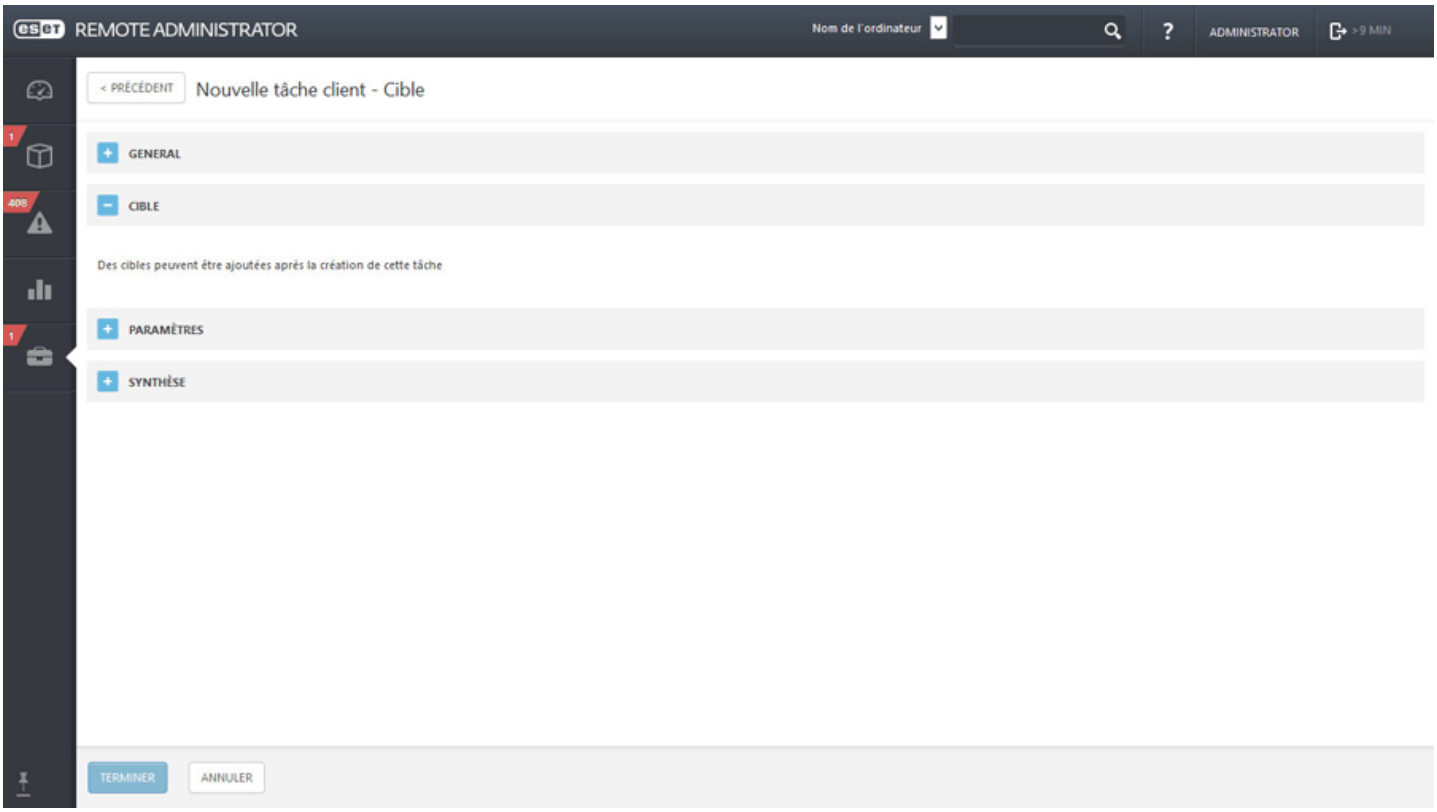
4.4.8 Redéfinir l'agent cloné

La tâche **Redéfinir l'agent cloné** peut servir à distribuer l'Agent ESET sur votre réseau par le biais d'une image prédéfinie. Les Agents clonés possèdent le même SID, ce qui peut entraîner des problèmes (plusieurs agents dotés du même SID). Pour résoudre ce problème, utilisez la tâche Redéfinir l'agent cloné pour redéfinir le SID afin d'attribuer aux agents une identité unique.

REMARQUE : aucun **paramètre** n'est disponible pour cette tâche.

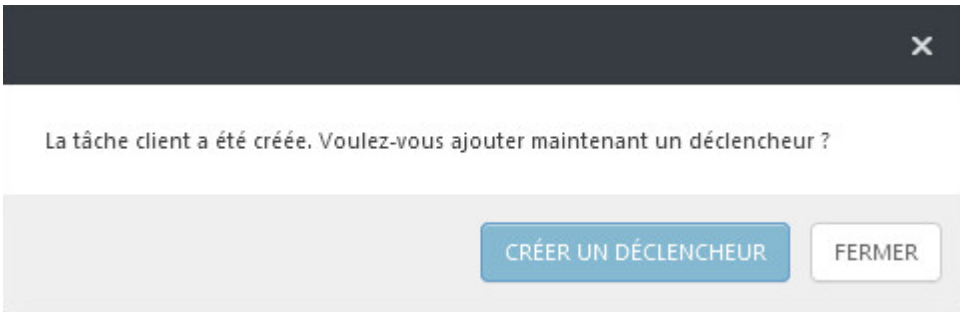
Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.9 Exécuter une commande

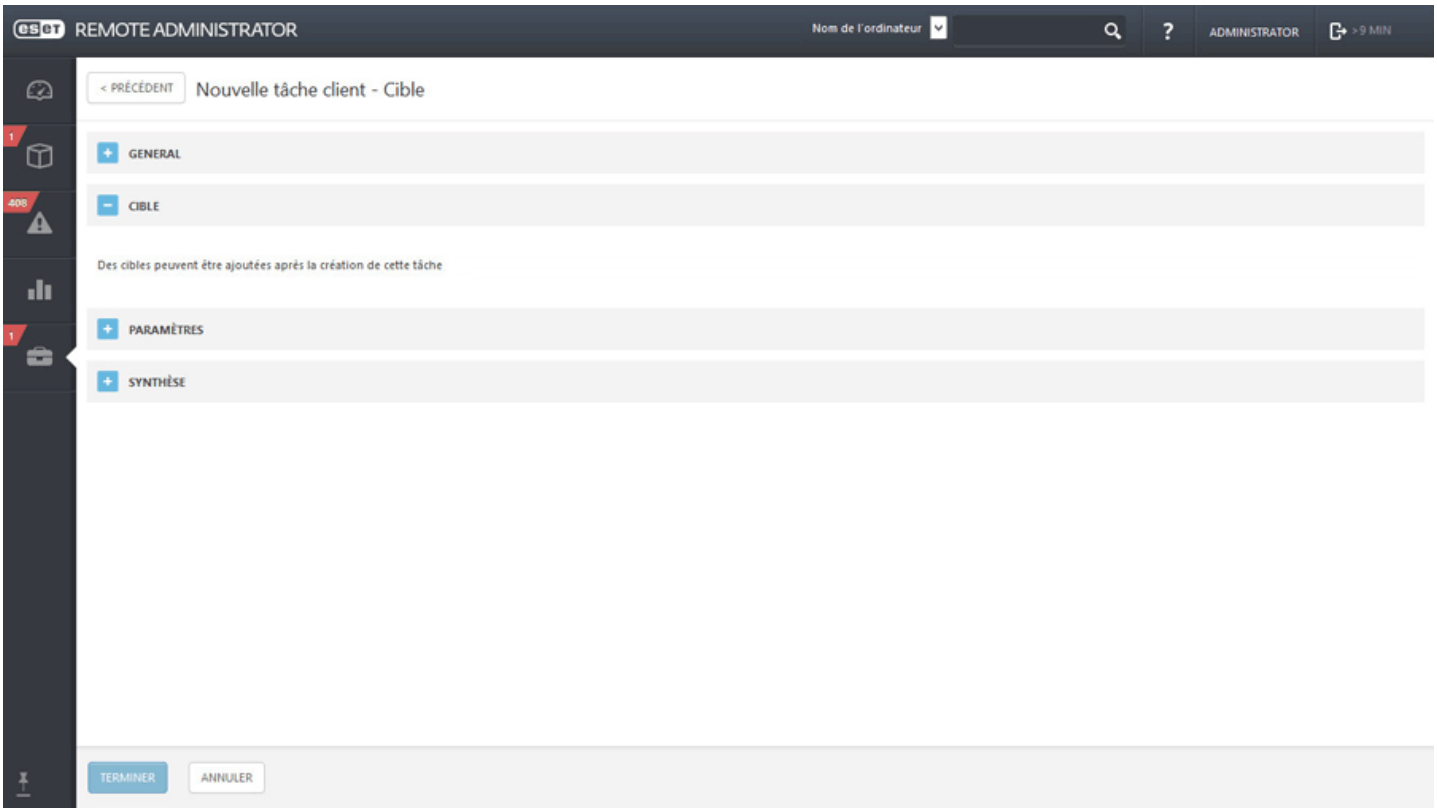
La tâche **Exécuter une commande** peut servir à exécuter des instructions de ligne de commande spécifiques sur le client. L'administrateur peut spécifier l'entrée de ligne de commande à exécuter.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Exécuter une commande**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



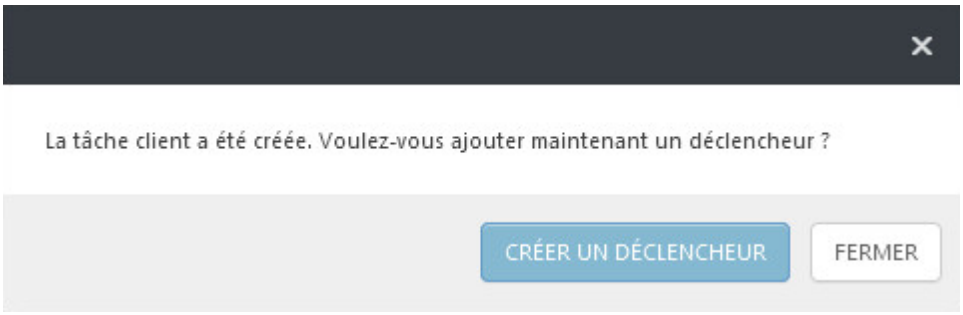
Paramètres

- **Ligne de commande à exécuter** : saisissez la ligne de commande à exécuter sur le ou les clients.
- **Répertoire de travail** : saisissez un répertoire dans lequel la ligne de commande ci-dessus sera exécutée.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un

déclencheur ultérieurement.



4.4.10 Exécuter un script SysInspector

La tâche **Exécuter le script SysInspector** sert à supprimer les objets indésirables du système. Avant d'utiliser cette tâche, un **script SysInspector** doit être exporté à partir d'ESET SysInspector. Une fois le script exporté, vous pouvez marquer les objets à supprimer et exécuter le script avec les données modifiées. Les objets marqués sont alors supprimés.

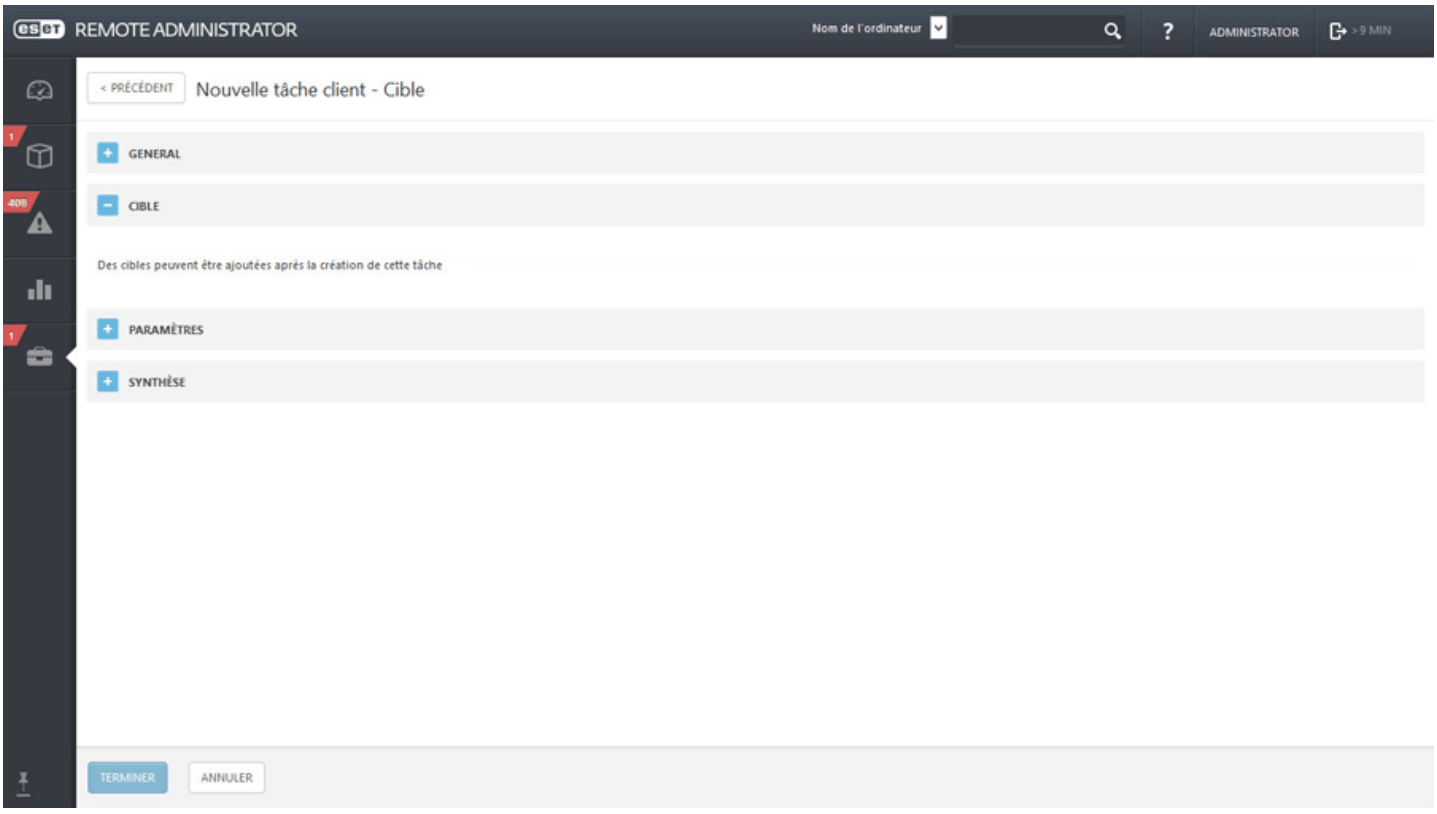
Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Exécuter un script SysInspector**.

REMARQUE : une fois la tâche terminée, vous pouvez consulter les résultats dans un rapport.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.

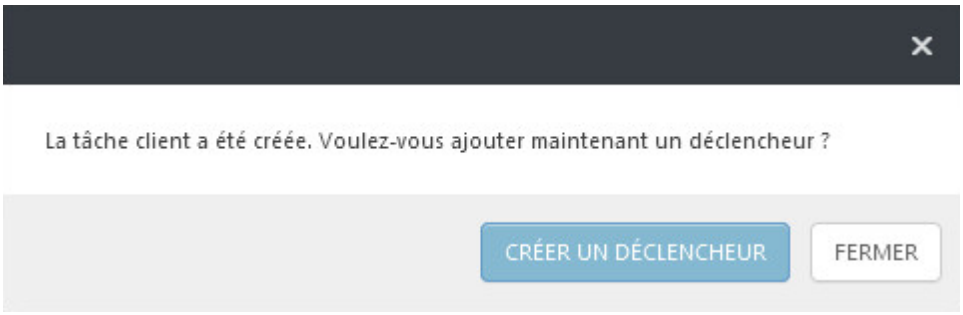


Paramètres

- **Script SysInspector** : cliquez sur **Parcourir** pour accéder au script de service. Le script de service doit être créé avant l'exécution de la tâche.
- **Action** : vous pouvez **charger** ou **télécharger** un script sur la console ERA.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



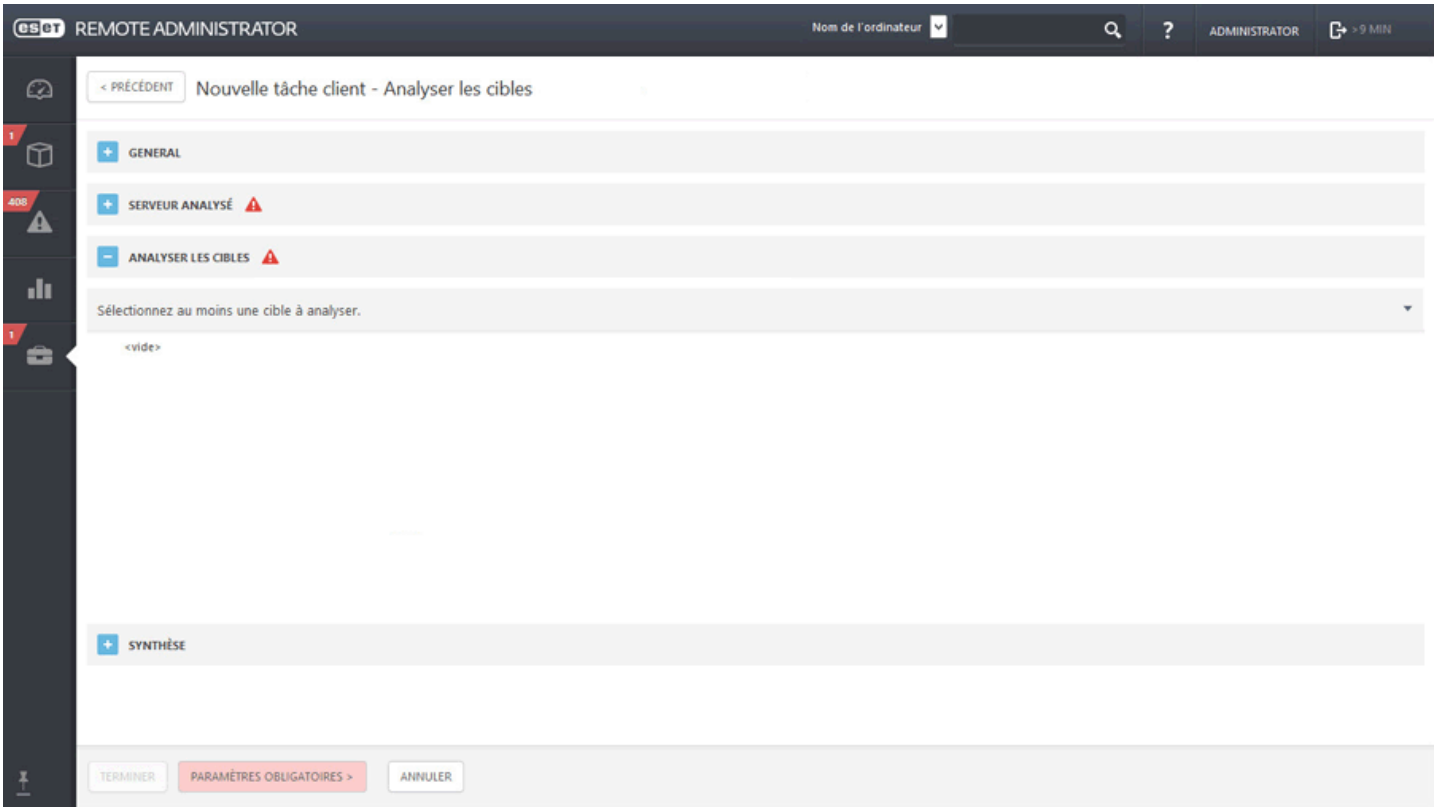
4.4.11 Analyse du serveur

Vous pouvez utiliser la tâche **Analyse du serveur** pour analyser les clients sur lesquels des solutions ESET Server sont installées (actuellement ESET File Security 6 et ESET Mail Security 6).

Serveur analysé : cliquez sur **Sélectionner** pour choisir un serveur à analyser. Un seul serveur peut être sélectionné.

Cibles à analyser : affiche les ressources disponibles pour l'analyse sur le serveur sélectionné.

REMARQUE : la première fois que vous utilisez l'option **Générer la liste des cibles**, patientez environ la moitié de la durée de la **période de mise à jour** spécifiée pour obtenir la liste. Par exemple, si la **période de mise à jour** est définie sur 60 minutes, patientez 30 minutes avant de recevoir la liste des cibles à analyser. Pour plus d'informations, consultez Cibles à analyser ERA.



REMARQUE : vous pouvez utiliser la tâche **Analyse du serveur** pour effectuer une analyse Hyper-V sur ESET File Security 6, ainsi qu'une analyse de base de données de boîtes aux lettres à la demande et une analyse Hyper-V sur ESET Mail Security 6. D'autres méthodes d'analyse ne sont pas disponibles pour l'instant.

4.4.12 Installer un logiciel

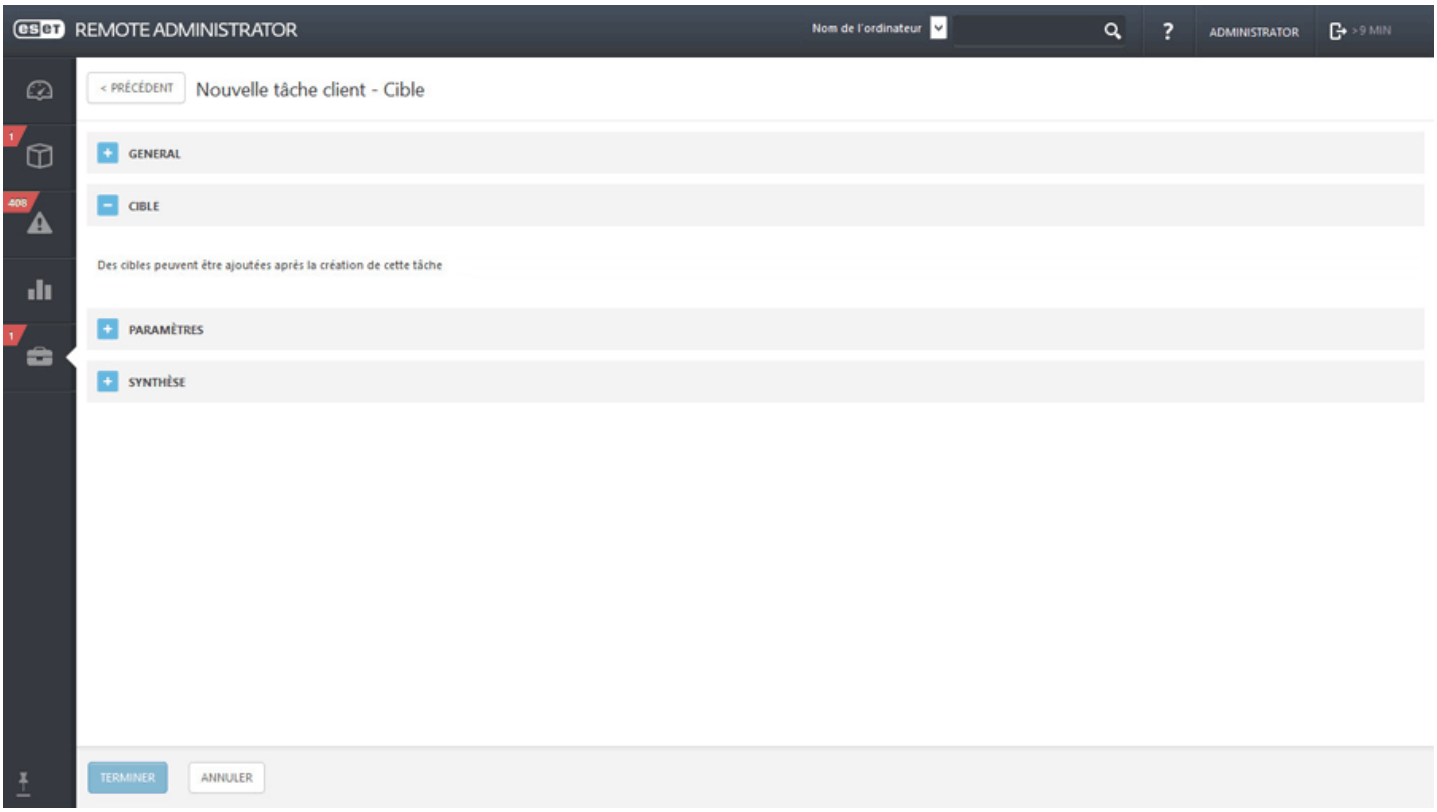
La tâche **Installer un logiciel** sert à installer des logiciels sur les ordinateurs clients. Bien qu'elle soit principalement destinée à installer des produits ESET, vous pouvez l'utiliser pour installer n'importe quel logiciel.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Installation de logiciel**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



Paramètres

Cochez la case en regard de l'option **J'accepte les termes du Contrat de Licence Utilisateur Final de l'application** si vous les acceptez. Pour plus d'informations, reportez-vous à Gestion de licences ou CLUF.

Cliquez sur **<Choisir une licence ESET>**, puis sélectionnez la licence adéquate pour le produit installé dans la liste des licences disponibles.

Cliquez sur **<Sélectionner un package>** pour sélectionner un package d'installation dans le référentiel ou indiquez une URL de package. Une liste de packages disponibles s'affiche dans laquelle vous pouvez sélectionner le produit ESET à installer (ESET Endpoint Security, par exemple). Sélectionnez le package d'installation souhaité, puis cliquez sur **OK**. Si vous souhaitez indiquer une URL vers l'emplacement du package d'installation, saisissez-la ou copiez-la et collez-la (par exemple, *file://\\pc22\install\ees_nt64_ENU.msi*) dans le champ de texte (n'utilisez pas d'URL qui requiert une authentification).

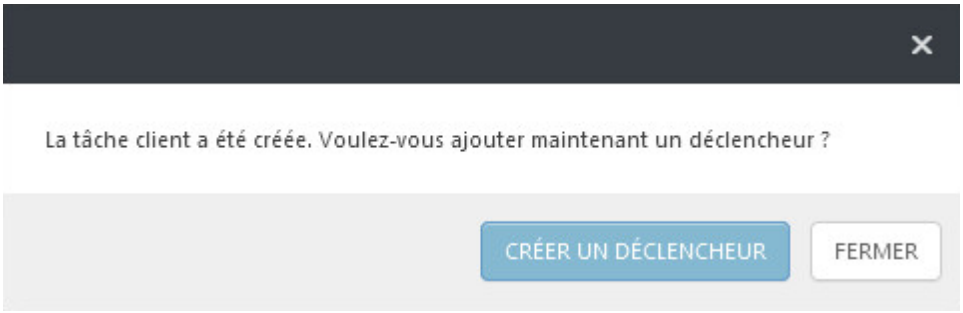
http://server_address/ees_nt64_ENU.msi : si vous effectuez l'installation à partir d'un serveur Web public ou de votre serveur HTTP.
file://\\pc22\install\ees_nt64_ENU.msi : si vous effectuez l'installation à partir d'un chemin d'accès réseau.
file://C:\installs\ees_nt64_ENU.msi : si vous effectuez l'installation à partir d'un chemin d'accès local.

REMARQUE : notez qu'ERA Server et ERA Agent doivent avoir accès à Internet pour accéder au référentiel et effectuer l'installation. Si vous ne disposez pas d'un accès Internet, vous pouvez installer manuellement le logiciel client.

Si nécessaire, vous pouvez spécifier des paramètres dans le champ Paramètres d'installation. Sinon, laissez ce champ vide. Cochez la case en regard de l'option **Redémarrage automatique si nécessaire** pour forcer un redémarrage automatique de l'ordinateur client après l'installation. Vous pouvez également décocher cette option pour redémarrer manuellement l'ordinateur client.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.13 Désinstaller un logiciel

La tâche **Désinstallation de logiciel** sert à désinstaller des produits ESET des clients lorsqu'ils ne sont plus nécessaires/souhaités. Si vous désinstallez ERA Agent, les produits ESET administrés par celui-ci peuvent conserver certains paramètres après sa désinstallation.

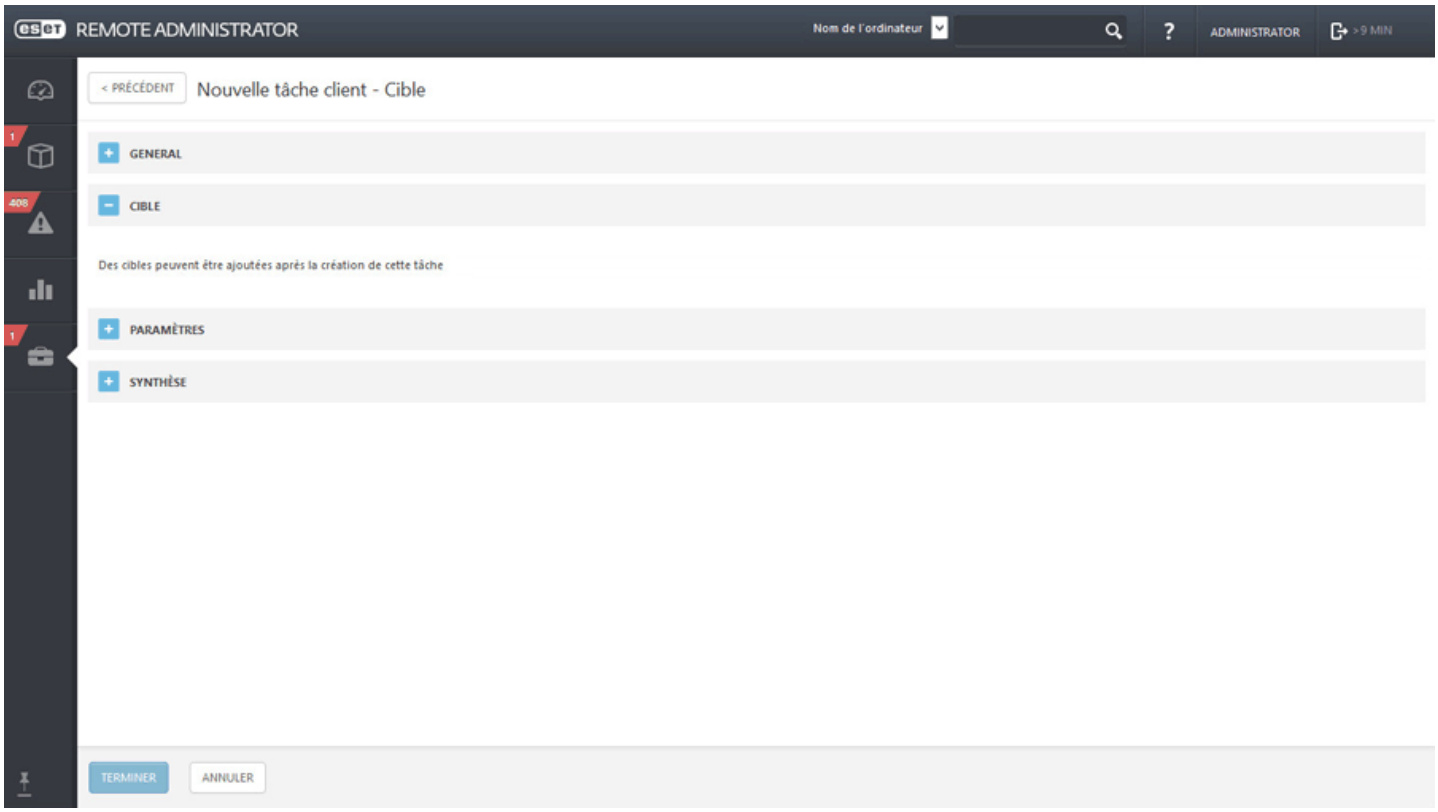
IMPORTANT : Il est recommandé de rétablir la valeur par défaut de certains paramètres (protection par mot de passe, par exemple) à l'aide d'une stratégie avant d'interrompre la gestion d'un périphérique. De plus, tous les tâches s'exécutant sur l'Agent sont annulées. L'état d'exécution **En cours**, **Terminé** ou **Échoué** de cette tâche peut ne pas être affiché précisément dans ERA Web Console selon la réplication.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



Paramètres

Paramètres de désinstaller un logiciel

- **Désinstaller** : **application de la liste :**

Nom du package : sélectionnez un composant ERA ou un produit de sécurité client. Tous les packages installés sur le ou les clients sélectionnés sont affichés dans cette liste.
Version du package : vous pouvez supprimer une version spécifique (une version spécifique peut parfois poser problème) du package ou désinstaller toutes les versions d'un package.
Redémarrage automatique si nécessaire : vous pouvez forcer le redémarrage du système d'exploitation client si la désinstallation le requiert.

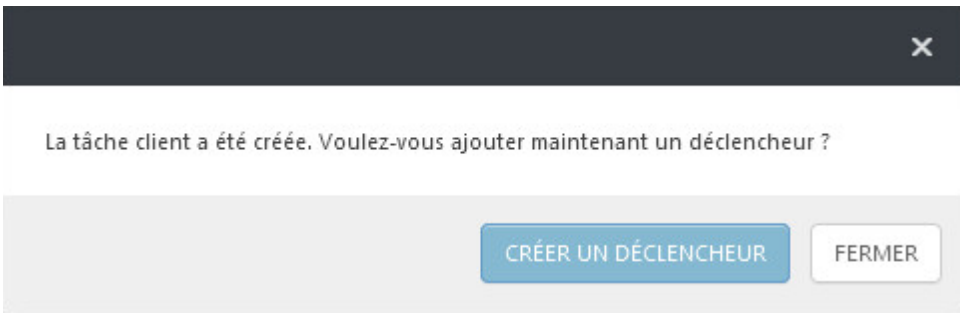
- **Désinstaller** - **Antivirus tiers (créé avec OPSWAT) :** pour obtenir la liste des antivirus compatibles, consultez notre article de la base de connaissances. Cette suppression est différente de la désinstallation effectuée par **Ajout/ suppression de programmes**. Elle utilise d'autres méthodes pour supprimer entièrement les antivirus tiers, y compris les entrées de registre résiduelles ou d'autres traces.

Suivez les instructions détaillées de l'article How do I remove third-party antivirus software from client computers using ESET Remote Administrator? (6.x) (en anglais) pour envoyer une tâche afin de supprimer les antivirus tiers des ordinateurs clients.

- Si vous souhaitez autoriser la désinstallation des applications protégées par mot de passe, consultez cet article de la base de connaissances. (Voir l'étape 12)

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.14 Activation du produit

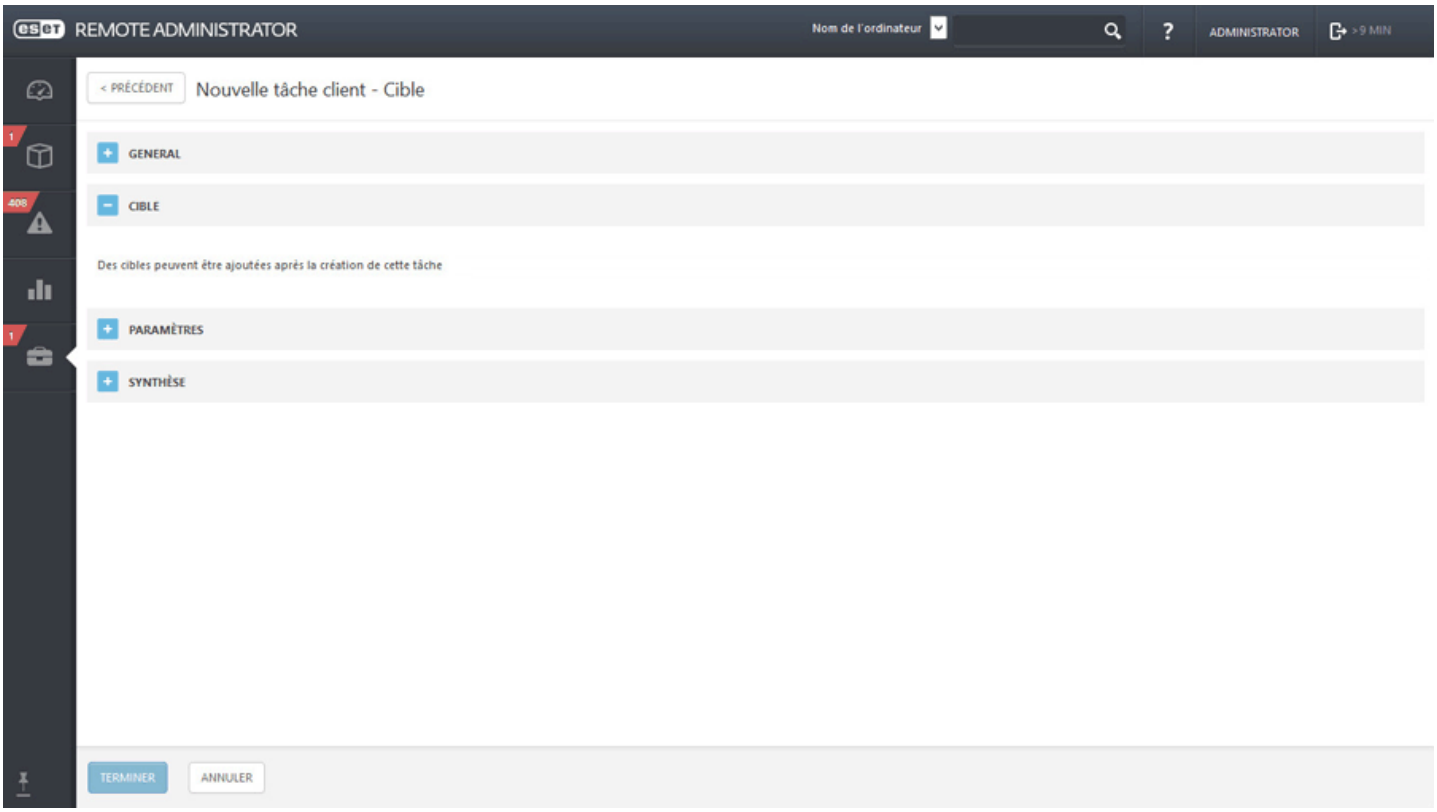
Suivez ces étapes pour pour activer un produit de sécurité ESET sur un ordinateur client ou un périphérique mobile.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.

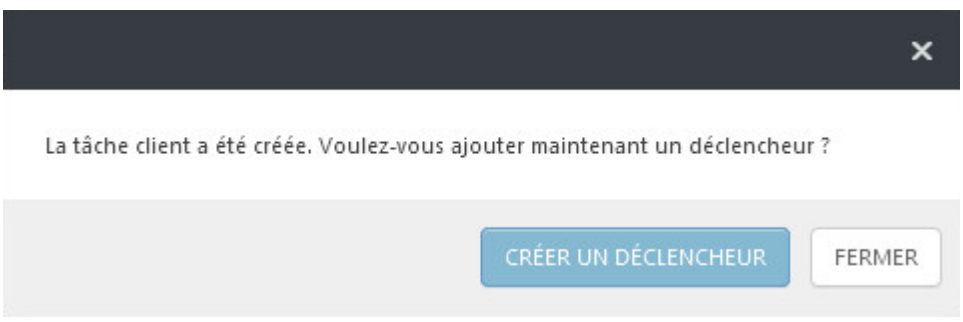


Paramètres

Paramètres d'activation du produit : sélectionnez dans la liste une licence pour le client. Cette licence est appliquée aux produits déjà installés sur le client. Si vous ne voyez aucune licence, accédez à Gestion de licences pour ajouter des licences.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.15 Demander un rapport SysInspector

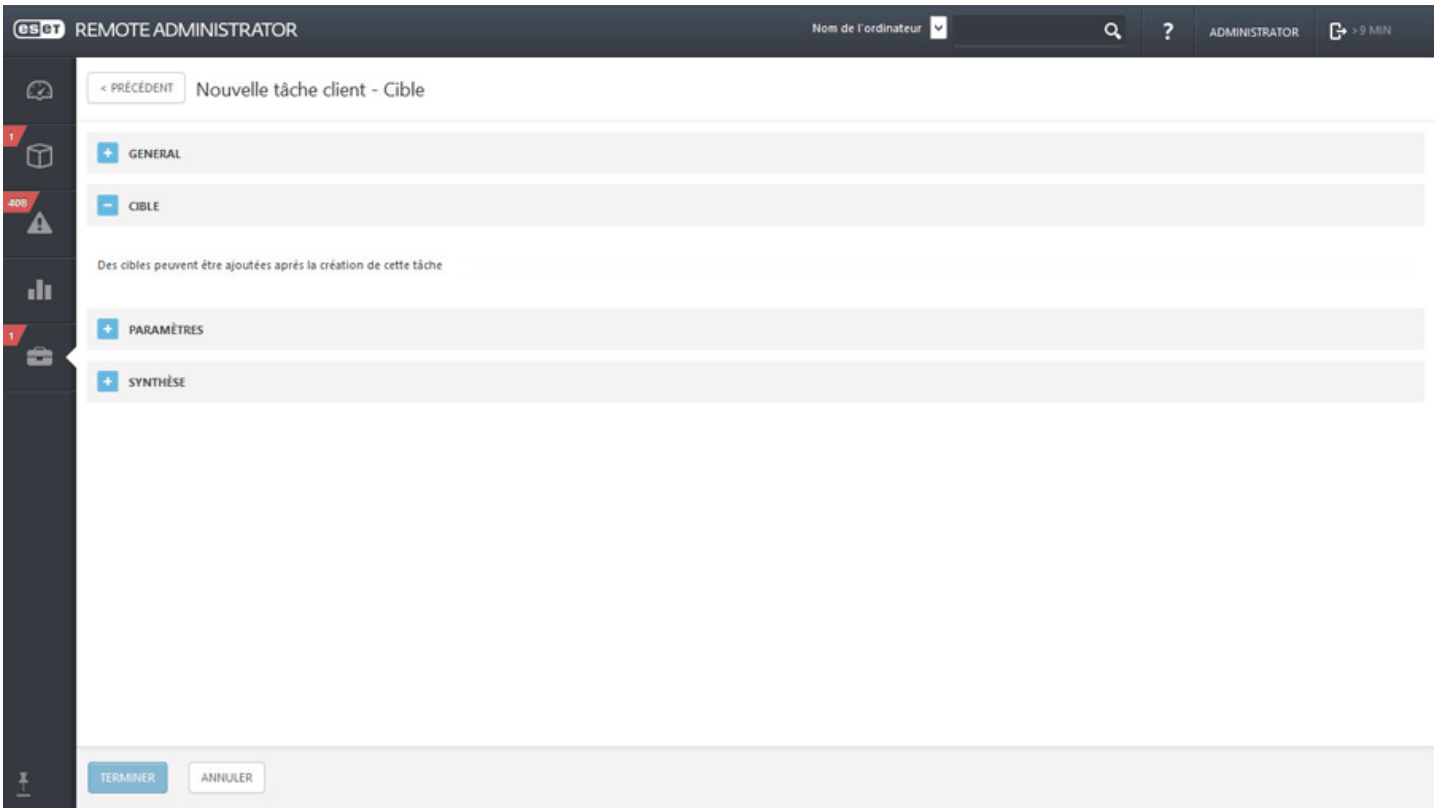
La tâche **Demander un rapport SysInspector** sert à demander le journal SysInspector d'un produit de sécurité client qui possède cette fonction.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Demander un rapport SysInspector**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.

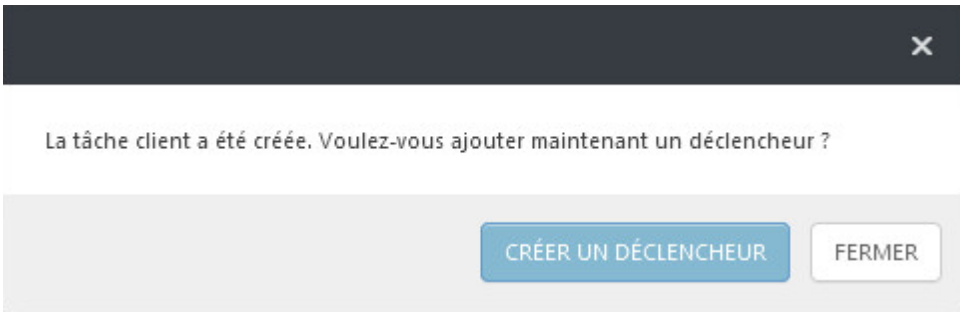


Paramètres

- **Stocker le journal sur le client** : sélectionnez cette option si vous souhaitez stocker le journal SysInspector sur le client et dans ERA Server. Lorsqu'un client dispose par exemple d'ESET Endpoint Security, le journal est généralement stocké sous *C:\Program Data\ESET\ESET Endpoint Antivirus\SysInspector*.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.16 Charger un fichier mis en quarantaine

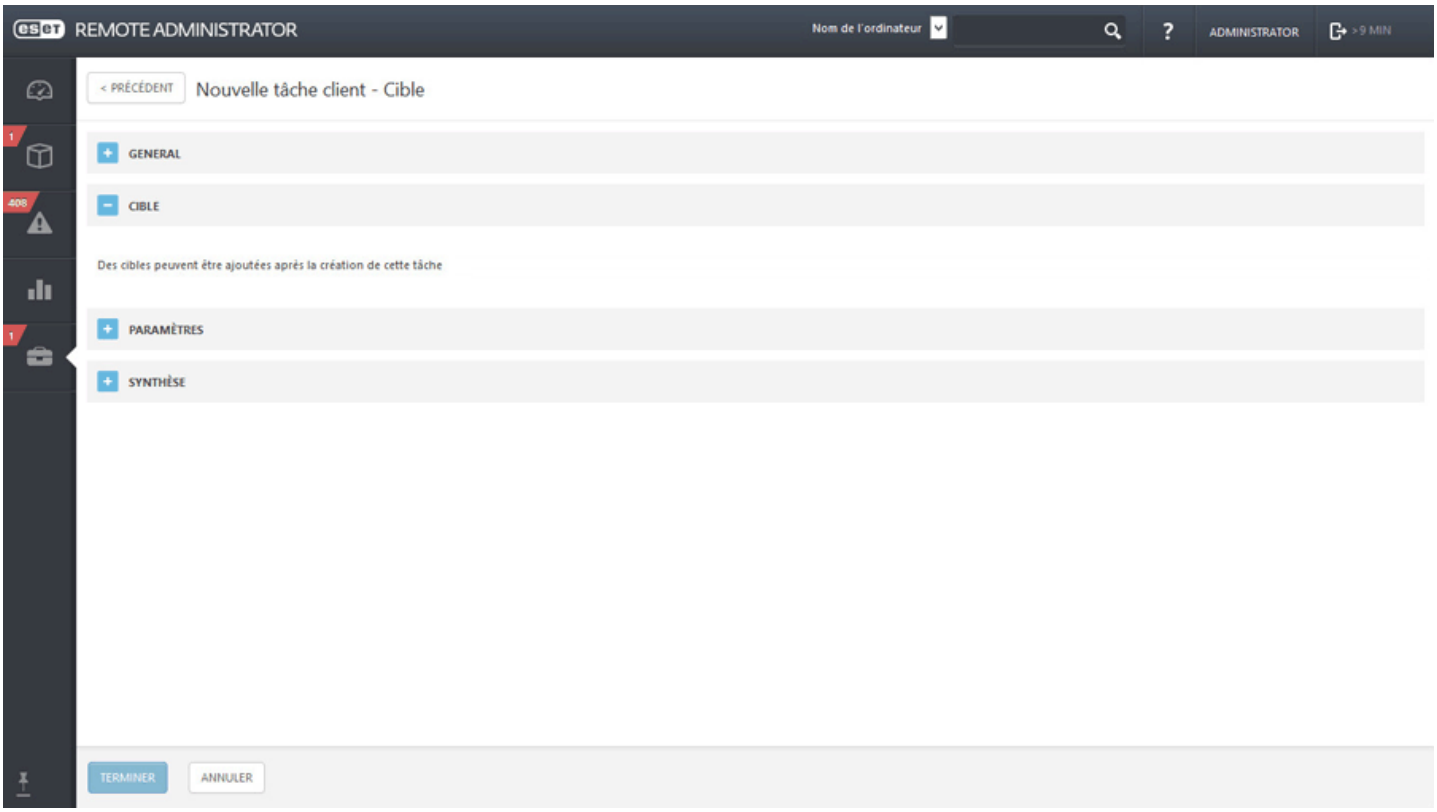
La tâche **Charger un fichier mis en quarantaine** sert à gérer les fichiers mis en quarantaine sur les clients.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Charger un fichier mis en quarantaine**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.

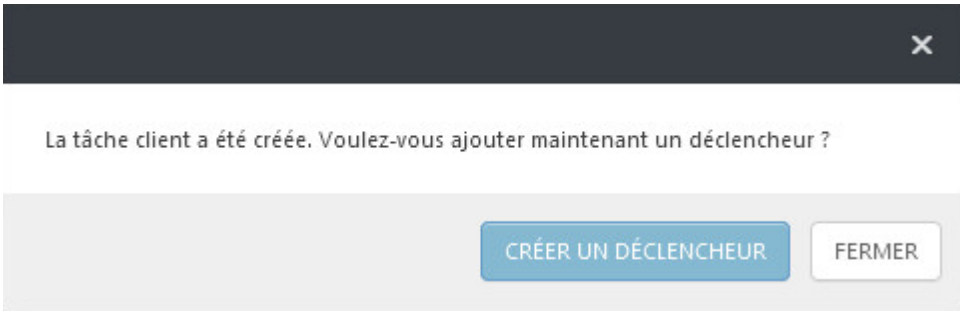


Paramètres

- **Objets mis en quarantaine** : sélectionnez un objet spécifique mis en quarantaine.
- **Mot de passe de l'objet** : saisissez un mot de passe pour chiffrer l'objet à des fins de sécurité. Veuillez noter que le mot de passe sera affiché dans le rapport correspondant.
- **Chemin de chargement** : saisissez un chemin d'accès à un emplacement dans lequel charger l'objet.
- **Mot de passe/nom d'utilisateur de chargement** : si l'emplacement requiert une authentification (partage réseau, etc.), saisissez les informations d'identification pour accéder à ce chemin.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.

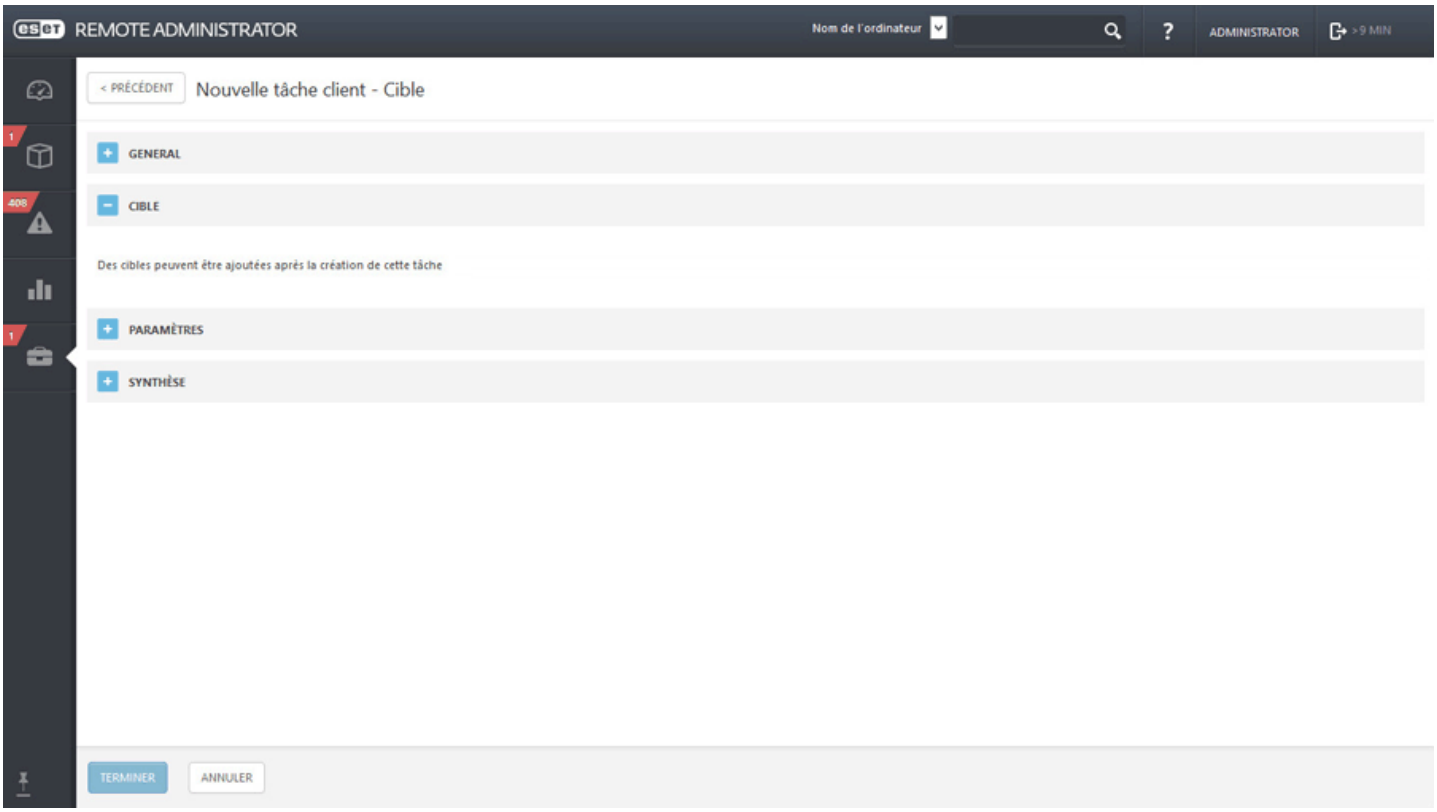


4.4.17 Mise à jour de la base des signatures de virus

La tâche **Mise à jour du produit** force la mise à jour de la base des signatures de virus du produit de sécurité installé sur les clients. Il s'agit d'une tâche générale pour tous les produits sur tous les systèmes.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



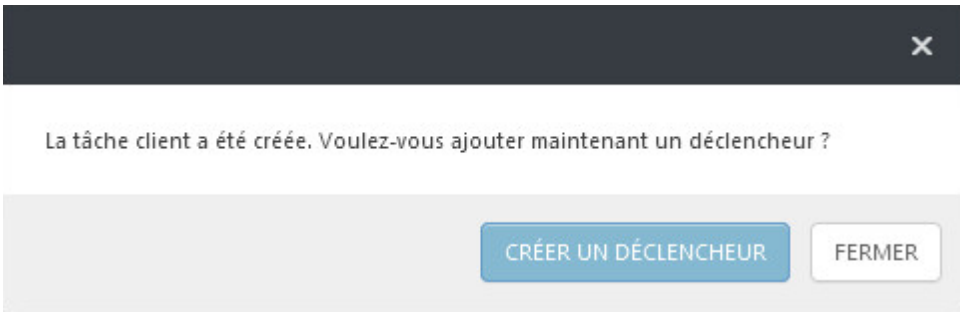
Paramètres

- **Effacer le cache de mise à jour** : cette option supprime les fichiers de mise à jour temporaires du cache sur le client. Elle peut être souvent utilisée pour corriger les erreurs de mise à jour de la base des signatures de virus.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier

quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.

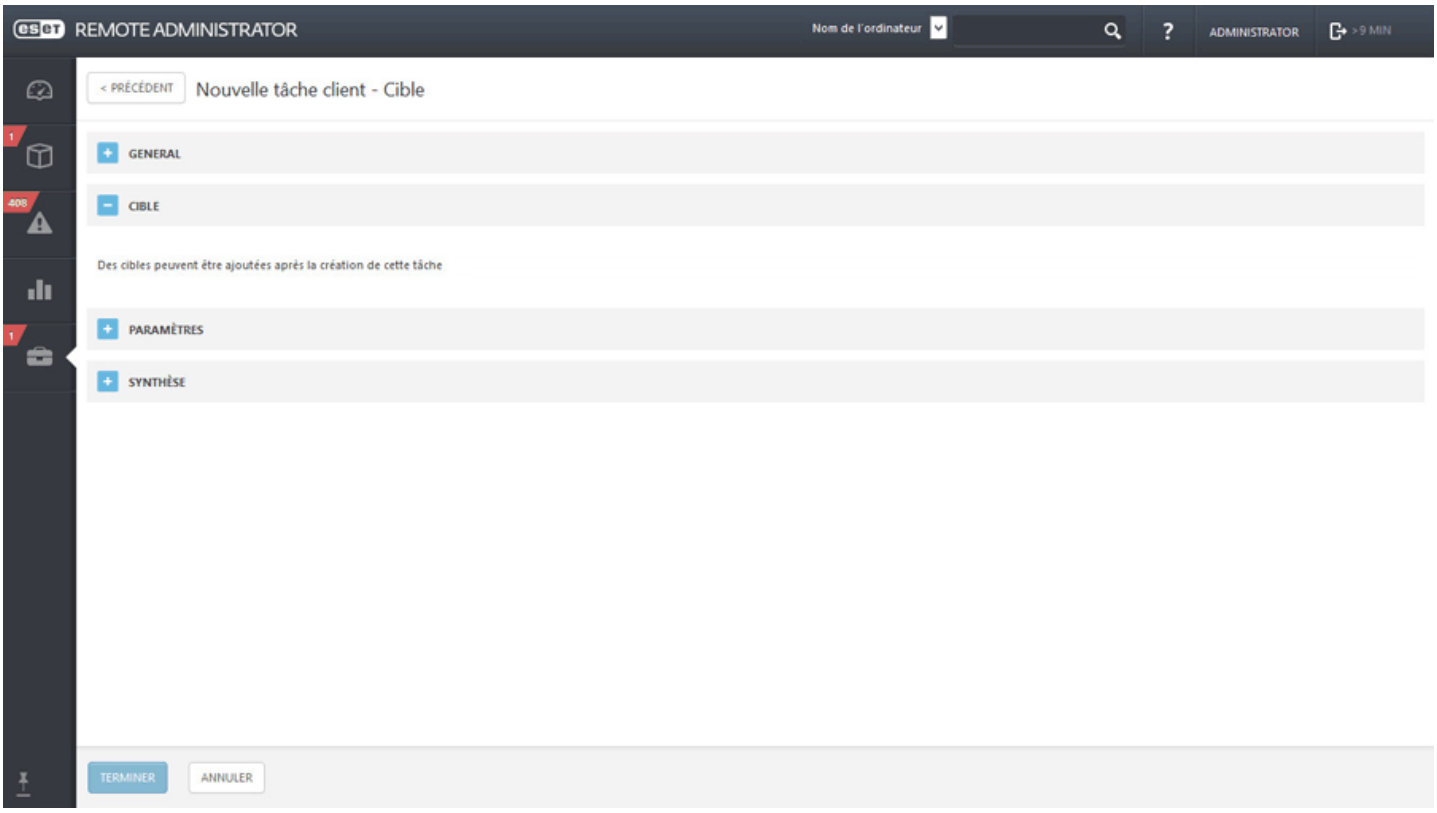


4.4.18 Restauration de la mise à jour de la base des signatures de virus

Une mise à jour de la base des signatures de virus peut parfois entraîner des problèmes ou ne pas être souhaitée sur tous clients (en cas de test ou lors de l'utilisation de mises à jour de versions bêta, par exemple). Vous pouvez dans ce cas utiliser la tâche **Restauration de la mise à jour de la base des signatures de virus**. Lorsque vous exécutez cette tâche, la version précédente de la base des signatures de virus est rétablie.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



Paramètres

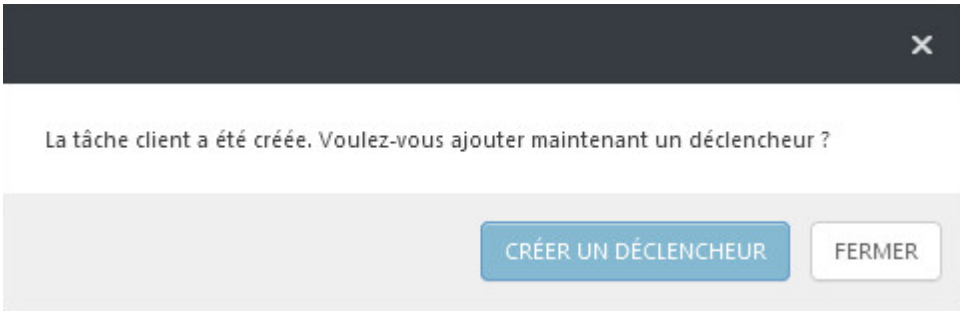
Vous pouvez personnaliser dans cette section les paramètres de restauration de la mise à jour de la base des signatures de virus.

Action

- **Mises à jour activées** : les mises à jour sont activées et le client recevra la prochaine mise à jour de la base des signatures de virus.
- **Restaurer et désactiver les mises à jour pendant les prochaines** : les mises à jour sont désactivées pendant la période spécifiée dans le menu déroulant **Désactiver l'intervalle** : 24, 36, 48 heures ou jusqu'à révocation. Utilisez l'option Jusqu'à révocation avec prudence, car elle présente un risque pour la sécurité.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.19 Inscription de périphérique - Tâche client

Les périphériques mobiles peuvent être gérés par ERA Server et par l'application mobile Android ESET Endpoint Security proprement dite. Pour commencer à gérer les périphériques mobiles, vous devez les inscrire dans ERA. L'inscription des périphériques s'effectue à l'aide d'une tâche de client.

- Inscription de périphérique Android
- Inscription de périphérique iOS

4.4.19.1 Inscription de périphérique Android

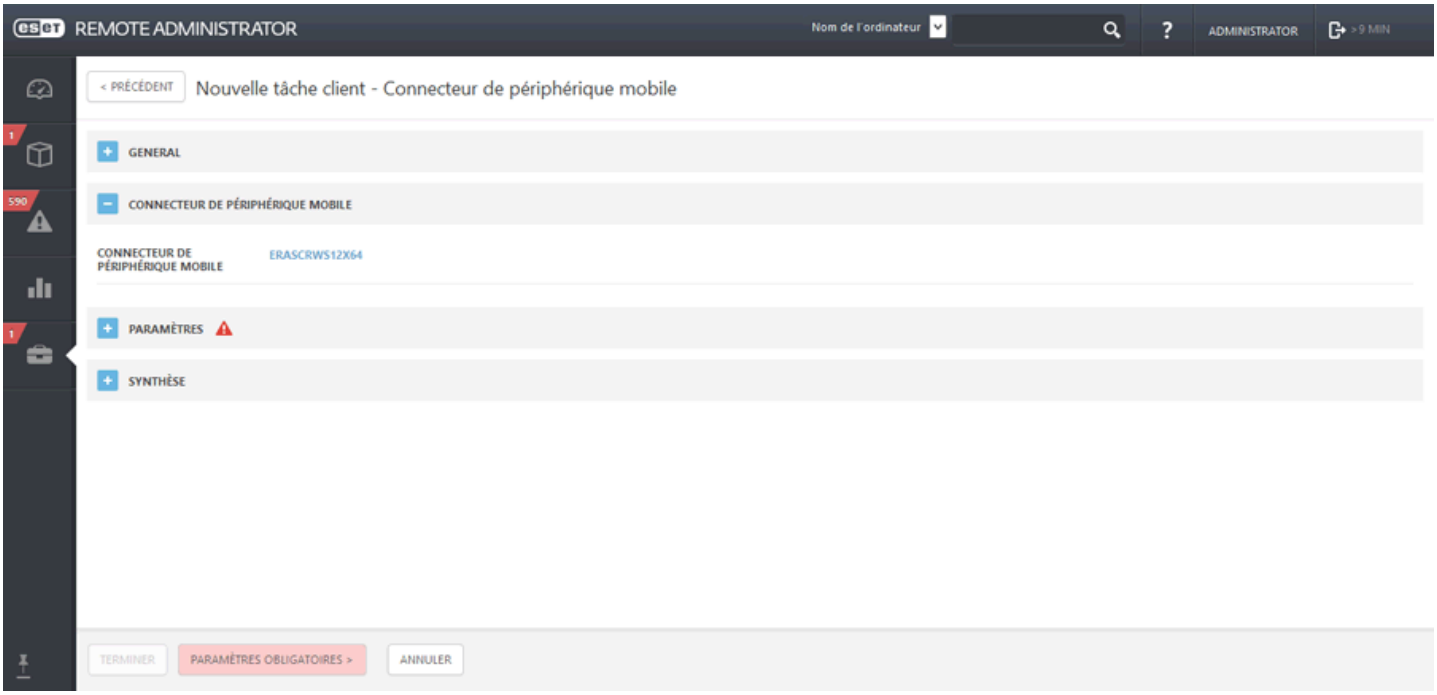
Pour inscrire un périphérique mobile Android dans ERA, procédez comme suit :

Général

Saisissez un **nom** et une **description** (facultative) pour la tâche.

Connecteur de périphérique mobile

Sélectionnez l'ordinateur sur lequel est installé le Connecteur de périphérique mobile. Un lien d'inscription (URL) s'affiche automatiquement. Si aucun lien ne s'affiche après avoir cliqué sur Sélectionner, vérifiez que le serveur Connecteur de périphérique mobile est accessible. Si vous n'avez pas encore installé le Connecteur de périphérique mobile, reportez-vous aux chapitres Installation du Connecteur de périphérique mobile - Windows ou Linux de ce guide pour obtenir des instructions d'installation.

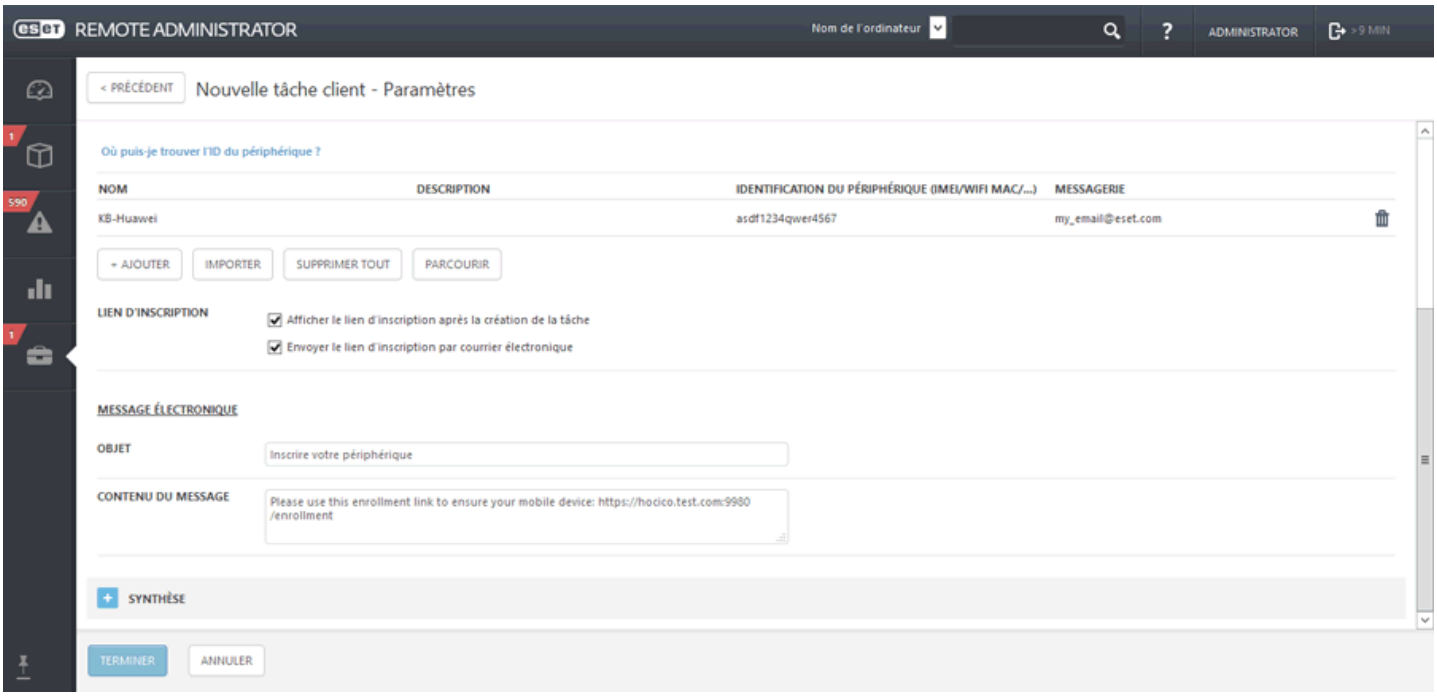


Paramètres

Saisissez le **Nom** du périphérique mobile (ce nom sera affiché dans la liste des Ordinateurs) et éventuellement une **description**.
Saisissez le numéro IMEI du périphérique mobile spécifique à ajouter. Il est également recommandé de saisir l'**adresse électronique** associée au périphérique mobile (le lien d'inscription sera envoyé à cette adresse électronique).

Cliquez sur **+ Ajouter** si vous souhaitez ajouter un autre périphérique mobile. Vous pouvez ajouter simultanément plusieurs périphériques. Vous pouvez également cliquer sur **Importer** pour charger un fichier `.csv` qui contient la liste de périphériques mobiles à ajouter. Cliquez sur **Parcourir** et sélectionnez des périphériques mobiles existants.

Indiquez une **action** en cochant la case en regard de l'option **Afficher le lien d'inscription** et/ou **Envoyer le lien d'inscription** (l'URL sera envoyée aux adresses électroniques associées au périphérique). Si vous souhaitez envoyer un lien d'inscription (recommandé) au périphérique mobile, modifiez l'**objet** et le **contenu du message**, tout en conservant l'URL d'inscription telle quelle.



Résumé

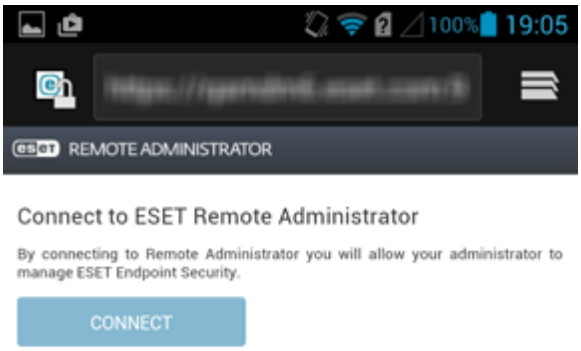
Toutes les options configurées sont affichées dans cette section. Examinez les paramètres et s'ils sont corrects, cliquez sur Terminer. La tâche est alors créée et prête à être utilisée.

Une fois que vous avez cliqué sur **Terminer**, le lien d'inscription (URL) s'affiche. Si vous n'avez pas spécifié d'adresse électronique et sélectionné **Envoyer le lien d'inscription**, vous devez saisir manuellement l'URL dans le navigateur Web du périphérique mobile ou l'entrer d'une autre manière.

Quand ESET Endpoint Security pour Android (EESA) est activé sur le périphérique mobile, il existe deux scénarios d'inscription. Vous pouvez activer ESET Endpoint Security pour Android sur le périphérique mobile à l'aide de la tâche de client Activation du produit ERA (recommandé). L'autre scénario correspond aux périphériques mobiles dont l'application ESET Endpoint Security pour Android est déjà activée.

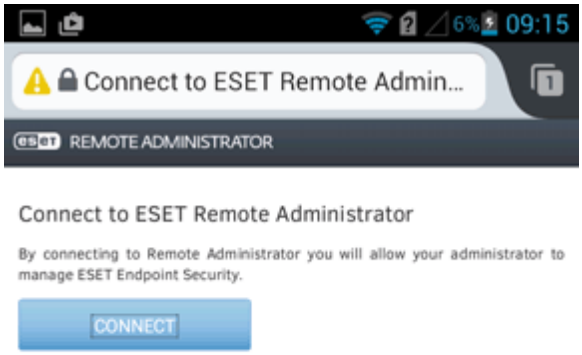
EESA pas encore activé : pour activer le produit et inscrire le périphérique, procédez comme suit :

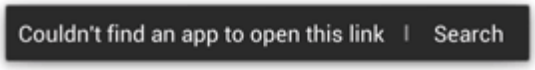
1. Appuyez sur l'URL d'inscription reçue par courrier électronique ou saisissez-la manuellement dans le navigateur, en incluant le numéro de port (*https://eramdm:9980/enrollment*, par exemple). Le système peut vous demander d'accepter un certificat SSL. Cliquez sur le bouton **Accepter** si vous êtes d'accord, puis sur **Connexion**.



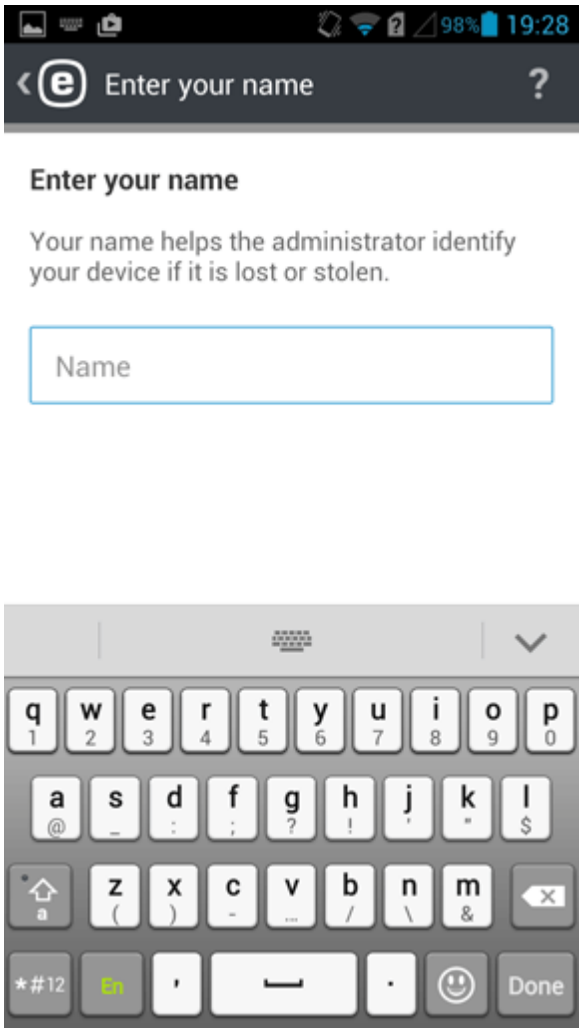
2. si l'application ESET Endpoint Security n'est pas installée sur le périphérique mobile, vous êtes automatiquement redirigé vers la boutique Google Play à partir de laquelle vous pouvez la télécharger.

REMARQUE : si la notification **Impossible de trouver une application pour ouvrir ce lien** s'affiche, essayez d'ouvrir le lien d'inscription dans le navigateur Web par défaut d'Android.

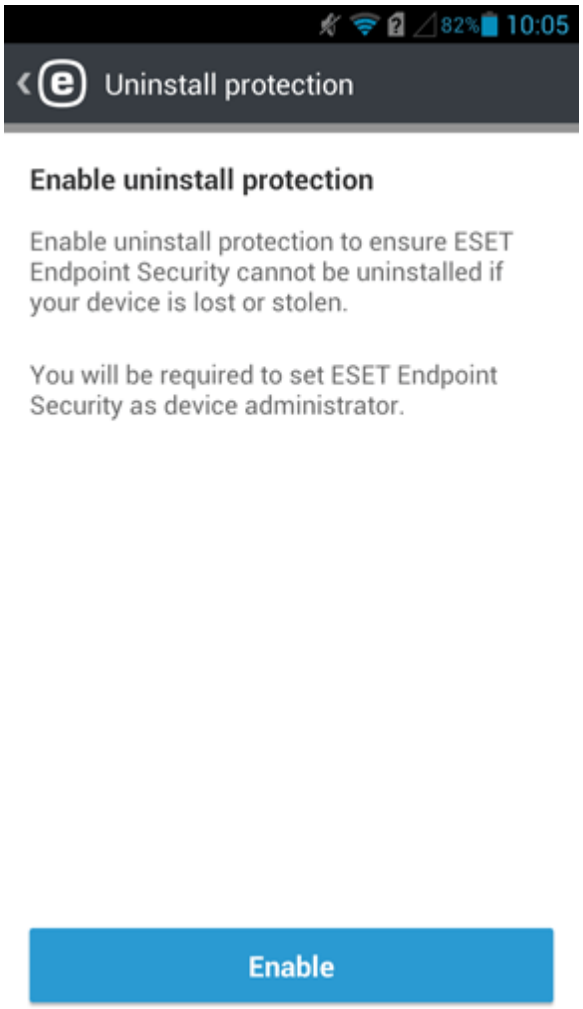




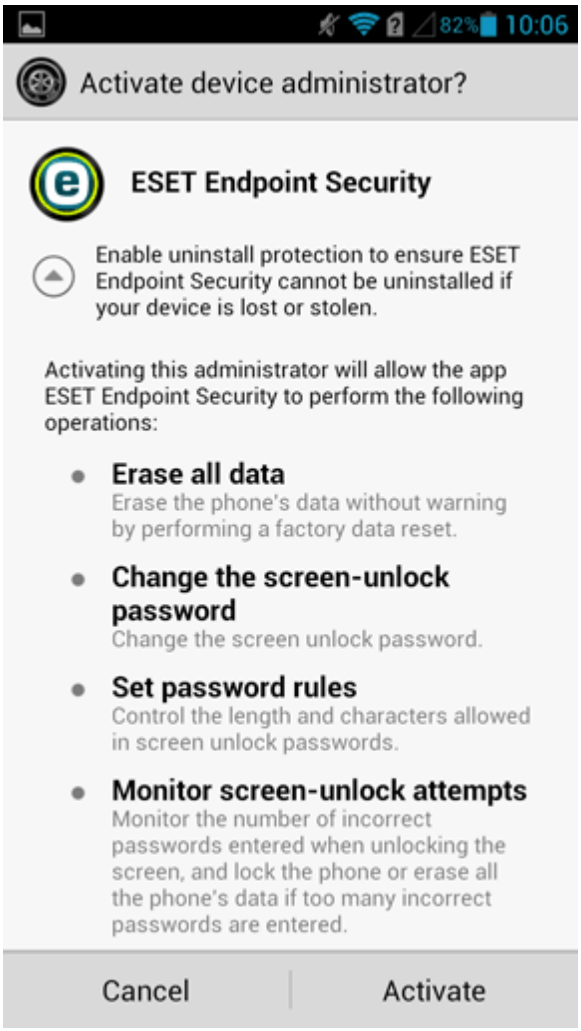
3. Saisissez le nom de l'utilisateur du périphérique mobile.



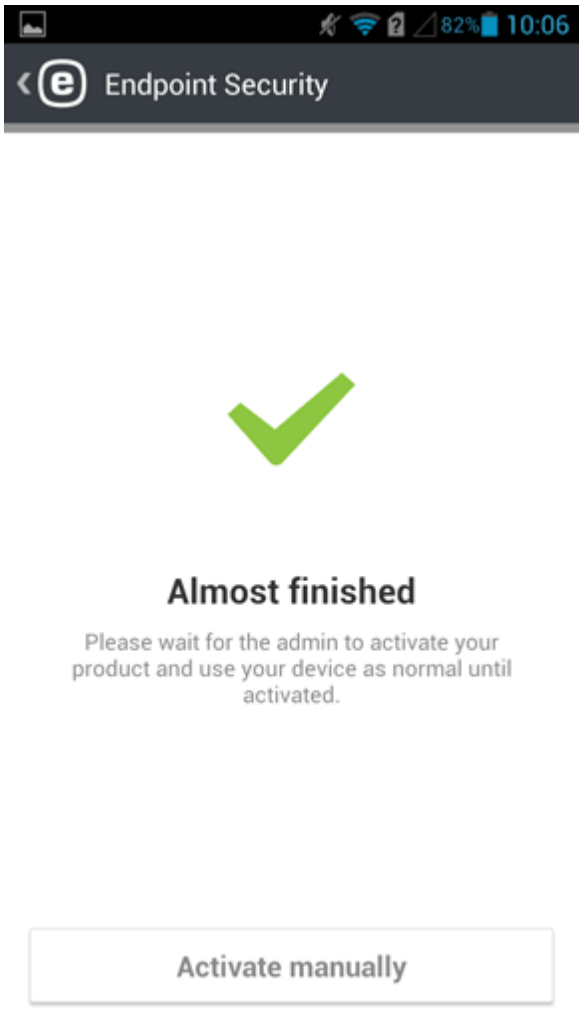
4. Appuyez sur **Activer** pour activer la protection contre les désinstallations.



5. Appuyez sur **Activer** pour activer l'administrateur de périphérique.

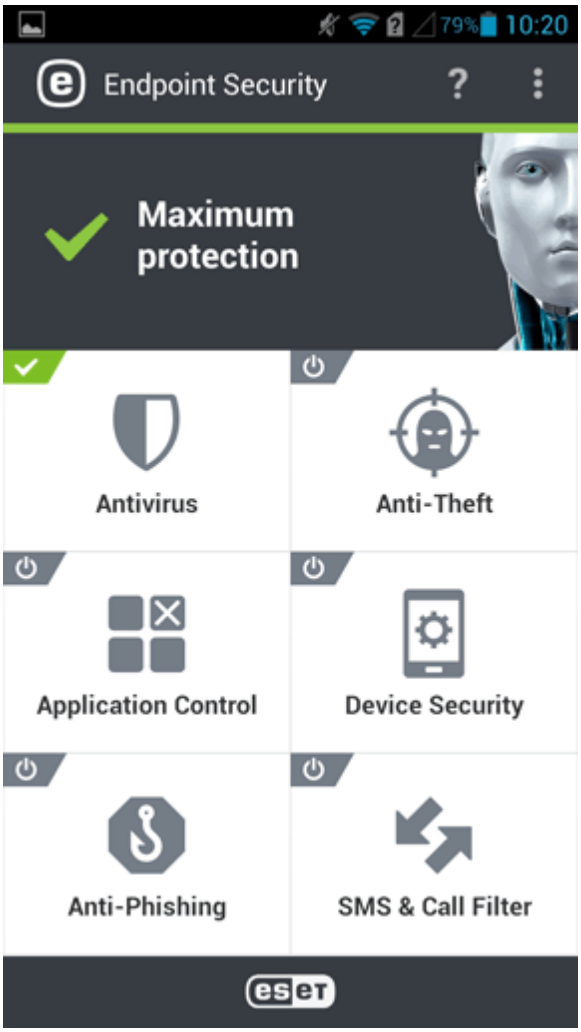


6. À ce stade, vous pouvez quitter l'application ESET Endpoint Security pour Android et ouvrir ERA Web Console.



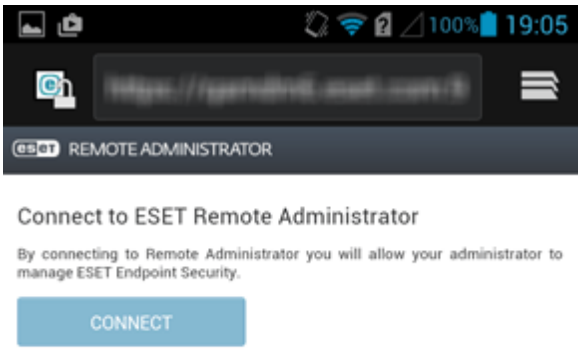
7. Dans ERA Web Console, accédez à **Admin** > **Tâches client** > **Mobile** > Activation du produit, puis cliquez sur **Nouveau**.
8. Sélectionnez le périphérique mobile en cliquant sur **Ajouter des cibles**.
9. Sous Paramètres, cliquez sur <Choisir une licence ESET>, sélectionnez la licence adéquate, puis cliquez sur **Terminer**.

L'exécution de la tâche de client Activation du produit peut prendre du temps sur le périphérique mobile. Une fois la tâche exécutée, l'application ESET Endpoint Security pour Android est activée. Le périphérique mobile est alors géré par ERA. L'utilisateur est désormais en mesure d'utiliser l'application ESET Endpoint Security pour Android. Lorsque l'application ESET Endpoint Security pour Android est ouverte, le menu principal s'affiche :



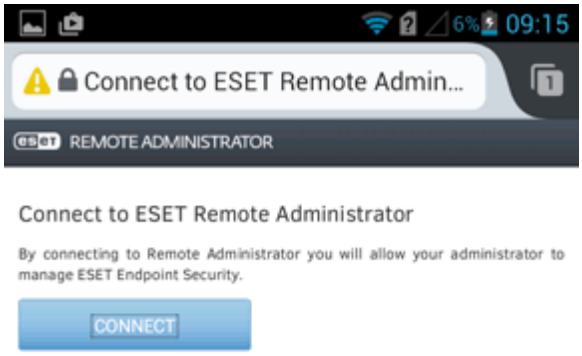
EESA déjà activé : pour inscrire le périphérique, procédez comme suit :

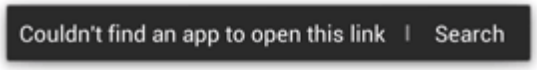
1. Appuyez sur l'URL d'inscription reçue par courrier électronique ou saisissez-la manuellement dans le navigateur, en incluant le numéro de port (https://eramdm:9980/enrollment, par exemple). Le système peut vous demander d'accepter un certificat SSL. Cliquez sur le bouton d'acceptation si vous êtes d'accord, puis sur **Connexion**.


100%
19:05
REMOTE ADMINISTRATOR
Connect to ESET Remote Administrator
By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.
CONNECT

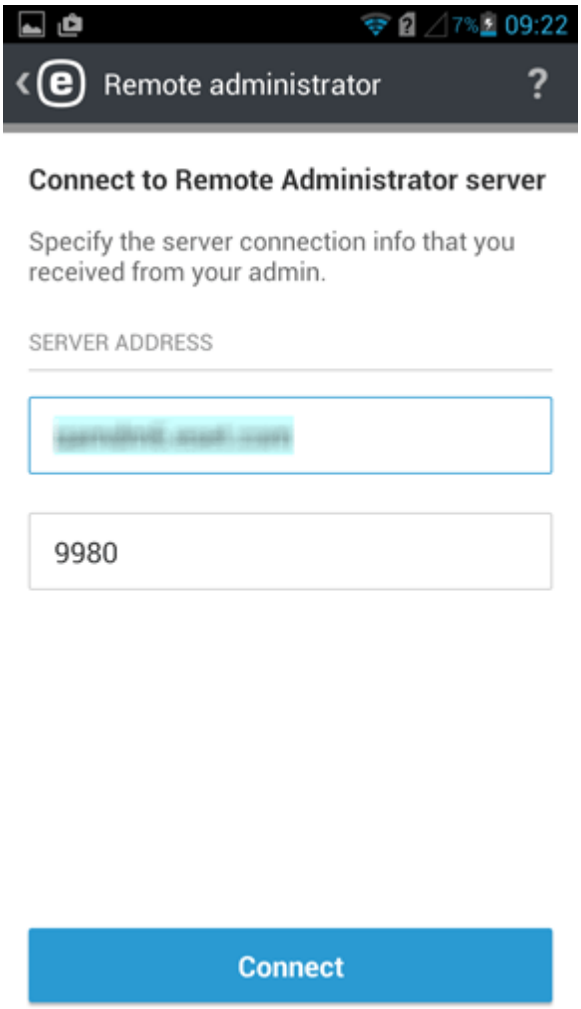
REMARQUE : si l'application ESET Endpoint Security n'est pas installée sur le périphérique mobile, vous êtes automatiquement redirigé vers la boutique Google Play à partir de laquelle vous pouvez la télécharger.

REMARQUE : si la notification **Impossible de trouver une application pour ouvrir ce lien** s'affiche, essayez d'ouvrir le lien d'inscription dans le navigateur Web par défaut d'Android.

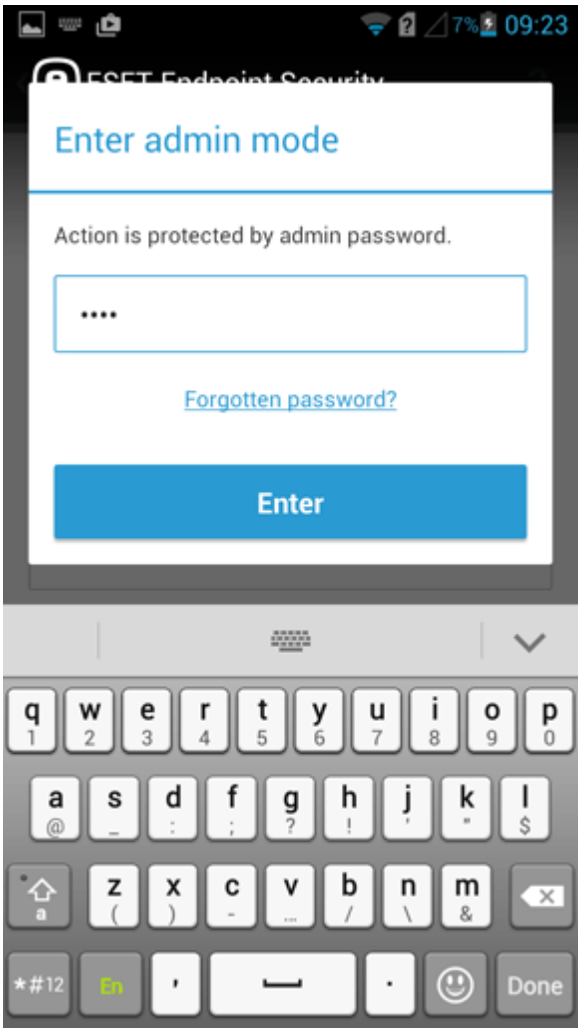




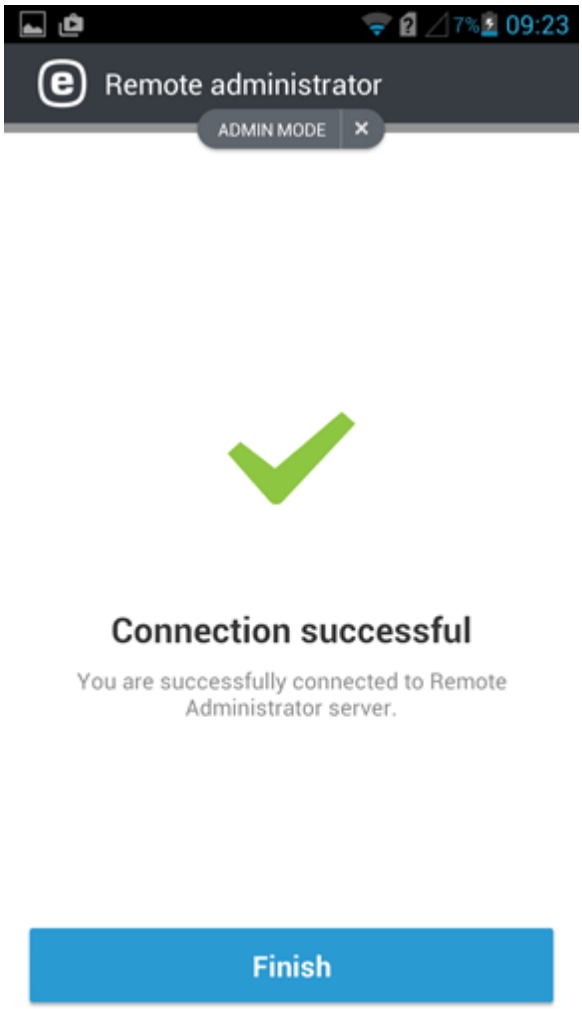
2. Vérifiez les informations de connexion (port et adresse du serveur Connecteur de périphérique mobile), puis cliquez sur **Connexion**.



3. Saisissez le mot de passe du mode administrateur ESET Endpoint Security dans le champ vide, puis appuyez sur Entrée.



4. Ce périphérique mobile est désormais géré par ERA. Appuyez sur Terminer.



4.4.19.2 Inscription de périphérique iOS

Pour inscrire un périphérique mobile iOS dans ERA, procédez comme suit :

Général

Saisissez un **nom** et une **description** (facultative) pour la tâche.

Connecteur de périphérique mobile

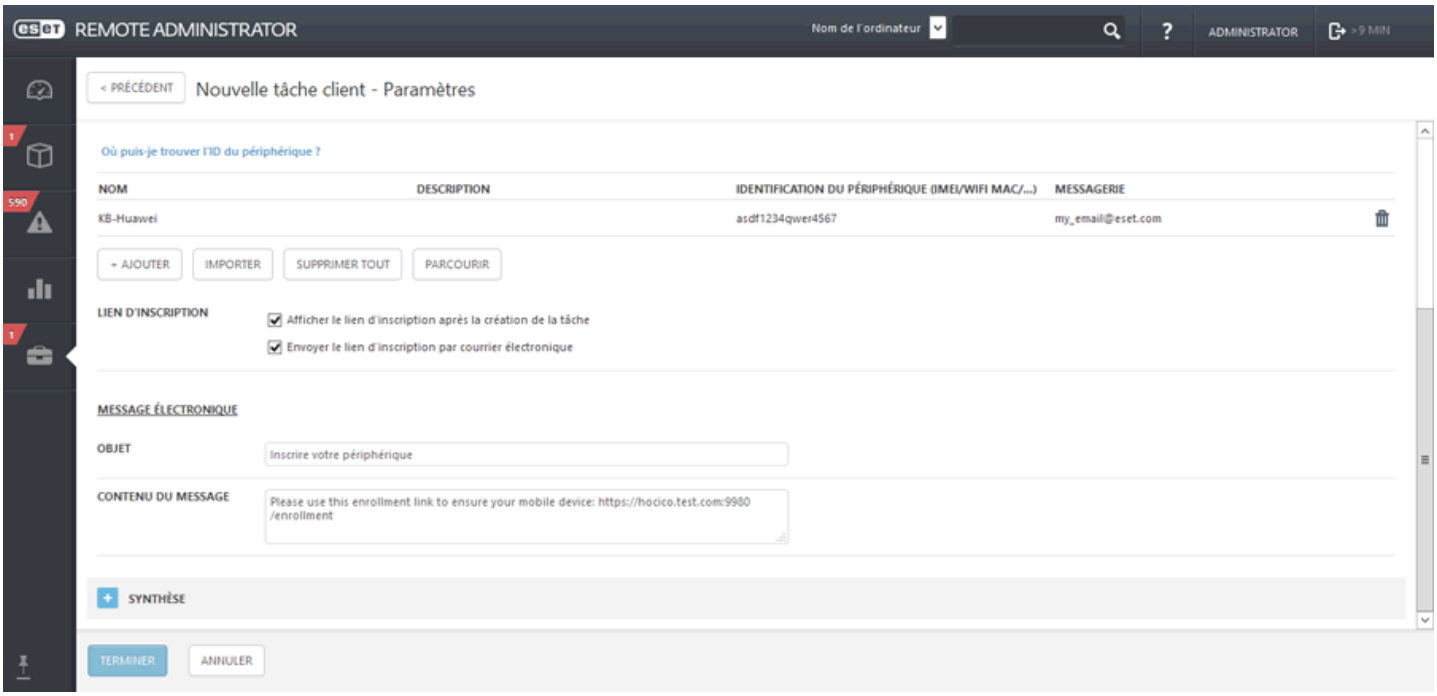
Sélectionnez l'ordinateur sur lequel est installé le Connecteur de périphérique mobile. Un lien d'inscription (URL) s'affiche automatiquement. Si aucun lien ne s'affiche après avoir cliqué sur Sélectionner, vérifiez que le serveur Connecteur de périphérique mobile est accessible. Si vous n'avez pas encore installé le Connecteur de périphérique mobile, reportez-vous aux chapitres Installation du Connecteur de périphérique mobile - Windows ou Linux de ce guide pour obtenir des instructions d'installation.

Paramètres

Saisissez le **Nom** du périphérique mobile (ce nom sera affiché dans la liste des Ordinateurs) et éventuellement une **description**.
Saisissez le numéro de série du périphérique mobile spécifique à ajouter. Il est également recommandé de saisir l'**adresse électronique** associée au périphérique mobile (le lien d'inscription sera envoyé à cette adresse électronique).

Cliquez sur **+ Ajouter** si vous souhaitez ajouter un autre périphérique mobile. Vous pouvez ajouter simultanément plusieurs périphériques. Vous pouvez également cliquer sur **Importer** pour charger un fichier `.csv` qui contient la liste des périphériques mobiles à ajouter. Cliquez sur **Parcourir** et sélectionnez des périphériques mobiles existants.

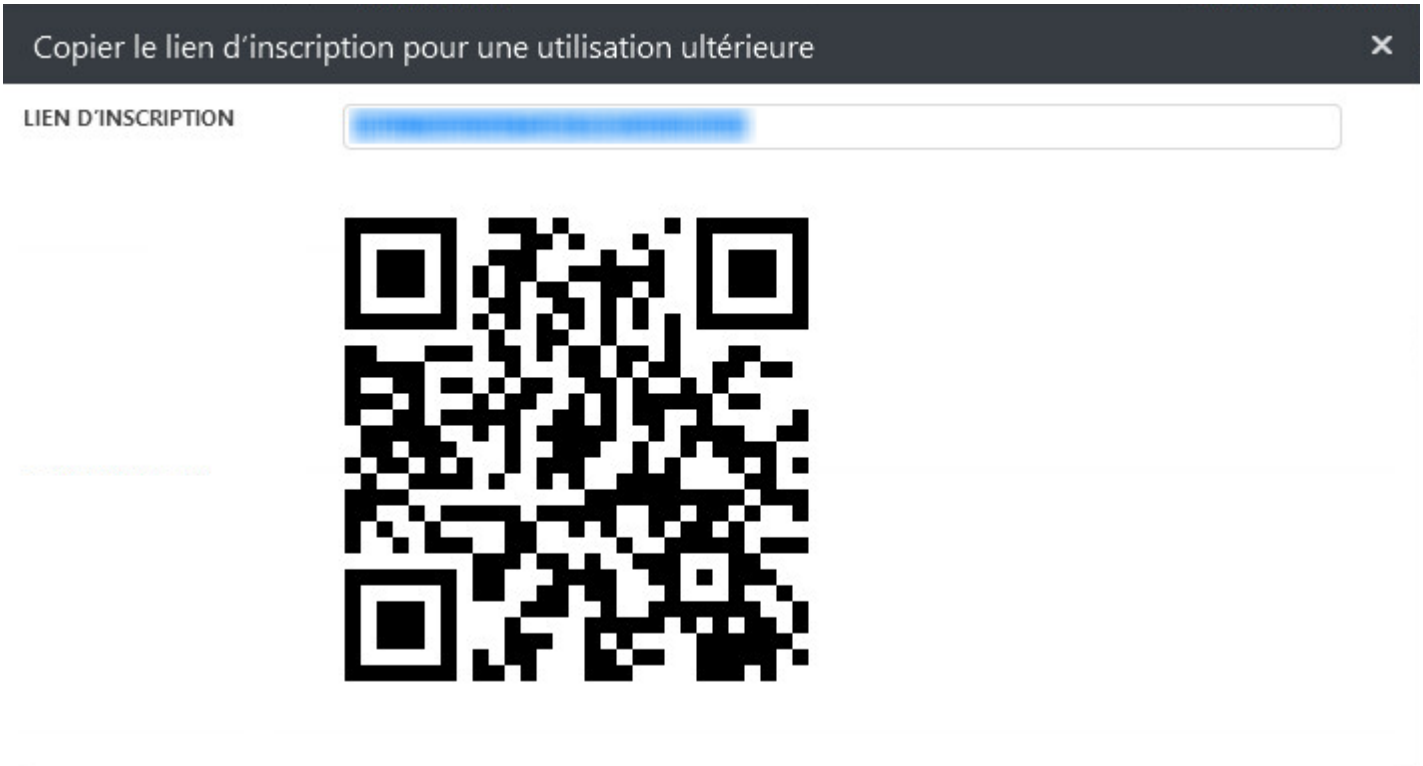
Indiquez une **action** en cochant la case en regard de l'option **Afficher le lien d'inscription** et/ou **Envoyer le lien d'inscription** (l'URL sera envoyée aux adresses électroniques associées au périphérique). Si vous souhaitez envoyer un lien d'inscription (recommandé) au périphérique mobile, vous pouvez modifier l'**objet** et le **contenu du message**, tout en conservant l'URL d'inscription telle quelle.



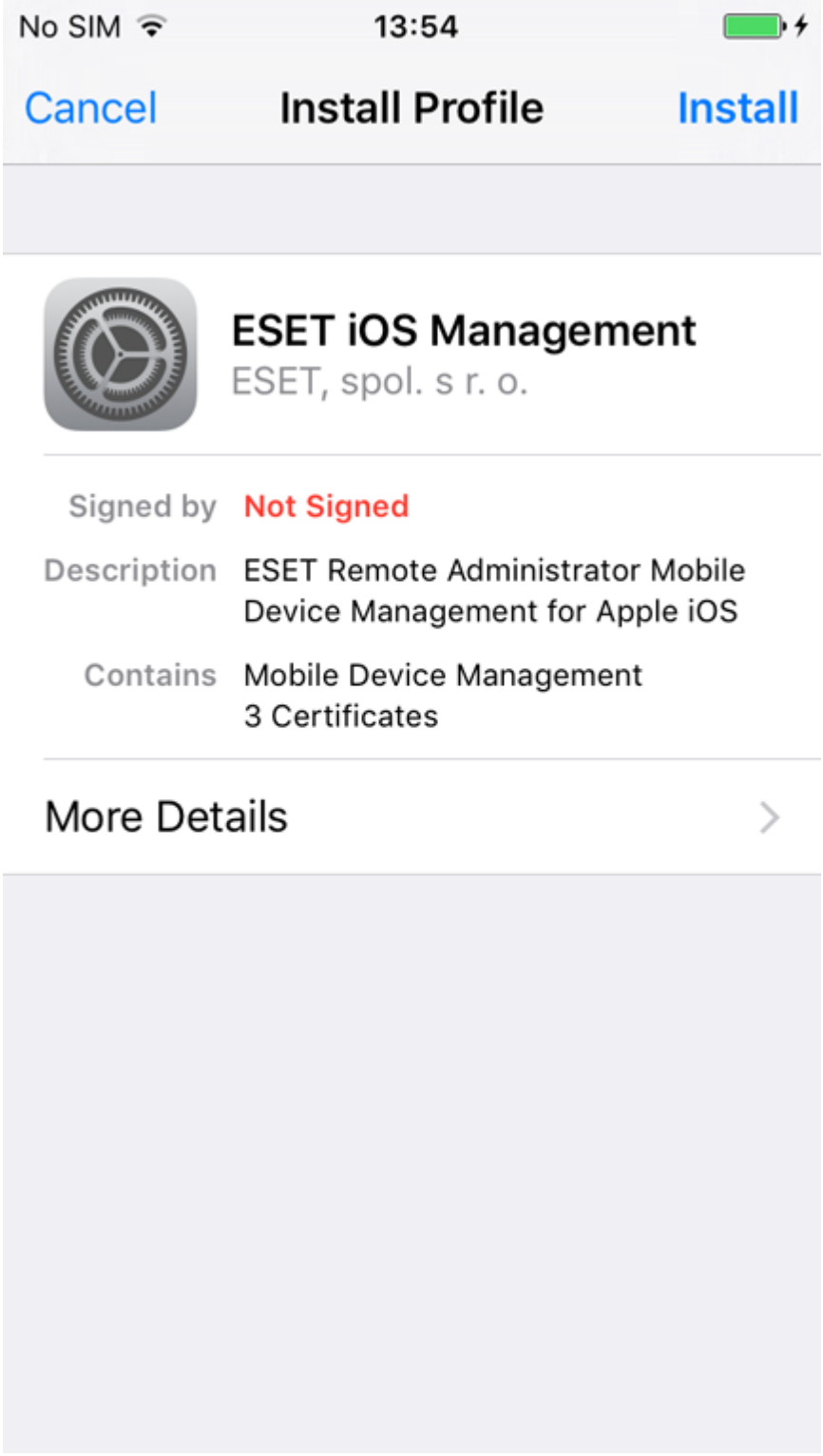
Résumé

Toutes les options configurées sont affichées dans cette section. Examinez les paramètres et s'ils sont corrects, cliquez sur Terminer. La tâche est alors créée et prête à être utilisée.

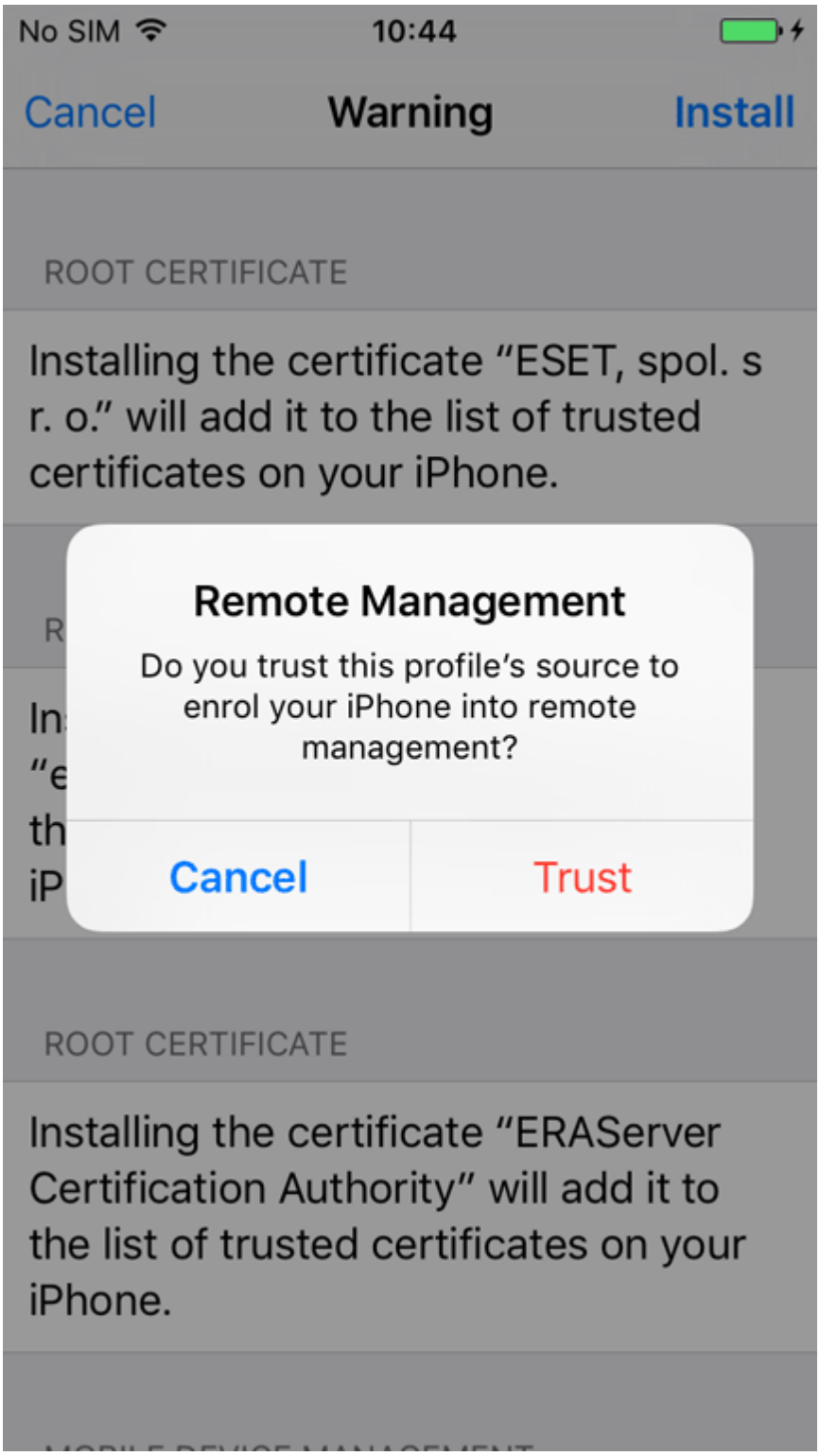
Une fois que vous avez cliqué sur **Terminer**, le lien d'inscription (URL) s'affiche. Si vous n'avez pas spécifié d'adresse électronique et sélectionné **Envoyer le lien d'inscription**, vous devez saisir manuellement l'URL dans le navigateur Web du périphérique mobile ou l'entrer d'une autre manière. Vous pouvez également utiliser un **code QR**.



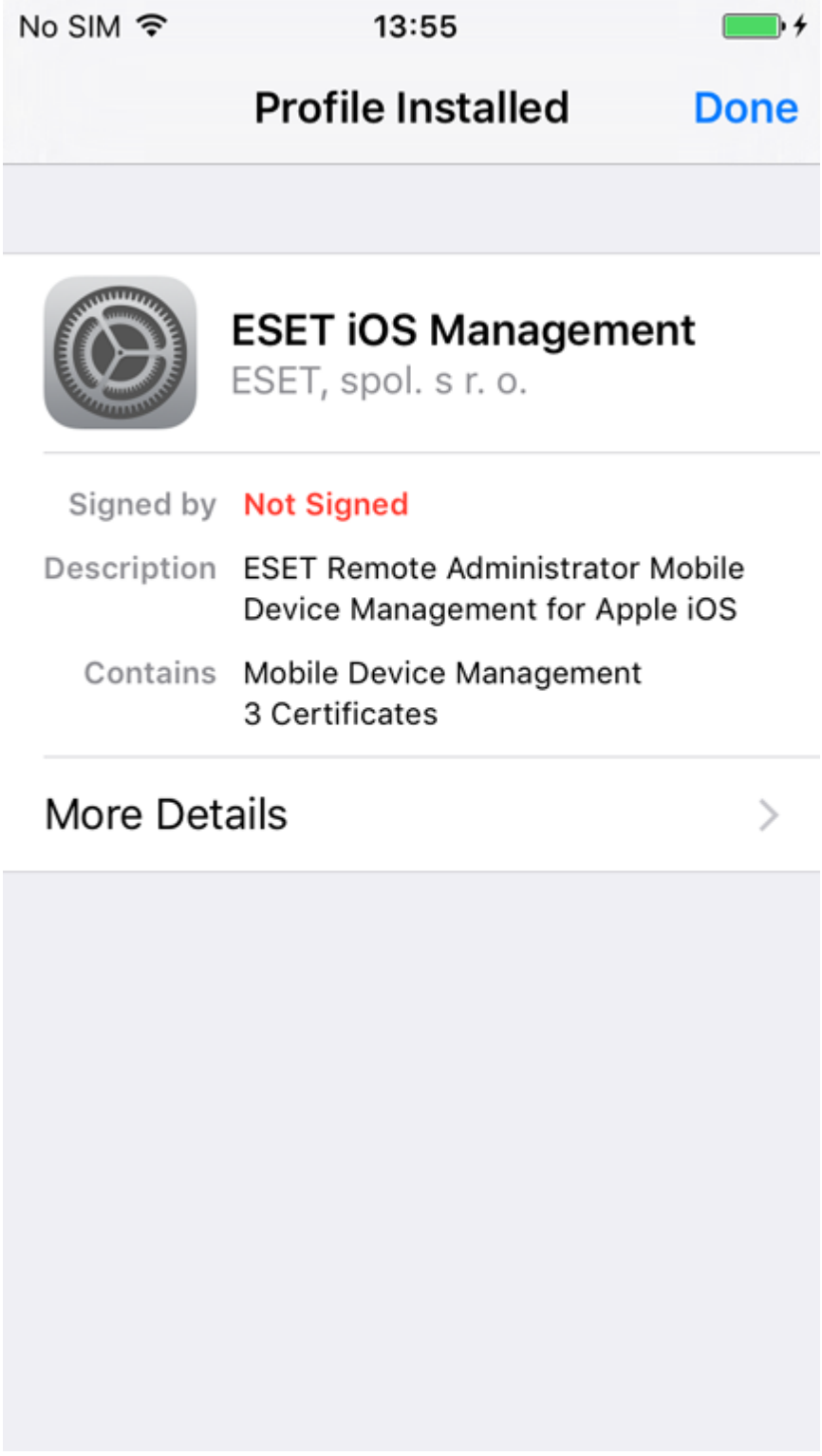
Cliquez sur **Installer** pour passer à l'écran **Installer le profil** de l'inscription MDM.



Appuyez sur **Faire confiance** pour autoriser l'installation du nouveau profil.

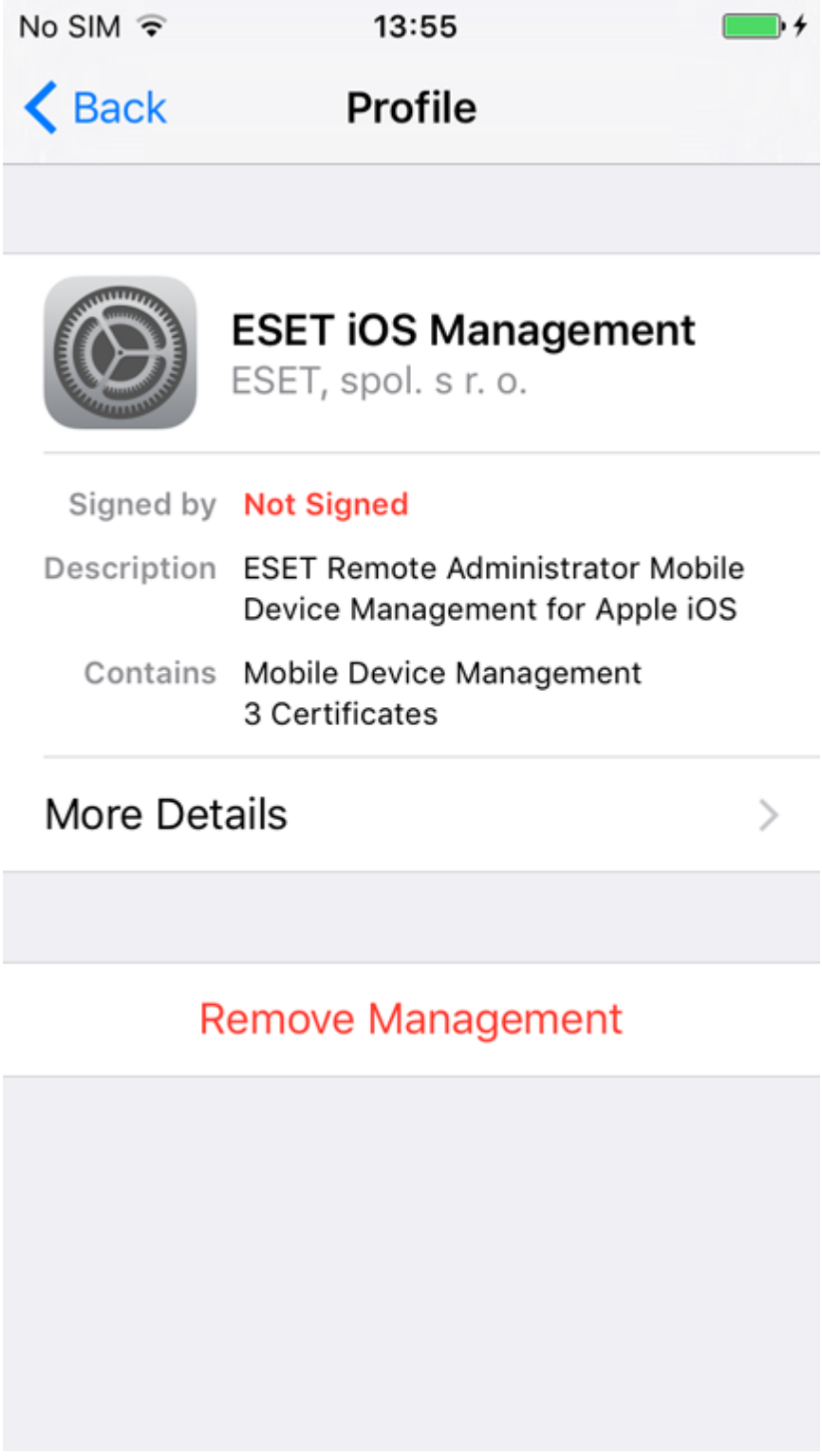


Après l'installation du nouveau profil, le champ Signé par indiquera que le profil est Non signé. C'est normal pour toute inscription MDM. Le profil est en fait signé avec un certificat, même s'il apparaît comme « **non signé** ». Il en est ainsi parce qu'iOS ne reconnaît pas encore le certificat.



Ce profil d'inscription vous permet de configurer des périphériques et de définir des stratégies de sécurité pour des utilisateurs ou des groupes.

IMPORTANT : La suppression de ce profil d'inscription supprime tous les paramètres de l'entreprise (Mail, Calendrier, Contacts, etc.) et le périphérique mobile iOS n'est pas géré. Si un utilisateur supprime le profil d'inscription, ERA n'aura pas l'information et l'état de le périphérique deviendra et ensuite . Cela arrivera après 14 jours en raison de l'absence de connexion du périphérique mobile iOS. Aucune autre indication que le profil d'inscription a été supprimé ne sera fournie.



4.4.19.3 Emplacement ID de périphérique mobile

iOS :

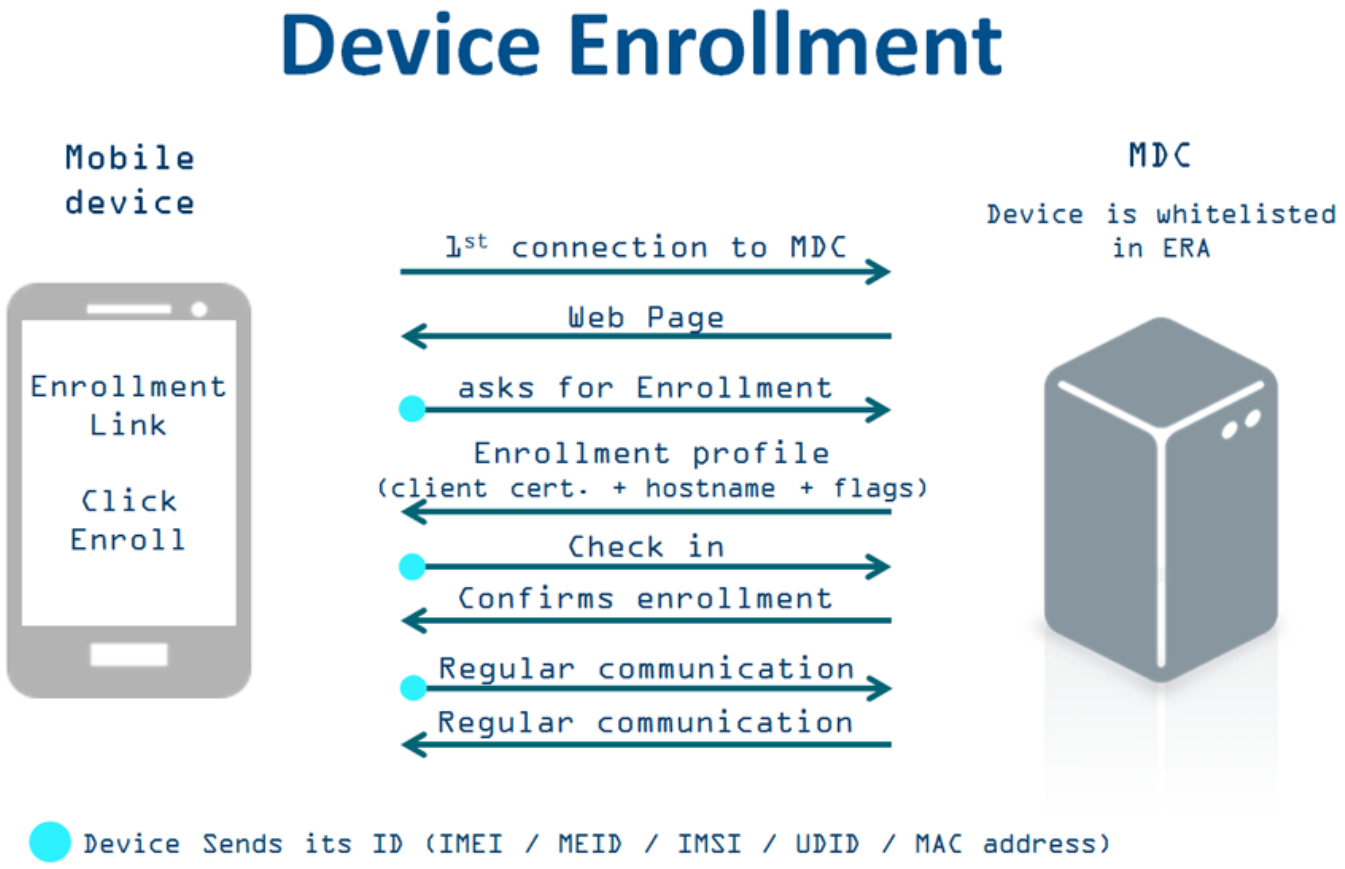
- **IMEI/Numéro de série** : pour déterminer l'ID, accédez à **Réglages** > **Général** > **Informations** et faites défiler vers le bas. Voir https://support.apple.com/en-us/HT204073 pour plus d'informations. Vous pouvez également entrer `*#06#` pour afficher automatiquement l'ID.
- **UDID** : chaque iPhone, iPod touch et iPad est associé à un numéro d'identification unique (UDID), voir http://www.macworld.co.uk/how-to/iphone/how-find-out-your-iphone-or-ipad-udid-3530239 pour plus d'informations.

Android :

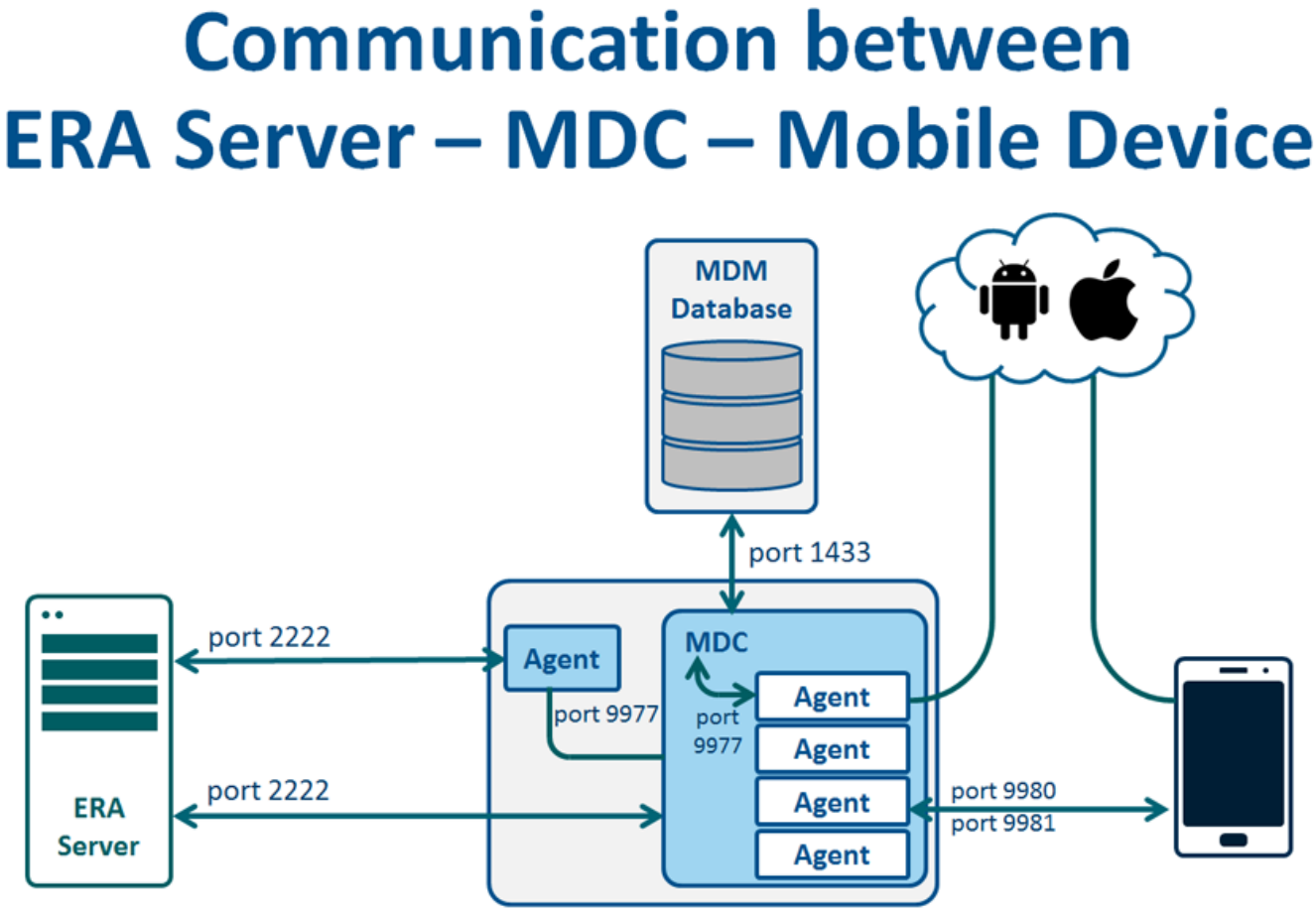
- **ID du périphérique** : le numéro **IMEI/MEID/IMSI** apparaît sur la page d'état du périphérique, appuyez sur **Menu** > **Paramètres** > **À propos du périphérique** > **Etat**. Vous pouvez également entrer `*#06#` pour afficher automatiquement l'ID. Voir http://www.wikihow.com/Find-the-IMEI-or-MEID-Number-on-a-Mobile-Phone pour plus d'informations.

4.4.19.4 Inscription de périphérique et communication MDC

Ce diagramme montre la communication d'un périphérique mobile avec le Connecteur de périphérique mobile (MDC) pendant le processus d'inscription :



Le diagramme suivant illustre la communication entre les composants ESET Remote Administrator et un périphérique mobile :



4.4.20 Afficher le message

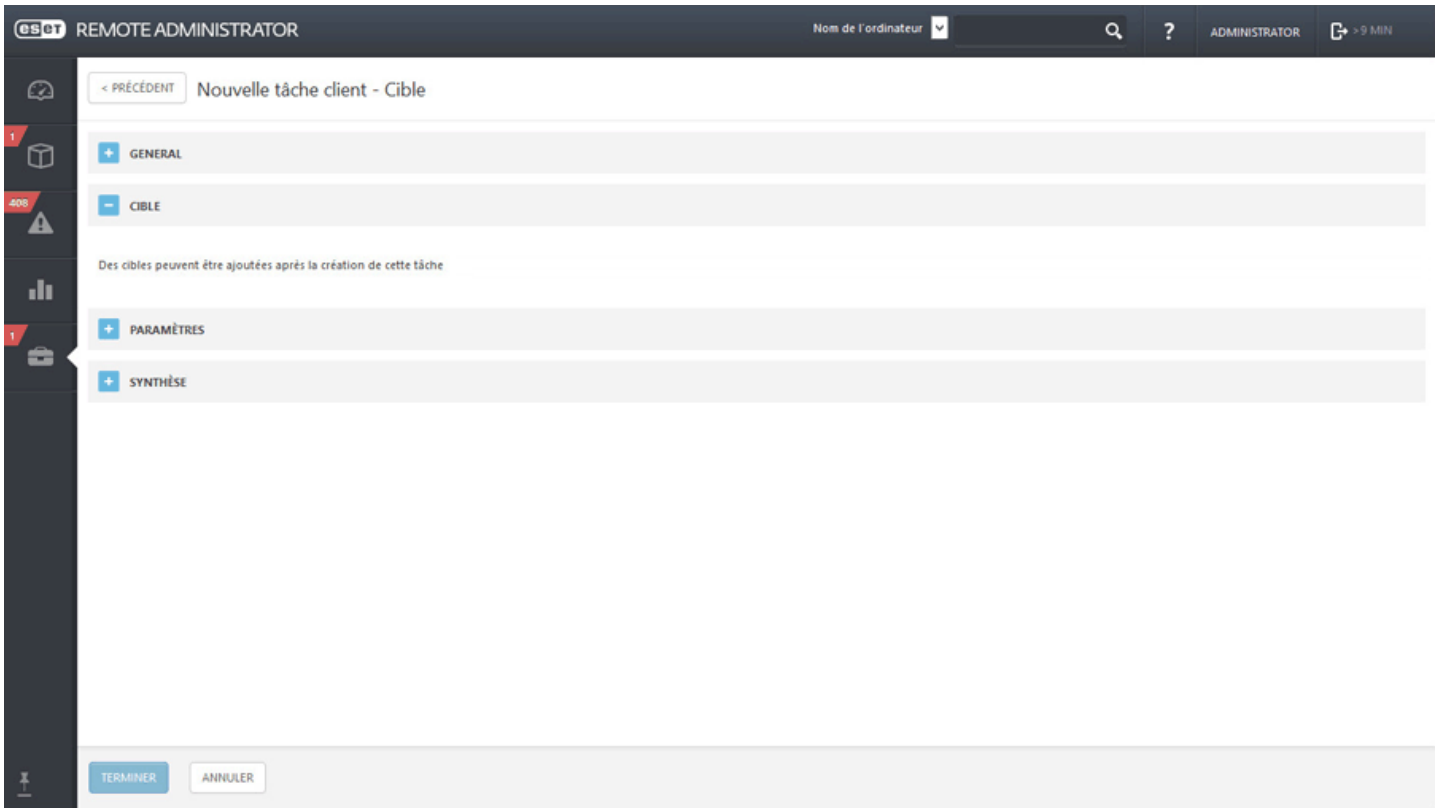
Cette fonctionnalité vous permet d'envoyer un message à n'importe quel périphérique (ordinateur client, tablette, périphérique mobile, etc.). Le message est affiché à l'écran afin d'informer l'utilisateur.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Afficher le message**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.

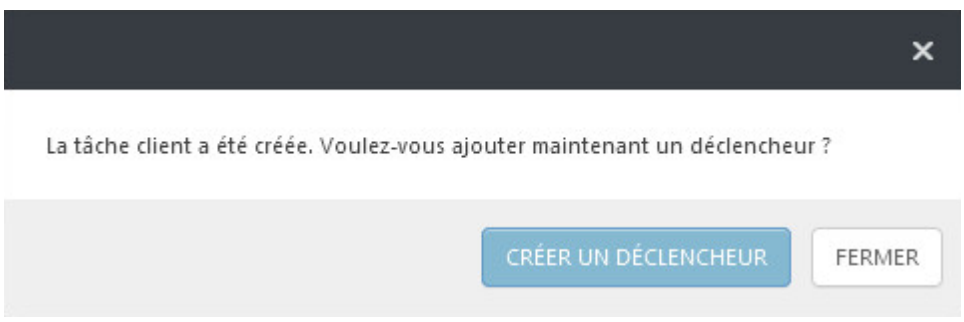


Paramètres

Vous pouvez saisir un **titre** et votre **message**.

Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.

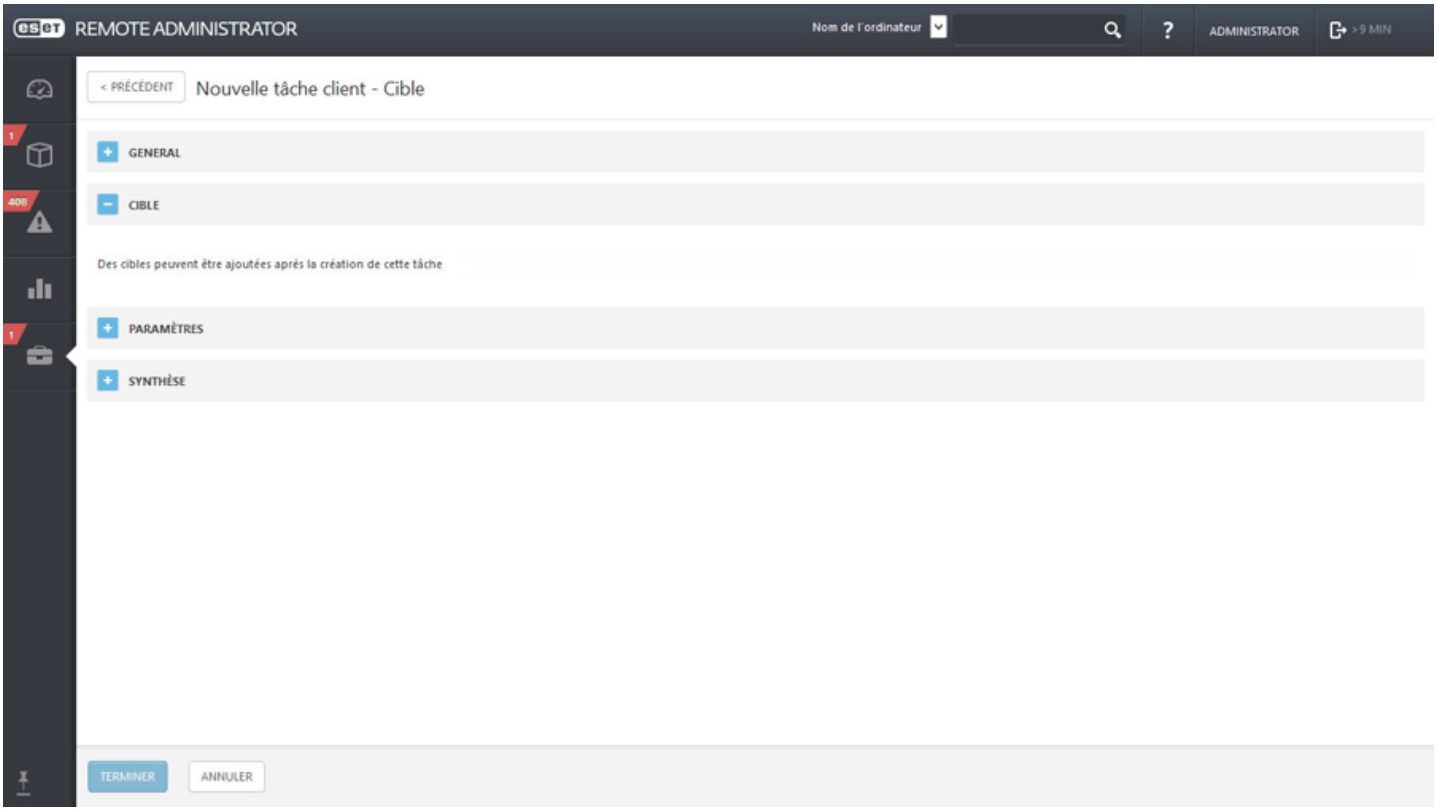


4.4.21 Actions Antivol

La fonction **Antivol** protège un périphérique mobile contre les accès non autorisés. En cas de perte ou de vol d'un périphérique mobile (inscrit et géré par ERA) appartenant à un utilisateur, certaines actions sont automatiquement exécutées et d'autres peuvent être effectuées à l'aide d'une tâche de client. Si une personne non autorisée remplace une carte SIM approuvée par carte non approuvée, le périphérique est automatiquement **verrouillé** par ESET Endpoint Security pour Android. En outre, une alerte est envoyée par SMS aux numéros de téléphone définis par l'utilisateur. Ce message contient le numéro de téléphone de la carte SIM en cours d'utilisation, le numéro **IMSI** (International Mobile Subscriber Identity) et le numéro **IMEI** (International Mobile Equipment Identity) du téléphone. L'utilisateur non autorisé n'est pas avisé de l'envoi de ce message, car il est automatiquement supprimé des fils des messages du périphérique. Il est également possible de demander les coordonnées **GPS** du périphérique mobile égaré ou d'effacer à distance toutes les données stockées sur le périphérique à l'aide d'une tâche de client.

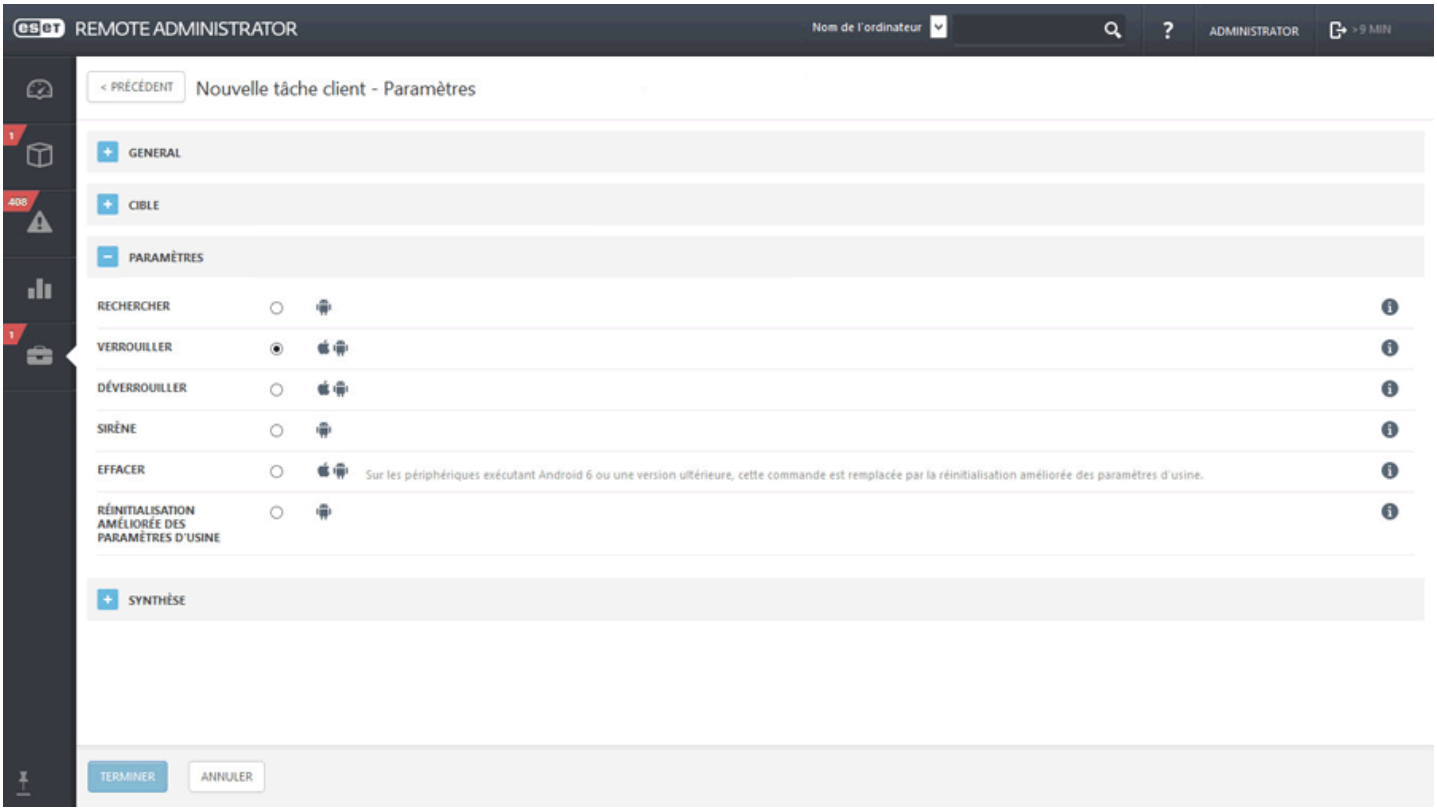
Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



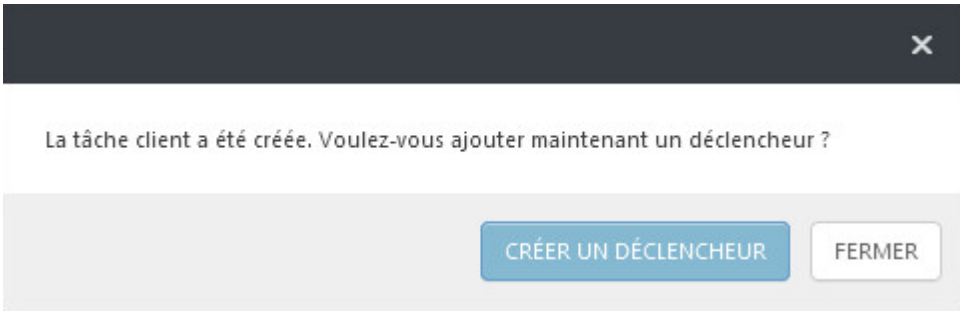
Paramètres

- **Rechercher** : le périphérique répondra en envoyant un message texte contenant ses coordonnées GPS. En cas de localisation plus précise dans les 10 minutes, il renverra le message. Les informations reçus s'affichent dans les détails de l'ordinateur.
- **Verrouiller** : le périphérique sera verrouillé. Il pourra être déverrouillé à l'aide du mot de passe Administrateur ou de la commande de déverrouillage.
- **Déverrouiller** : le périphérique sera déverrouillé pour pouvoir être réutilisé. La carte SIM actuelle du périphérique sera enregistrée en tant que carte SIM approuvée.
- **Sirène** : le périphérique sera verrouillé et il émettra un son très fort pendant 5 minutes (ou jusqu'à ce qu'il soit déverrouillé).
- **Effacer** : toutes les données accessibles sur le périphérique seront effacées (les fichiers seront remplacés). ESET Endpoint Security sera conservé sur le périphérique. Cette opération peut prendre plusieurs heures.
- **Réinitialisation améliorée des paramètres d'usine** : toutes les données accessibles sur le périphérique seront effacées (les en-têtes des fichiers seront détruits) et les paramètres d'usine par défaut seront rétablis. Cette opération peut prendre plusieurs minutes.



Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.22 Arrêter l'administration (désinstaller l'agent ERA)

- **Bureau** : cette tâche supprime l'Agent installé sur l'ordinateur sur lequel est installé MDM.
- **Mobile** : cette tâche annule l'inscription MDM du périphérique mobile.

Une fois que le périphérique n'est plus géré (l'Agent est supprimé), certains paramètres peuvent être conservés dans les produits gérés.

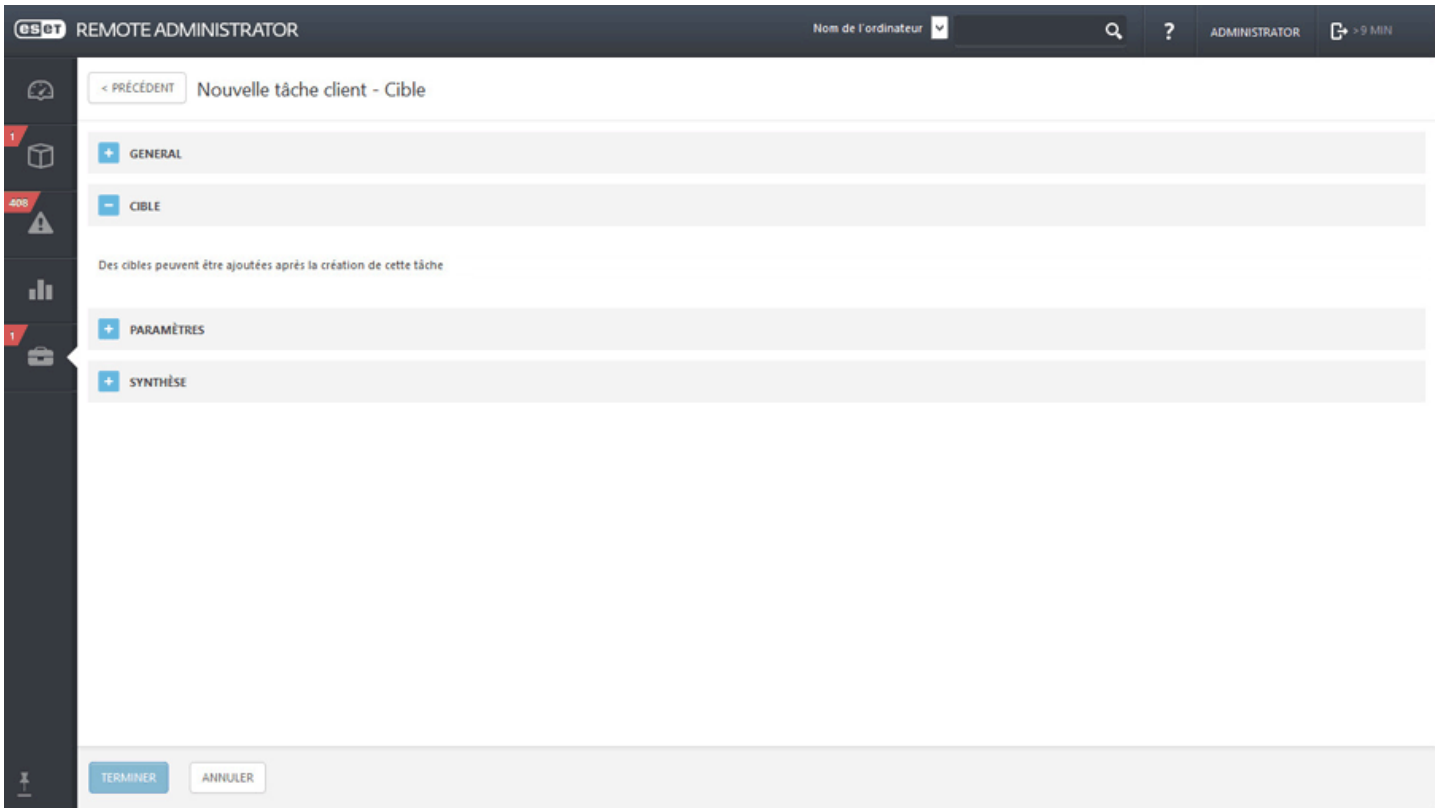
IMPORTANT : Il est recommandé de rétablir la valeur par défaut de certains paramètres (protection par mot de passe, par exemple) à l'aide d'une stratégie avant d'interrompre la gestion d'un périphérique. De plus, tous les tâches s'exécutant sur l'Agent sont annulées. L'état d'exécution **En cours**, **Terminé** ou **Échoué** de cette tâche peut ne pas être affiché précisément dans ERA Web Console selon la réplication.

1. Si le périphérique comporte des paramètres spéciaux que vous ne souhaitez pas conserver, définissez une stratégie de périphérique qui permet de rétablir les valeurs par défaut (ou les valeurs souhaitées) pour les paramètres non souhaités.
2. Avant d'effectuer cette étape, il est recommandé d'attendre suffisamment que les stratégies du point 1 aient terminé la réplication sur l'ordinateur cible avant de le supprimer de la liste dans ERA.
3. Avant de suivre cette étape, il est recommandé d'attendre que les stratégies du point 2 aient terminé avec certitude la réplication sur l'ordinateur cible.

aucun **paramètre** n'est disponible pour cette tâche.

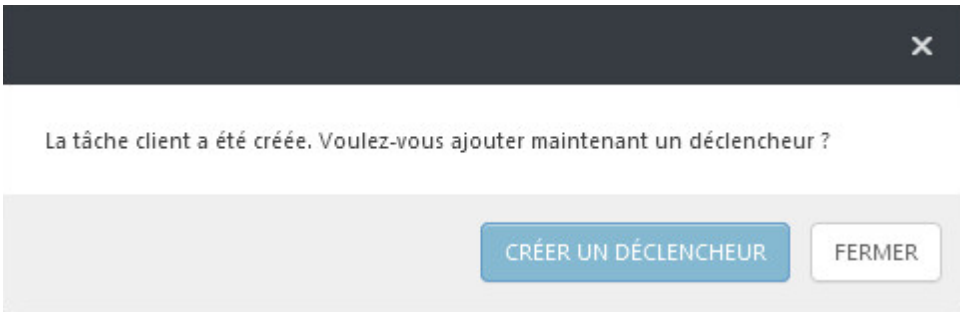
Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



Résumé

Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.23 Exporter la configuration des produits administrés

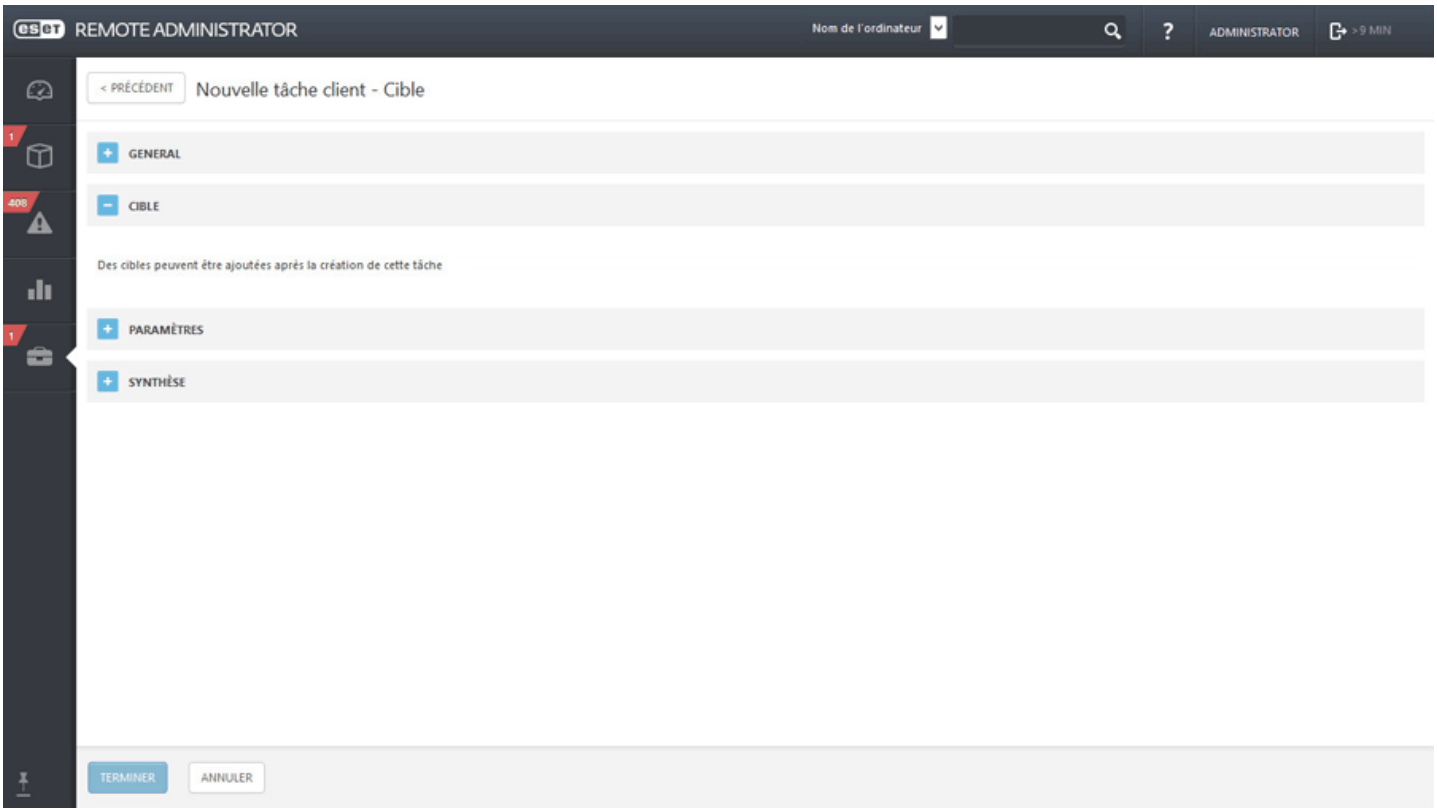
La tâche **Exporter la configuration des produits administrés** sert à exporter les paramètres d'un composant ERA ou d'un produit ESET installé sur le ou les clients.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** (voir la liste ci-dessus) définit les paramètres et le comportement de la tâche. Dans ce cas, vous pouvez utiliser la tâche **Exporter la configuration des produits administrés**.

Cible

IMPORTANT : Il n'est pas possible d'ajouter des cibles lors de la création d'une tâche client. Vous pourrez ajouter des cibles une fois la tâche créée. Configurez les paramètres de la tâche et cliquez sur Terminer pour créer la tâche, puis créez un déclencheur pour spécifier des cibles pour la tâche.



Paramètres

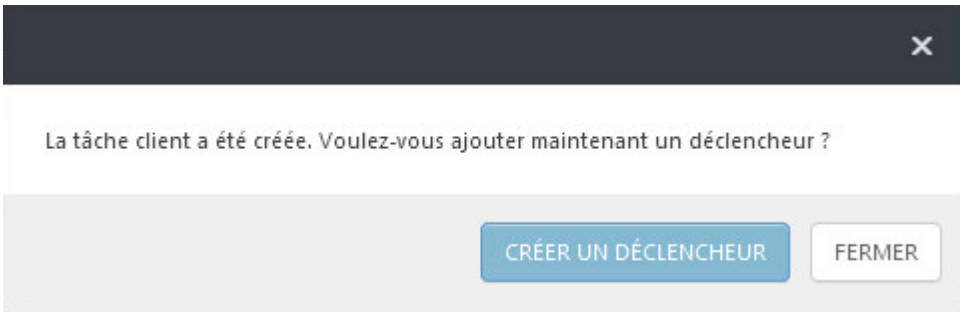
Exporter les paramètres de configuration des produits gérés

- **Produit** : sélectionnez un composant ERA ou un produit de sécurité client pour lequel vous souhaitez exporter la configuration.

Résumé

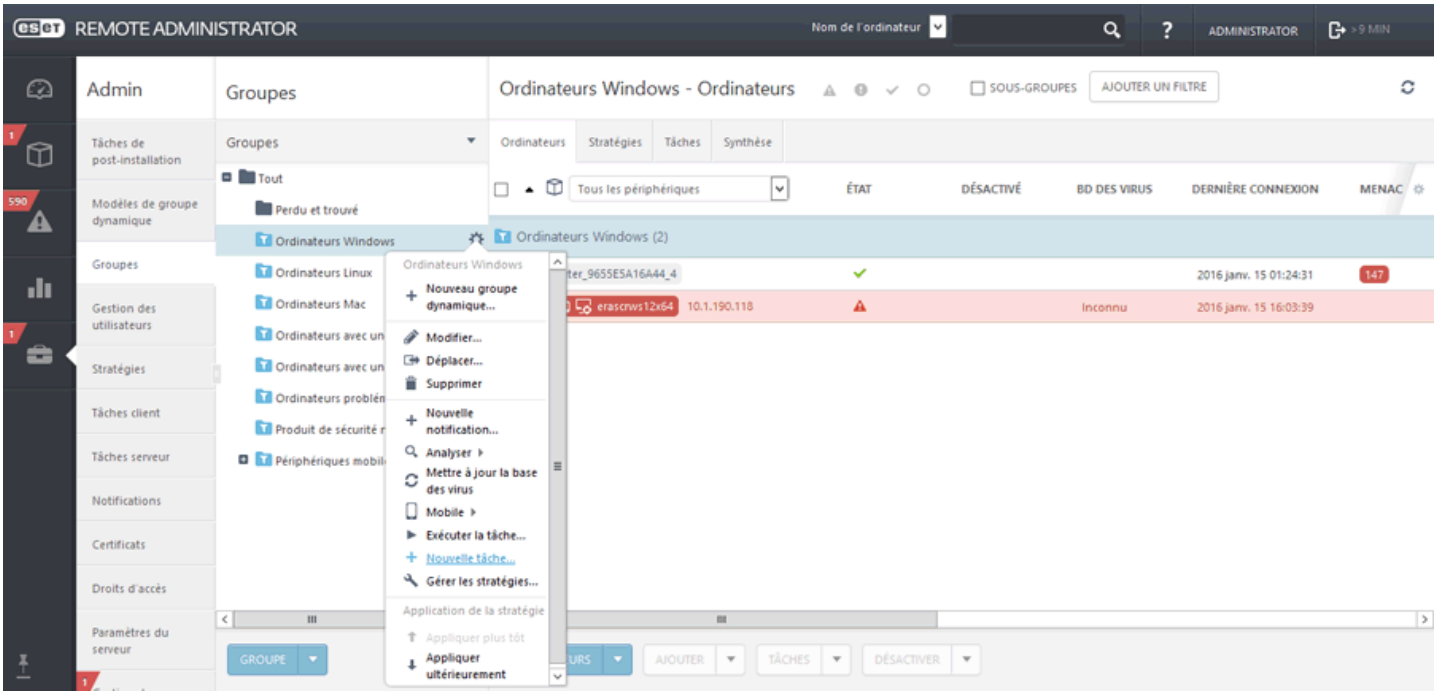
Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche client est alors créée et une fenêtre contextuelle s'ouvre. Nous vous recommandons de cliquer sur Créer un déclencheur pour spécifier

quand cette tâche client doit être exécutée et sur quelles cibles. Si vous cliquez sur **Fermer**, vous pouvez créer un déclencheur ultérieurement.



4.4.24 Attribuer une tâche à un groupe

Cliquez sur **Admin** > **Groupes**, sélectionnez **Groupe statique** ou **Groupe dynamique**, cliquez sur ⚙ en regard du groupe sélectionné ou sur **Groupe**, puis sur + **Nouvelle tâche**.

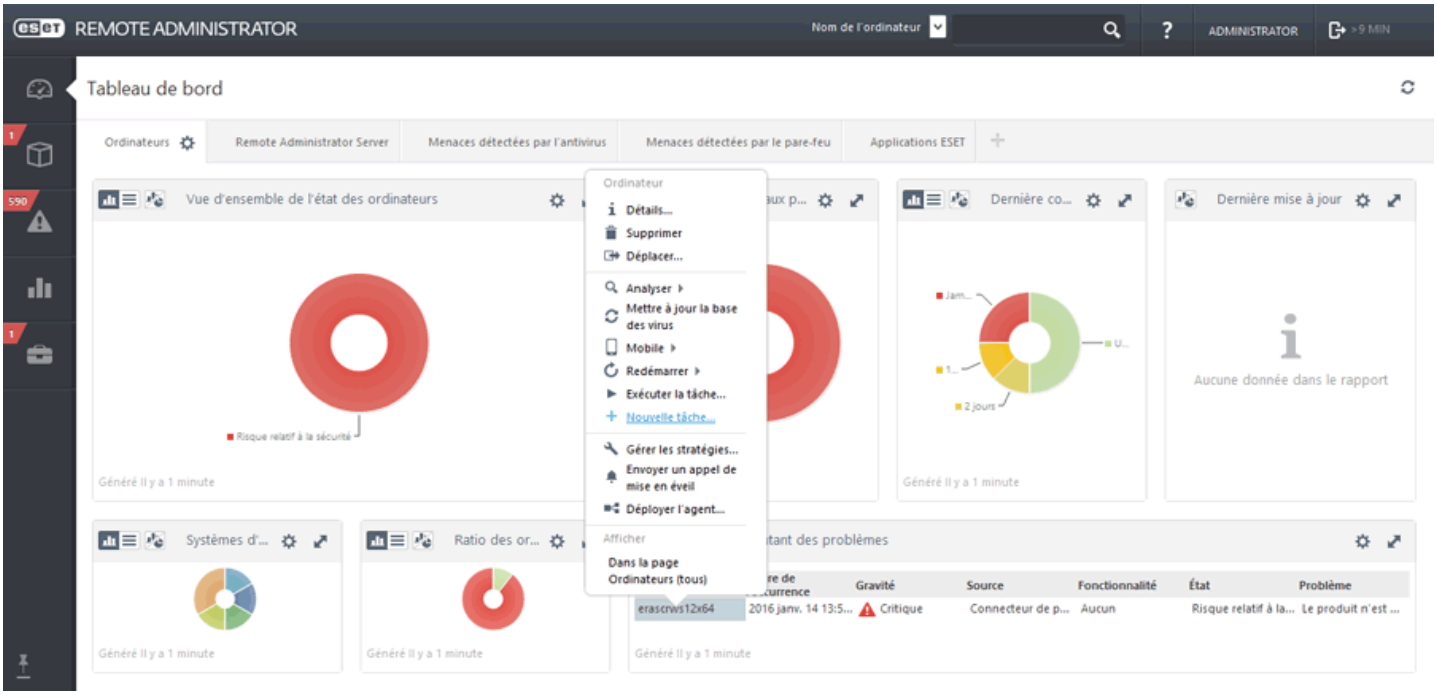


Vous pouvez également cliquer sur **Ordinateurs**, sélectionner **Statique** ou **Dynamique**, puis cliquer sur ⚙ > + **Nouvelle tâche**. La fenêtre Assistant Nouvelle tâche client s'ouvre.

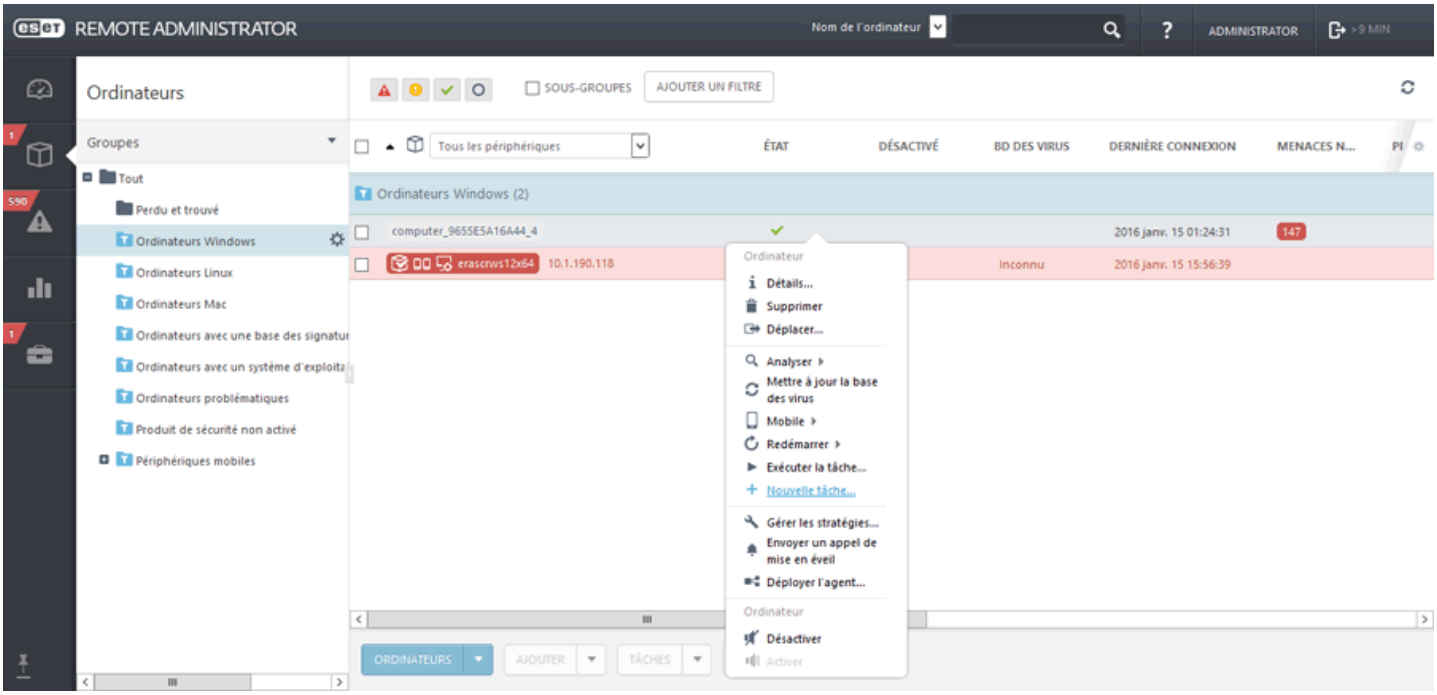
4.4.25 Attribuer une tâche à un ou des ordinateurs

Trois méthodes permettent d'attribuer une tâche à un ou des ordinateurs.

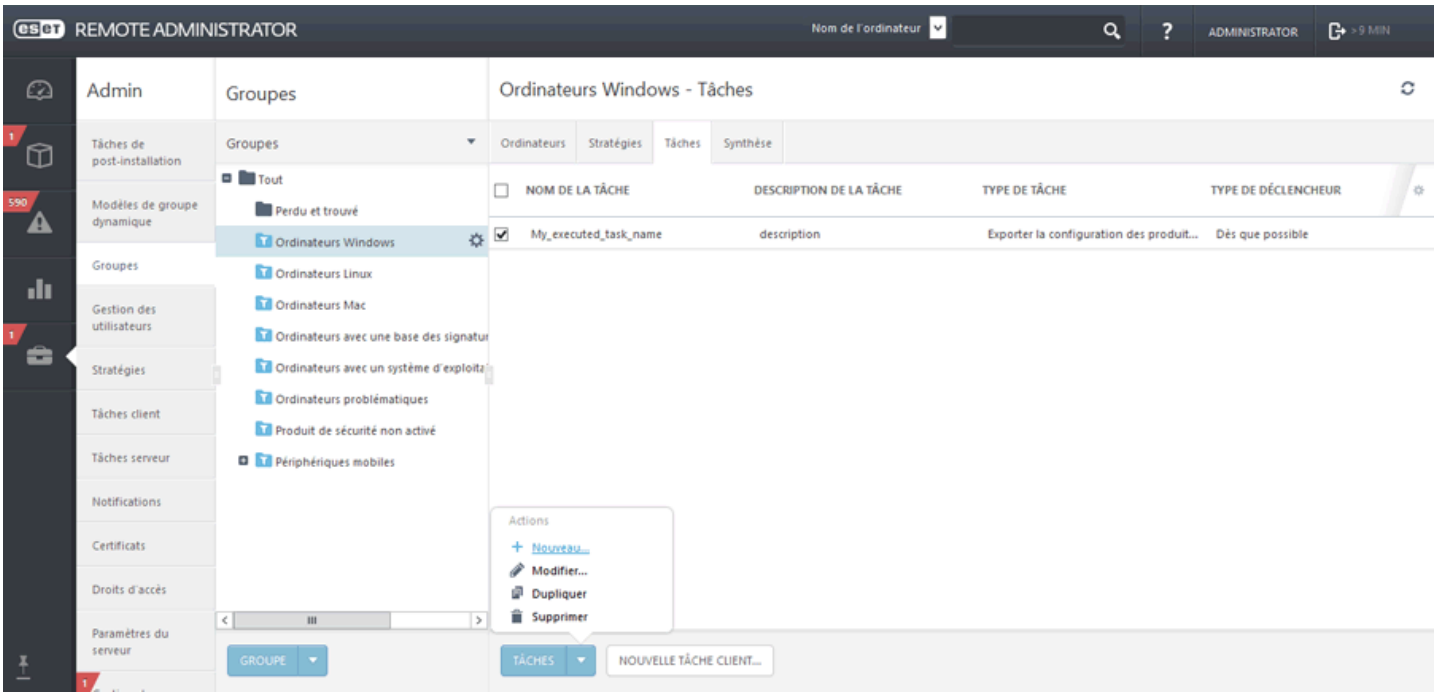
1. Accédez à **Tableau de bord** > **Ordinateurs présentant des problèmes**, puis sélectionnez + **Nouvelle tâche...**



2. Accédez à **Ordinateur**, sélectionnez un ou des ordinateurs à l'aide des cases à cocher, puis + **Nouvelle tâche...**



3. Accédez à **Admin** > **Groupes**, sélectionnez un ou des ordinateurs, cliquez sur le bouton **Tâches**, sélectionnez une action, puis cliquez sur + **Nouvelle tâche...**



La fenêtre Assistant Nouvelle tâche client s'ouvre.

4.4.26 Déclencheurs

Les déclencheurs peuvent être utilisés sur ERA Server et les agents (clients).

4.5 Tâches serveur

Les tâches serveur peuvent automatiser les tâches de routine. Une tâche de serveur peut être associée à des déclencheurs configurés, ce qui entraîne l'exécution de la tâche si une combinaison d'événements donnée se produit sur ERA Server.

REMARQUE : des tâches serveur ne peuvent pas être attribuées à un client ou à un groupe de clients spécifique.

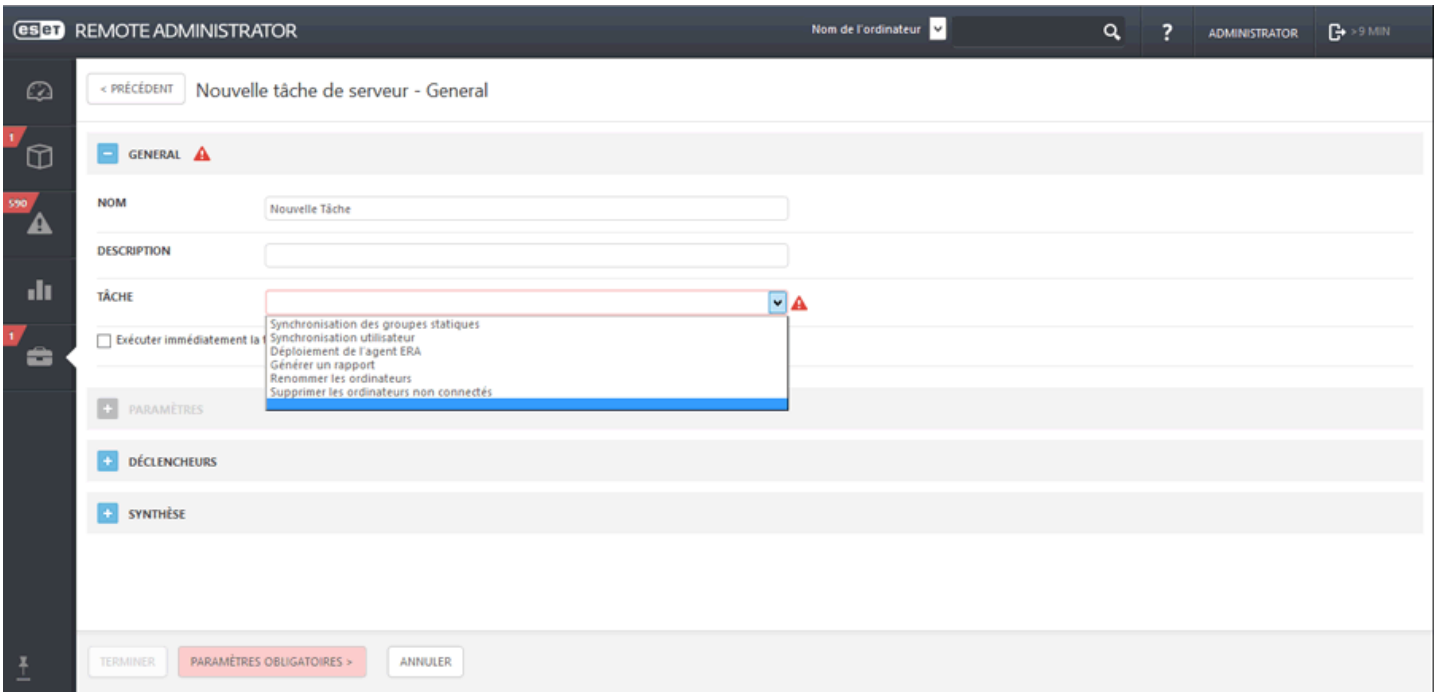
Les tâches serveur suivantes sont prédéfinies :

- Déploiement d'agent : distribue l'Agent aux ordinateurs clients.
- Supprimer les ordinateurs qui ne se connectent pas : supprime les clients qui ne se connectent plus à ESET Remote Administrator depuis la console Web.
- Générer un rapport : permet de générer les rapports dont vous avez besoin.
- Renommer les ordinateurs : cette tâche renomme de manière périodique les ordinateurs situés dans des groupes au format FQDN.
- Synchronisation des groupes statiques : met à jour les informations des groupes pour afficher des données actuelles.
- Synchronisation des utilisateurs : met à jour un utilisateur ou un groupe d'utilisateurs.

Pour commencer à créer votre tâche, cliquez sur **Admin** > **Tâches serveur** > **Nouveau**.

Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** définit les paramètres et le comportement de la tâche. Pour que la tâche s'exécute automatiquement lorsque vous cliquez sur Terminer, cochez la case en regard de l'option Exécuter immédiatement la tâche après la fin.

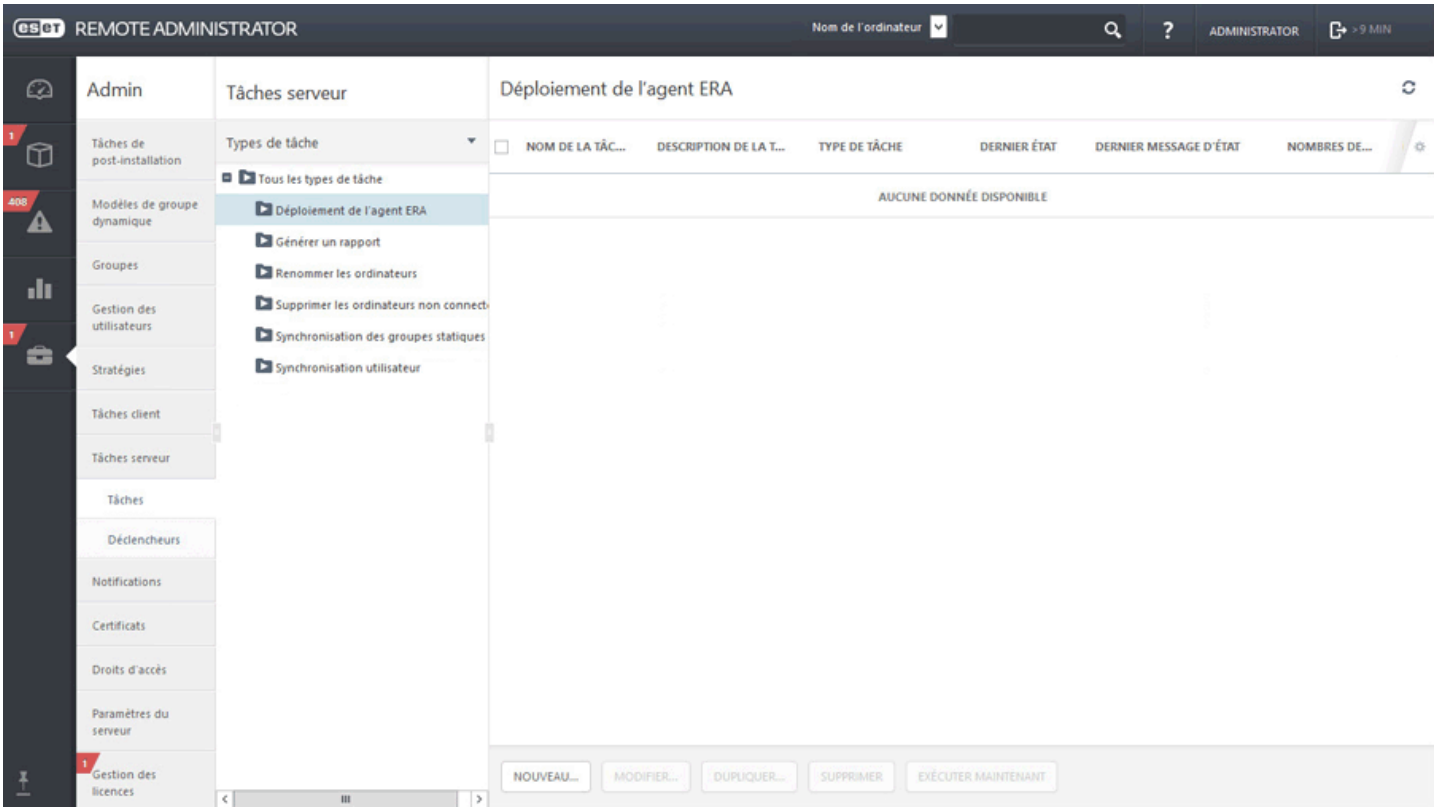


4.5.1 Déploiement d'agent

Le déploiement à distance d'ERA Agent est effectué dans la section **Admin**. Vous pouvez suivre les instructions de l'article de la base de connaissances.

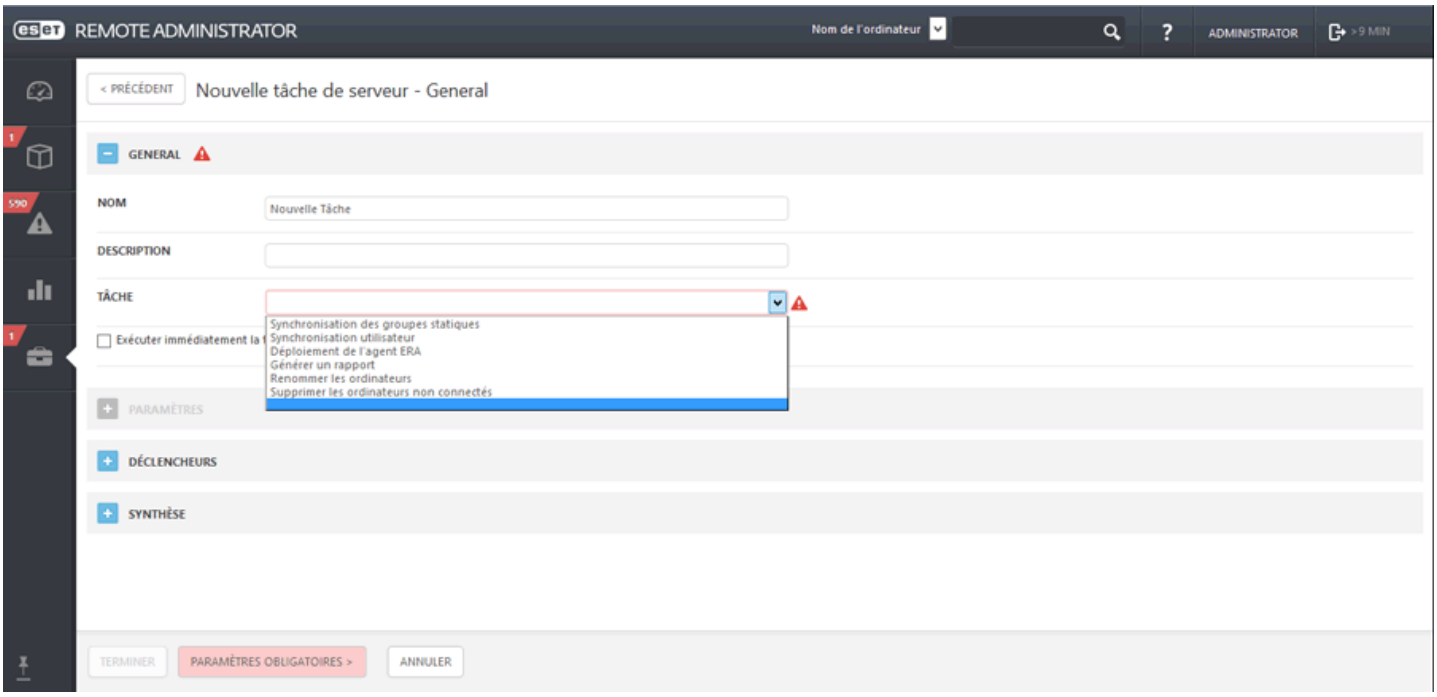
REMARQUE : il est recommandé de tester au préalable le déploiement en masse de l'Agent dans votre environnement. Une fois qu'il fonctionne correctement, vous pouvez commencer le déploiement réel sur les ordinateurs clients des utilisateurs. Avant de tester le déploiement en masse, vous devez également modifier l'intervalle de connexion de l'Agent.

Cliquez sur **Tâche de serveur** > **Déploiement d'agent** > **Nouveau...** pour configurer une nouvelle tâche.



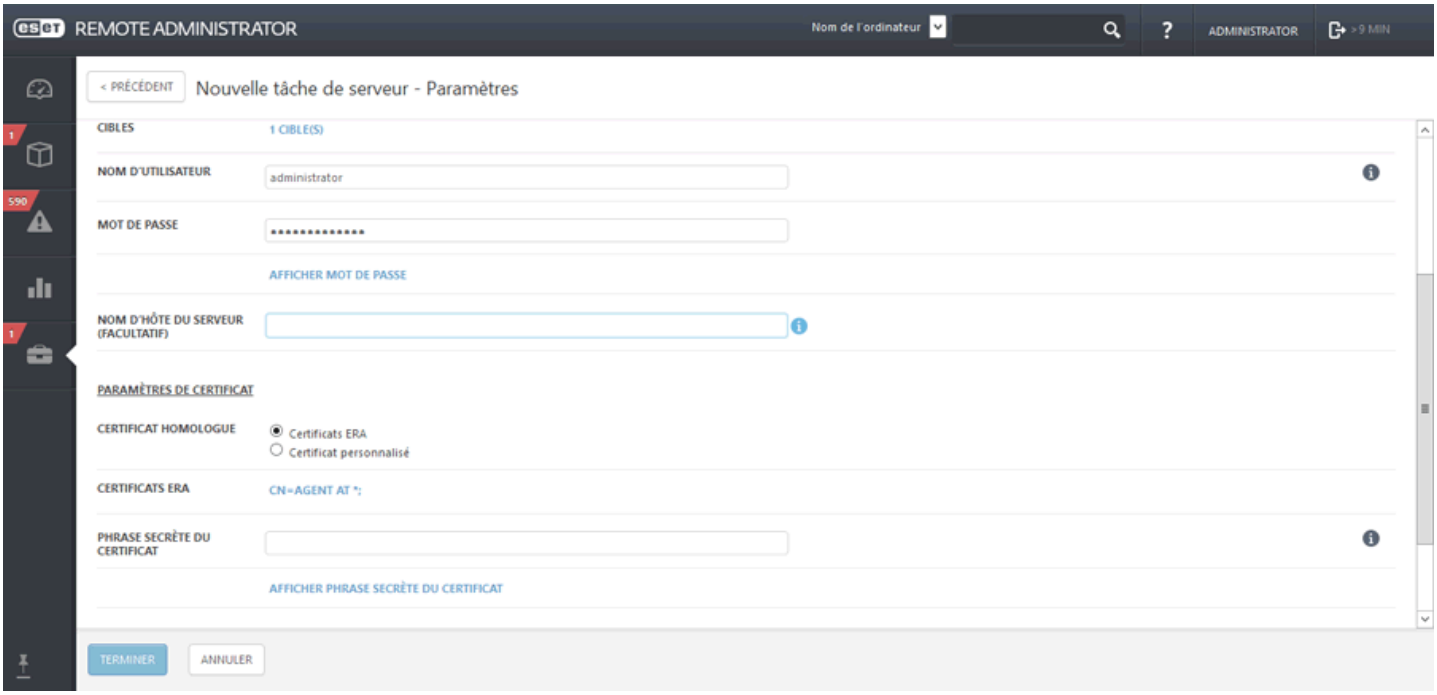
Général

Saisissez des informations de base sur la tâche dans les champs **Nom**, **Description** (facultatif) et **Type de tâche**. Le **type de tâche** définit les paramètres et le comportement de la tâche. Pour que la tâche s'exécute automatiquement lorsque vous cliquez sur Terminer, cochez la case en regard de l'option Exécuter immédiatement la tâche après la fin.



Paramètres

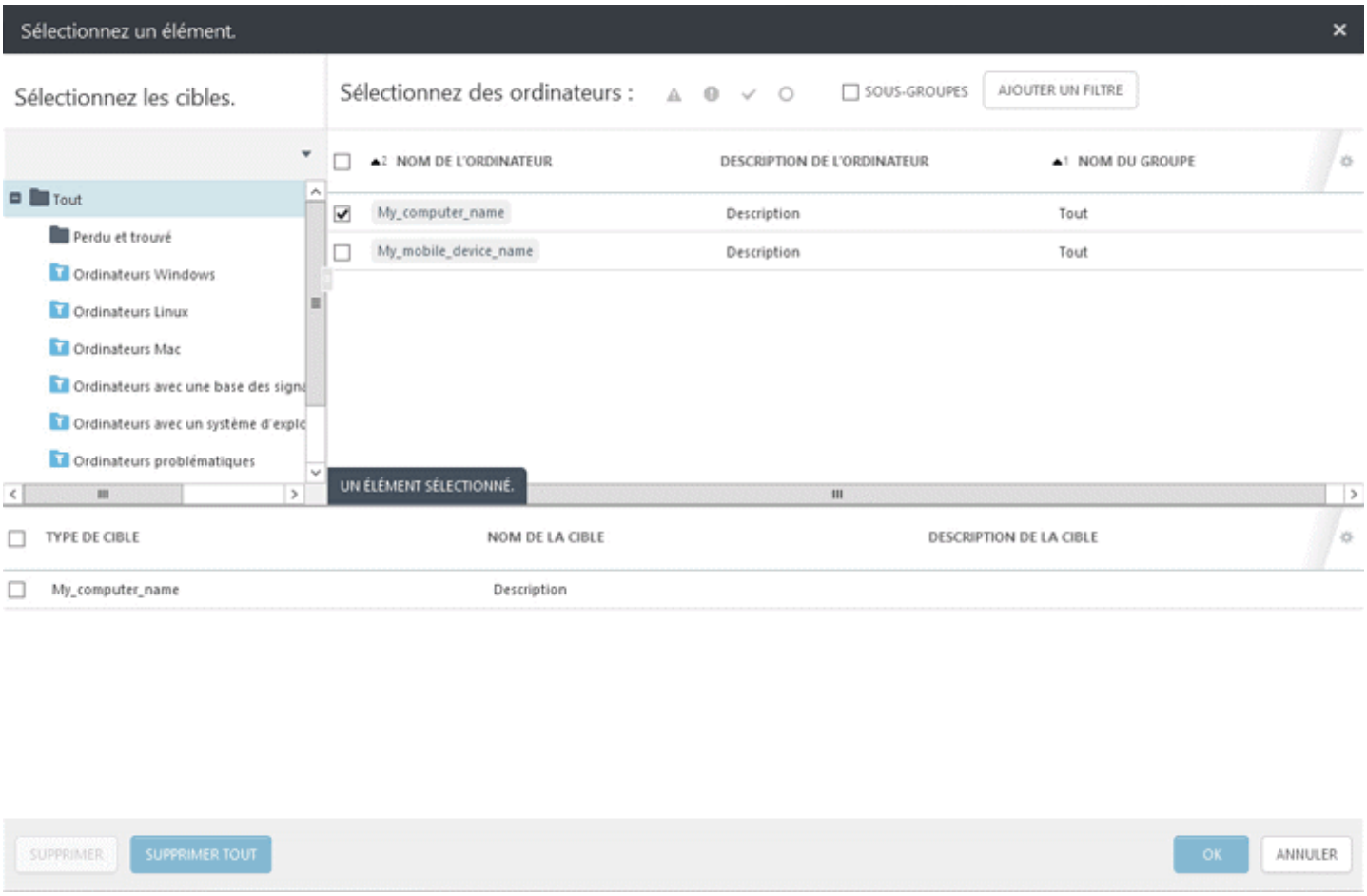
- **Résolution automatique de l'Agent adéquat** : si vous disposez de plusieurs systèmes d'exploitation (Windows, Linux, Mac OS) dans votre réseau, sélectionnez cette option. La tâche recherche automatiquement le package d'installation de l'Agent adéquat compatible avec le serveur pour chaque système.
- **Cibles** : cliquez sur cette option pour sélectionner les clients destinataires de cette tâche.
- **Nom d'utilisateur/Mot de passe** : il s'agit du nom d'utilisateur et du mot de passe de l'utilisateur disposant de droits suffisants pour effectuer une installation à distance de l'Agent.
- **Nom d'hôte du serveur (facultatif)** : vous pouvez saisir un nom d'hôte du serveur s'il est différent du côté client et serveur.
- **Certificat homologue/Certificat ERA** : il s'agit du certificat de sécurité et de l'autorité de certification pour l'installation de l'Agent. Vous pouvez utiliser le certificat et l'autorité de certification par défaut ou des certificats personnalisés. Pour plus d'informations, reportez-vous au chapitre Certificats.
- **Certificat personnalisé** : si vous utilisez un certificat personnalisé pour l'authentification, accédez à celui-ci et sélectionnez-le lors de l'installation de l'Agent.
- **Phrase secrète du certificat** : il s'agit du mot de passe du certificat que vous avez saisi lors de l'installation du serveur (à l'étape de création d'une autorité de certification) ou du mot de passe de votre certificat personnalisé.



REMARQUE : ERA Server peut automatiquement sélectionner le package d'installation de l'Agent adéquat pour les systèmes d'exploitation. Pour sélectionner manuellement un package, décochez l'option **Résolution automatique de l'Agent adéquat**, puis choisissez le package à utiliser parmi la liste des Agents disponibles dans le référentiel ERA.

Cible

La fenêtre **Cible** vous permet de spécifier les clients (ordinateurs ou groupes) destinataires de cette tâche. Cliquez sur **Ajouter des cibles** pour afficher tous les groupes statiques et dynamiques et leurs membres.



Sélectionnez des clients, cliquez sur **OK**, puis passez à la section Déclencheur.

Déclencheur : détermine l'événement qui déclenche la tâche.

- **Dès que possible** : exécute la tâche dès que le client se connecte à ESET Remote Administrator Server et la reçoit. Si la tâche ne peut pas être effectuée avant la **date d'expiration**, elle est retirée de la file d'attente. La tâche n'est pas supprimée, mais elle ne sera pas exécutée.
- **Déclencheur planifié** : exécute la tâche à une date sélectionnée. Vous pouvez planifier la tâche une seule fois, de manière répétée ou à l'aide d'une expression CRON.
- **Déclencheur lié au Journal des événements** : exécute la tâche selon les événements spécifiés dans cette zone. Ce déclencheur est invoqué lorsqu'un événement d'un certain type se produit dans les journaux. Définissez le **type de journal**, l'**opérateur logique** et les critères de **filtrage** qui déclencheront cette tâche.
- **Déclencheur A rejoint le groupe dynamique** : ce déclencheur exécute la tâche lorsqu'un client rejoint le groupe dynamique sélectionné dans l'option cible. Si un groupe statique ou un client a été sélectionné, cette option ne sera pas disponible.

REMARQUE : pour plus d'informations sur les déclencheurs, reportez-vous au chapitre Déclencheurs.

Paramètres avancés de la limitation : une limitation sert à limiter l'exécution d'une tâche si cette dernière est déclenchée par un événement qui se produit fréquemment, comme dans les cas **Déclencheur lié au Journal des événements** et **Déclencheur A rejoint le groupe dynamique** (voir ci-dessus). Pour plus d'informations, reportez-vous au chapitre Limitation.

Lorsque vous avez défini les destinataires et les déclencheurs de cette tâche, cliquez sur **Terminer**.

Résumé

Toutes les options configurées sont affichées dans cette section. Examinez les paramètres et s'ils sont corrects, cliquez sur Terminer. La tâche est alors créée et prête à être utilisée.

Le déploiement de l'Agent ERA peut être effectué de plusieurs manières différentes : Vous pouvez déployer l'Agent :

Utiliser GPO et SCCM à distance : cette méthode est recommandée pour le déploiement en masse d'ERA Agent sur des ordinateurs clients (vous pouvez aussi utiliser une tâche de serveur pour déployer ERA Agent).
Localement : à l'aide d'un package d'installation de l'Agent ou des programmes d'installation Agent Live, en cas de problème lors du déploiement à distance, par exemple.

Le déploiement local peut être effectué de trois manières différentes :

- Programmes d'installation Agent Live : à l'aide d'un script généré à partir de la console web ERA, vous pouvez distribuer les programmes d'installation Agent Live par courrier électronique ou les exécuter à partir d'un support amovible (clé USB, etc.).
- Installation assistée du serveur : à l'aide du package d'installation de l'Agent, cette méthode permet de télécharger automatiquement les certificats d'ERA Server (méthode de déploiement local recommandée).
- Installation hors ligne : à l'aide du package d'installation de l'Agent, vous devez exporter manuellement les certificats et les utiliser avec cette méthode de déploiement.

La tâche de serveur de déploiement d'agent à distance peut être utilisée pour la distribution en masse de l'Agent aux ordinateurs clients. Il s'agit de la méthode de distribution la plus pratique, car elle est peut être effectuée à partir de la console Web sans avoir à déployer manuellement l'Agent sur chaque ordinateur.

ERA Agent est un composant très important, car les solutions de sécurité ESET s'exécutant sur les clients communiquent avec ERA Server exclusivement par le biais de l'Agent.

REMARQUE : si vous rencontrez des problèmes lors du déploiement à distance d'ERA Agent (la tâche de serveur **Déploiement d'agent** échoue), reportez-vous au guide Dépannage.

4.5.2 Supprimer les ordinateurs qui ne se connectent pas

La tâche **Supprimer les ordinateurs qui ne se connectent pas** permet de supprimer des ordinateurs selon des critères spécifiés. Par exemple, si l'ERA Agent sur un ordinateur client ne s'est pas connecté depuis 30 jours, il peut être supprimé d'ERA Web Console.

Général

Saisissez des informations de base sur la tâche telles que le **Nom**, la **Description** (facultatif) et le **Type de tâche**. Le **type de tâche** définit les paramètres et le comportement de la tâche. Pour que la tâche s'exécute automatiquement lorsque vous cliquez sur **Terminer**, cochez la case en regard de l'option **Exécuter immédiatement la tâche après la fin**.

Paramètres- **Nom du groupe** : sélectionnez un groupe statique ou dynamique ou créez un nouveau groupe dans lequel les ordinateurs seront renommés.

Nombre de jours pendant lesquels l'ordinateur n'a pas été connecté : saisissez le nombre de jours au-delà duquel les ordinateurs seront supprimés.

Désactiver la licence : utilisez cette option si vous souhaitez également désactiver les licences des ordinateurs supprimés.

Supprimer les ordinateurs non gérés : si vous cochez cette case, les ordinateurs non gérés seront également supprimés.

Déclencheurs

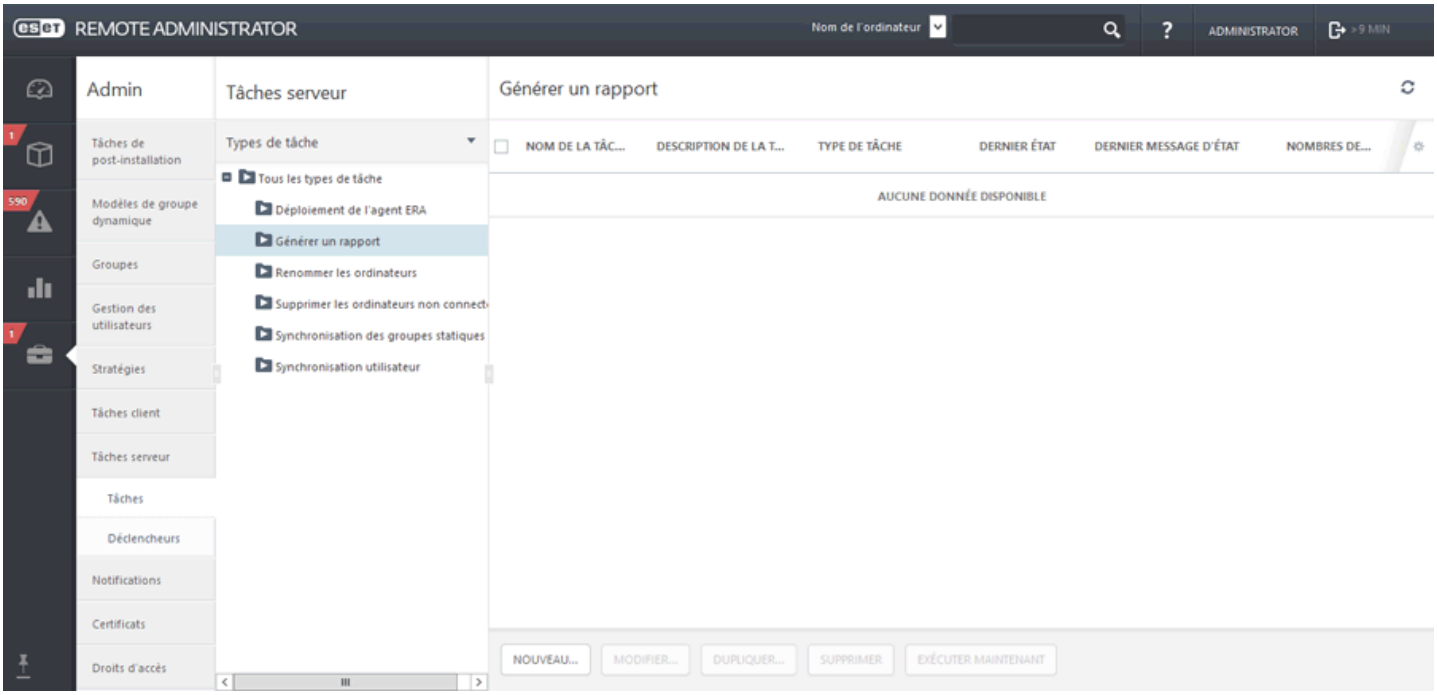
Sélectionnez un déclencheur existant pour cette tâche ou créez un déclencheur. Il est également possible de **supprimer** ou de **modifier** un déclencheur sélectionné.

Résumé

Passez en revue les informations de configuration affichées dans cette section. Si elles sont correctes, cliquez sur **Terminer**. La tâche est alors créée et prête à être utilisée.

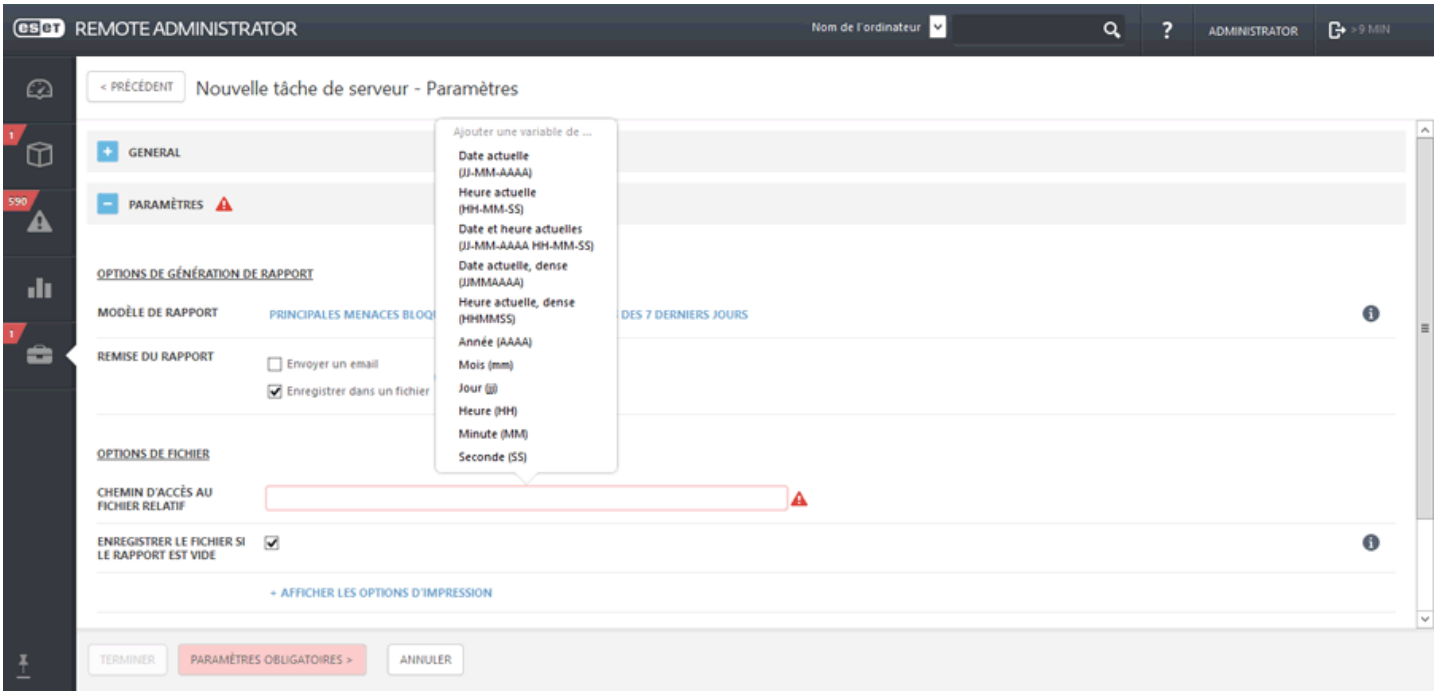
4.5.3 Générer un rapport

La tâche **Générer un rapport** sert à générer des rapports à partir de modèles de rapport prédéfinis ou précédemment créés.



Paramètres

Modèle de rapport : sélectionnez un modèle de rapport dans la liste.



Sélectionnez Envoyer un courrier électronique ou Enregistrer dans un fichier pour obtenir le rapport généré.

ENVOYER UN COURRIER ÉLECTRONIQUE

Pour envoyer/recevoir des messages électroniques, vous devez configurer les paramètres SMTP sous Paramètres du serveur > Paramètres avancés.

Message électronique

- **Envoyer à** : saisissez les adresses électroniques des destinataires des messages électroniques de rapport. Séparez plusieurs adresses par une virgule (,). Il est également possible d'ajouter des champs Cc et Cci. Ces derniers fonctionnent comme dans tous les clients de messagerie.
- **Objet** : objet du message de rapport. Saisissez un objet distinctif pour que les messages entrants puissent être triés. Il s'agit d'un paramètre facultatif. Il est toutefois conseillé de ne pas laisser ce champ vide.
- **Contenu du message** : définissez le corps du message de rapport.
- **Envoyer un courrier électronique si le rapport est vide** : utilisez cette option si vous souhaitez envoyer le rapport même s'il ne contient pas de données.

Options d'impression

Cliquez sur **Afficher les options d'impression** pour afficher les paramètres suivants :

- **Format de sortie** : sélectionnez le format de fichier adéquat. Le rapport généré est joint au message et peut être imprimé ultérieurement.
- **Langue de sortie** : sélectionnez la langue du message. La langue par défaut repose sur celle sélectionnée pour ERA Web Console.
- **Taille de la page/Résolution/Orientation du papier/Format de couleur/Unités des marges/Marges** : ces options sont pertinentes si vous souhaitez imprimer le rapport. Sélectionnez les options qui répondent à vos besoins. Ces options s'appliquent uniquement aux formats PDF et PS, et non au format CSV.

REMARQUE : la tâche **Générer un rapport** vous permet d'effectuer un choix parmi plusieurs formats de fichier de sortie. Si vous sélectionnez le format CSV, les valeurs de date et d'heure du rapport sont stockées au format UTC. Lorsque vous sélectionnez l'une des deux options de sortie restantes (PDF, PS), le serveur utilise l'heure du serveur local.

ENREGISTRER DANS UN FICHIER

Options de fichier

- **Chemin d'accès au fichier relatif** : le rapport est généré dans un répertoire spécifique, par exemple : *C:\Users\All Users\ESET\RemoteAdministrator\Server\Data\GeneratedReports*
- **Enregistrer le fichier si le rapport est vide** : utilisez cette option si vous souhaitez enregistrer le rapport même s'il ne contient pas de données.

Options d'impression

Cliquez sur **Afficher les options d'impression** pour afficher les paramètres suivants :

- **Format de sortie** : sélectionnez le format de fichier adéquat. Le rapport généré est joint au message et peut être imprimé ultérieurement.
- **Langue de sortie** : sélectionnez la langue du message. La langue par défaut repose sur celle sélectionnée pour ERA Web Console.
- **Taille de la page/Résolution/Orientation du papier/Format de couleur/Unités des marges/Marges** : ces options sont pertinentes si vous souhaitez imprimer le rapport. Sélectionnez les options qui répondent à vos besoins. Ces options s'appliquent uniquement aux formats PDF et PS, et non au format CSV.

REMARQUE : la tâche **Générer un rapport** vous permet d'effectuer un choix parmi plusieurs formats de fichier de sortie. Si vous sélectionnez le format CSV, les valeurs de date et d'heure du rapport sont stockées au format UTC. Lorsque vous sélectionnez l'une des deux options de sortie restantes (PDF, PS), le serveur utilise l'heure du serveur local.

Déclencheurs

Sélectionnez un déclencheur existant pour cette tâche ou créez un déclencheur. Il est également possible de **supprimer** ou de **modifier** un déclencheur sélectionné.

Résumé

Toutes les options configurées sont affichées dans cette section. Examinez les paramètres et s'ils sont corrects, cliquez sur Terminer. La tâche est alors créée et prête à être utilisée.

REMARQUE : Ubuntu Server Edition requiert l'installation de **X Server** et **xinit** pour que l'impression des rapports (rapports PDF) fonctionne.

```
sudo apt-get install server-xorg
sudo apt-get install xinit
startx
```

4.5.4 Renommer les ordinateurs

Vous pouvez utiliser la tâche **Renommer les ordinateurs** pour renommer les ordinateurs au format FQDN dans ERA. Vous pouvez utiliser la tâche de serveur existante fournie par défaut avec l'installation d'ERA. Cette tâche renomme automatiquement toutes les heures les ordinateurs synchronisés situés dans le groupe Perdu et trouvé. Pour créer une nouvelle tâche, cliquez sur **Tâche de serveur** > **Renommer les ordinateurs** > **Nouveau**.

Général

Saisissez des informations de base sur la tâche telles que le **Nom**, la **Description** (facultatif) et le **Type de tâche**. Le **type de tâche** définit les paramètres et le comportement de la tâche. Pour que la tâche s'exécute automatiquement lorsque vous cliquez sur **Terminer**, cochez la case en regard de l'option **Exécuter immédiatement la tâche après la fin**.

Paramètres

Nom du groupe : sélectionnez un groupe statique ou dynamique ou créez un nouveau groupe dans lequel les ordinateurs seront renommés.

Renommer selon :

- **Nom de l'ordinateur**
- **FQDN (nom de domaine complet) de l'ordinateur**

Résolution des conflits de nom entre les ordinateurs déjà présents dans ERA (le nom de l'ordinateur doit être unique) et ceux ajoutés lors de la synchronisation. Les vérifications s'appliquent uniquement aux noms des ordinateurs situés en dehors de la sous-arborescence en cours de synchronisation.

Déclencheurs

Sélectionnez un déclencheur existant pour cette tâche ou créez un déclencheur. Il est également possible de **supprimer** ou de **modifier** un déclencheur sélectionné.

Résumé

Passez en revue les informations de configuration affichées dans cette section. Si elles sont correctes, cliquez sur **Terminer**. La tâche est alors créée et prête à être utilisée.

4.5.5 Synchronisation des groupes statiques

La tâche **Synchronisation des groupes statiques** permet de rechercher des ordinateurs sur le réseau (Active Directory, Open Directory, LDAP, réseau local ou VMware) et de les placer dans un groupe statique. Si vous sélectionnez **Synchroniser avec Active Directory** pendant l'installation du serveur, les ordinateurs détectés sont ajoutés au groupe **Tous**.

Cliquez sur **Admin** > **Tâche de serveur** > **Synchronisation des groupes statiques** > **Nouveau...**

General

Saisissez des informations de base sur la tâche, telles que le **Nom** et la **Description** (facultatif). Le **type de tâche** définit les paramètres et le comportement de la tâche. Pour que la tâche s'exécute automatiquement lorsque vous cliquez sur **Terminer**, cochez la case en regard de l'option **Exécuter immédiatement la tâche après la fin**.

Paramètres

Développez les paramètres et cliquez sur **Sélectionner** sous **Nom du groupe statique** : Par défaut, la racine des ordinateurs synchronisés sera utilisée. Vous pouvez également créer un groupe statique.

- **Objets à synchroniser** : **ordinateurs et groupes** ou **ordinateurs uniquement**.
- **Gestion des collisions de création d'ordinateur** : si la synchronisation ajoute des ordinateurs qui sont déjà membres du groupe statique, vous pouvez choisir une méthode de résolution des conflits : Ignorer (les ordinateurs synchronisés ne sont pas ajoutés) ou Déplacer (les nouveaux ordinateurs sont déplacés vers un sous-groupe).
- **Gestion des extinctions d'ordinateur** : si un ordinateur n'existe plus, vous pouvez le **supprimer** ou l'**ignorer**.
- **Gestion des extinctions de groupe** : si un groupe n'existe plus, vous pouvez le **supprimer** ou l'**ignorer**.

Il existe trois **modes de synchronisation** :

- **Réseau MS Windows :** entrez le **groupe de travail** à utiliser et l'utilisateur avec ses informations d'identification.
- **Active Directory/Open Directory/LDAP** : saisissez les informations de connexion au serveur. Reportez-vous à la section mode de synchronisation pour obtenir des instructions détaillées.
- **VMware** : saisissez les informations de connexion à VMware vCenter Server. Reportez-vous à la section mode de synchronisation pour obtenir des instructions détaillées.

Dans la section **Paramètres de synchronisation du réseau Microsoft Windows**, entrez les informations suivantes :

- **Groupe de travail :** Entrez le domaine ou le groupe de travail qui contient les ordinateurs à synchroniser. Si vous ne spécifiez aucun groupe de travail, tous les ordinateurs visibles seront synchronisés.
- **Connexion :**Entrez les informations d'authentification utilisées pour la synchronisation dans votre réseau Windows.
- **Mot de passe :** Entrez le mot de passe utilisé pour vous connecter au réseau Windows.

➖ Déclencheurs

Sélectionnez un déclencheur existant pour cette tâche ou créez un déclencheur. Il est également possible de **supprimer** ou de **modifier** un déclencheur sélectionné.

➖ Résumé

Passez en revue les informations de configuration affichées dans cette section. Si elles sont correctes, cliquez sur **Terminer**. La tâche est alors créée et prête à être utilisée.
Seuls les ordinateurs Windows recevront la tâche à l'aide des paramètres par défaut. Si vous disposez d'ordinateurs Linux dans votre domaine Windows et si vous souhaitez qu'ils reçoivent aussi cette tâche, rendez-les d'abord visibles. Les ordinateurs Linux dans un domaine Windows n'affichent aucun texte dans les propriétés d'ordinateur Utilisateurs et ordinateurs Active Directory. Ces informations doivent donc être saisies manuellement.

4.5.5.1 Mode de synchronisation - Active Directory

Cliquez sur **Admin** > **Tâche de serveur** > **Synchronisation des groupes statiques** > **Nouveau...**

General

Saisissez des informations de base sur la tâche, telles que le **Nom** et la **Description** (facultatif). Le **type de tâche** définit les paramètres et le comportement de la tâche. Pour que la tâche s'exécute automatiquement lorsque vous cliquez sur **Terminer**, cochez la case en regard de l'option **Exécuter immédiatement la tâche après la fin**.

Paramètres

Développez les paramètres et cliquez sur **Sélectionner** sous **Nom du groupe statique** : Par défaut, la racine des ordinateurs synchronisés sera utilisée. Vous pouvez également créer un groupe statique.

- **Objets à synchroniser** : **ordinateurs et groupes** ou **ordinateurs uniquement**.
- **Gestion des collisions de création d'ordinateur** : si la synchronisation ajoute des ordinateurs qui sont déjà membres du groupe statique, vous pouvez choisir une méthode de résolution des conflits : Ignorer (les ordinateurs synchronisés ne sont pas ajoutés) ou Déplacer (les nouveaux ordinateurs sont déplacés vers un sous-groupe).
- **Gestion des extinctions d'ordinateur** : si un ordinateur n'existe plus, vous pouvez le **supprimer** ou l'**ignorer**.
- **Gestion des extinctions de groupe** : si un groupe n'existe plus, vous pouvez le **supprimer** ou l'**ignorer**.

Il existe trois **modes de synchronisation** :

- **Réseau MS Windows :** entrez le **groupe de travail** à utiliser et l'utilisateur avec ses informations d'identification.
- **Active Directory/Open Directory/LDAP** : saisissez les informations de connexion au serveur. Reportez-vous à la section mode de synchronisation pour obtenir des instructions détaillées.
- **VMware** : saisissez les informations de connexion à VMware vCenter Server. Reportez-vous à la section mode de synchronisation pour obtenir des instructions détaillées.

Paramètres de connexion au serveur :

- **Serveur** : saisissez le nom du serveur ou l'adresse IP du contrôleur de domaine.
- **Connexion** : saisissez les informations d'identification de connexion du contrôleur de domaine sous la forme **DOMAINE\nom_utilisateur**.
- **Mot de passe** : saisissez le mot de passe utilisé pour se connecter au contrôleur de domaine.

- **Utiliser les paramètres LDAP :** si vous souhaitez utiliser le protocole LDAP, cochez la case **Utiliser le protocole LDAP au lieu d'Active Directory**, puis saisissez des attributs spécifiques qui correspondent à votre serveur. Vous pouvez également sélectionner une **valeur prédéfinie** en cliquant sur **Personnaliser...** pour que les paramètres soient renseignés automatiquement.

- **Active Directory** - Cliquez sur **Parcourir** jusqu'à **Nom unique**. Votre arborescence Active Directory va s'afficher. Sélectionnez l'entrée supérieure pour synchroniser tous les groupes avec ERA ou ne sélectionnez que des groupes spécifiques à ajouter. Cliquez sur **OK** lorsque vous avez terminé.
- **Open Directory de Mac OS X Server (noms d'hôte des ordinateurs)**
- **Open Directory de Mac OS X Server (adresses IP des ordinateurs)**
- **OpenLDAP avec les enregistrements d'ordinateur Samba** : configuration des paramètres de nom DNS dans Active Directory.

Paramètres de synchronisation :

- **Nom unique** : chemin d'accès (nom unique) au nœud dans l'arborescence d'Active Directory. Si ce champ est laissé vide, l'arborescence entière d'Active Directory est synchronisée.
- **Nom(s) unique(s) exclu(s)** : vous pouvez choisir d'exclure (ignorer) des nœuds spécifiques dans l'arborescence d'Active Directory.
- **Ignorer les ordinateurs désactivés (uniquement dans Active Directory)** : vous pouvez choisir d'ignorer les ordinateurs désactivés dans Active Directory. La tâche ignore alors ces ordinateurs.

Déclencheurs

Sélectionnez un déclencheur existant pour cette tâche ou créez un déclencheur. Il est également possible de **supprimer** ou de **modifier** un déclencheur sélectionné.

Résumé

Passez en revue les informations de configuration affichées dans cette section. Si elles sont correctes, cliquez sur **Terminer**. La tâche est alors créée et prête à être utilisée.

4.5.5.2 Synchronisation des groupes statiques - Ordinateurs Linux

Un ordinateur Linux qui a rejoint un domaine Windows n'affiche aucun texte dans les propriétés d'ordinateur Utilisateurs et ordinateurs Active Directory. Ces informations doivent donc être saisies manuellement.

- Vérifiez les conditions préalables requises pour le serveur et celles-ci :

- Les ordinateurs Linux figurent dans Active Directory.
- Un serveur DNS est installé sur le contrôleur de domaine.
- **ADSI Edit** est installé.

1. Ouvrez une invite de commande, puis exécutez adsiedit.msc.
2. Accédez à **Action** > **Connexion**. La fenêtre des paramètres de connexion s'affiche.
3. Cliquez sur **Sélectionnez un contexte d'attribution de noms connu**.
4. Dans la zone de liste déroulante, sélectionnez le contexte d'attribution de noms **Par défaut**.
5. Cliquez sur **OK**. La valeur ADSI à gauche doit correspondre au nom de votre contrôleur de domaine, Contexte d’attribution de noms par défaut (votre contrôleur de domaine).
6. Cliquez sur la valeur **ADSI** et développez le sous-groupe.
7. Cliquez sur le **sous-groupe**, puis accédez au CN (nom commun) ou au OU (unité d'organisation) dans lequel sont affichés les ordinateurs Linux.
8. Cliquez sur le **nom d'hôte** de l'ordinateur Linux, puis sélectionnez **Propriétés** dans le menu contextuel. Accédez au paramètre **dNSHostName**, puis cliquez sur **Modifier**.
9. Remplacez la valeur **<non défini>** par du texte valide (*ubuntu.TEST*, par exemple).
10. Cliquez sur **OK** > **OK**. Ouvrez **Utilisateurs et ordinateurs Active Directory**, puis sélectionnez les **propriétés** de l'ordinateur Linux. Le nouveau texte doit s'afficher.

4.5.5.3 Mode de synchronisation - VMware

Il est possible de synchroniser des machines virtuelles s'exécutant sur VMware vCenter Server.

Cliquez sur **Admin** > **Tâche de serveur** > **Synchronisation des groupes statiques** > **Nouveau...**

General

Saisissez des informations de base sur la tâche, telles que le **Nom** et la **Description** (facultatif). Le **type de tâche** définit les paramètres et le comportement de la tâche. Pour que la tâche s'exécute automatiquement lorsque vous cliquez sur **Terminer**, cochez la case en regard de l'option **Exécuter immédiatement la tâche après la fin**.

Paramètres

Développez les paramètres et cliquez sur **Sélectionner** sous **Nom du groupe statique** : Par défaut, la racine des ordinateurs synchronisés sera utilisée. Vous pouvez également créer un groupe statique.

- **Objets à synchroniser** : **ordinateurs et groupes** ou **ordinateurs uniquement**.
- **Gestion des collisions de création d'ordinateur** : si la synchronisation ajoute des ordinateurs qui sont déjà membres du groupe statique, vous pouvez choisir une méthode de résolution des conflits : Ignorer (les ordinateurs synchronisés ne sont pas ajoutés) ou Déplacer (les nouveaux ordinateurs sont déplacés vers un sous-groupe).
- **Gestion des extinctions d'ordinateur** : si un ordinateur n'existe plus, vous pouvez le **supprimer** ou l'**ignorer**.
- **Gestion des extinctions de groupe** : si un groupe n'existe plus, vous pouvez le **supprimer** ou l'**ignorer**.

Il existe trois **modes de synchronisation** :

- **Réseau MS Windows :** entrez le **groupe de travail** à utiliser et l'utilisateur avec ses informations d'identification.
- **Active Directory/Open Directory/LDAP** : saisissez les informations de connexion au serveur. Reportez-vous à la section mode de synchronisation pour obtenir des instructions détaillées.
- **VMware** : saisissez les informations de connexion à VMware vCenter Server. Reportez-vous à la section mode de synchronisation pour obtenir des instructions détaillées.

Paramètres de connexion au serveur :

- **Serveur** : saisissez le nom DNS ou l'adresse IP de VMware vCenter Server.
- **Connexion** : saisissez les informations d'identification de VMware vCenter Server.
- **Mot de passe** : saisissez le mot de passe utilisé pour vous connecter à VMware vCenter Server.

Paramètres de synchronisation :

Vue Structure : sélectionnez le type de vue Structure, **Dossiers** ou **Pool de ressources**.
Chemin d'accès à la structure : cliquez sur **Parcourir** et accédez au dossier que vous souhaitez synchroniser. Si le champ n'est pas renseigné, la structure entière sera synchronisée.
Vue Ordinateur : indiquez si vous souhaitez afficher les ordinateurs par **nom**, **nom d'hôte** ou **adresse IP** après la synchronisation.

Déclencheurs

Sélectionnez un déclencheur existant pour cette tâche ou créez un déclencheur. Il est également possible de **supprimer** ou de **modifier** un déclencheur sélectionné.

Résumé

Passez en revue les informations de configuration affichées dans cette section. Si elles sont correctes, cliquez sur **Terminer**. La tâche est alors créée et prête à être utilisée.

4.5.6 Synchronisation utilisateur

Cette tâche serveur synchronise les informations des utilisateurs et des groupes d'utilisateurs à partir d'une source comme Active Directory, les paramètres LDAP, etc.

Pour exécuter cette tâche, cliquez sur **Admin** > **Tâche de serveur** > **Synchronisation utilisateur** > **Nouveau...**

Général

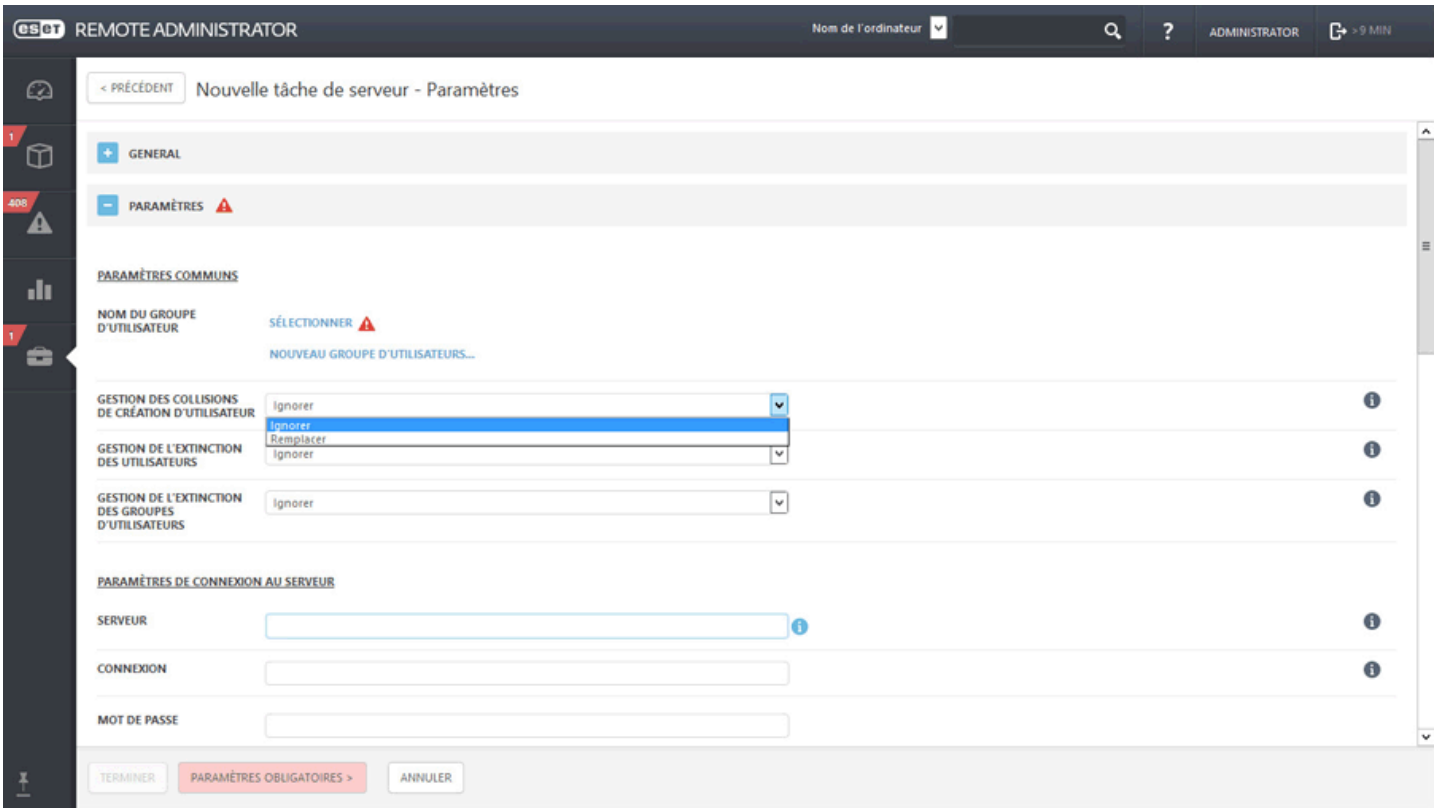
Saisissez des informations de base sur la tâche telles que le **Nom**, la **Description** (facultatif) et le **Type de tâche**. Le **type de tâche** définit les paramètres et le comportement de la tâche. Pour que la tâche s'exécute automatiquement lorsque vous cliquez sur **Terminer**, cochez la case en regard de l'option **Exécuter immédiatement la tâche après la fin**.

Paramètres

Développez les paramètres et cliquez sur **Sélectionner** sous **Nom du groupe d'utilisateurs** : par défaut, la racine des utilisateurs synchronisés est utilisée (par défaut, il s'agit du groupe **Tous**). Vous pouvez également créer un groupe d'utilisateurs.

- **Gestion des collisions de création d'utilisateur** : deux types de conflit peuvent se produire :
  1. Un même groupe contient deux utilisateurs portant le même nom.
  2. Un utilisateur existant possède le même SID (n'importe où dans le système).

  Vous pouvez définir la gestion des collisions sur les options suivantes :
  Ignorer : l'utilisateur n'est pas ajouté à ERA pendant la synchronisation avec Active Directory.
  Remplacer : l'utilisateur existant dans ERA est remplacé par celui d'Active Directory. Dans le cas d'un conflit de SID, l'utilisateur existant dans ERA est supprimé de son précédent emplacement (même si l'utilisateur figurait dans un autre groupe).
- **Gestion des extinctions d'utilisateur** : si un utilisateur n'existe plus, vous pouvez le **supprimer** ou l'**ignorer**.
- **Gestion des extinctions de groupe d'utilisateurs** : si un groupe d'utilisateurs n'existe plus, vous pouvez le **supprimer** ou l'**ignorer**.



REMARQUE : si vous utilisez des attributs personnalisés pour un utilisateur, définissez **Gestion des collisions de création d'utilisateur** sur **Ignorer**. Sinon, l'utilisateur (et tous les détails) est remplacé par les données d'Active Directory et perd les attributs personnalisés. Si vous voulez remplacer l'utilisateur, choisissez **Ignorer** pour Gestion des extinctions d'utilisateur.

Paramètres de connexion au serveur :

- **Serveur** : saisissez le nom du serveur ou l'adresse IP du contrôleur de domaine.
- **Connexion** : saisissez les informations d'identification de connexion du contrôleur de domaine sous la forme **DOMAINE\nom_utilisateur**.
- **Mot de passe** : saisissez le mot de passe utilisé pour se connecter au contrôleur de domaine.

- **Utiliser les paramètres LDAP :** si vous souhaitez utiliser le protocole LDAP, cochez la case **Utiliser le protocole LDAP au lieu d'Active Directory**, puis saisissez des attributs spécifiques qui correspondent à votre serveur. Vous pouvez également sélectionner une **valeur prédéfinie** en cliquant sur **Personnaliser...** pour que les paramètres soient renseignés automatiquement :

- **Active Directory**
- **Open Directory de Mac OS X Server (noms d'hôte d'ordinateur)**
- **Open Directory de Mac OS X Server (adresses IP d'ordinateur)**
- **OpenLDAP avec les enregistrements d'ordinateur Samba** : configuration des paramètres de nom DNS dans Active Directory.

Paramètres de synchronisation :

Nom unique : chemin d'accès (nom unique) au nœud dans l'arborescence d'Active Directory. Si ce champ est laissé vide, l'arborescence entière d'Active Directory est synchronisée.

Attributs d'utilisateur et de groupe d'utilisateurs :

Les attributs par défaut d'un utilisateur sont spécifiques à l'annuaire auquel l'utilisateur appartient.

Attributs d'utilisateur avancés :

Si vous souhaitez utiliser des attributs personnalisés avancés, sélectionnez **Ajouter**. Ce champ hérite des informations de l'utilisateur et peut être utilisé dans un éditeur de stratégie MDM iOS en tant qu'espace réservé.

Déclencheurs

Sélectionnez un déclencheur existant pour cette tâche ou créez un déclencheur. Il est également possible de **supprimer** ou de **modifier** un déclencheur sélectionné.

Résumé

Passez en revue les informations de configuration affichées dans cette section. Si elles sont correctes, cliquez sur **Terminer**. La tâche est alors créée et prête à être utilisée.

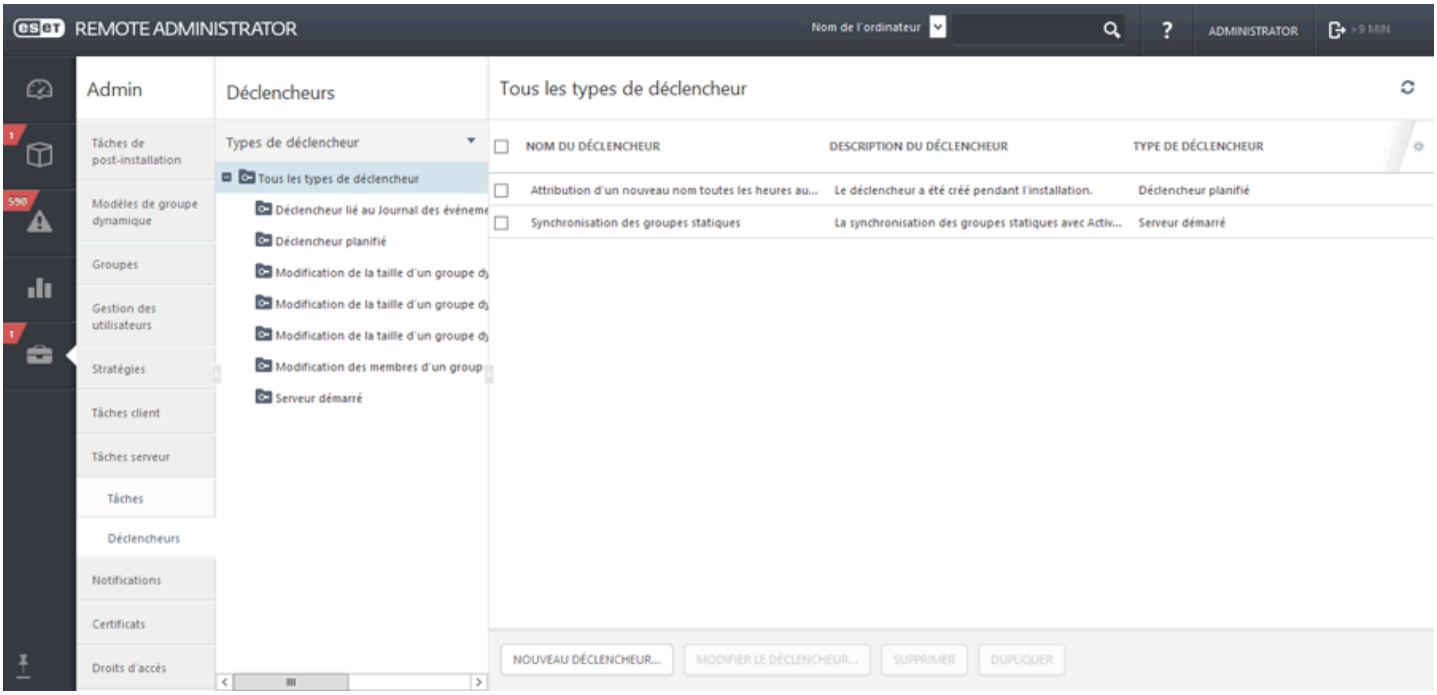
4.5.7 Déclencheurs

Les déclencheurs sont essentiellement des capteurs qui réagissent à certains événements d'une manière prédéfinie. Ils servent à exécuter une action (exécuter une tâche, dans la plupart des cas). Ils peuvent être activés par le planificateur (événements temporels) ou lorsqu'un événement système spécifique se produit.

Un déclencheur exécute toutes les tâches qui lui sont attribuées au moment de son activation. Il n'exécute pas immédiatement les tâches nouvellement attribuées. Celles-ci sont exécutées dès que le déclencheur est déclenché. La sensibilité d'un déclencheur face aux événements peut être réduite à l'aide d'une limitation.

Types de déclencheurs de serveur :

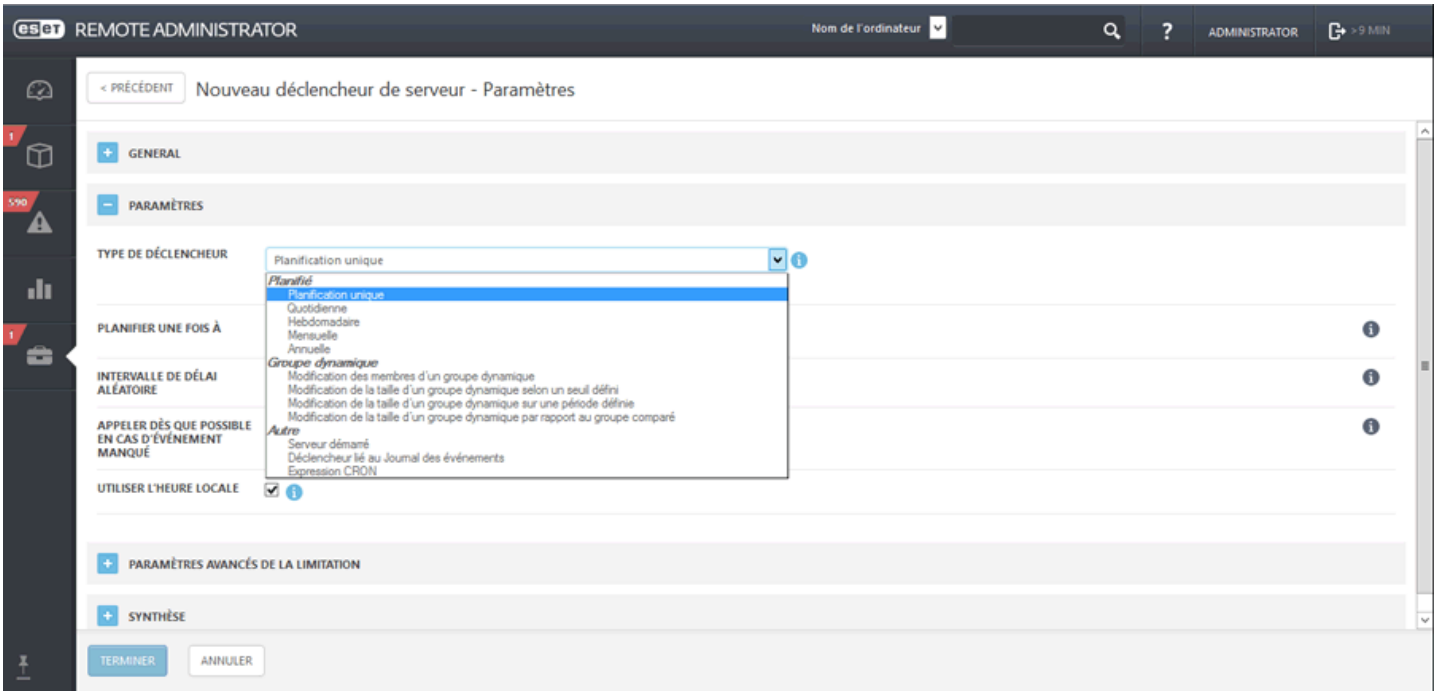
- **Membres du groupe dynamique modifiés :** ce déclencheur est appelé lorsque le contenu d'un groupe dynamique change, lorsque des clients rejoignent ou quittent un groupe dynamique appelé *Infecté*, par exemple.
- **Taille du groupe dynamique modifiée selon le groupe comparé :** ce déclencheur est appelé lorsque le nombre de clients d'un groupe dynamique observé change par rapport à un groupe de comparaison (statique ou dynamique), par exemple, si plus de 10 % de tous les ordinateurs sont infectés (groupe Tous comparé au groupe Infecté).
- **Taille du groupe dynamique modifiée selon le seuil :** ce déclencheur est appelé lorsque le nombre de clients d'un groupe dynamique devient supérieur ou inférieur au seuil spécifié, par exemple, si plus de 100 ordinateurs figurent dans le groupe Infecté.
- **Taille du groupe dynamique modifiée pendant la période :** ce déclencheur est appelé lorsque le nombre de clients d'un groupe dynamique change pendant une période définie, par exemple, si le nombre d'ordinateurs du groupe Infecté augmente de 10 % en une heure,
- **Déclencheur lié au Journal des événements :** ce déclencheur est appelé lorsqu'un événement d'un certain type se produit dans les journaux, en cas de menace dans le journal d'analyse, par exemple.
- **Déclencheur planifié :** ce déclencheur est appelé à une date et une heure spécifiques.
- **Serveur démarré :** ce déclencheur est appelé lorsque le serveur démarre. Il est par exemple utilisé pour la tâche Synchronisation des groupes statiques.



- **Dupliquer :**vous permet de créer un nouveau type de déclencheur selon le déclencheur sélectionné. Un nouveau nom est requis pour la tâche en double.

4.5.7.1 Assistant Déclencheur de serveur

Pour créer et gérer des déclencheurs, cliquez sur l'onglet **Admin** > **Tâches serveur** > **Déclencheurs**. Sélectionnez **Types de déclencheur** > **Nouveau déclencheur**.



4.5.7.2 Planification d'une tâche de serveur

Un déclencheur planifié exécute la tâche selon des paramètres de date et d'heure. La tâche peut être planifiée pour **s'exécuter une seule fois**, de manière répétée ou selon une expression CRON.

4.5.7.3 Limitation

Dans des circonstances définies, une limitation peut empêcher le déclenchement d'un déclencheur. Les conditions temporelles sont toujours prioritaires par rapport aux conditions statistiques.

Si aucune des conditions définies n'est remplie, toutes les informations d'état de tous les observateurs sont réinitialisées (l'observation recommence de 0). Cela s'applique aux conditions temporelles et statistiques. Les informations d'état des observateurs ne sont pas persistantes. Elles sont réinitialisées même si l'Agent ou le serveur est redémarré.

Toute modification apportée à un déclencheur entraîne la réinitialisation de son état.

Plusieurs méthodes permettent de contrôler le déclenchement :

Statistique

Les déclencheurs statistiques sont déclenchés en fonction de n'importe quelle combinaison des paramètres suivants :

- S1 : le déclencheur doit se déclencher toutes les **N** occurrences de l'événement de déclenchement (modulo **N**) , en commençant par le dernier événement d'une série (par exemple, depuis le départ à partir du nième événement.
- S2 : le déclencheur est déclenché si **N** événements se produisent **X fois** (le nombre de fois peut être choisi parmi un ensemble prédéfini) [**N** <= 100] dans la logique flottante ; seul le nombre d'événements au cours de la dernière X fois est pris en compte. Le déclenchement du déclencheur entraîne la réinitialisation du tampon.
- S3 : **N** événements avec un symbole **S** unique se produisent [N <= 100] dans une ligne. Le tampon est réinitialisé si le déclencheur est déclenché et si un événement se trouve déjà dans le tampon. Le tampon est en mode « fenêtre flottante » (file d'attente premier entré, premier sorti). Le nouveau symbole est comparé à chaque symbole du tampon.

  Remarque : une valeur manquante (n/d) est considérée comme non unique. Le tampon est donc réinitialisé

depuis le dernier déclenchement

Ces conditions peuvent être associées à l'opérateur ET (toutes celles définies doivent être satisfaites) ou OU (la condition qui est remplie la première).

Temporelle

Toutes les conditions suivantes doivent être simultanément satisfaites (si elles sont définies) :

- T1 : le déclencheur peut être déclenché **X périodes**. La période est une série répétée d'heures marginales (entre 13:00 et 14:00 OU 17:00 et 23:30, par exemple).
- T2 : le déclencheur peut être déclenché une fois toutes les **X fois** au maximum.

Propriétés supplémentaires

Comme indiqué ci-dessus, tous les événements n'entraînent pas le déclenchement d'un déclencheur. Les actions exécutées pour les événements non-déclencheurs peuvent être les suivantes :

- Si plusieurs événements sont ignorés, les derniers **N** événements sont regroupés en un (stockage des données des cycles supprimés) [**N** <= 100]
- Lorsque **N** == 0, seul le dernier événement est traité (**N** indique la durée de l'historique ; le dernier événement est toujours traité).
- Tous les événements non-déclencheurs sont fusionnés (fusion du dernier cycle avec **N** cycles historiques).

Exemples :

S1 : critère pour les occurrences (autoriser tous les 3ème cycles)

Heure	00	01	02	03	04	05	06	le déclencheur est modifié	07	08	09	10	11	12	13	14	15
Cycles	x	x	x	x	x	x	x		x	x		x	x		x		x
S1			1			1						1					1

S2 : critère pour les occurrences dans le délai (autoriser si 3 cycles ont lieu en 4 secondes)

Heure	00	01	02	03	04	05	06	le déclencheur est modifié	07	08	09	10	11	12	13
Cycles	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3 : critère pour des valeurs de symbole uniques (autoriser si 3 valeurs uniques se suivent)

Heure	00	01	02	03	04	05	06	le déclencheur est modifié	07	08	09	10	11	12	13
Valeur	A	B	B	C	D	G	H		J	K	s/o	L	M	N	N
S3					1									1	

S3 : critère pour des valeurs de symbole uniques (autoriser si 3 valeurs uniques existent depuis le dernier cycle)

Heure	00	01	02	03	04	05	06	07	le déclencheur est modifié	08	09	10	11	12	13	14
Valeur	A	B	B	C	D	G	H	I		J	K	s/o	L	M	N	N
S3				1			1						1			

T1 : autoriser un cycle pendant certaines périodes (autoriser tous les jours à partir de 8:10, durée de 60 secondes)

Heure	8:09:50	8:09:59	8:10:00	8:10:01	le déclencheur est modifié	8:10:59	8:11:00	8:11:01
Cycles	x	x	x	x		x	x	x

T1			1	1		1		

Ce critère n'est associé à aucun état. Par conséquent, les modifications du déclencheur n'ont aucun effet sur les résultats.

T2 : autoriser un cycle unique dans un intervalle de temps (autoriser une fois toutes les 5 secondes au maximum)

Heure	00	01	02	03	04	05	06	le déclencheur est modifié	07	08	09	10	11	12	13
Cycles	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

Combinaison S1+S2

- S1 : tous les 5ème cycles
- S2 : 3 cycles en 4 secondes

Heure	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Cycles	x	x	x	x	x		x	x	x			x		x	x		
S1															1		
S2			1				1								1		
Résultat			1				1								1		

Le résultat est énuméré en tant que : S1 (opérateur logique ou) S2

Combinaison S1+T1

- S1 : autoriser tous les 3ème cycles
- T1 : autoriser tous les jours à partir de 8:08, durée de 60 secondes

Heure :	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Cycles	x	x	x	x	x	x	x	x	x	x
S1			1			1			1	
T1					1	1	1	1	1	
Résultat						1			1	

Le résultat est énuméré en tant que : S1 (opérateur logique et) T1

Combinaison S2+T1

- S2 : 3 cycles en 10 secondes
- T1 : autoriser tous les jours à partir de 8:08, pour une durée de 60 secondes

Heure :	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Cycles	x	x	x	x	x	x	x	x	x	x
S2			1	1			1			1
T1					1	1	1	1	1	
Résultat							1			

Le résultat est énuméré en tant que : S2 (opérateur logique et) T1.
Notez que l'état de S2 est réinitialisé uniquement lorsque le résultat global est égal à 1.

Combinaison S2+T2

- S2 : 3 cycles en 10 secondes
- T2 : autoriser une fois toutes les 20 secondes au maximum

Heure :	00	01	02	03	04	05	06	07	...	16	17	18	19	20	21	22	23	24
Cycles	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
S2			1			1	1	1				1	1	1	1	1		
T2	1	1	1													1		
Résultat			1													1		

Le résultat est énuméré en tant que : S2 (opérateur logique et) T2.
Notez que l'état de S2 est réinitialisé uniquement lorsque le résultat global est égal à 1.

4.5.7.3.1 Le déclencheur est trop sensible

Utilisez les mêmes conditions de limitation que celles indiquées dans la section Le déclencheur se déclenche trop souvent de ce guide.

4.5.7.4 Gérer les déclencheurs de serveur

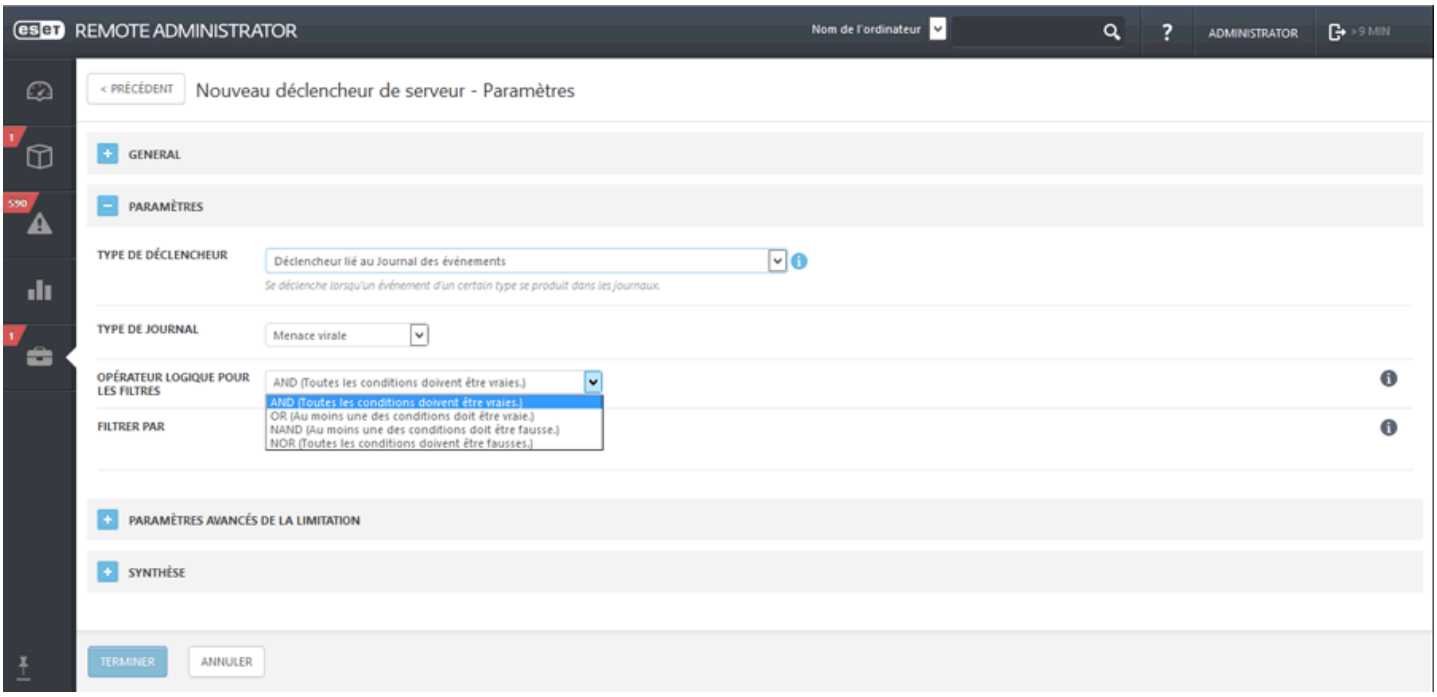
Pour gérer les déclencheurs de serveur, sous l'onglet **Admin**, cliquez sur **Tâches serveur** > **Déclencheurs**, sélectionnez **Type de déclencheur**, puis cliquez sur **Modifier**.

General

Attribuez un **nom** au déclencheur. Vous pouvez également saisir une **description** du déclencheur, si vous le souhaitez.

Paramètres

- Sélectionnez un type de déclencheur. Le type de déclencheur définit la méthode d'activation du déclencheur. Sélectionnez **Déclencheur lié au Journal des événements**, puis continuez.
- Sélectionnez un **type de journal**. Ce déclencheur est activé lorsqu'un événement d'un certain type se produit dans ce journal.
- Définissez l'événement qui doit se produire pour activer le déclencheur. Sélectionnez un **opérateur logique** pour filtrer les événements. Dans le cas présent, sélectionnez **ET (Toutes les conditions doivent être vraies.)**.
- Si nécessaire, ajoutez un **filtre** de la liste (comme un événement), puis sélectionnez l'opérateur logique de la chaîne personnalisée.

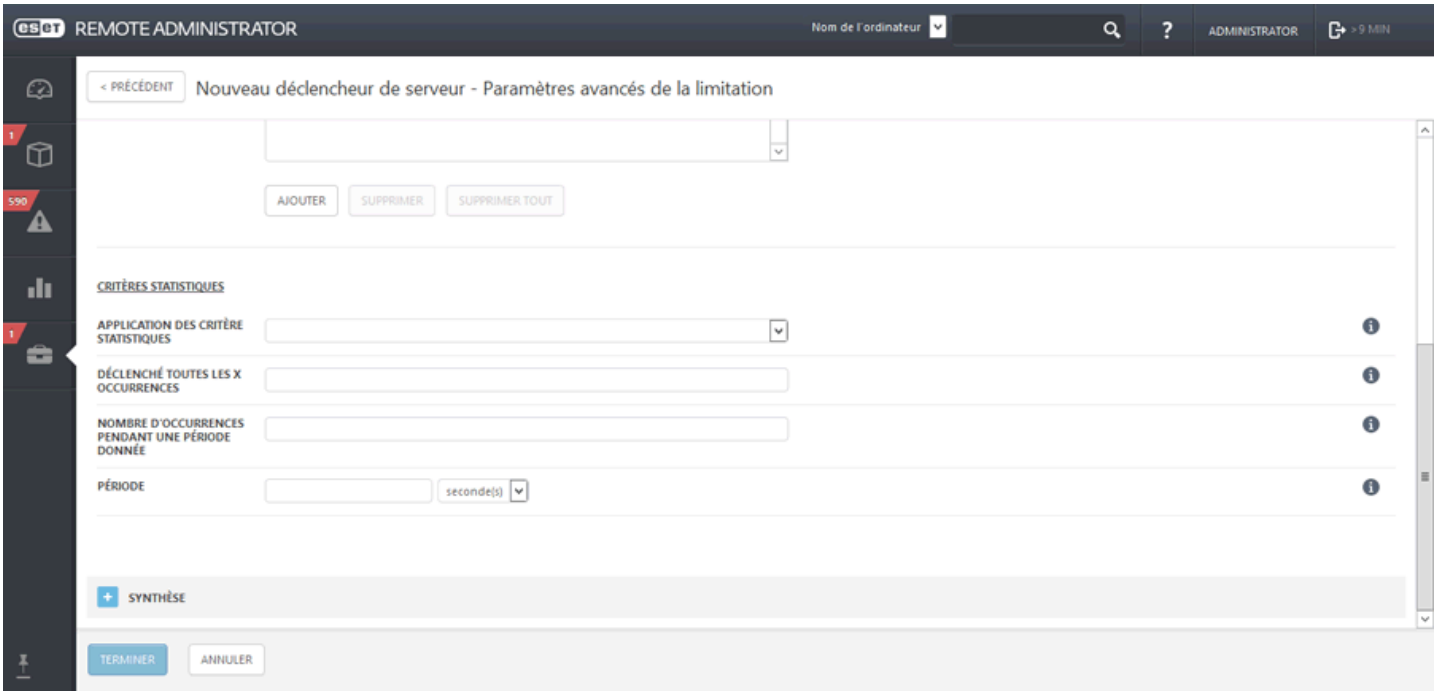


Sélectionnez un opérateur logique dans le menu **Opération**.

- **ET** : toutes les conditions doivent être vraies.
- **OU** : au moins une des conditions doit être vraie.
- **NON ET** : au moins une des conditions doit être fausse.
- **NI** : toutes les conditions doivent être fausses.

Paramètres avancés de la limitation

Indiquez une valeur dans **Nombre de cycles à agréger**. Cette valeur définit le nombre de cycles (accès au déclencheur) nécessaires pour activer le déclencheur. Pour plus d'informations spécifiques, reportez-vous au chapitre Limitation.



Résumé

Passez en revue les paramètres du nouveau déclencheur, effectuez des ajustements, puis cliquez sur **Terminer**. Le déclencheur est enregistré sur le serveur et prêt à être utilisé. Vous pouvez également consulter les déclencheurs que vous avez créés dans la liste de droite. Pour modifier ou supprimer le déclencheur, cliquez sur celui-ci dans la liste, puis sélectionnez l'action adéquate dans le menu contextuel. Pour supprimer simultanément plusieurs déclencheurs, cochez les cases en regard des déclencheurs à supprimer, puis cliquez sur **Supprimer**.

4.5.7.4.1 Gérer la sensibilité des déclencheurs

Une limitation sert à limiter l'exécution d'une tâche si cette dernière est déclenchée par un événement qui se produit fréquemment. Dans certains cas, une limitation peut empêcher le déclenchement d'un déclencheur. Si aucune des conditions définies n'est remplie, les informations empilées sont réinitialisées pour tous les observateurs (le décompte redémarre de 0). Ces informations sont également réinitialisées si l'Agent ou ERA Server sont redémarrés. Toutes les modifications apportées à un déclencheur réinitialisent son état.

Les conditions de limitation temporelles sont toujours prioritaires par rapport aux conditions statistiques. Il est recommandé d'utiliser une seule condition statistique et plusieurs conditions temporelles. Plusieurs conditions statistiques peuvent représenter une complication inutile et modifier les résultats des déclencheurs.

- **Conditions statistiques**

Les conditions statistiques peuvent être associées à l'opérateur logique **ET** (toutes les conditions doivent être remplies) ou **OU** (la première condition remplie déclenche l'action).

- **Conditions temporelles**

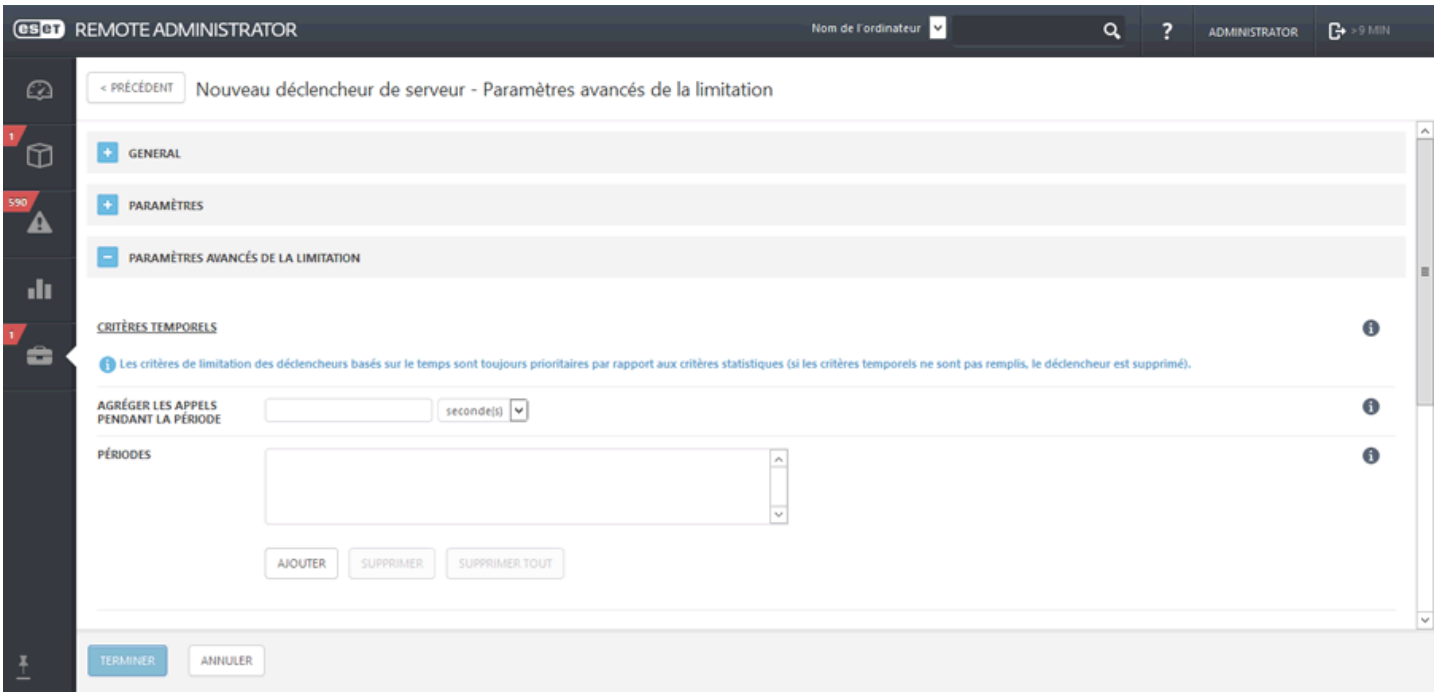
Toutes les conditions configurées doivent être remplies pour déclencher un événement. Les critères de limitation sont axés sur l'heure/la date auxquelles l'événement a eu lieu.

Agrégation

- **Nombre de cycles à agréger** : nombre de cycles (fréquence d'accès au déclencheur) nécessaires pour activer le déclencheur. L'activation du déclencheur est empêchée jusqu'à ce que ce nombre soit atteint. Lorsque cette option est définie par exemple sur 100 et que 100 menaces sont détectées, vous ne recevez pas 100 notifications mais une seule contenant les 100 menaces. Si 200 menaces sont détectées, seules les 100 dernières figurent dans la notification.

Critères temporels

- **Agréger les appels pendant la période** : vous pouvez autoriser un accès toutes les X secondes. Si vous définissez cette option sur 10 secondes et si 10 appels ont lieu pendant cette période, un seul appel est comptabilisé.
- **Périodes** : permet d'autoriser uniquement les cycles pendant la période définie. Vous pouvez ajouter plusieurs périodes à la liste. Elles seront triées par ordre chronologique.



Critères statistiques

- **Application des critères statistiques** : cette option définit la méthode selon laquelle sont évalués les critères statistiques. Tous les critères doivent être satisfaits (**ET**) ou au moins l'un d'entre eux (**OU**).
- **Déclenché toutes les X occurrences** : permet d'autoriser uniquement chaque **X** cycle (accès). Si vous saisissez par exemple la valeur 10, seul chaque 10ème cycle est comptabilisé.
- **Nombre d'occurrences pendant une période donnée** : permet d'autoriser uniquement le ou les cycles pendant la période définie, ce qui définit la fréquence. Vous pouvez par exemple autoriser l'exécution de la tâche si l'événement est détecté 10 fois pendant une heure.
  - **Période** : permet de définir la période pour l'option décrite ci-dessus.
- **Nombre d'événements avec un symbole** : enregistre un cycle (accès) lorsque **X** événements avec un symbole spécifique ont lieu. Si vous saisissez par exemple la valeur 10, un cycle est comptabilisé toutes les 10 installations d'une application donnée.
  - **S'applique lorsque le nombre d'événements** : saisissez un nombre d'événements consécutifs après le dernier cycle pour comptabiliser un autre cycle. Si vous saisissez par exemple la valeur 10, un cycle est comptabilisé après 10 événements depuis le dernier cycle.
- **S'applique lorsque le nombre d'événements** : le déclencheur est appliqué lorsque les cycles ont la valeur **Reçues dans une ligne** (l'exécution du déclencheur n'est pas prise en compte) ou **Reçues depuis la dernière exécution du déclencheur** (lorsque le déclencheur est exécuté, le nombre est réinitialisé sur 0).

4.5.7.4.2 Le déclencheur se déclenche trop souvent

Si vous souhaitez être averti moins souvent, tenez compte des suggestions suivantes :

- Si l'utilisateur souhaite réagir lorsque les événements sont plus nombreux (et pas en cas d'un seul événement), reportez-vous à la condition statistique S1 dans Limitation.
- Si le déclencheur doit se déclencher uniquement lorsqu'un groupe d'événements se produisent, reportez-vous à la condition statistique S2 dans Limitation.
- Lorsque des événements avec des valeurs non souhaitées sont supposés être ignorés, reportez-vous à la condition statistique S3 dans Limitation.
- Lorsque des événements hors des heures pertinentes (les heures de travail, par exemple) doivent être ignorés, reportez-vous à la condition temporelle T1 dans Limitation.
- Pour définir une durée minimale entre deux déclenchements de déclencheur, utilisez la condition temporelle T2 de la section Limitation.

REMARQUE : les conditions peuvent être également associées pour créer des scénarios de limitation plus complexes.

4.5.7.4.3 Expression CRON

Une expression CRON sert à configurer des instances spécifiques d'un déclencheur. Il s'agit d'une chaîne composée de 7 sous-expressions (champs) qui représentent les valeurs distinctes de la planification. Ces champs sont séparés par un espace. Ils contiennent les valeurs autorisées dans des combinaisons variées.

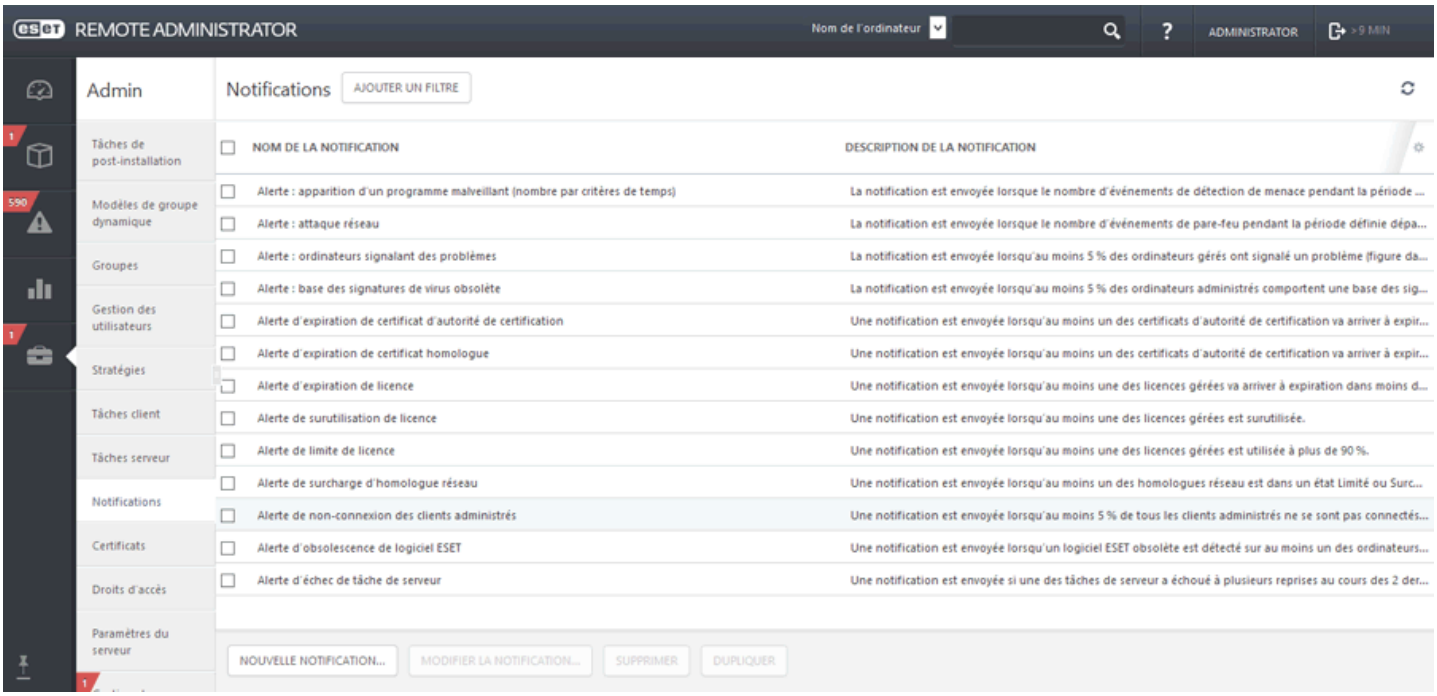
Nom	Obligatoire	Valeur	Caractères spéciaux autorisés
Secondes	Oui	0-59	,-*/
Minutes	Oui	0-59	,-*/
Heures	Oui	0-23	,-*/
Jour du mois	Oui	1-31	,-*/ L W C
Mois	Oui	0 à 11 ou JAN-DEC	,-*/
Jour de la semaine	Oui	1 à 7 ou LUN-SAM	,-*/ L C #
Année	Non	Vide ou 1970 à 2099	,-*/

Vous trouverez des exemples ici.

4.6 Notifications

Les **notifications** sont essentielles pour effectuer le suivi de l'état global de votre réseau. Lorsqu'un nouvel événement se produit (selon votre configuration), vous êtes averti à l'aide d'une méthode définie (interception SNMP ou message électronique) afin que vous puissiez réagir en conséquence.

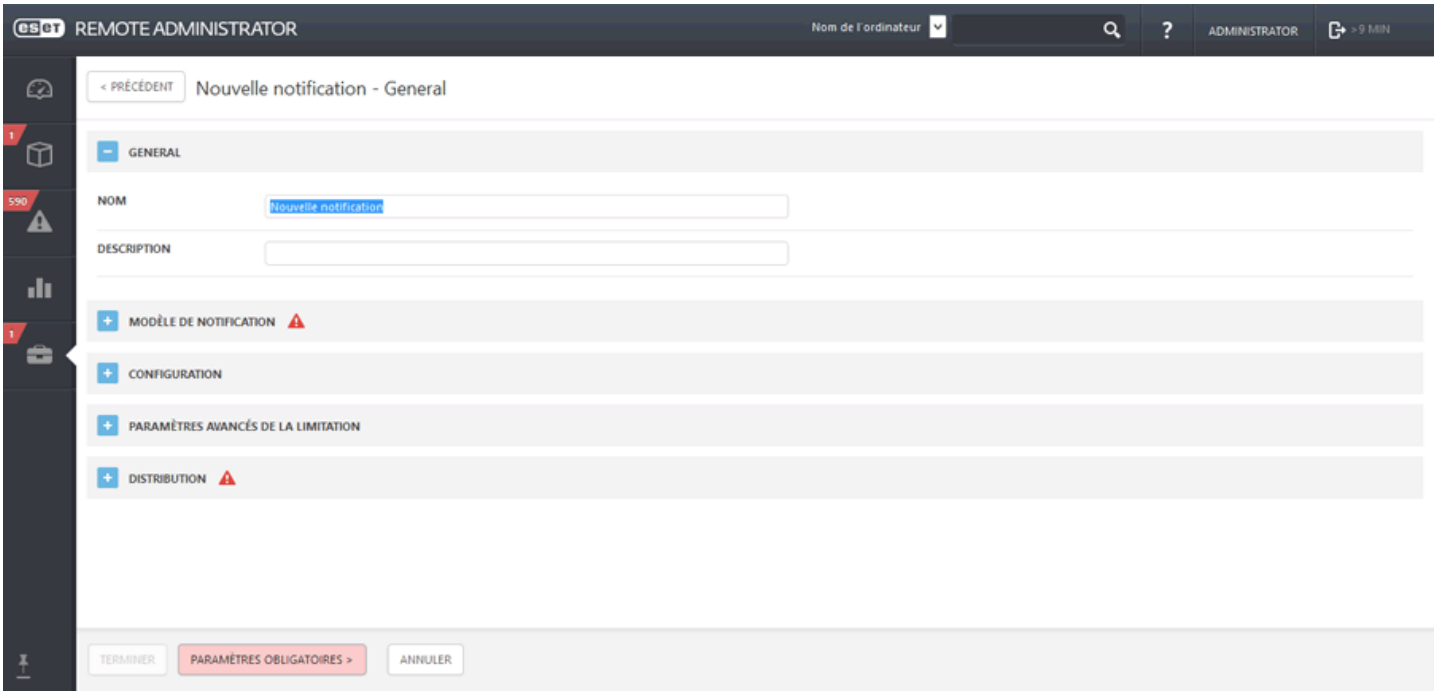
- Tous les modèles de notification sont affichés dans la liste et peuvent être filtrés par **Nom** ou par **Description**.
- Cliquez sur **Ajouter un filtre** pour ajouter des critères de filtrage et/ou saisir une chaîne dans le champ **Nom/ Notification**.
- Si vous sélectionnez une notification existante, vous avez la possibilité de la **modifier** ou de la **supprimer** entièrement.
- Pour créer une notification, cliquez sur Nouvelle notification dans la partie inférieure de la page.
- **Dupliquer :**vous permet de créer une nouvelle notification selon la notification sélectionnée. Un nouveau nom est requis pour la tâche en double.



4.6.1 Assistant de notifications

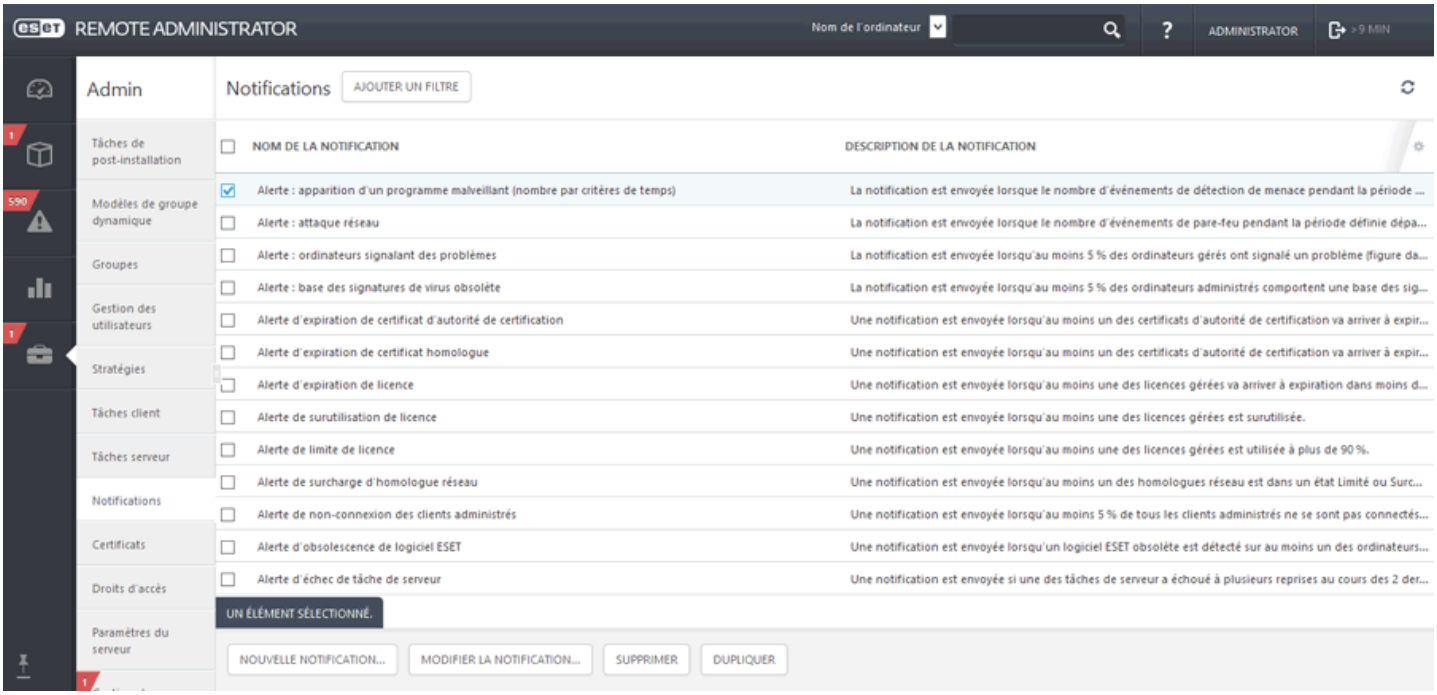
General

Contient le **nom** et la **description** de la notification. Ces informations sont importantes pour filtrer plusieurs notifications. Le filtre se trouve dans la partie supérieure de la page **Notification**.



4.6.2 Gérer les notifications

Les notifications sont gérées sous l'onglet **Admin**. Sélectionnez une notification, puis cliquez sur **Modifier la notification** ou **Dupliquer**.



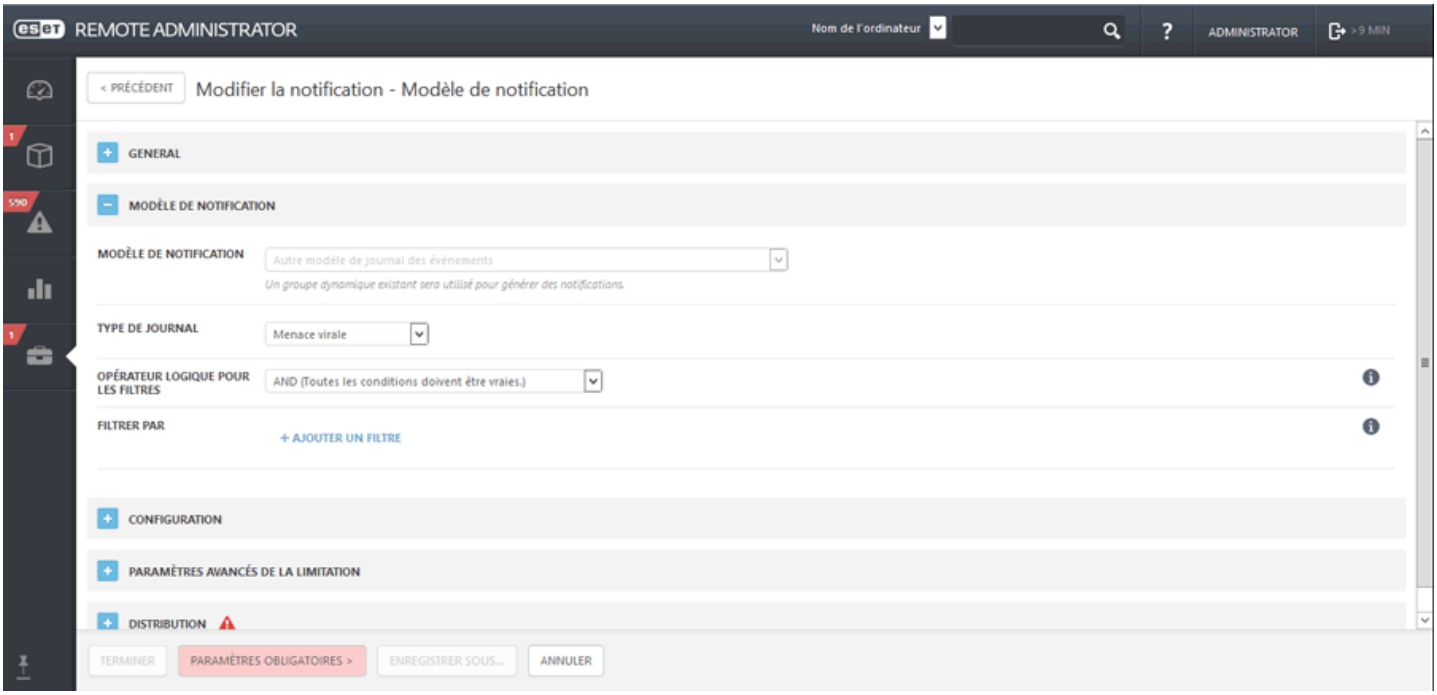
General

Vous pouvez modifier le **nom** et la **description d'une notification** pour filtrer plus aisément les différentes notifications.

Modèle de notification

Groupe dynamique existant : un groupe dynamique existant sera utilisé pour générer des notifications. Sélectionnez un groupe dynamique dans la liste, puis cliquez sur **OK**.
Modification de la taille d'un groupe dynamique par rapport au groupe comparé : si le nombre de clients d'un groupe dynamique observé change par rapport à un groupe de comparaison (statique ou dynamique), la notification est appelée.
Autre modèle de journal des événements
Cette option est utilisée pour les notifications qui ne sont pas associées à un groupe dynamique, mais basées sur les événements système exclus du journal des événements. Sélectionnez un **type de journal** sur lequel sera basée la notification et un **opérateur logique** pour les filtres.
État suivi : cette option vous avertit en cas de modifications de l'état de l'objet en fonction de vos filtres définis par l'utilisateur.

REMARQUE : vous pouvez modifier l'état suivi et **+ ajouter un filtre** ou un **opérateur logique** pour les filtres.



Configuration

Envoyer une notification à chaque modification du contenu des groupes dynamiques : activez cette option pour être averti lorsque des membres sont ajoutés, supprimés ou modifiés dans un groupe dynamique.
Période de notification : définissez la durée (en minutes, heures ou jours) de la comparaison au nouvel état. Par exemple, il y a 7 jours, le nombre de clients avec des produits de sécurité obsolètes était de 10 et le **seuil** (voir ci-dessous) était défini à 20. Si le nombre de clients avec des produits de sécurité obsolètes atteint 30, vous êtes averti.
Seuil : définissez un seuil qui déclenchera l'envoi d'une notification. Vous pouvez définir un nombre ou un pourcentage de clients (membres du groupe dynamique).
Message généré : il s'agit d'un message prédéfini qui apparaît dans la notification. Il contient des paramètres configurés sous la forme de texte.
Message : en plus du message prédéfini, vous pouvez ajouter un message personnalisé (il apparaît à la suite du message prédéfini ci-dessus). Cette option est facultative. Elle est toutefois recommandée pour optimiser le filtrage des notifications et la vue d'ensemble.

REMARQUE : les options disponibles dépendent du modèle de notification sélectionné.

Paramètres avancés de la limitation

Critères temporels

- Indiquez une valeur dans **Nombre de cycles à agréger**. Cette valeur définit le nombre de cycles (accès au déclencheur) nécessaires pour activer le déclencheur. Pour plus d'informations spécifiques, reportez-vous au chapitre Limitation.

Critères statistiques

- **Application des critères statistiques** : cette option définit la méthode selon laquelle sont évalués les critères statistiques. Tous les critères doivent être satisfaits (**ET**) ou au moins l'un d'entre eux (**OU**).
- **Déclenché toutes les X occurrences** : permet d'autoriser uniquement chaque **X** cycle (accès). Si vous saisissez par exemple la valeur 10, seul chaque 10ème cycle est comptabilisé.
- **Nombre d'occurrences pendant une période donnée** : permet d'autoriser uniquement le ou les cycles pendant la période définie, Vous pouvez par exemple autoriser l'exécution de la tâche si l'événement est détecté 10 fois pendant une heure. **Période** : permet de définir la période pour l'option décrite ci-dessus.
- **Nombre d'événements avec un symbole** : permet d'autoriser un cycle (accès) lorsque **X** événements avec un symbole spécifique ont lieu. Si vous saisissez par exemple la valeur 10, un cycle est comptabilisé toutes les 10 installations d'un logiciel donné. **S'applique lorsque le nombre d'événements** : saisissez un nombre d'événements consécutifs après le dernier cycle pour comptabiliser un autre cycle. Si vous saisissez par exemple la valeur 10, un cycle sera comptabilisé après 10 événements depuis le dernier cycle.
- **S'applique lorsque le nombre d'événements** : le déclencheur est appliqué lorsque les cycles ont la valeur **Reçues successivement** (l'exécution du déclencheur n'est pas prise en compte) ou **Reçues depuis la dernière exécution du déclencheur** (lorsque le déclencheur est exécuté, le nombre est réinitialisé sur 0).

Distribution

Objet : l'objet du message de notification. Cette option est facultative. Elle est toutefois recommandée pour optimiser le filtrage ou lors de la création de règles pour le tri des messages.

Distribution

- **Envoyer l'interruption SNMP** : envoie une interception SNMP. Elle avertit le serveur à l'aide d'un message SNMP non sollicité. Pour plus d'informations, reportez-vous à Comment configurer un service d'interruption SNMP.
- **Envoyer un message électronique** : envoie un message électronique selon les paramètres de votre messagerie.
- **Envoyer syslog** - Vous pouvez utiliser ERA pour envoyer les notifications et les messages d'événement à votre serveur Syslog. Il est également possible d'exporter les journaux à partir du produit de sécurité ESET d'un client et de les envoyer au serveur Syslog.

Adresses électroniques : saisissez les adresses électroniques des destinataires des messages de notification, en les séparant par une virgule (« , »).

Gravité Syslog : choisissez un niveau de gravité dans la liste déroulante. Les notifications apparaîtront alors avec cette sévérité sur le serveur Syslog.

Cliquez sur **Enregistrer sous** pour créer un nouveau modèle selon le modèle que vous êtes en train de modifier. Vous serez invité à donner un nom au nouveau modèle.

4.6.3 Comment configurer un service d'interruption SNMP

Pour recevoir des messages SNMP, le service d'interruption SNMP doit être configuré. Étapes de configuration selon le système d'exploitation :

WINDOWS

Conditions préalables requises

- Le service **SNMP (Simple Network Management Protocol)** doit être installé sur l'ordinateur sur lequel est installé ERA Server et sur celui sur lequel sera installé le logiciel d'interruption SNMP.
- Les deux ordinateurs (ci-dessus) doivent se trouver dans le même sous-réseau.
- Le service SNMP doit être configuré sur l'ordinateur ERA Server.

Configuration du service SNMP (ERA Server)

- Appuyez sur la touche Windows + R pour ouvrir la boîte de dialogue Exécuter, saisissez *Services.msc* dans le champ **Ouvrir**, puis appuyez sur **Entrée**. Recherchez le service SNMP.
- Cliquez sur l'onglet **Interruptions**, saisissez **public** dans le champ **Nom de la communauté**, puis cliquez sur **Ajouter à la liste**.
- Cliquez sur **Ajouter**, saisissez le **nom d'hôte, l'adresse IP** ou **l'adresse IPX** de l'ordinateur sur lequel le logiciel d'interception SNMP est installé dans le champ correspondant, puis cliquez sur **Ajouter**.
- Cliquez sur l'onglet **Sécurité**. Cliquez sur **Ajouter** pour afficher la fenêtre **Configuration du service SNMP**. Saisissez **public** dans le champ **Nom de la communauté**, puis cliquez sur **Ajouter**. Les droits sont définis sur **LECTURE SEULE**, ce qui est acceptable.
- Vérifiez que l'option **Accepter les paquets SNMP provenant de ces hôtes** est sélectionnée, puis cliquez sur **OK**. Le service SNMP est configuré.

Configuration du logiciel d'interception SNMP (client)

- Le service SNMP est installé et il n'est pas nécessaire de le configurer.
- Installez **AdRem SNMP Manager** ou **AdRem NetCrunch**.
- **AdRem SNMP Manager** : démarrez l'application, puis sélectionnez **Create New SNMP Node List (Créer une liste de nœuds SNMP)**. Cliquez sur **Yes (Oui)** pour confirmer.
- Recherchez l'adresse réseau de votre sous-réseau (affiché dans cette fenêtre). Cliquez sur **OK** pour effectuer une recherche sur le réseau.
- Patientez jusqu'à la fin de la recherche. Les résultats de la recherche sont affichés dans la fenêtre **Discovery results (Résultats de la détection)**. L'adresse IP d'ERA Server doit être affichée dans cette liste.
- Sélectionnez l'adresse IP du serveur, puis cliquez sur **OK**. L'adresse du serveur est affichée dans la section **Nodes (Nœuds)**.
- Cliquez sur **Trap Receiver Stopped (Récepteur d'interruption arrêté)**, puis sélectionnez **Start (Démarrer)**. **Trap Receiver Started (Récepteur d'interruption démarré)** s'affiche. Vous pouvez désormais recevoir des messages SNMP d'ERA Server.

LINUX

1. Installez le package snmpd en exécutant l'une des commandes suivantes :
   `apt-get install snmpd snmp` (distributions Debian, Ubuntu)
   `yum install net-snmp` (distributions Red-Hat, Fedora)
2. Ouvrez le fichier */etc/default/snmpd*, puis apportez les modifications d'attribut suivantes :

   ```
   #SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
   ```
   L'ajout d'un # désactive complètement cette ligne.

   ```
   SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'
   ```
   Ajoutez cette ligne au fichier.

   ```
   TRAPDRUN=yes
   ```
   Changez l'attribut *trapdrun* en *yes*.
3. Créez une copie de sauvegarde du fichier *snmpd.conf* d'origine. Ce fichier sera modifié ultérieurement.

   ```
   mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
   ```
4. Créez un fichier *snmpd.conf* et ajoutez les lignes suivantes :

   ```
   rocommunity public
   syslocation "Testing ERA6"
   syscontact admin@ERA6.com
   ```
5. Ouvrez le fichier */etc/snmp/snmptrapd.conf*, puis ajoutez la ligne suivante à la fin du fichier :

   ```
   authCommunity log,execute,net public
   ```
6. Saisissez la commande suivante pour démarrer les services de gestionnaire SNMP et consigner les interceptions entrantes :

```
/etc/init.d/snmpd restart
```
ou
```
service snmpd restart
```

7. Pour vérifier que l'intercepteur fonctionne et qu'il intercepte les messages, exécutez la commande suivantes :

```
tail -f /var/log/syslog | grep -i TRAP
```

4.7 Certificats

Les certificats sont importants dans ESET Remote Administrator. Ils sont nécessaires pour que les composants ERA puissent communiquer avec ERA Server. Pour s'assurer que tous les composants communiquent correctement, tous les certificats homologues doivent être valides et signés par la même autorité de certification.

Vous pouvez créer une autorité de certification et des certificats homologues dans ERA Web Console. Suivez les instructions en vue de :

- Créer une nouvelle autorité de certification
  - Importer une clé publique
  - Exporter une clé publique
  - Exporter une clé publique au format BASE64

- Créer un nouveau certificat homologue
  - Créer un certificat
  - Exporter un certificat
  - Créer un certificat APN
  - Révoquer un certificat
  - Utilisation du certificat
  - Définir un nouveau certificat ERA Server

4.7.1 Certificats homologues

Si une autorité de certification se trouve sur votre système, vous devez créer un certificat homologue pour les différents composants ESET Remote Administrator. Chaque composant (ERA Agent, ERA Proxy et ERA Server) nécessite un certificat spécifique.

+ Nouveau...
Cette option permet de créer un nouveau certificat. Ces certificats sont utilisés par ERA Agent, ERA Proxy et ERA Server.

+ Certificat APN
Cette option permet de créer un certificat APN. Ce certificat est utilisé par MDM.

Utilisation du certificat
Vous pouvez également vérifier quels clients utilisent ce certificat ERA.

Modifier...
Sélectionnez cette option pour modifier un certificat existant de la liste. Les options sont identiques à celles qui s'appliquent lors de la création d'un certificat.

Exporter...
Cette option permet d'exporter un certificat sous la forme d'un fichier. Ce fichier est nécessaire si vous installez ERA Agent localement sur un ordinateur ou lors de l'installation de MDM.

Exporter en Base64...
Cette option permet d'exporter un certificat sous la forme d'un fichier `.txt`.

Révoquer...
Si vous ne souhaitez plus utiliser un certificat, sélectionnez Révoquer. Cette option rend le certificat non valide. Les certificats non valides ne sont pas acceptés par ESET Remote Administrator.

IMPORTANT : la révocation est irréversible ; vous ne pourrez plus utiliser un certificat qui a été révoqué. Vérifiez qu'il ne reste pas d'Agents ERA utilisant ce certificat avant de le révoquer. Vous éviterez ainsi la perte de la connexion aux ordinateurs client ou aux serveurs (ERA Server, ERA Proxy, Connecteur de périphérique mobile, Hôte de l'agent virtuel).

Afficher les certificats révoqués : vous montre tous les certificats révoqués.

Certificat d'agent pour l'installation assistée du serveur : ce certificat est généré pendant l'installation du serveur, pour autant que vous ayez sélectionnez l'option **Générer les certificats**.

4.7.1.1 Créer un nouveau certificat

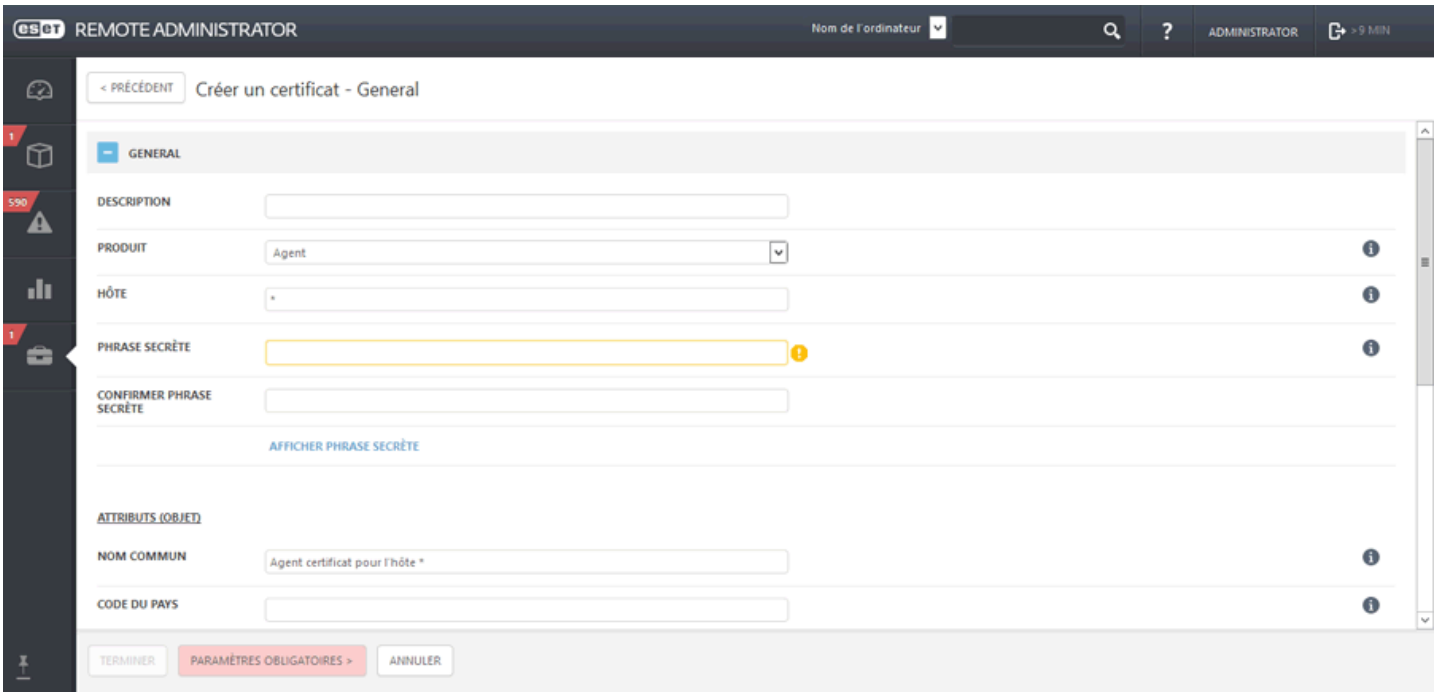
Dans le cadre du processus d'installation, ESET Remote Administrator requiert la création d'un certificat homologue pour les Agents. Ces certificats servent à authentifier les produits distribués sous votre licence.

REMARQUE : Il existe une exception, le **certificat d'agent pour l'installation assistée du serveur** ne peut pas être créé manuellement. Ce certificat est généré pendant l'installation du serveur, pour autant que vous ayez sélectionné l'option **Générer les certificats**.

Pour créer un certificat dans **ERA Web Console**, accédez à **Admin** > **Certificats**, puis cliquez sur **Actions** > **Nouveau**.

General

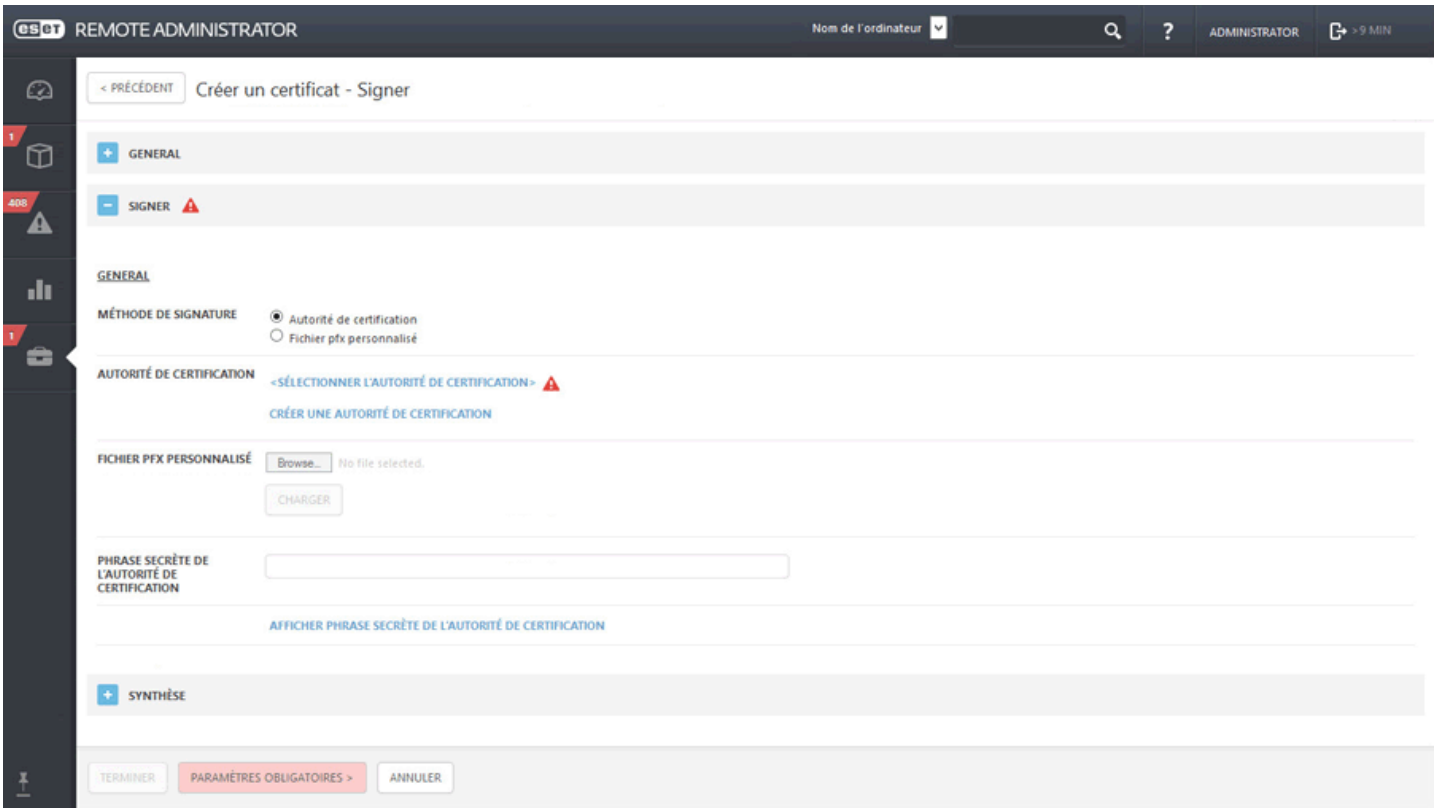
- Entrez une **description** du certificat.
- **Produit** : sélectionnez dans le menu déroulant le type de certificat que vous souhaitez créer.
- **Nom d'hôte** : conservez la valeur par **défaut (astérisque) dans le** champ **Hôte afin** de permettre la distribution de ce certificat sans l'associer à un nom DNS ou une adresse IP spécifique.
- **Phrase secrète** : il est recommandé de laisser ce champ vide, mais vous pouvez définir une phrase secrète pour le certificat qui sera nécessaire lors d'une tentative d'activation par les clients.
- **Attributs** : ces champs ne sont pas obligatoires, mais vous pouvez les utiliser afin d'y faire figurer des informations détaillées sur le certificat.
- **Nom commun** : cette valeur doit contenir la chaîne « Agent », « Proxy » ou « Serveur » selon le **produit** sélectionné.
- Si vous le souhaitez, vous pouvez saisir des informations descriptives sur le certificat.
- Saisissez des valeurs dans les champs **Valide du** et **Valide jusqu'au** pour garantir la validité du certificat.



Signer

- La méthode de signature doit être **Autorité de certification**.
- Sélectionnez l'**autorité de certification ERA** créée lors de l'installation initiale.
- Ignorez l'option de fichier `.pfx` personnalisé. Cette option s'applique uniquement aux autorités de certification `pfx` automatiquement signées.

- La méthode de signature doit être **Fichier pfx personnalisé**.
- Cliquez sur Parcourir pour sélectionner un fichier `pfx` personnalisé. Accédez à votre fichier `pfx` personnalisé et cliquez sur **OK**. Cliquez sur **Charger** pour charger ce certificat sur le serveur.



Résumé

- Passez en revue les informations de certificat saisies, puis cliquez sur **Terminer**. Le certificat est créé. Il est désormais disponible dans la liste **Certificats** en vue de son utilisation lors de l'installation de l'Agent.

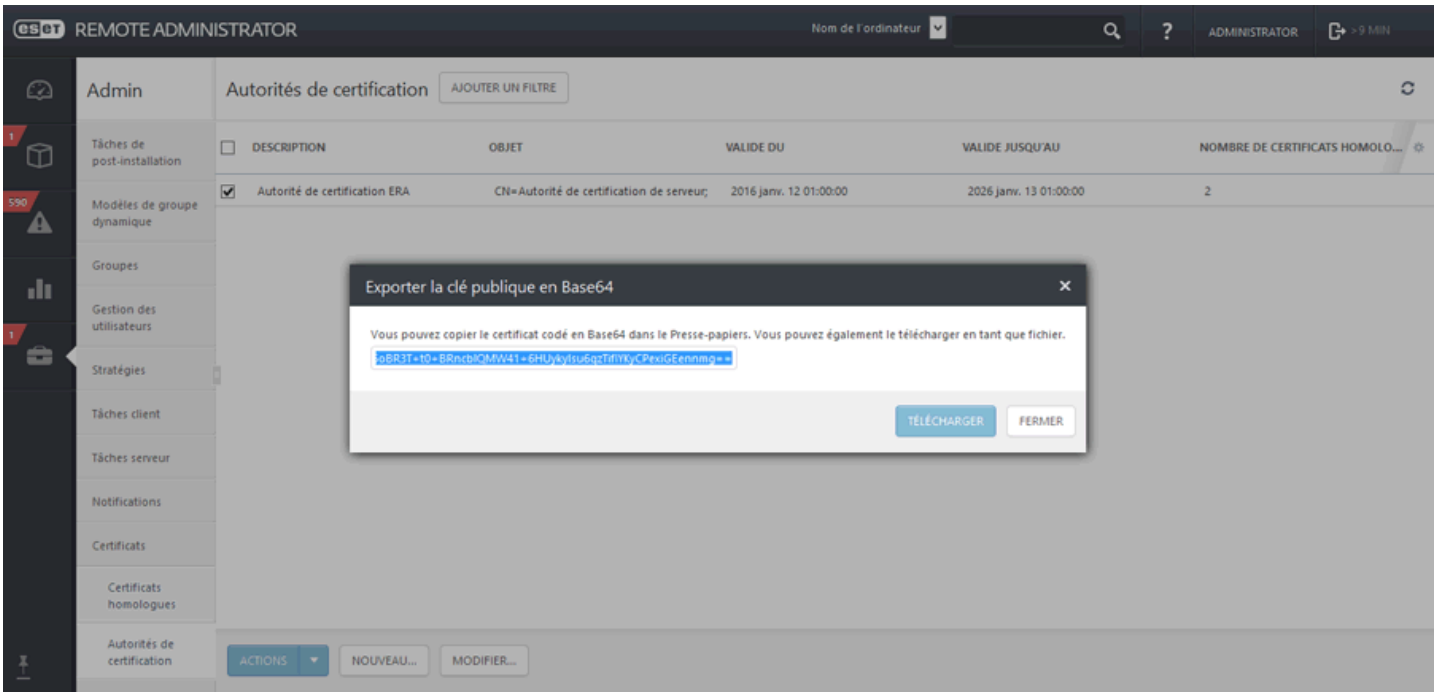
4.7.1.2 Exporter un certificat homologue

Exporter un Certificats homologues

1. Dans la liste, sélectionnez le **certificat homologue** que vous souhaitez utiliser, puis cochez la case en regard de celui-ci.
2. Dans le menu contextuel, sélectionnez **Exporter**. Le certificat (y compris la clé privée) est exporté sous forme de fichier *.pfx*. Saisissez un nom pour votre clé publique, puis cliquez sur **Enregistrer**.

Exporter en Base64 à partir des certificats homologues :

Les certificats pour les composants ERA sont disponibles dans la console Web. Pour copier le contenu d'un certificat au format Base64, cliquez sur **Admin** > **Certificats homologues**, sélectionnez un certificat puis sélectionnez Exporter en Base64. Vous pouvez également télécharger le certificat codé au format Base64 en tant que fichier. Répétez cette étape pour les certificats des autres composants ainsi que pour votre autorité de certification.



REMARQUE : si vous utilisez des certificats qui ne sont pas au format **Base64**, il faudra les convertir en **Base64** (ou les exporter selon la procédure ci-dessus). C'est le seul format accepté par les composants ERA pour se connecter au serveur ERA. Pour plus d'informations sur la conversion des certificats, voir http://linux.die.net/man/1/base64 et https://developer.apple.com/library/mac/documentation/Darwin/Reference/ManPages/man1/base64.1.html. Par exemple :

```
'cat ca.der | base64 > ca.base64.txt' a 'cat agent.pfx | base64 > agent.base64.txt'
```

4.7.1.3 Certificat APN

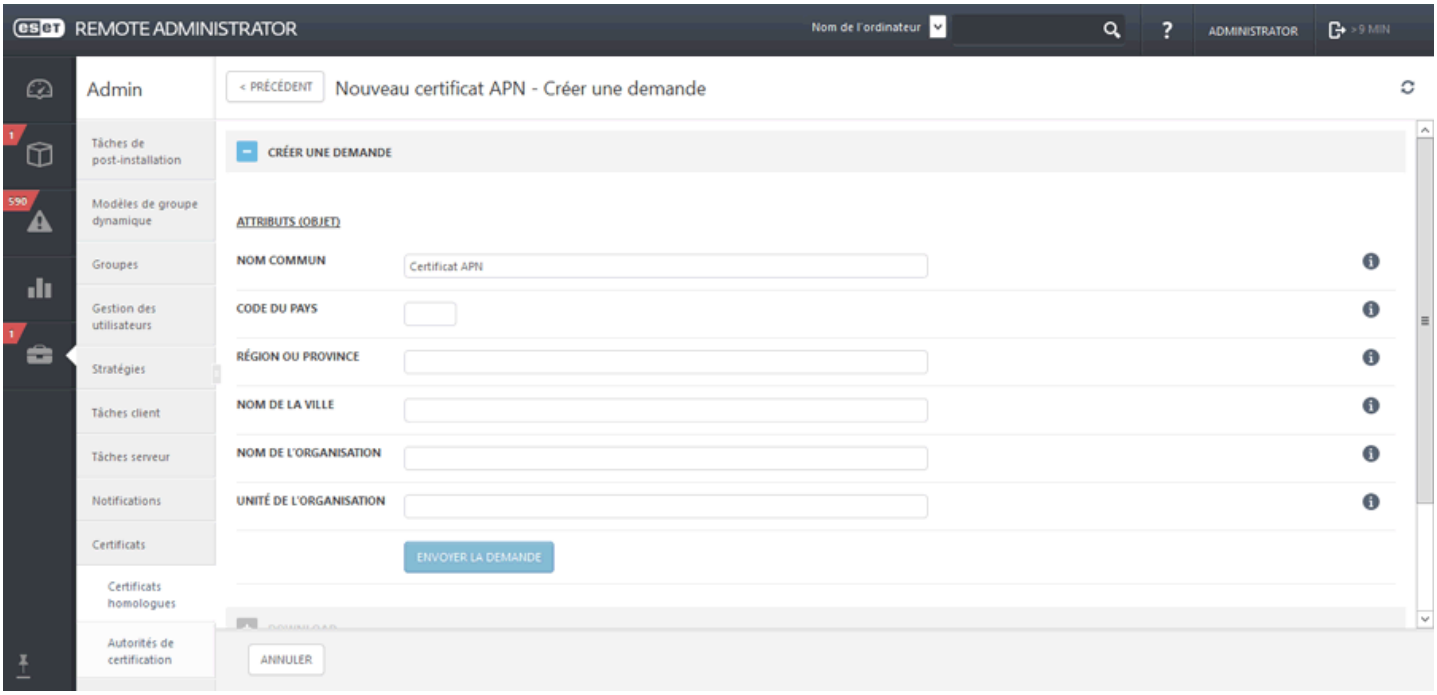
Un certificat APN (Apple Push Notification) est utilisé par l'inscription de périphérique ERA MDM pour iOS. Vous devez d'abord créer un **certificat Push fourni par Apple** et le faire signer par Apple pour pouvoir inscrire des périphériques iOS sur ERA. Vous devez également vous assurer que la licence d'ERA est valide.

Cliquez sur l'onglet **Admin** > **Certificats** > **Certificats homologues**, sur **Nouveau** , puis sélectionnez **Certificat APN**.

REMARQUE : Vous aurez besoin d'un identifiant Apple pour obtenir le certificat APN signé par Apple.

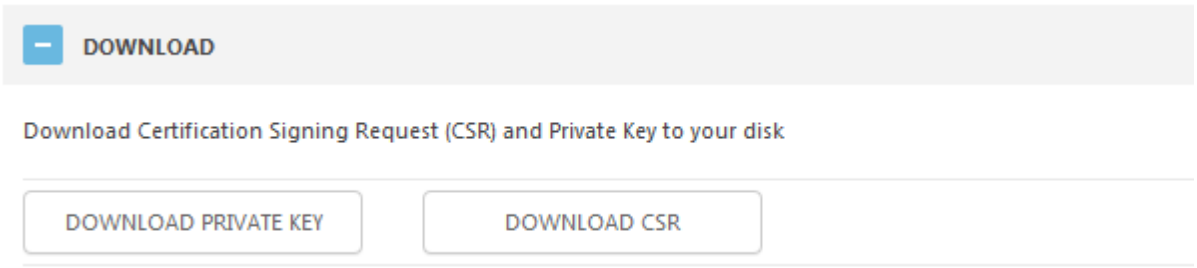
Créer une demande

Spécifiez les attributs du certificat (code de pays, nom d'organisation, etc.), puis cliquez sur **Envoyer la demande**.



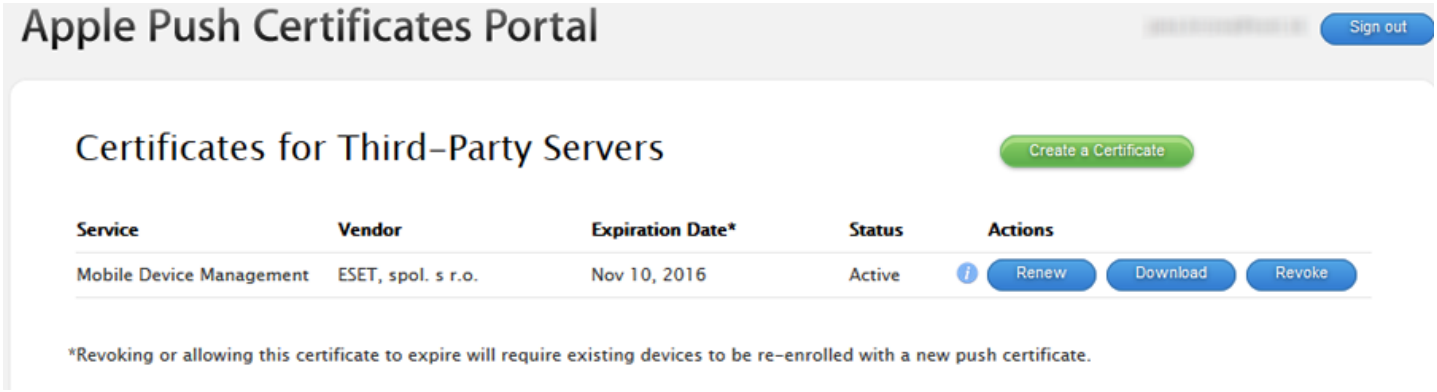
Télécharger

Téléchargez votre **demande de signature de certificat (CSR)** et une **clé privée**.



Certificat

Ouvrez le portail de certificats push Apple et connectez-vous à l'aide de votre identifiant Apple. Suivez les instructions à l'écran sur la page du portail et utilisez le fichier CSR pour obtenir le certificat APN signé par Apple (APNS).



Charger

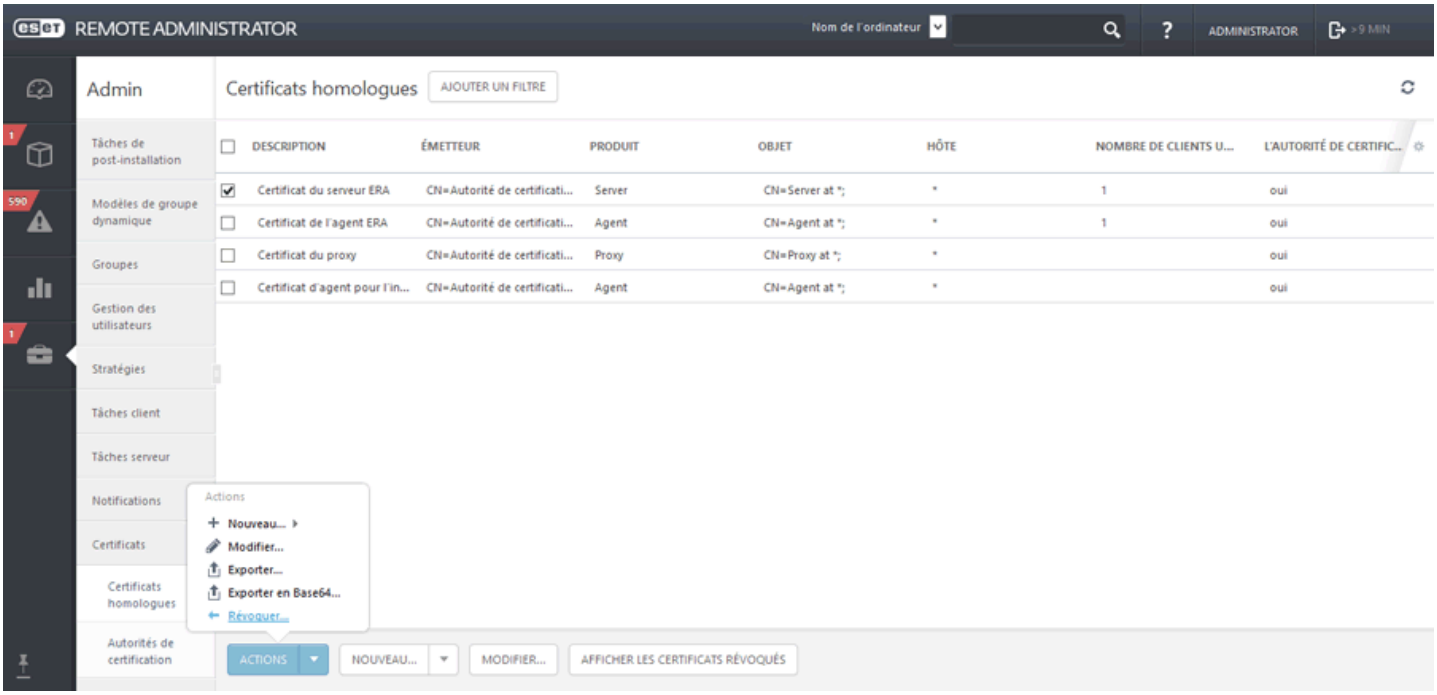
Une fois achevées toutes les étapes ci-dessus, vous pouvez créer une stratégie pour MDC pour activer APNS pour l'inscription iOS. Vous pouvez ensuite inscrire n'importe quel périphérique iOS, comme vous le feriez pour un périphérique Android, en accédant au site *https://<mdmcore>:<enrollmentport>/enrollment* à partir du navigateur du périphérique.

4.7.1.4 Afficher les certificats révoqués

Cette liste contient tous les certificats qui ont été créés et rendus non valides par ERA Server. Les certificats révoqués sont automatiquement supprimés de l'écran principal **Certificat homologue**. Cliquez sur **Afficher les certificats révoqués** pour afficher les certificats qui ont été révoqués dans la fenêtre principale.

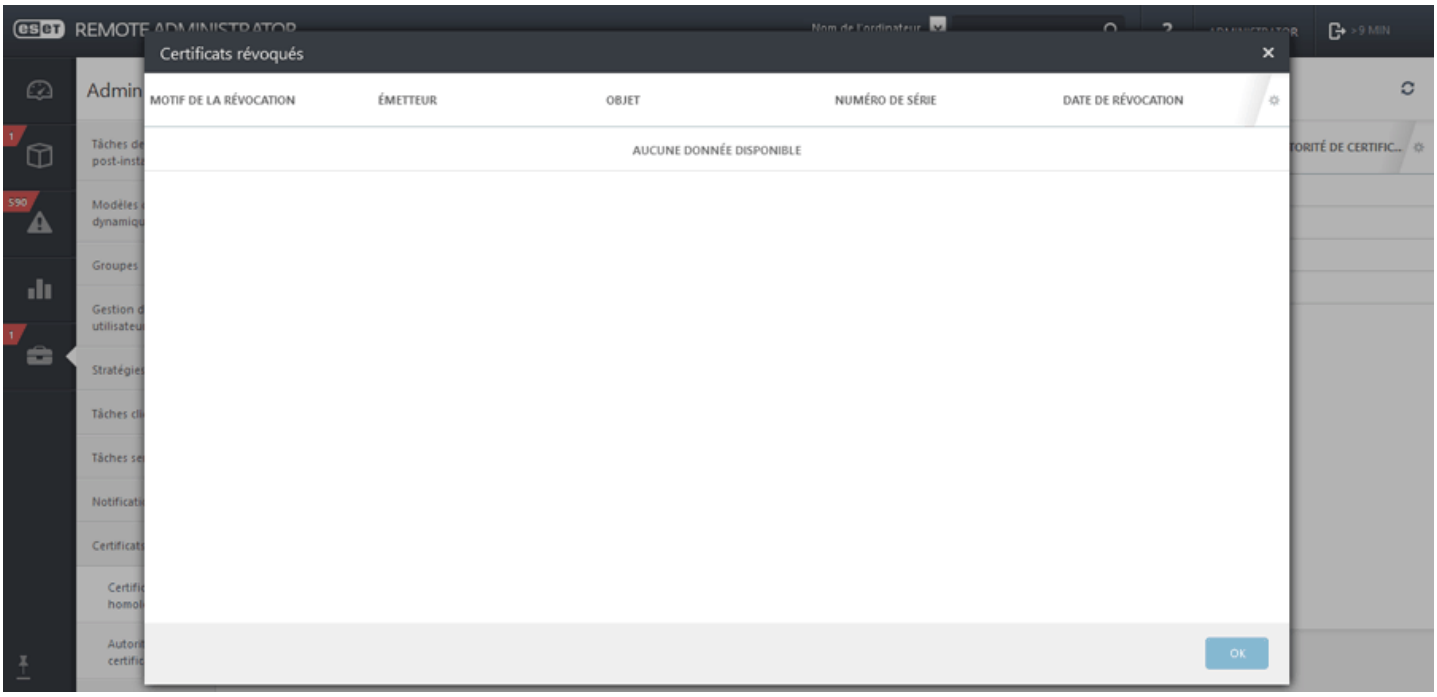
Pour révoquer un certificat, procédez comme suit :

1. Accédez à **Admin** > **Certificats** > **Certificats homologues**, sélectionnez un certificat, puis cliquez sur **Révoquer**...



2. Indiquez le **motif** de la révocation, puis cliquez sur **Révoquer**.

3. Cliquez sur **OK**.

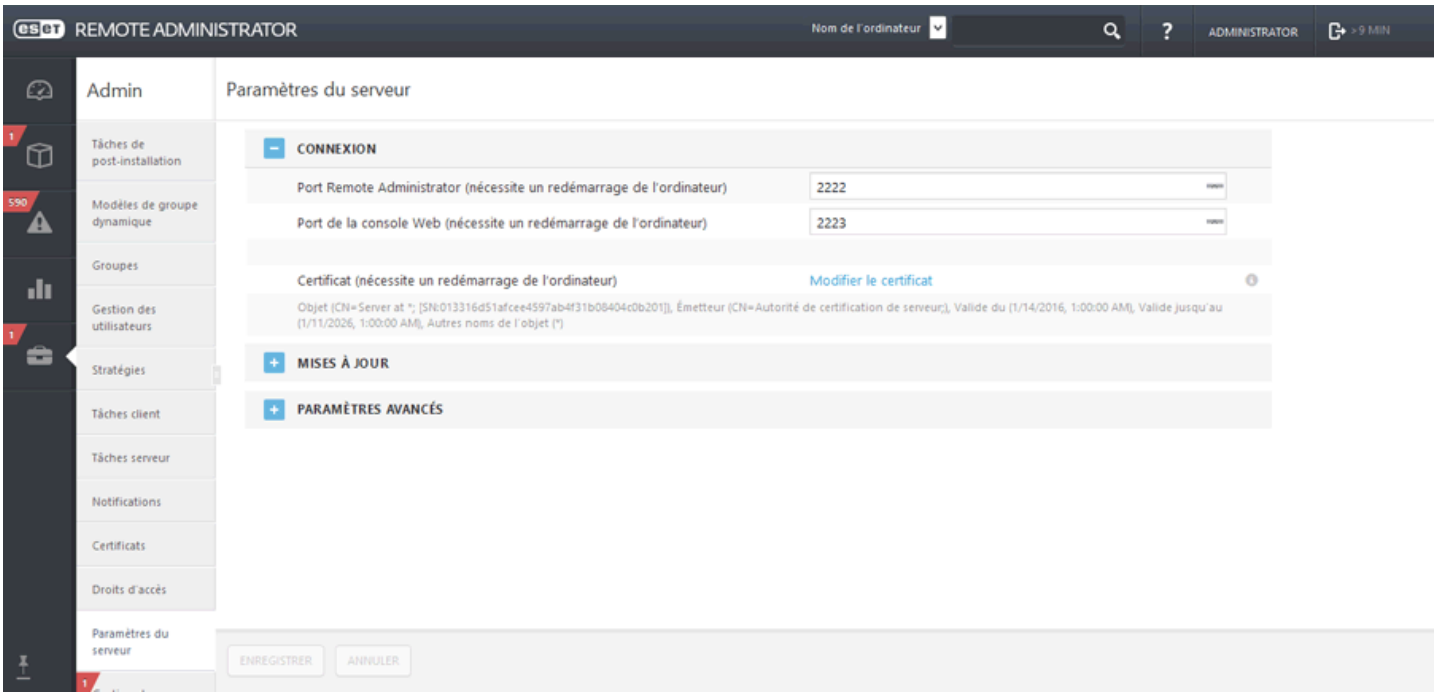


Le certificat disparaît alors de la liste des certificats homologues. Pour afficher les certificats précédemment révoqués, cliquez sur le bouton **Afficher les certificats révoqués**.

4.7.1.5 Définir un nouveau certificat ERA Server

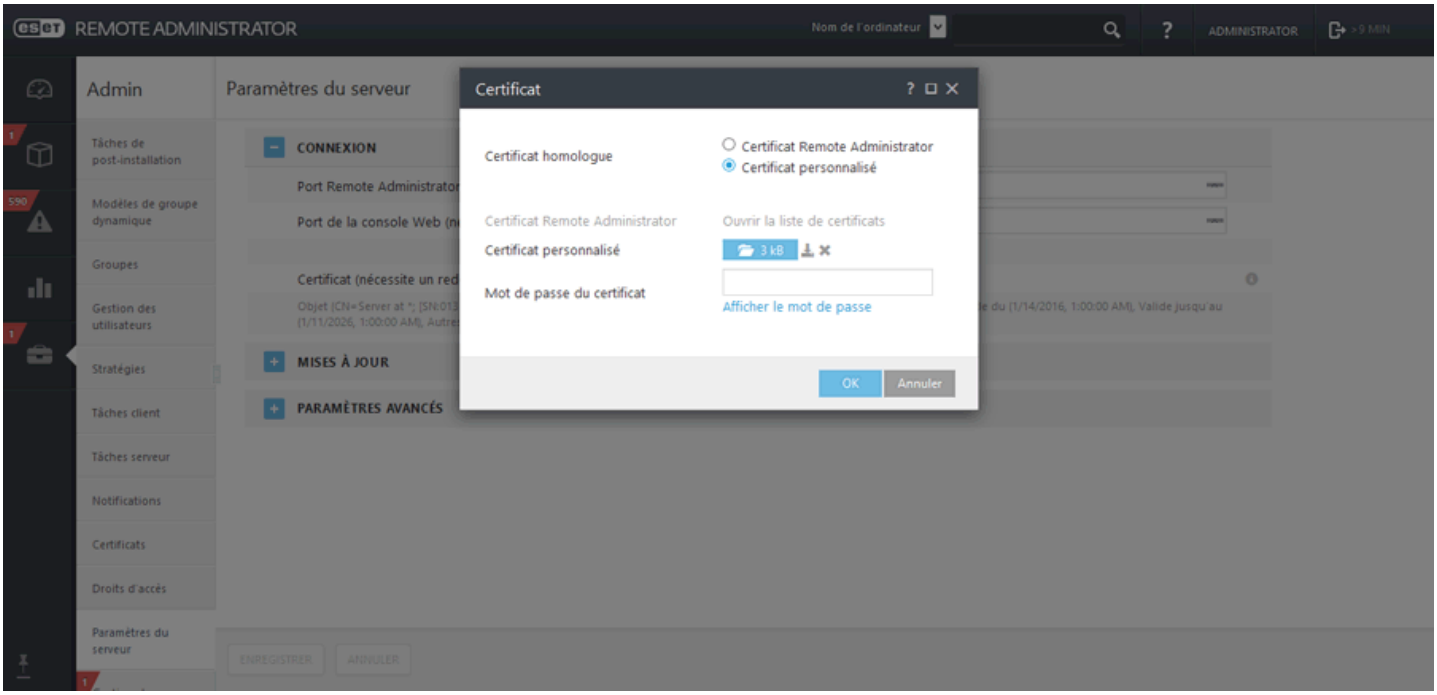
Le certificat ERA Server est créé pendant l'installation, puis il est distribué aux ERA Agents et aux autres composants pour permettre les communications avec ERA Server. Si nécessaire, vous pouvez configurer ERA Server afin d'utiliser un autre certificat homologue. Vous pouvez utiliser le certificat ERA Server (automatiquement généré pendant l'installation) ou un **certificat personnalisé.** Le certificat ERA Server est requis pour l'authentification et une connexion TSL sécurisée. Le certificat du serveur sert à s'assurer que les ERA Agents et ERA Proxys ne se connectent pas à un serveur illégitime. Cliquez sur Outils > Paramètres du serveur pour modifier les paramètres du certificat.

- Cliquez sur **Admin** > **Paramètres du serveur**, développez la section **Connexion**, puis sélectionnez **Modifier le certificat**.



Effectuez un choix parmi les deux types de certificat homologue :

- **Certificat Remote Administrator** : cliquez sur **Ouvrir le certificat**, puis sélectionnez le certificat à utiliser.
- **Certificat personnalisé** : accédez au certificat personnalisé. Si vous effectuez une migration, sélectionnez le certificat exporté depuis votre ancien serveur ERA Server.



- Sélectionnez **Certificat personnalisé**, le fichier de certificat ERA Server (*.pfx*) que vous avez exporté à partir de l'ancien serveur, puis cliquez sur **OK**.
- **Redémarrez** le service ERA Server (consultez notre article de la base de connaissances).

4.7.2 Autorités de certification

Les autorités de certification sont répertoriées dans la section **Autorités de certification** dans laquelle vous pouvez les gérer. Si vous possédez plusieurs autorités de certification, vous pouvez appliquer un filtre pour les trier.

- Créer une nouvelle autorité de certification
- Importer la clé publique
- Exporter la clé publique

4.7.2.1 Créer une nouvelle autorité de certification

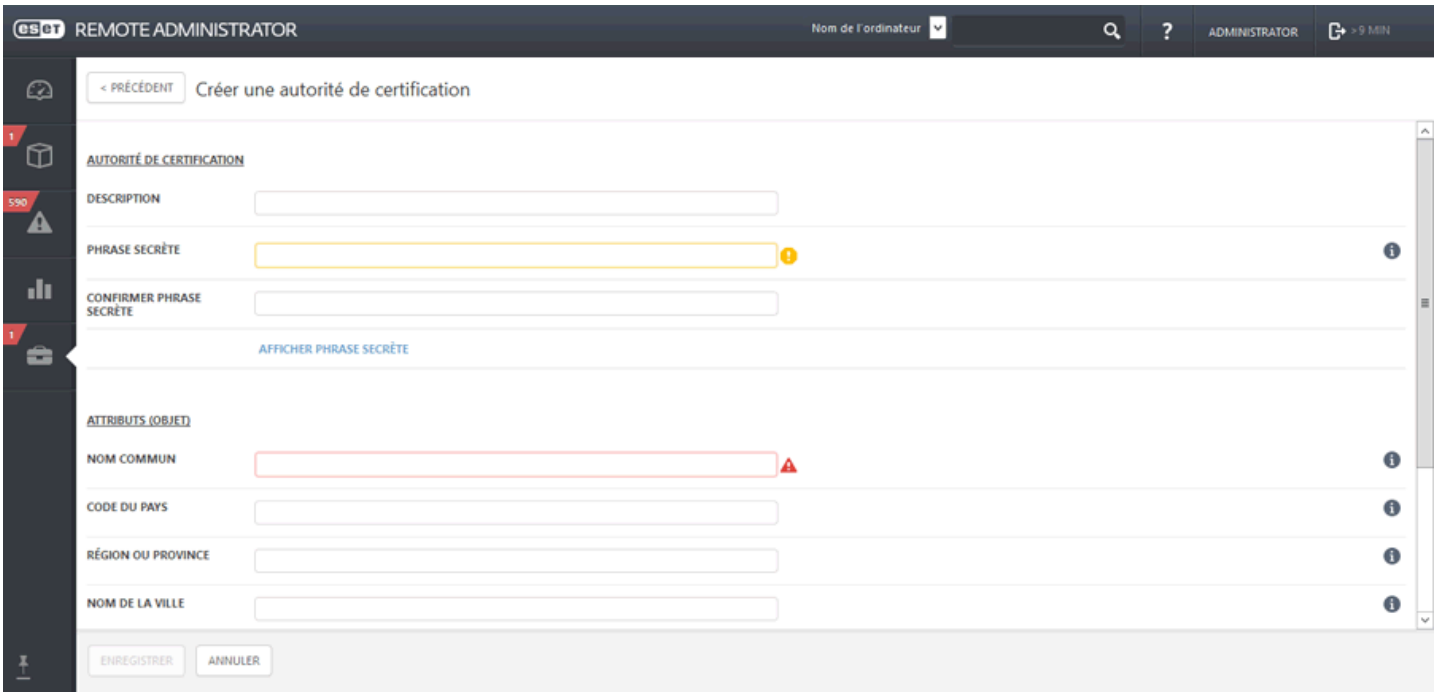
Pour créer une autorité, accédez à **Admin** > **Certificats** > **Autorité de certification**, puis cliquez sur **Action** > + **Nouveau...** ou **Nouveau** dans la partie inférieure de la page.

Autorité de certification

Saisissez une **description** de l'autorité de certification et sélectionnez une **phrase secrète**. Cette **phrase secrète** doit contenir au moins 12 caractères.

Attributs (objet)

1. Saisissez un **nom commun** (nom) pour l'autorité de certification. Sélectionnez un nom unique afin de faire la distinction entre plusieurs autorités de certification.
   Vous pouvez éventuellement saisir des informations descriptives sur l'autorité de certification.
2. Saisissez des valeurs dans les champs **Valide du** et **Valide jusqu'au** pour garantir la validité du certificat.
3. Cliquez sur **Enregistrer** pour enregistrer la nouvelle autorité de certification. Elle est désormais répertoriée dans la liste des autorités de certification située sous **Admin** > **Certificats** > **Autorité de certification**, et prête à être utilisée.



Pour gérer l'autorité de certification, cochez la **case** en regard de celle-ci dans la liste et utilisez le menu de contact (cliquez avec le bouton gauche sur l'autorité de certification) ou le bouton **Action** situé dans la partie inférieure de la page. Vous pouvez **modifier** l'autorité de certification (voir les étapes ci-dessus), la **supprimer** entièrement ou importer une clé publique et exporter une clé publique.

4.7.2.2 Exporter une clé publique

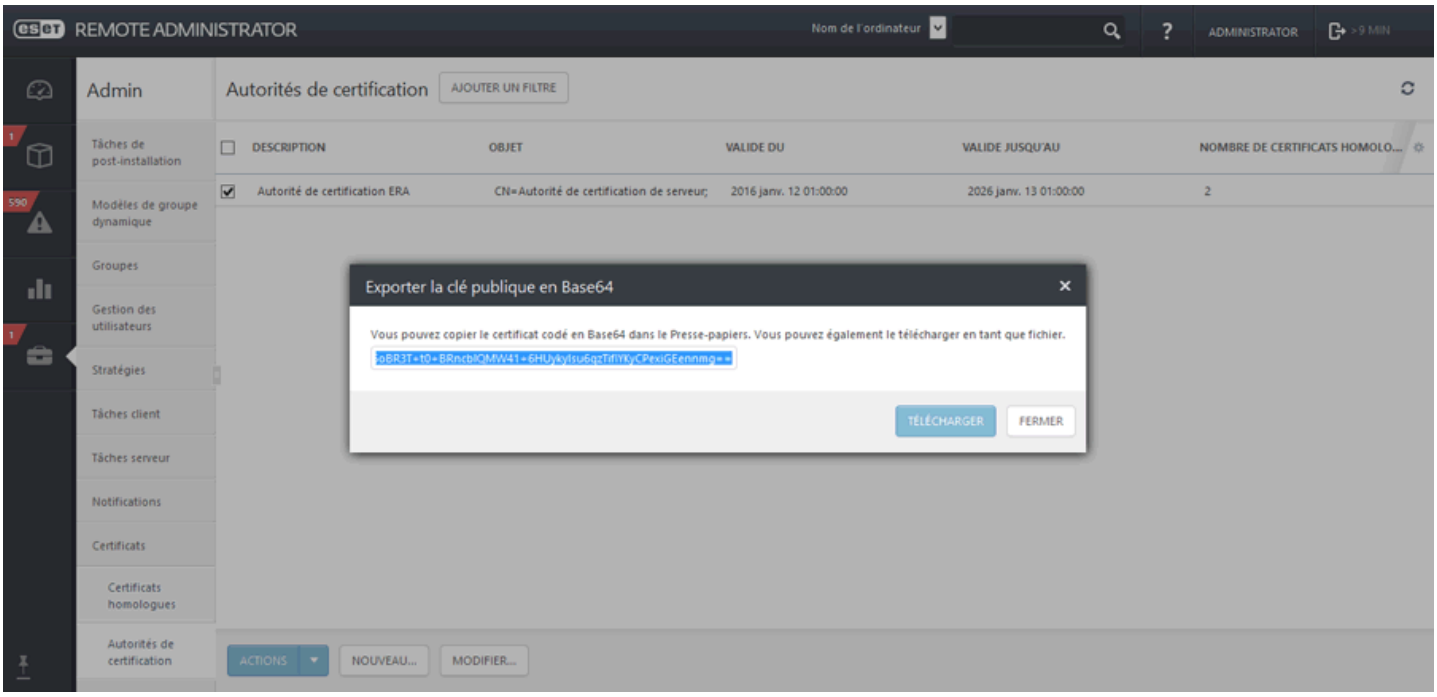
Exporter une clé publique à partir d'une autorité de certification :

1. Dans la liste, sélectionnez l'autorité de certification que vous souhaitez utiliser, puis cochez la case en regard de celle-ci.
2. Dans le menu contextuel, sélectionnez **Exporter la clé publique**. La clé publique est exportée sous forme de fichier *.der*. Saisissez un nom pour la clé publique, puis cliquez sur **Enregistrer**.

REMARQUE : si vous supprimez l'autorité de certification ERA par défaut et en créez une autre, celle-ci ne fonctionnera pas. Vous devez également l'attribuer à votre ordinateur ERA Server et redémarrer le service ERA Server.

Exporter une clé publique en Base64 à partir d'une autorité de certification :

Dans la liste, sélectionnez l'autorité de certification que vous souhaitez utiliser, puis cochez la case en regard de celle-ci.
Dans le menu contextuel, sélectionnez **Exporter une clé publique en Base64**. Vous pouvez également télécharger le certificat codé au format Base64 en tant que fichier. Répétez cette étape pour les certificats des autres composants ainsi que pour votre autorité de certification.

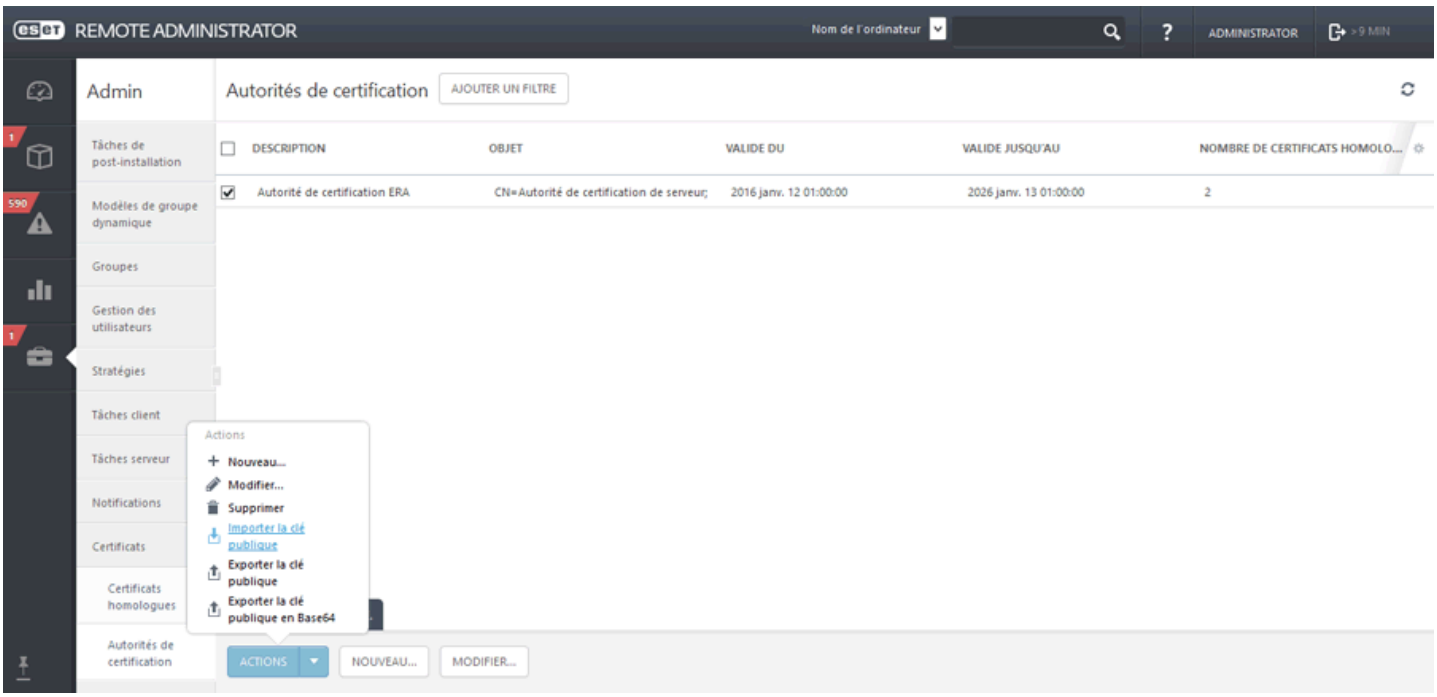


REMARQUE : si vous utilisez des certificats qui ne sont pas au format **Base64**, il faudra les convertir en **Base64** (ou les exporter selon la procédure ci-dessus). C'est le seul format accepté par les composants ERA pour se connecter au serveur ERA. Pour plus d'informations sur la conversion des certificats, voir http://linux.die.net/man/1/base64 et https://developer.apple.com/library/mac/documentation/Darwin/Reference/ManPages/man1/base64.1.html. Par exemple :

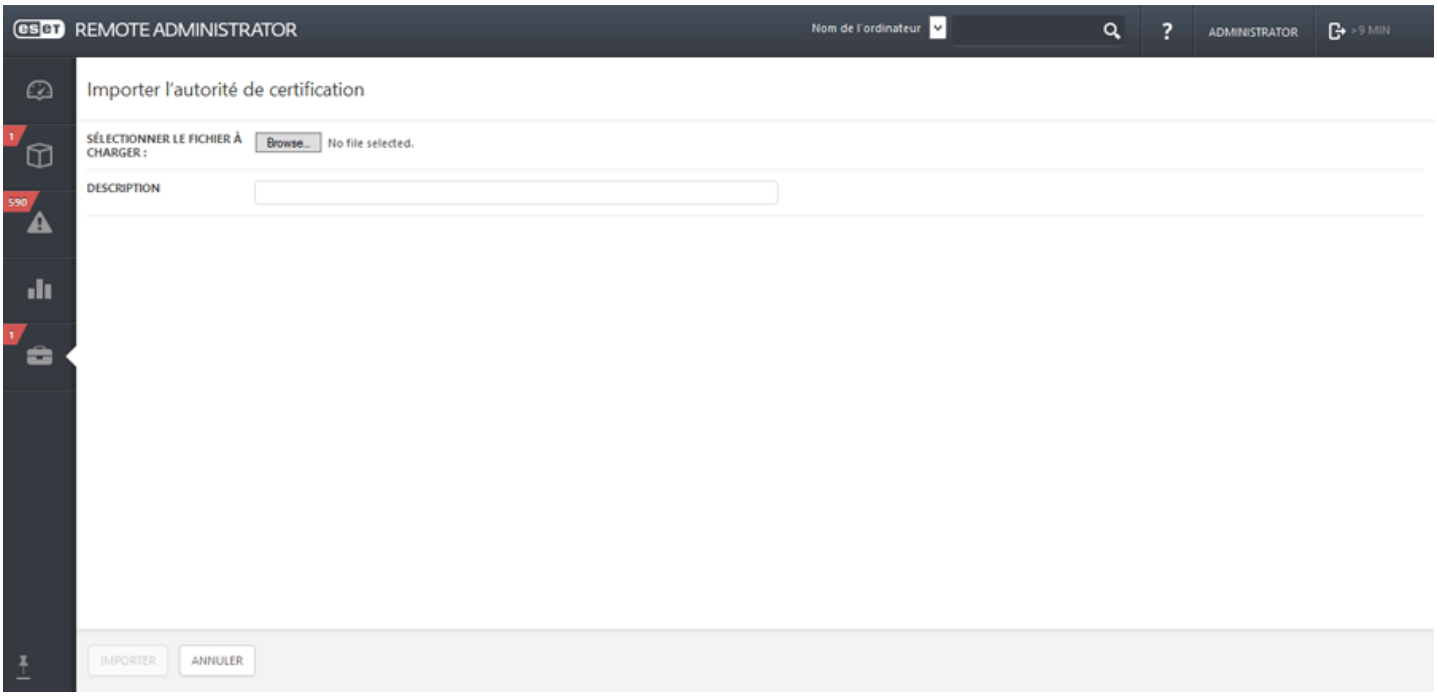
```
'cat ca.der | base64 > ca.base64.txt' a 'cat agent.pfx | base64 > agent.base64.txt'
```

4.7.2.3 Importer une clé publique

Pour importer une autorité de certification tierce, cliquez sur **Admin** > **Certificats** > **Autorités de certification**. Cliquez sur **Actions**, puis sur **Importer la clé publique**.



- **Sélectionnez le fichier à charger** : cliquez sur **Parcourir** pour accéder au fichier que vous souhaitez importer.



- Entrez une **description** du certificat, puis cliquez sur **Importer**. L'autorité de certification est importée.

4.8 Droits d'accès

Les droits d'accès vous permettent de gérer les utilisateurs d'ERA Web Console et leurs autorisations. On distingue deux types :

1. Utilisateurs natifs - comptes utilisateurs créés et gérés depuis la console Web.
2. Groupes de sécurité du domaine mappé - comptes utilisateurs gérés et authentifiés par Active Directory.

Vous pouvez également configurer l'authentification à 2 facteurs pour les utilisateurs natifs et les groupes de sécurité du domaine mappé. Cela renforcera la sécurité lors de la connexion et de l'accès à la console Web ERA.

L'accès aux éléments des deux catégories doit être octroyé (à l'aide des jeux d'autorisations) à chaque utilisateur d'ERA Web Console.

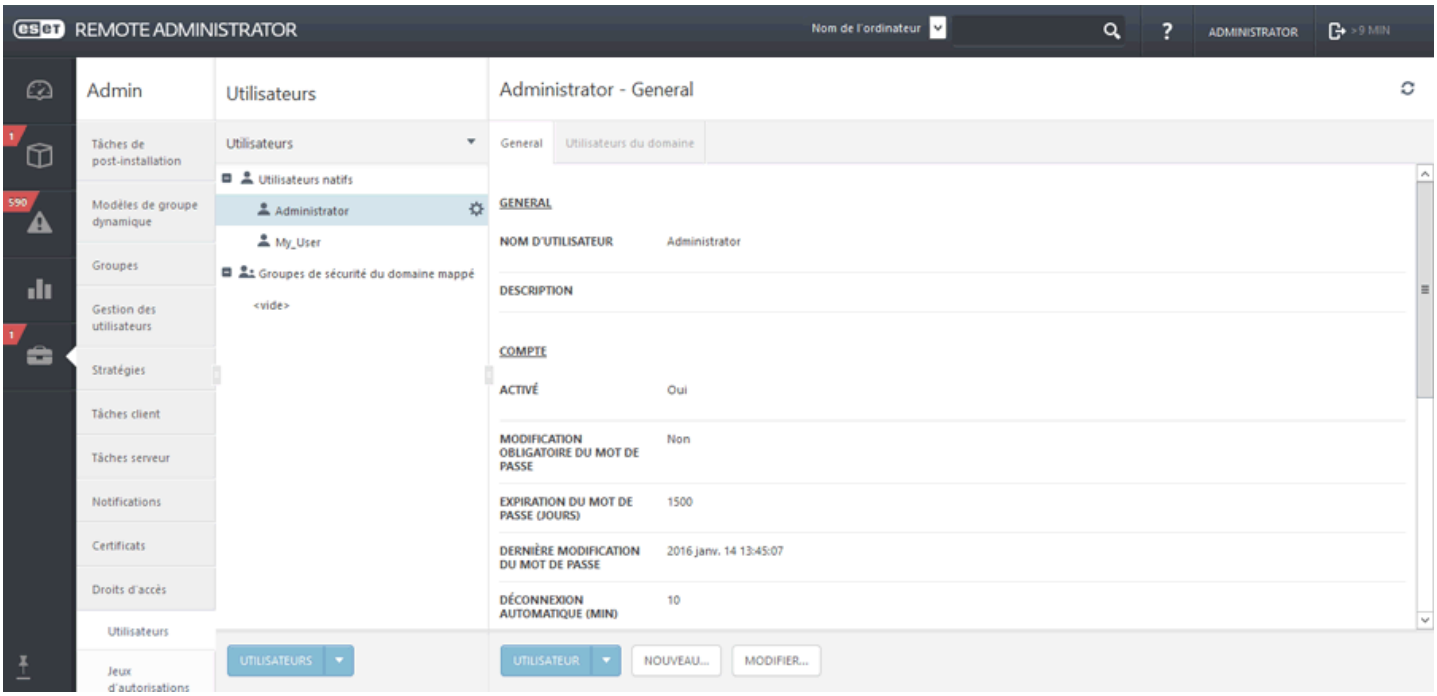
IMPORTANT : Le compte de l'utilisateur natif **Administrateur** a accès à tout. Il n'est pas conseillé d'utiliser ce compte de façon régulière. Nous vous recommandons vivement de créer un autre compte 'admin' ou d'utiliser les administrateurs des groupes de sécurité du domaine mappé en leur attribuant le jeu d'autorisations de l'administrateur. Vous disposerez ainsi d'une solution de secours en cas de problème avec le compte de l'administrateur. Vous pouvez également créer d'autres comptes avec des droits d'accès restreints selon les compétences souhaitées. Utilisez uniquement le compte Administrateur par défaut comme option de secours.

Les utilisateurs sont gérés dans la zone Utilisateurs de la section Admin. Les jeux d'autorisations définissent les niveaux d'accès des différents utilisateurs à différents éléments.

4.8.1 Utilisateurs

ERA Web Console peut comporter des utilisateurs disposant de différents jeux d'autorisations. L'utilisateur disposant des autorisations et des droits d'accès complets est l'**administrateur**.. Pour faciliter l'utilisation d'Active Directory, les utilisateurs des groupes de sécurité du domaine peuvent être autorisés à se connecter à ERA. Ces utilisateurs peuvent exister à côté des **utilisateurs natifs ERA**, les jeux d'autorisations sont toutefois définis pour le groupe de sécurité Active Directory (au lieu des utilisateurs, comme dans le cas des utilisateurs natifs).

La gestion des utilisateurs s'effectue dans la section **Admin** de la console Web ERA.

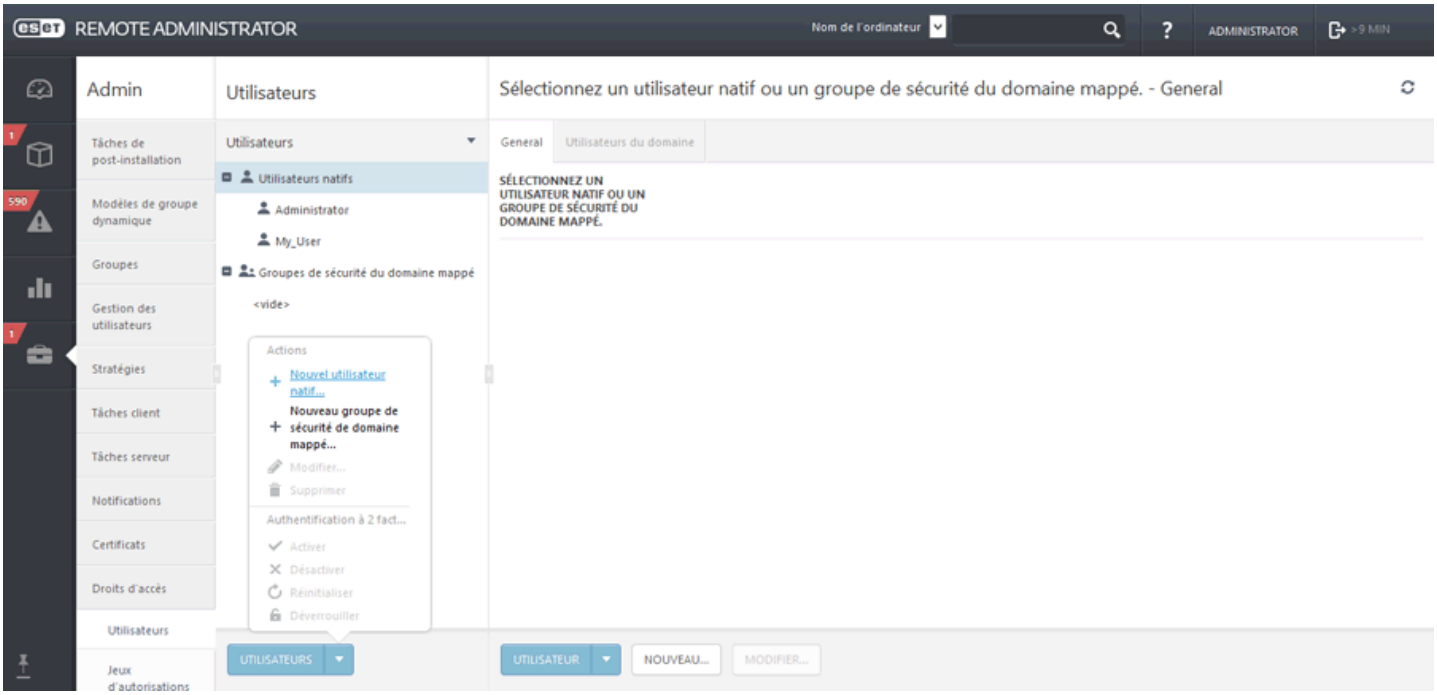


REMARQUE : Une nouvelle installation d'ERA comporte uniquement le compte Administrateur (utilisateurs natifs).

4.8.1.1 Créer un utilisateur natif

Pour créer un utilisateur natif, sous l'onglet **Admin**, cliquez sur **Droits d'accès** > **Utilisateur**, puis sur **Utilisateurs** ou **Nouveau** dans la partie inférieure de la page.

Pour créer un second compte Administrateur, suivez la procédure pour créer un compte d'utilisateur natif et attribuez le jeu d'autorisations de l'administrateur à ce compte.



General

Saisissez un **Nom d'utilisateur** et une **Description** facultative pour le nouvel utilisateur.

Authentification

Le mot de passe de l'utilisateur doit contenir au moins 8 caractères. Il ne doit pas comporter le nom d'utilisateur.

Compte

- Conservez l'option **Activé** sélectionnée, sauf si vous souhaitez que le compte soit inactif (en vue de l'utiliser ultérieurement).
- Conservez l'option **Modification obligatoire du mot de passe** désélectionnée (si cette option est sélectionnée, l'utilisateur devra modifier son mot de passe lors de sa première connexion à ERA Web Console).
- L'option **Expiration du mot de passe** définit le nombre de jours de validité du mot de passe. Lorsque ce nombre de jours est atteint, le mot de passe doit être modifié.
- L'option **Déconnexion automatique (min)** définit la durée d'inactivité (en minutes) après laquelle l'utilisateur est déconnecté de la console Web.
- Les options **Nom complet**, **Adresse électronique de contact** et **Numéro de téléphone du contact** peuvent être définies pour identifier l'utilisateur.

Jeu d'autorisations

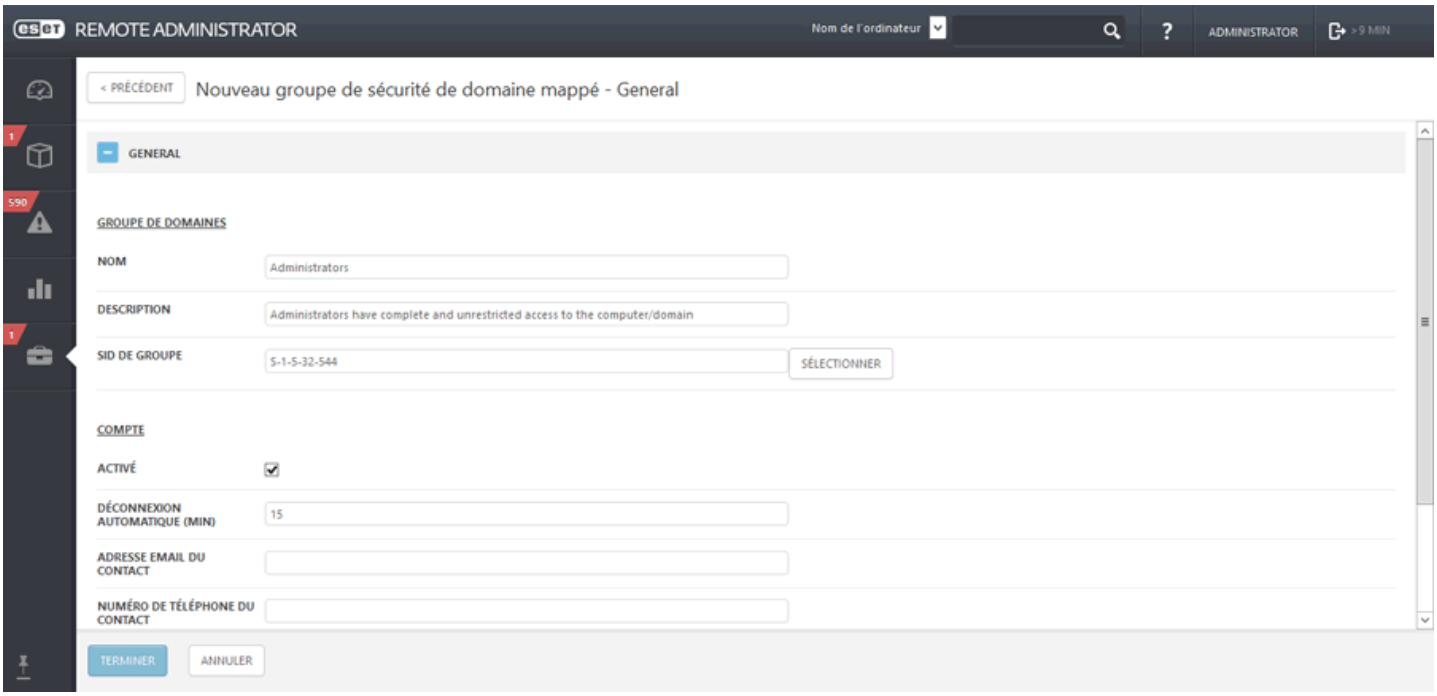
Attribuez des compétences (droits) à l'utilisateur. Vous pouvez sélectionner une compétence prédéfinie : **Jeu d'autorisations du réviseur** (similaire aux droits d'accès en lecture seule) ou **Jeu d'autorisations de l'administrateur** (similaire à des droits d'accès total) ou **Jeu d'autorisations d'installation assistée du serveur** (similaire à des droits d'accès en lecture seule). Vous pouvez également utiliser un jeu d'autorisations personnalisé.

Résumé

Passez en revue les paramètres configurés pour cet utilisateur, puis cliquez sur **Terminer** pour créer le compte.

4.8.1.2 Assistant Groupe de sécurité de domaine mappé

Pour accéder à l'**Assistant Groupe de sécurité de domaine mappé**, accédez à **Admin** > **Droits d'accès** > **Groupes de sécurité du domaine mappé** > **Nouveau** ou simplement à **Nouveau** (lorsque le groupe de sécurité mappé est sélectionné dans l'arborescence).



General

Groupe de domaines

Saisissez un nom de groupe dans le champ **Nom**. Vous pouvez également saisir une description du groupe. Le groupe est défini par un **SID de groupe** (identifiant de sécurité). Cliquez sur **Sélectionner** pour sélectionner un groupe dans la liste, puis sur **OK** pour confirmer la sélection.

Compte

- Conservez l'option **Activé** sélectionnée pour rendre l'utilisateur actif.
- L'option **Déconnexion automatique (min)** définit la durée d'inactivité (en minutes) après laquelle l'utilisateur est déconnecté d'ERA Web Console.
- Les options facultatives **Adresse électronique de contact** et **Numéro de téléphone du contact** peuvent être utilisées pour identifier l'utilisateur.

Jeu d'autorisations

Attribuez des compétences (droits) à l'utilisateur. Vous pouvez utiliser une compétence prédéfinie :

Jeu d'autorisations de l'administrateur(similaire à des droits d'accès total). Vous avez aussi la possibilité d'utiliser un jeu d'autorisations personnalisé.

Jeu d'autorisations d'installation assistée du serveur - (similaire aux droits d'accès en lecture seule)

Jeu d'autorisations du réviseurl (similaire aux droits d'accès en lecture seule)

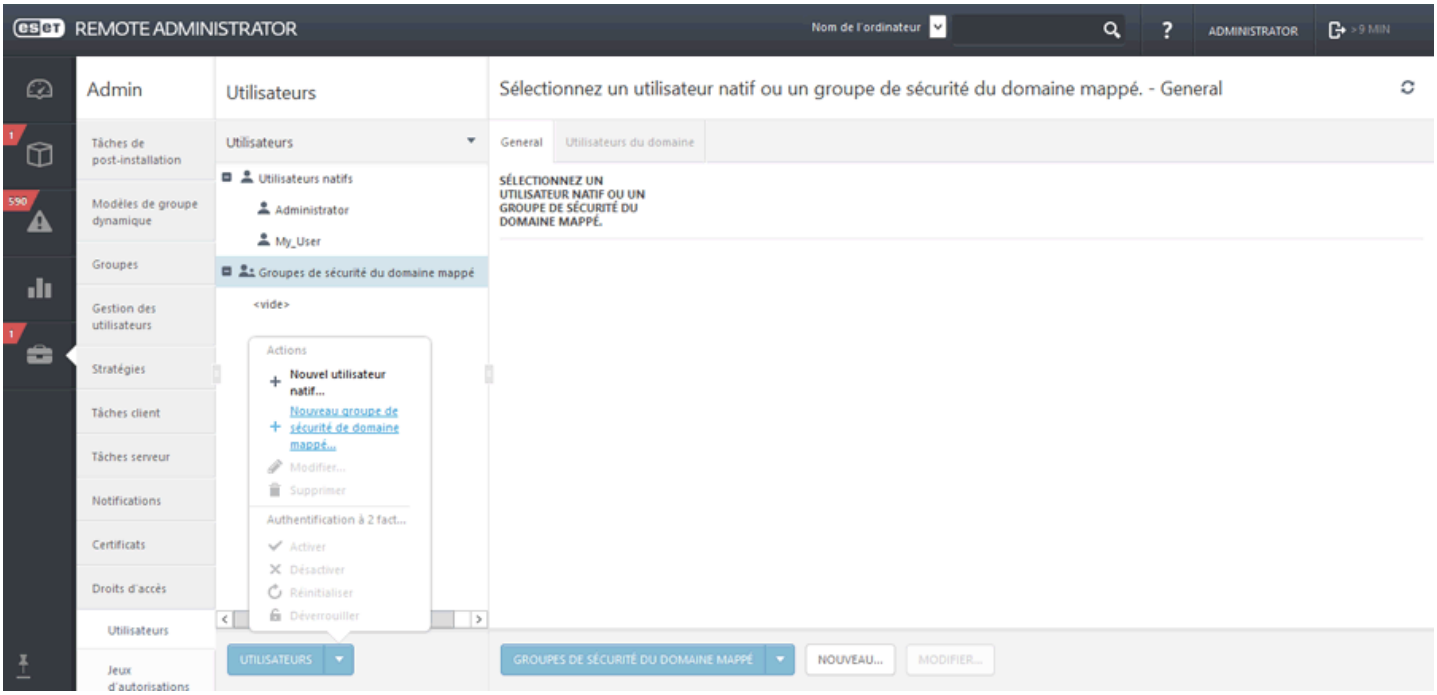
Résumé

Passez en revue les paramètres configurés pour cet utilisateur, puis cliquez sur **Terminer** pour créer le groupe.

4.8.1.3 Mapper un groupe sur un groupe de sécurité de domaine

Vous pouvez mapper un groupe de sécurité de domaine sur ERA Server et autoriser les utilisateurs existants (membres de ces groupes de sécurité de domaine) à devenir utilisateurs d'ERA Web Console.

Cliquez sur **Admin** > **Droits d'accès** > **Groupes de sécurité du domaine mappé** > **Nouveau** ou simplement sur **Nouveau** (lorsque le groupe de sécurité de domaine mappé est sélectionné dans l'arborescence).



General

Groupe de domaines

Saisissez un nom de groupe dans le champ **Nom**. Vous pouvez également saisir une description du groupe. Le groupe est défini par un **SID de groupe** (identifiant de sécurité). Cliquez sur **Sélectionner** pour sélectionner un groupe dans la liste, puis sur **OK** pour confirmer la sélection.

Compte

- Conservez l'option **Activé** sélectionnée pour rendre l'utilisateur actif.
- L'option **Déconnexion automatique (min)** définit la durée d'inactivité (en minutes) après laquelle l'utilisateur est déconnecté de la console Web.
- Les options facultatives **Adresse électronique de contact** et **Numéro de téléphone du contact** peuvent être utilisées pour identifier l'utilisateur.

Jeu d'autorisations

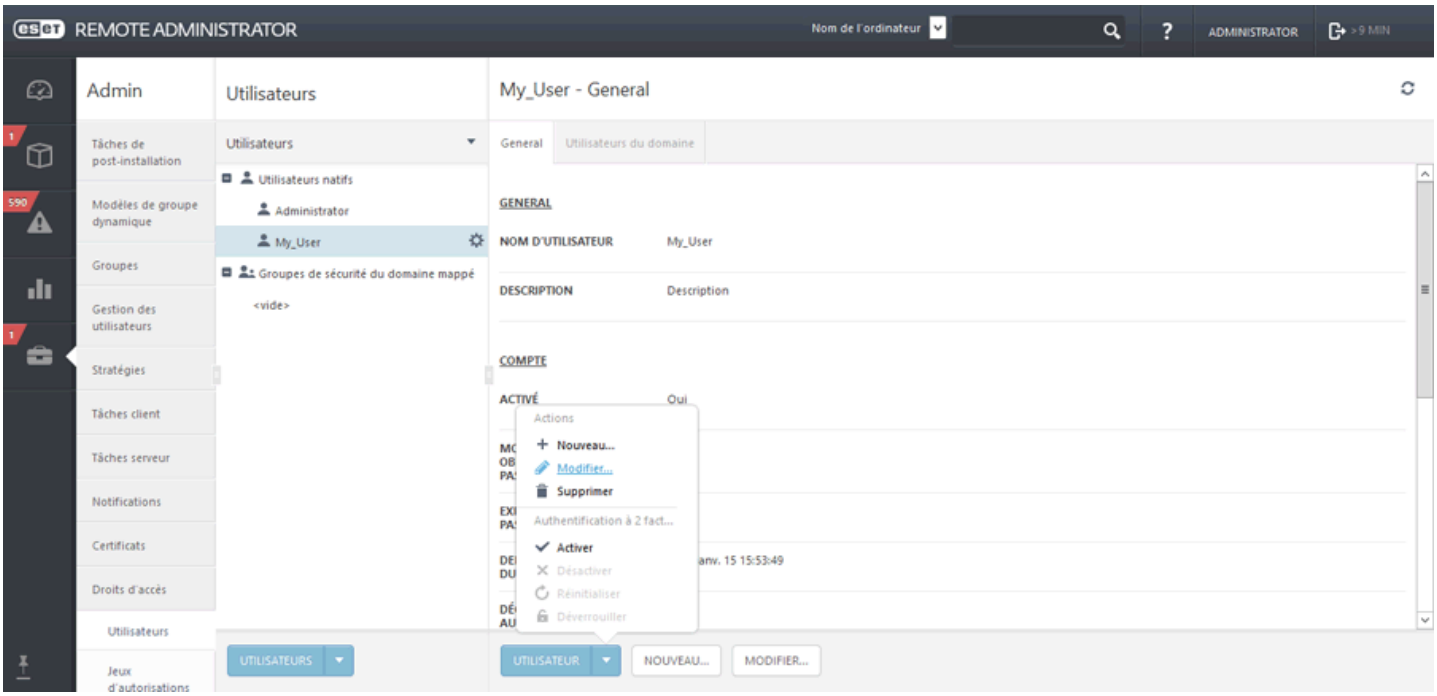
Attribuez des compétences (droits) à l'utilisateur. Vous pouvez utiliser une compétence prédéfinie : **Jeu d'autorisations du réviseur** (similaire à des droits d'accès en lecture seule), **Jeu d'autorisations de l'administrateur** (similaire à des droits d'accès total) ou **Jeu d'autorisations d'installation assistée du serveur** (autorisation d'effectuer l'installation de l'Agent ERA localement sur un ordinateur client). Vous pouvez également utiliser un jeu d'autorisations personnalisé.

Résumé

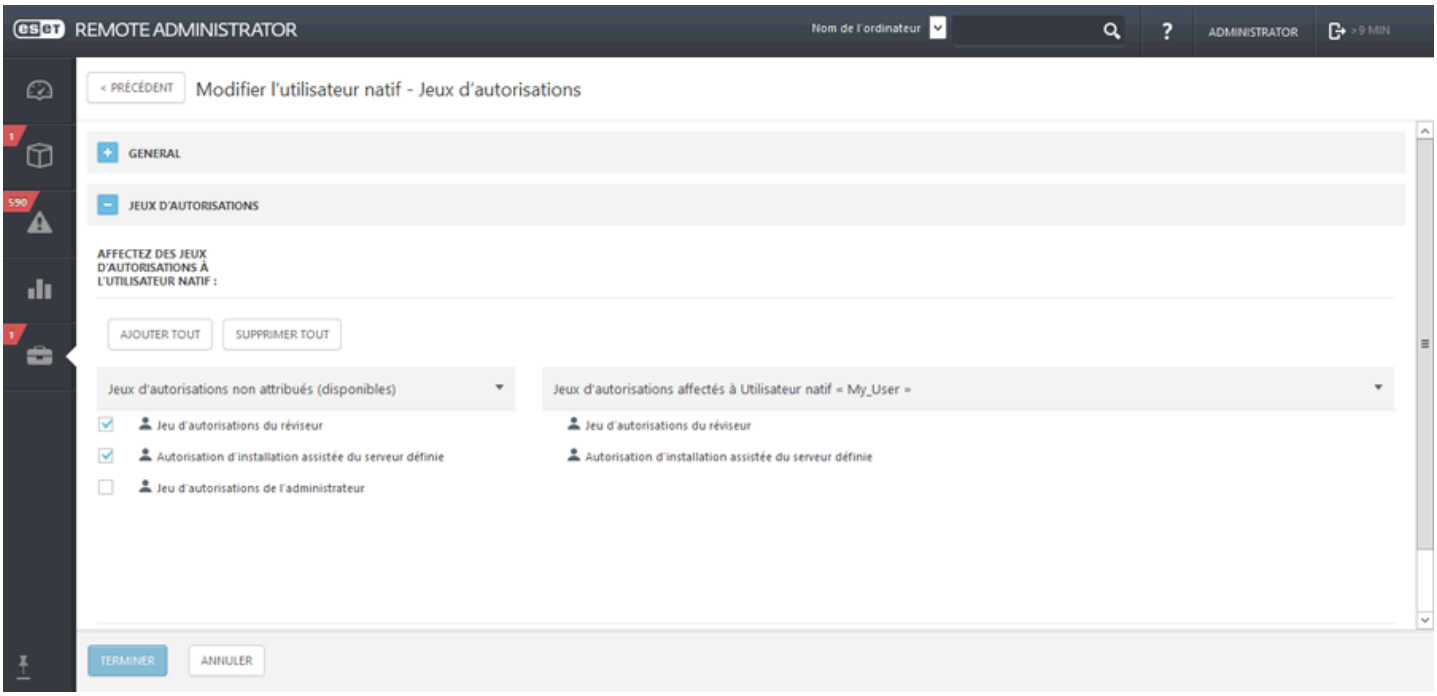
Passez en revue les paramètres configurés pour cet utilisateur, puis cliquez sur **Terminer** pour créer le groupe.

4.8.1.4 Attribuer un jeu d'autorisations à un utilisateur

Pour attribuer un jeu d'autorisations spécifique à un utilisateur, cliquez sur **Admin** > **Droits d'accès** > **Jeux d'autorisations**, puis sur **Modifier**. Pour plus d'informations, reportez-vous à la section Gérer les jeux d'autorisations.



Dans la section **Utilisateurs**, modifiez un utilisateur spécifique en cliquant sur **Modifier...**, puis cochez une case en regard d'un jeu d'autorisations spécifique dans la section **Jeux d'autorisations non attribués (disponibles)**.



4.8.1.5 Authentification à 2 facteurs

L'authentification à 2 facteurs offre un moyen sécurisé de se connecter à ERA Web Console et d'y accéder.

- Seul l'administrateur ERA peut activer l'authentification à 2 facteurs pour les comptes d'autres utilisateurs. Une fois l'authentification à 2 facteurs activée, un utilisateur doit la configurer par lui-même avant de se connecter. Les utilisateurs reçoivent un lien dans un message texte (SMS) qu'ils peuvent ouvrir dans le navigateur Web de leur téléphone pour lire les instructions relatives à la configuration de l'authentification à 2 facteurs.
- L'authentification à 2 facteurs est fournie par ESET et sa technologie ESET Secure Authentication. Il n'est pas nécessaire de déployer ou d'installer ESET Secure Authentication dans votre environnement. ERA se connecte automatiquement aux serveurs ESET afin d'authentifier les utilisateurs qui se connectent à ERA Web Console.
- Les utilisateurs pour lesquels l'authentification à 2 facteurs est activée devront se connecter à ESET Remote Administrator à l'aide de ESET Secure Authentication.

REMARQUE : l'utilisation d'utilisateurs employant l'authentification à 2 facteurs pour l'installation assistée du serveur n'est pas autorisée.

4.8.2 Jeux d'autorisations

Un jeu d'autorisations représente les autorisations des utilisateurs qui accèdent à la console Web ERA. Il définit les actions que les utilisateurs peuvent effectuer ou les éléments qu'ils peuvent afficher dans la console Web. Les utilisateurs natifs possèdent leurs propres autorisations, tandis que les utilisateurs du domaine disposent des autorisations de leur groupe de sécurité mappé.

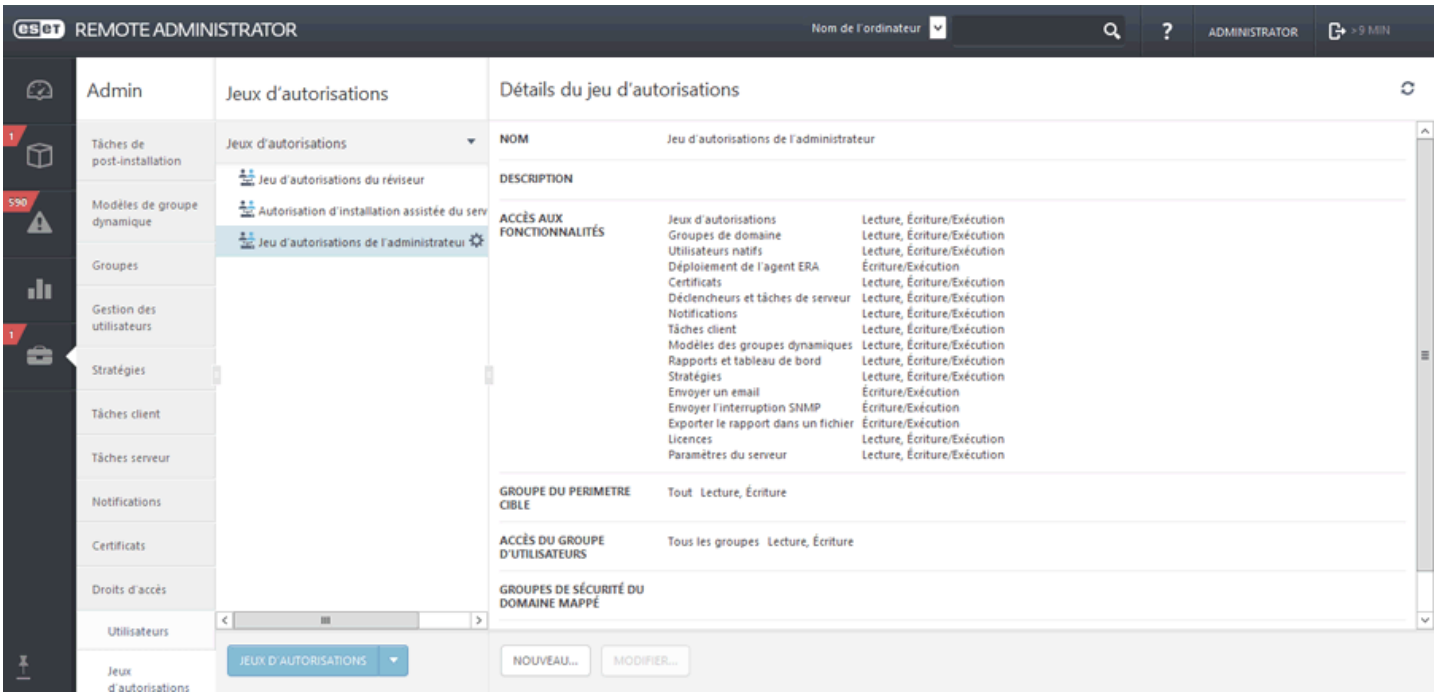
Les autorisations de la console Web ERA sont classées dans des catégories (Utilisateurs natifs, Certificats, Stratégies, etc.). Pour chaque fonctionnalité, un jeu d'autorisations donné peut autoriser un accès en lecture seule ou en écriture/exécution.

Les autorisations **Lecture seule** sont destinées aux utilisateurs effectuant des audits. Ils peuvent afficher les données mais ne sont pas autorisés à apporter des modifications.

Les autorisations **Écriture/Exécution** permettent aux utilisateurs de modifier les objets respectifs ou de les exécuter (dans le cas des tâches, par exemple).

En plus des autorisations pour les fonctionnalités d'ERA, il est possible d'octroyer un accès aux groupes statiques ou aux groupes d'utilisateurs. Chaque utilisateur peut se voir octroyer un accès à **tous les groupes statiques** ou des **sous-ensemble de groupes statiques**. L'accès à un groupe statique donné donne automatiquement accès à tous ses sous-groupes. Dans ce cas :

- Un accès **Lecture seule** signifie la liste des ordinateurs.
- Les autorisations **Écriture/Exécution** permettent aux utilisateurs de manipuler les ordinateurs dans un groupe statique et d'attribuer des tâches client et des stratégies.

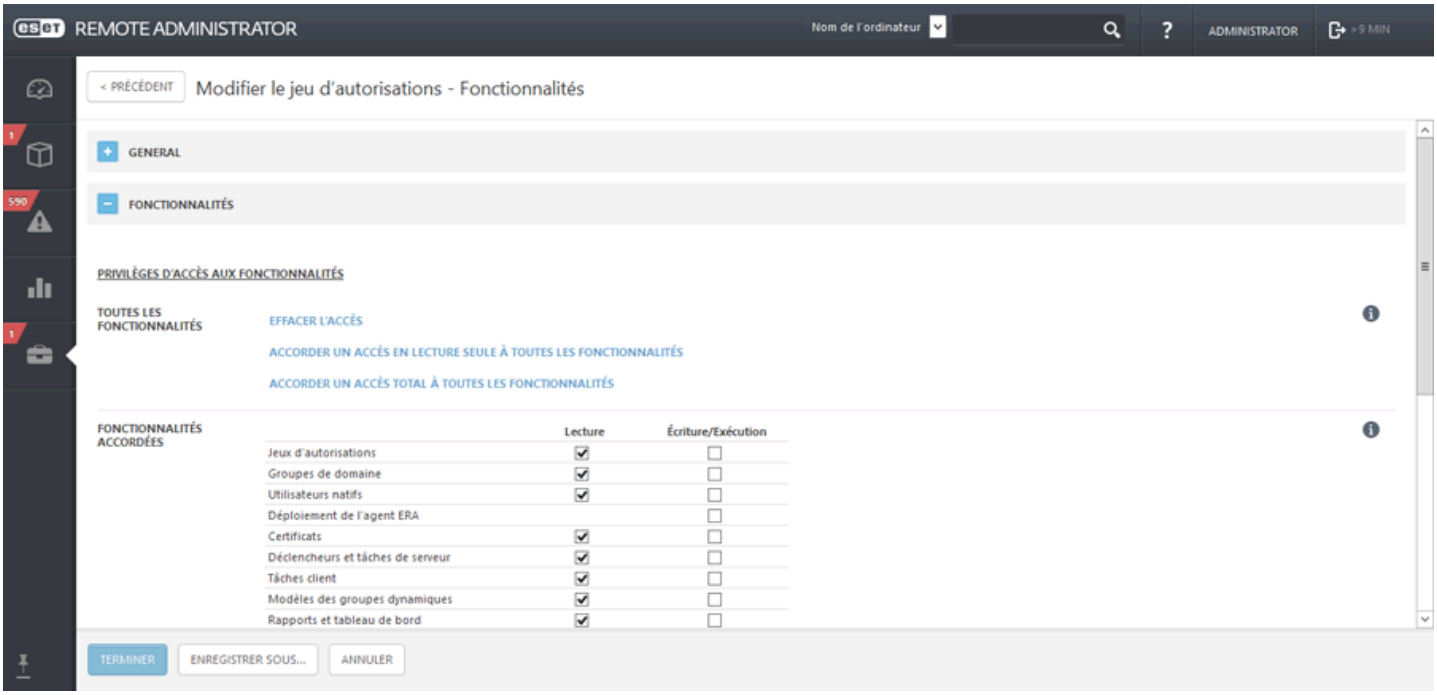


4.8.2.1 Gérer les jeux d'autorisations

Pour apporter des modifications à un jeu d'autorisations spécifique, cliquez dessus, puis sur **Modifier**. Cliquez sur **Copier** pour créer un jeu d'autorisations **en double** que vous pouvez modifier et attribuer à un utilisateur spécifique.

Général

Saisissez un **nom** pour le jeu (paramètre obligatoire). Vous pouvez également saisir une description dans le champ **Description**.



Fonctionnalités

Sélectionnez les modules auxquels vous souhaitez donner accès. L'utilisateur doté de cette compétence a accès à ces tâches spécifiques. Il est également possible d'octroyer les compétences suivantes : **Accorder un accès en lecture seule à tous les modules** et **Accorder un accès total à tous les modules**. Ces compétences existent toutefois déjà : **Compétence Administrateur** (accès total) et **Compétence Réviseur** (lecture seule). Si vous octroyez les droits **Écriture/Exécution**, les droits **Lire** sont automatiquement octroyés.

Groupes statiques

Vous pouvez ajouter un groupe statique (ou plusieurs groupes statiques) qui hérite de cette compétence (et reprend les droits définis dans la section **Modules**) et accorder un accès total ou en lecture seule à tous les groupes statiques. Vous pouvez uniquement ajouter des groupes statiques, car les jeux d'autorisations accordés sont fixes pour certains utilisateurs ou groupes.

Groupe d'utilisateurs

Vous pouvez ajouter un groupe d'utilisateurs (ou plusieurs groupes d'utilisateurs) d'ESET Mobile Device Management pour iOS.

Utilisateurs

Tous les utilisateurs disponibles sont répertoriés à gauche. Sélectionnez des utilisateurs spécifiques ou choisissez tous les utilisateurs à l'aide du bouton **Ajouter tout**. Les utilisateurs attribués sont répertoriés à droite.

Résumé

Passez en revue les paramètres configurés pour cette compétence, puis cliquez sur **Terminer**.

Cliquez sur **Enregistrer sous** pour créer un nouveau modèle selon le modèle que vous êtes en train de modifier. Vous serez invité à donner un nom au nouveau modèle.

4.9 Paramètres du serveur

Dans cette section, vous pouvez configurer des paramètres spécifiques pour ESET Remote Administrator Server.

Connexion

- **Port Remote Administrator (nécessite un redémarrage de l'ordinateur)** : il s'agit du port de connexion entre ESET Remote Administrator Server et le ou les agents. Si vous modifiez cette option, le service ERA Server doit être redémarré pour que la modification soit prise en compte.
- **Port d'ERA Web Console (nécessite un redémarrage de l'ordinateur)** : port de connexion entre la console Web et ERA Server.
- **Certificat (redémarrage requis)** : vous pouvez gérer ici les certificats ERA Server. Cliquez sur Modifier le certificat et sélectionnez le certificat ERA Server à utiliser par ERA Server. Pour plus d'informations, reportez-vous au chapitre Certificats homologues.

Mises à jour

- **Intervalle de mise à jour** : intervalle de réception des mises à jour. Vous pouvez sélectionner un intervalle régulier et configurer les paramètres ou utiliser une expression CRON.
- **Serveur de mise à jour** : il s'agit du serveur de mise à jour à partir duquel ERA Server reçoit les mises à jour pour les produits de sécurité et les composants ERA.
- **Type de mise à jour** : sélectionnez le type des mises à jour que vous souhaitez recevoir. Il peut s'agir de mises à jour régulières, retardées ou de versions bêta. Il n'est pas recommandé de sélectionner les mises à jour de versions bêta pour les systèmes de production, car cela présente un risque.

Paramètres avancés

- **Proxy HTTP** : vous pouvez utiliser un serveur proxy pour faciliter le trafic Internet vers les clients de votre réseau.
- **Wakeup** : permet au serveur de déclencher une réplication instantanée de l'agent sélectionné.
- **Serveur SMTP** : vous pouvez utiliser un serveur SMTP pour recevoir ou envoyer des messages différents. Dans cette section, vous pouvez configurer les paramètres de votre serveur SMTP.
- **Serveur Syslog** : vous pouvez utiliser ERA pour envoyer les notifications et les messages d'événement à votre serveur Syslog. Il est également possible d'exporter les journaux à partir du produit de sécurité ESET d'un client et de les envoyer au serveur Syslog.

- **Référentiel** : emplacement du référentiel dans lequel sont stockés tous les fichiers d'installation.

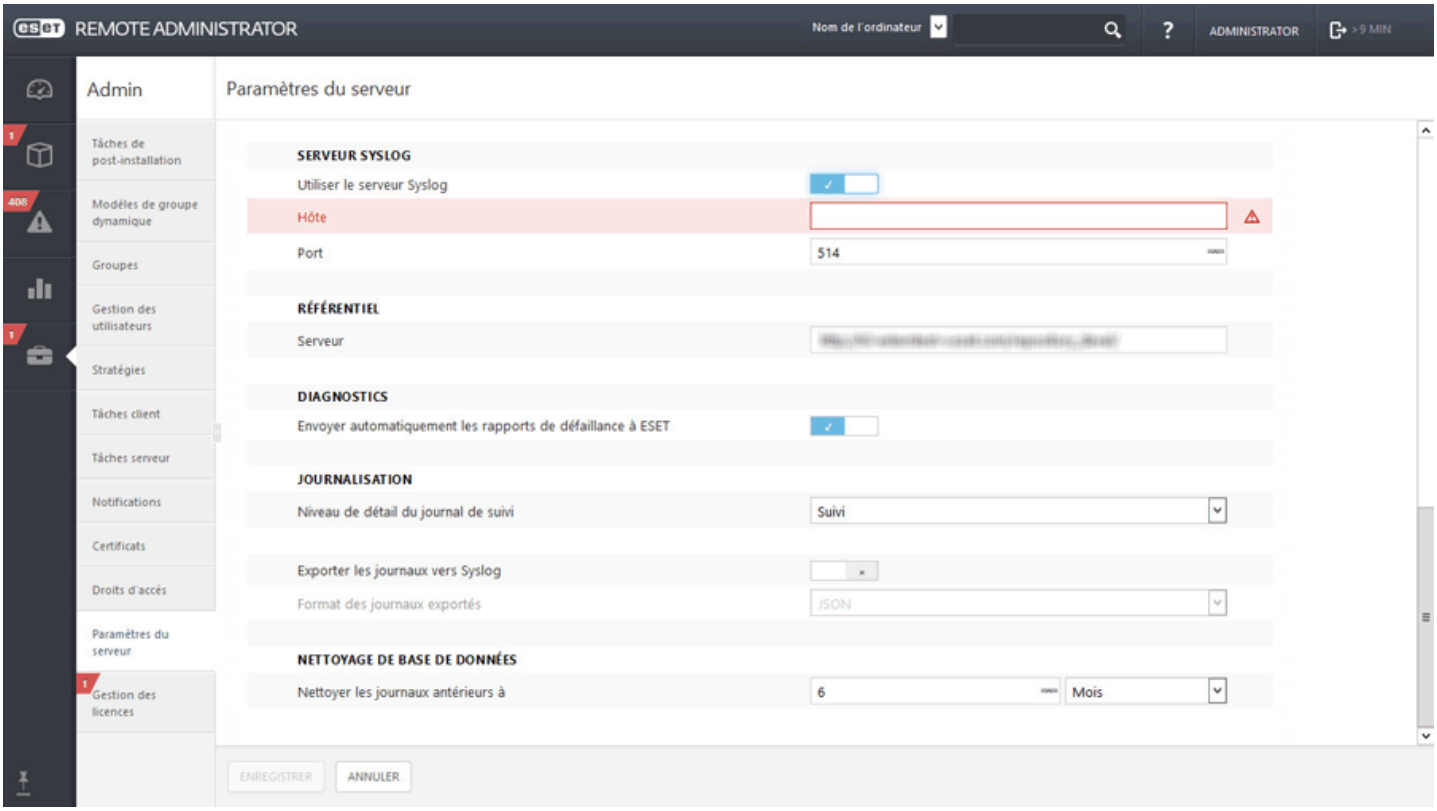
REMARQUE : Le référentiel par défaut est **AUTOSELECT**.

- **Diagnostics** : vous pouvez activer ou désactiver la transmission des rapports de défaillance à ESET.
- **Journalisation** : vous pouvez définir le détail de journal qui détermine le niveau d'informations collectées et journalisées, de **Trace** (informations) à **Fatal** (informations critiques les plus importantes). Le dernier fichier journal d'ERA Server se trouve à cet emplacement : *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs* ou *var/log/eset/RemoteAdministrator/Server/*
- **Nettoyage de base de données** : pour éviter toute surcharge d'une base de données, vous pouvez utiliser cette option pour nettoyer régulièrement les journaux.

4.9.1 Serveur Syslog

Si votre réseau comprend un serveur Syslog, vous pouvez configurer ERA Server pour envoyer des Notifications à votre serveur Syslog. Vous pouvez également activer Exporter les journaux vers Syslog pour recevoir certains événements (événement de menace, événement agrégé de pare-feu, événement agrégé HIPS, etc.) des ordinateurs clients exécutant ESET Endpoint Security, par exemple.

Pour activer Syslog, accédez à **Admin** > **Paramètres du serveur** > **Serveur Syslog** et utilisez le bouton bascule en regard de **Utiliser le serveur Syslog**. Spécifiez les paramètres obligatoires suivants - **Hôte** (adresse IP ou nom d'hôte - destination des messages Syslog) et un numéro de **Port** (la valeur par défaut est 514).



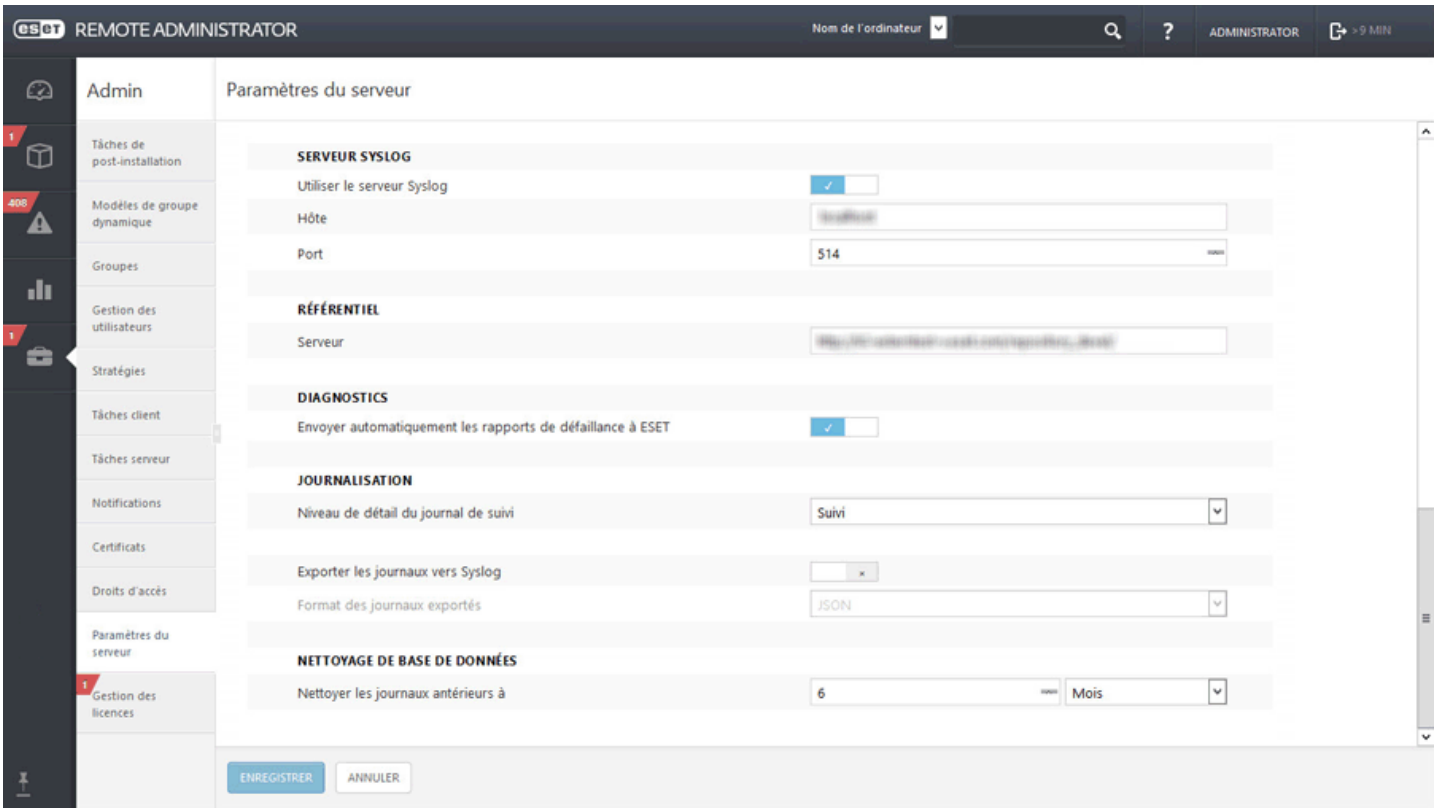
Les messages Syslog seront envoyés au serveur Syslog à l'aide du protocole UPD (User Datagram Protocol). Si vous souhaitez également que les journaux/événements de l'ordinateur client soient envoyées à votre serveur Syslog, utilisez le bouton bascule en regard de Exporter les journaux vers Syslog pour l'activer. Cliquez sur **Enregistrer**.

REMARQUE : des écritures sont effectuées en permanence dans le fichier journal d'application standard. Syslog ne sert que de support pour l'exportation de certains événements asynchrones, tels que des notifications ou divers événements d'ordinateur client.

4.9.2 Exporter les journaux vers Syslog

ESET Remote Administrator peut exporter certains journaux/événements et les envoyer ensuite à votre serveur Syslog. Des événements (événement de menace, événement agrégé de pare-feu, événement agrégé HIPS, etc.) sont générés sur un ordinateur client géré exécutant un produit de sécurité ESET (par exemple ESET Endpoint Security). Ces événements peuvent être traités par toute solution SIEM (Security Information and Event Management) capable d'importer des événements à partir d'un serveur Syslog. Les événements sont écrits sur le serveur Syslog par ESET Remote Administrator.

Lorsque vous avez activé Serveur Syslog, accédez à **Admin** > **Paramètres du serveur** > **Serveur Syslog** > **Journalisation** et activez **Exporter les journaux vers Syslog**. Les messages d'événement sont au format **JSON** (JavaScript Object Notation).



- **Evénements exportés**

Cette section contient des détails sur le format et la signification des attributs de tous les événements exportés. Le message d'événement prend la forme d'un objet JSON avec quelques clés obligatoires et facultatives. Chaque événement exporté contiendra la clé suivante :

event_type	string		Type d'événements exportés : Threat_Event, FirewallAggregated_Event, HipsAggregated_Event.
ipv4	string	facultatif	Adresse IPv4 de l'ordinateur générant l'événement.
ipv6	string	facultatif	Adresse IPv6 de l'ordinateur générant l'événement.
source_uuid	string		UUID de l'ordinateur générant l'événement.
occurred	string		Heure UTC d'occurrence de l'événement. Le format est %d-%b-%Y %H:%M:%S
severity	string		Gravité de l'événement. Les valeurs possibles (du moins grave au plus grave) sont les suivantes : Information Notice Warning Error CriticalFatal

- **Evénement de menace**

Tous les événements de menace générés par des points de terminaison gérés seront transférés à Syslog. Clé spécifique à un événement de menace :

threat_type	string	facultatif	Type de menace
threat_name	string	facultatif	Nom de la menace
threat_flags	string	facultatif	Indicateurs liés à des menaces
scanner_id	string	facultatif	ID d'analyseur
scan_id	string	facultatif	ID d'analyse
engine_version	string	facultatif	Version du moteur d'analyse
object_type	string	facultatif	Type d'objet lié à cet événement
object_uri	string	facultatif	URI de l'objet
action_taken	string	facultatif	Action prise par le point de terminaison
action_error	string	facultatif	Message d'erreur en cas d'échec de « l'action »
threat_handled	bool	facultatif	Indique si la menace a été gérée ou non
need_restart	bool	facultatif	Indique si un redémarrage est nécessaire ou non
username	string	facultatif	Nom du compte utilisateur associé à l'événement
processname	string	facultatif	Nom du processus associé à l'événement
circumstances	string	facultatif	Brève description de la cause de l'événement

- **Evénement agrégé de pare-feu**

Les journaux d'événements générés par le pare-feu personnel d'ESET sont agrégés par la gestion d'ESET Remote Administrator Agent pour éviter le gaspillage de bande passante pendant la réplication ERA Agent/ ERA Server. Clé spécifique à un événement de pare-feu :

event	string	facultatif	Nom de l'événement
source_address	string	facultatif	Adresse de la source de l'événement
source_address_type	string	facultatif	Type d'adresse de la source de l'événement
source_port	number	facultatif	Port de la source de l'événement
target_address	string	facultatif	Adresse de la destination de l'événement
target_address_type	string	facultatif	Type d'adresse de la destination de l'événement
target_port	number	facultatif	Port de la destination de l'événement
protocol	string	facultatif	Protocole
account	string	facultatif	Nom du compte utilisateur associé à l'événement
process_name	string	facultatif	Nom du processus associé à l'événement
rule_name	string	facultatif	Nom de la règle
rule_id	string	facultatif	ID de règle
inbound	bool	facultatif	Indique si la connexion était entrante ou non
threat_name	string	facultatif	Nom de la menace

event	string	facultatif	Nom de l'événement
aggregate_count	number	facultatif	Nombre de messages identiques générés par le point de terminaison entre deux réplications consécutives entre ERA Server et l'ERA Agent de gestion

- **Evénement agrégé HIPS**

Les événements du système HIPS (Host-based Intrusion Prevention System) sont filtrés sur la **gravité** avant d'être transmis plus avant en tant que messages Syslog. Seuls les événements dont les niveau de **gravité** sont *Error*, *Critical* et *Fatal* sont envoyés à Syslog. Les attributs spécifiques à HIPS sont les suivants :

application	string	facultatif	Nom de l'application
operation	string	facultatif	Opération
target	string	facultatif	Cible
action	string	facultatif	Action
rule_name	string	facultatif	Nom de la règle
rule_id	string	facultatif	ID de règle
aggregate_count	number	facultatif	Nombre de messages identiques générés par le point de terminaison entre deux réplications consécutives entre ERA Server et l'ERA Agent de gestion

4.10 Gestion de licences

ESET Remote Administrator utilise un système de licences ESET entièrement nouveau. Vous pouvez facilement gérer vos licences à l'aide de ESET Remote Administrator. Tout achat d'une licence pour un produit ESET vous donne automatiquement accès à ESET Remote Administrator.

Si vous possédez déjà un nom d'utilisateur et un mot de passe fournis par ESET et que vous voulez les convertir en clé de licence, consultez la section Convertir les informations d'identification de licence héritée. Les nom d'utilisateur et mot de passe ont été remplacés par une **clé de licence/ID public**. La **clé de licence** est une chaîne unique utilisée pour identifier le propriétaire de la licence et l'activation. Un **ID public** est une chaîne courte utilisée pour identifier la licence auprès d'un tiers (par exemple, le compte **Security Admin** chargé de la distribution d'unités).

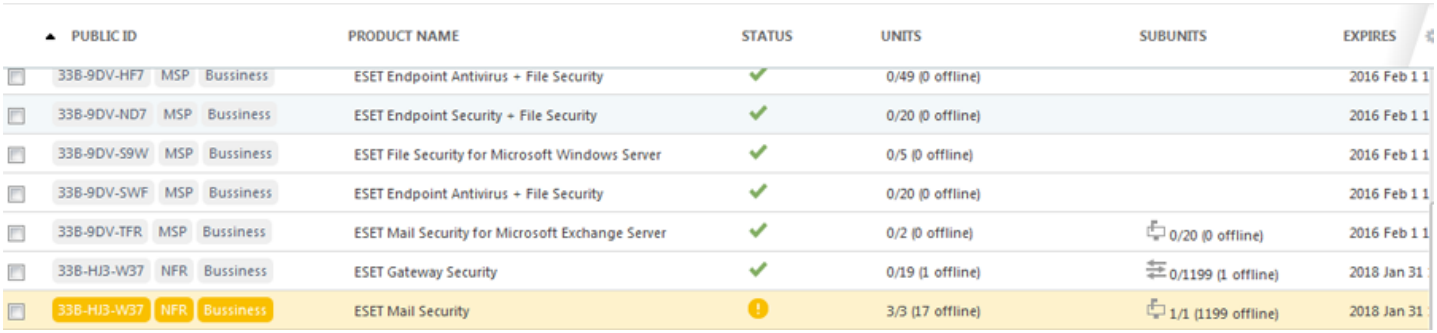
Security Admin permet de gérer des licences spécifiques. Il est différent du **Propriétaire de la licence**. Le propriétaire de la licence peut déléguer une licence à un administrateur de la sécurité pour l'autoriser à gérer des licences spécifiques. S'il accepte, des privilèges de gestion de licences lui sont octroyés. Nous recommandons à tous les propriétaires de licence de créer aussi des comptes Security Admin pour leur propre usage.

Les licences peuvent être gérées dans cette section, en ligne en cliquant sur **Ouvrir ELA** (ESET License Administrator) ou à l'aide de l'interface Web d'ESET License Administrator (reportez-vous à la section Security Admin).

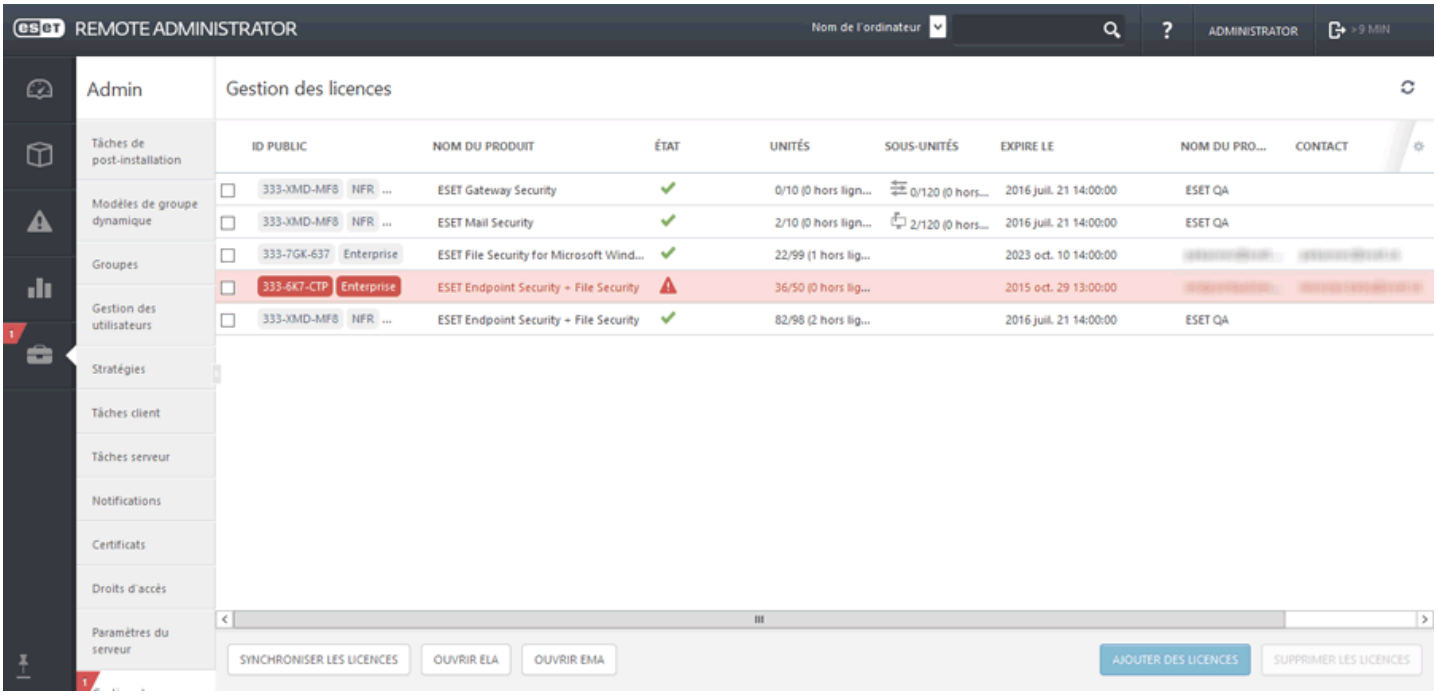
Dans ESET Remote Administrator, la section Gestion de licences est accessible à partir du menu principal sous **Admin** > **Gestion de licences**.

Il est possible d'idenitifier les licences par leur **ID public**. Dans ESET License Administrator et ERA, chaque licence est identifiée **ID public**, **Type de licence** et **Drapeaux** :

- **Type de licence** peut être **Full_Paid** - Licence payante, **Trial** - Licence d'essai et **NFR** - Licence Revente interdite.
- **Drapeaux** inclut **MSP**, **Business** et un **Consumer**.



- Le **Nom du produit** de sécurité pour lequel sa licence est destinée.
- L'**État** global de la licence (si la licence est arrivée à expiration, arrive bientôt à expiration ou est surutilisée, un message d'avertissement s'affiche ici).
- Le nombre d'**unités** pouvant être activées à l'aide de cette licence et le nombre d'unités hors ligne.
- Le nombre de **Sous-unités** de produits serveur ESET (boîtes aux lettres, protection de passerelle, connexions).
- La date d'**expiration** de la licence.
- Le **Nom du propriétaire** et le **Contact** de la licence.



État de la licence : affiché pour l'élément de menu actif.

Vert - licence activée.
Rouge - licence non enregistrée avec ESET License Administrator ou arrivée à expiration.
Orange : votre licence est épuisée ou proche de la date d'expiration (expiration dans moins de 30 jours).

Synchroniser les licences

ESET License Administrator est automatiquement synchronisé une fois par jour. Cliquez sur Synchroniser les licences pour rafraîchir immédiatement les informations des licences dans ERA.

Ajouter une licence ou une clé de licence

Cliquez sur Ajouter des licences, puis sélectionnez la méthode à utiliser pour ajouter la ou les nouvelles licences :

1. Clé de licence : saisissez une clé de licence pour une licence valide, puis cliquez sur **Ajouter une licence**. La clé de licence est vérifiée auprès du serveur d'activation puis ajoutée à la liste.
2. Informations d'identification de l'Administrateur Sécurité : connectent un compte Administrateur Sécurité et toutes ses licences à la section **Gestion de licences**.

3. Fichier de licence : ajoutez un fichier de licence (.lf), puis cliquez sur **Ajouter une licence**. Le fichier de licence est vérifié, et la licence est ajoutée à la liste.

Supprimer les licences

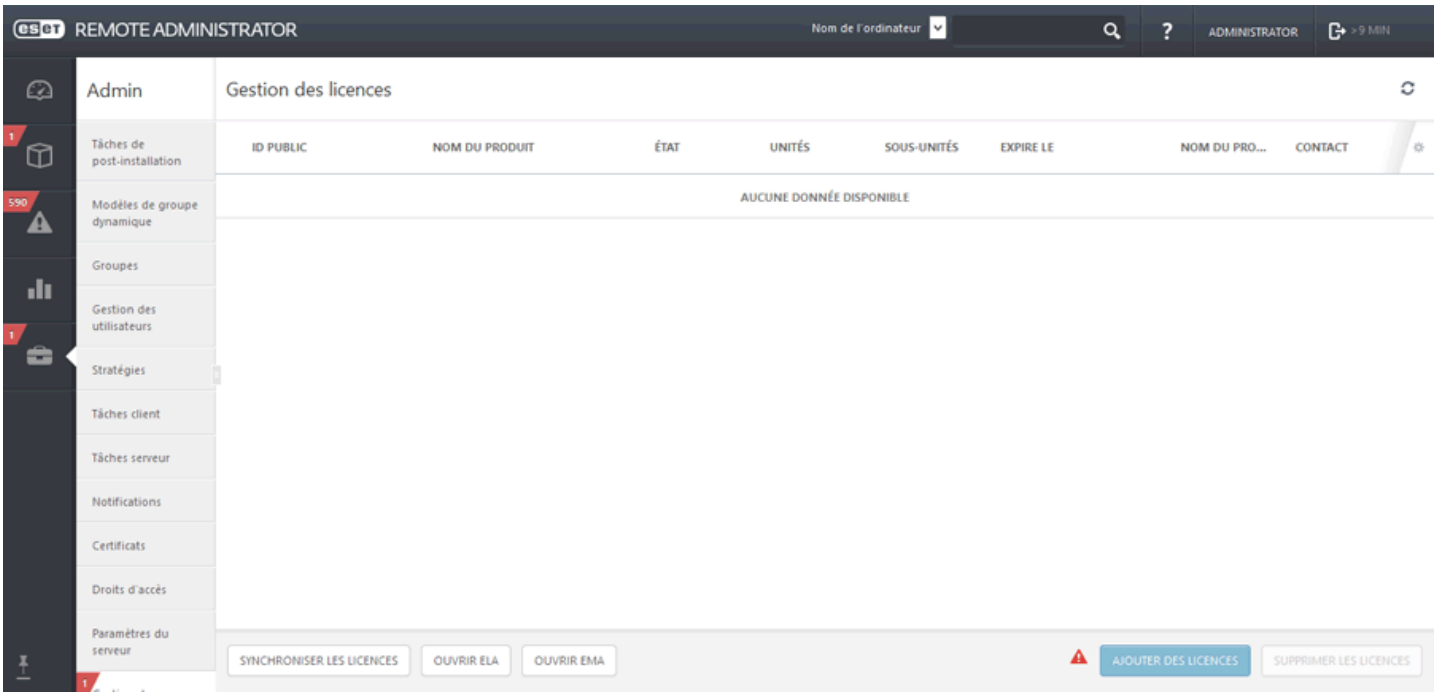
Sélectionnez une licence dans la liste ci-dessus, puis cliquez ici pour la supprimer entièrement. Il vous sera demandé de confirmer cette action. La suppression de la licence ne déclenche pas la désactivation du produit. Votre produit ESET restera activé même après que la licence a été supprimée dans ERA License Management.

Les licences peuvent être distribuées aux produits de sécurité ESET depuis ERA à l'aide de deux tâches :

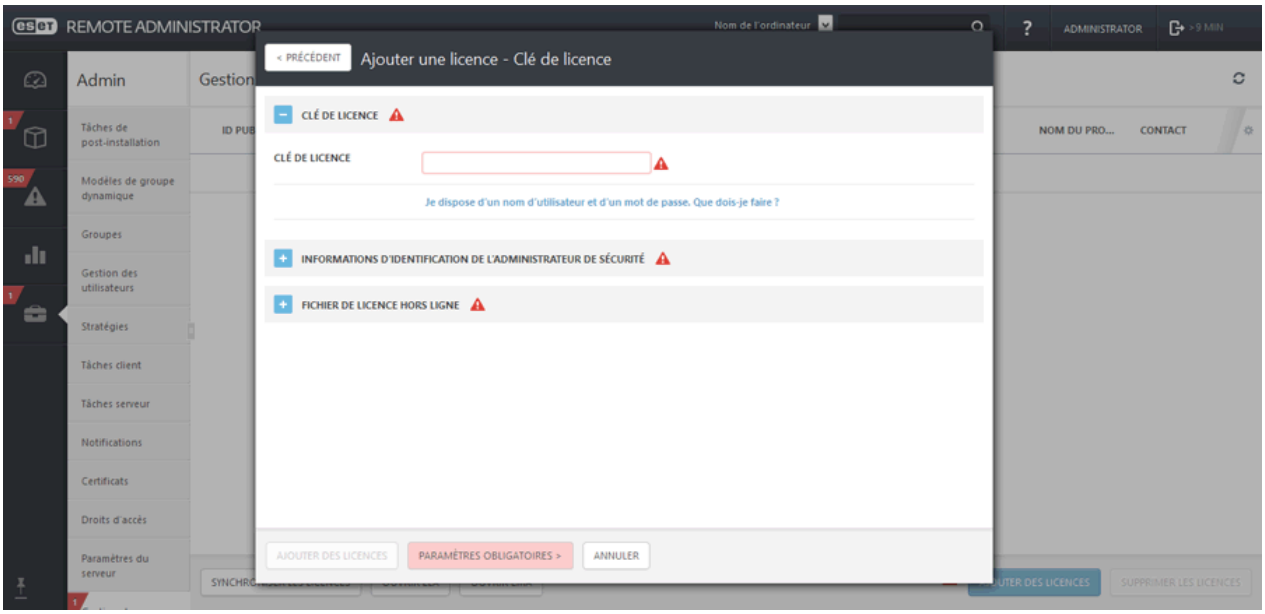
- Tâche Installer un logiciel
- Tâche Activation du produit

4.10.1 Activation

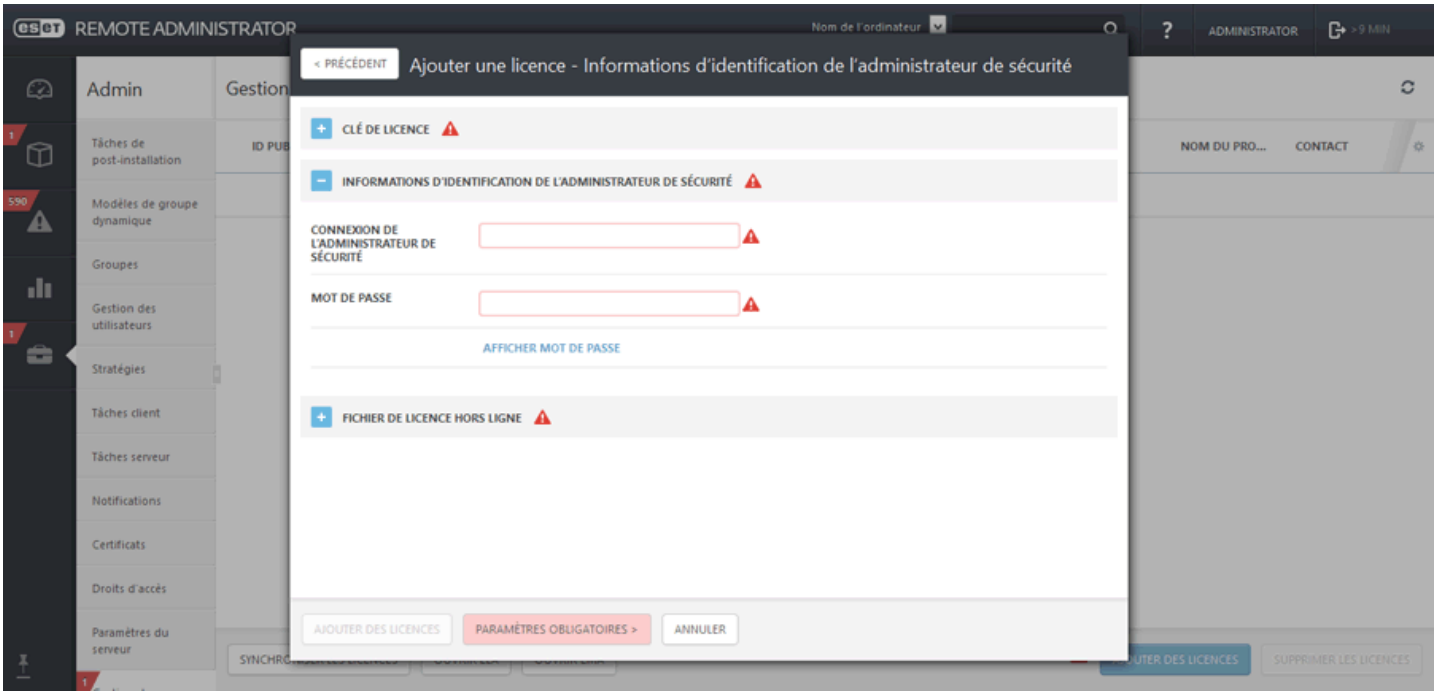
Accédez à **Admin** > **Gestion de licences**, puis cliquez sur **Ajouter des licences**.



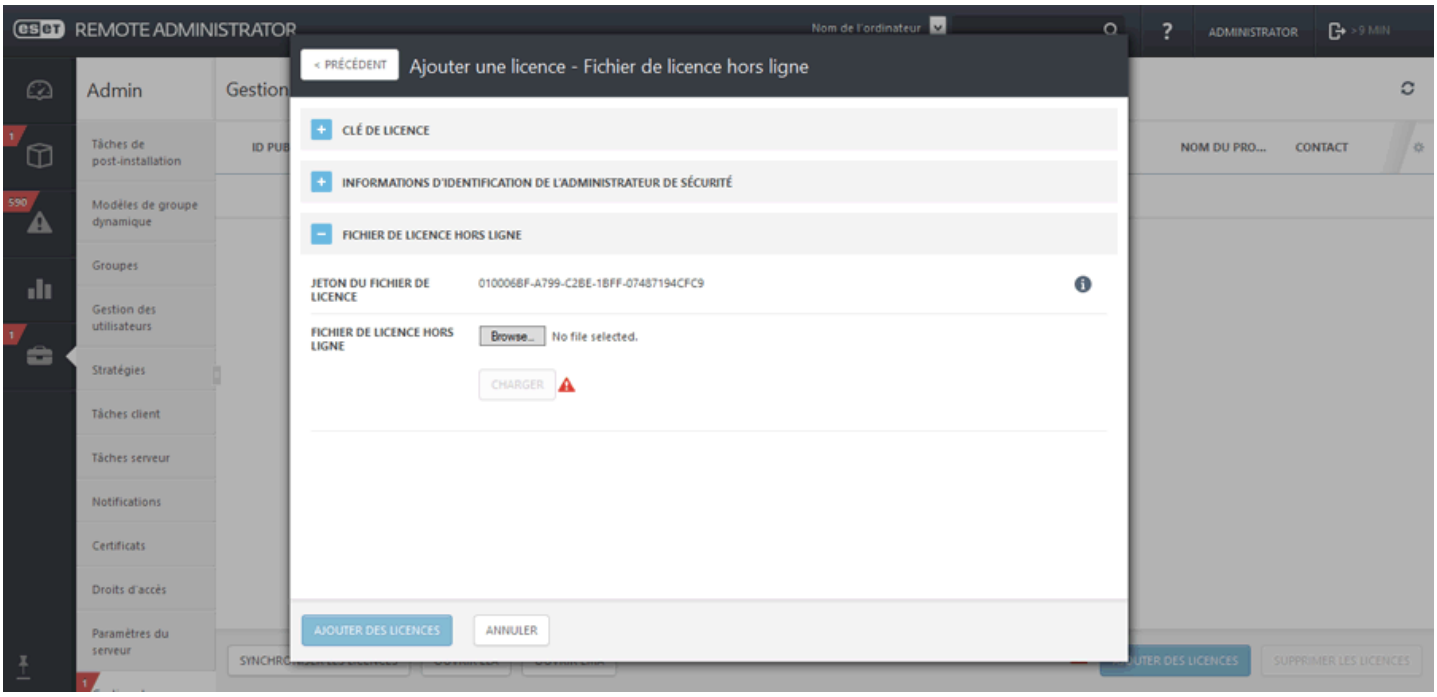
- Dans le champ Clé de licence, saisissez ou copiez et collez la **clé de licence** que vous avez reçue lors de l'achat de votre solution de sécurité ESET. Si vous utilisez des informations d'identification de licence héritée (nom d'utilisateur et mot de passe), convertissez-les en clé de licence. Si la licence n'est pas enregistrée, le processus d'enregistrement est déclenché. Celui-ci a lieu sur le portail ELA (ERA fournit l'URL valide pour l'enregistrement en fonction de l'origine de la licence).



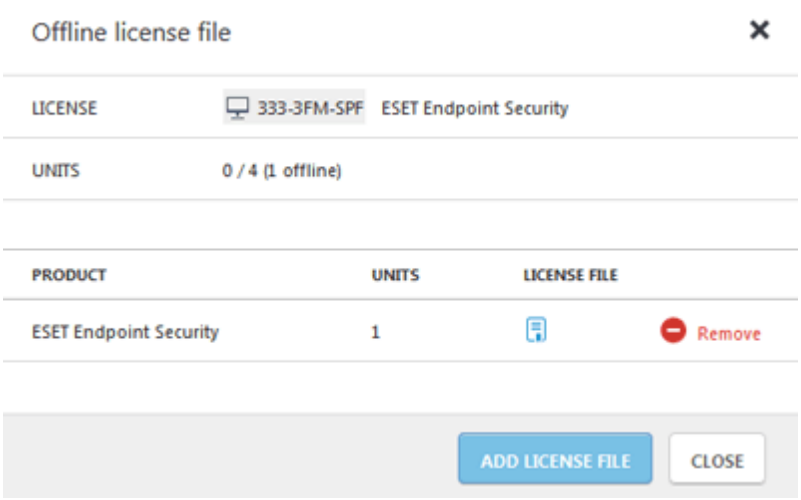
- Saisissez les informations d'identification du compte **Administrateur Sécurité** (ERA affichera ultérieurement toutes les licences déléguées dans Gestionnaire de licences ERA).



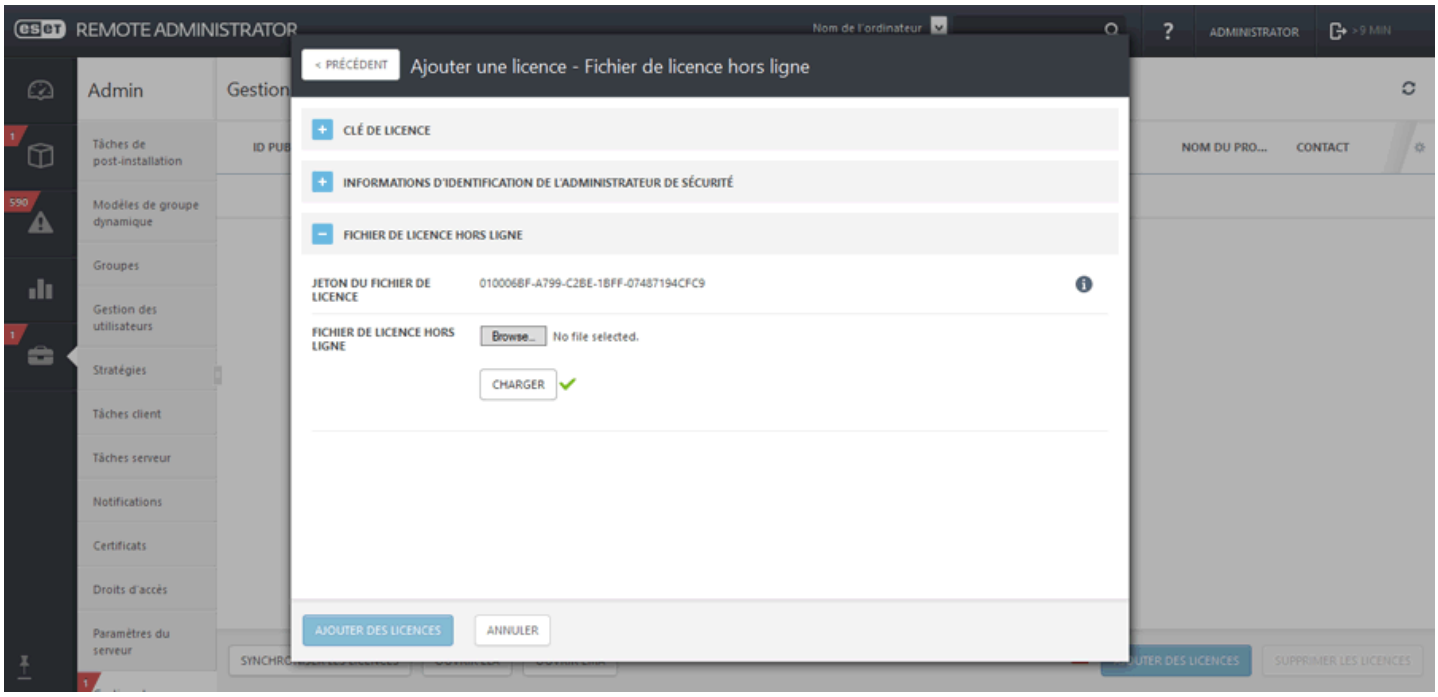
- Fournissez le **fichier de licence hors ligne** : vous devez l'exporter à partir du portail ELA et inclure les informations sur le ou les produits qu'ERA est en mesure de gérer. Vous devez entrer un **jeton de fichier de licence** sur le portail ESET License Administrator lors de la génération d'un fichier de licence hors ligne, sinon le fichier de licence n'est pas accepté par ESET Remote Administrator.



Cliquez sur le symbole de document pour enregistrer le fichier de licence hors ligne.



Retournez dans Gestion de licences ERA, cliquez sur Ajouter des licences, accédez au fichier de licence hors ligne que vous avez exporté dans ELA, puis cliquez sur **Charger**.


REMOTE ADMINISTRATOR
Nom de l'ordinateur
ADMINISTRATOR
Admin
Tâches de post-installation
Modèles de groupe dynamique
Groupes
Gestion des utilisateurs
Stratégies
Tâches client
Tâches serveur
Notifications
Certificats
Droits d'accès
Paramètres du serveur
NOM DU PRO...
CONTACT
« PRÉCÉDENT
Ajouter une licence - Fichier de licence hors ligne
CLÉ DE LICENCE
INFORMATIONS D'IDENTIFICATION DE L'ADMINISTRATEUR DE SÉCURITÉ
FICHIER DE LICENCE HORS LIGNE
JETON DU FICHIER DE LICENCE
0100068F-A799-C2BE-1BFF-07487194CFC9
FICHIER DE LICENCE HORS LIGNE
Browse...
No file selected.
CHARGER
AJOUTER DES LICENCES
ANNULER
SUPPRIMER LES LICENCES

5. Outil de diagnostic

L'outil de diagnostic fait partie de tous les composants ERA. Il sert à collecter et à compresser les journaux qui sont utilisés par les développeurs pour résoudre les problèmes liés aux composants du produit. Exécutez l'outil de diagnostic, sélectionnez un dossier racine où enregistrer les journaux, puis choisissez les actions à exécuter (voir la section **Actions** ci-dessous).

Emplacement de l'**outil de diagnostic** :

Windows

Dossier *C:\Program Files\ESET\RemoteAdministrator\<product>* , fichier appelé **Diagnostic.exe**.

Linux

Chemin d'accès sur le serveur : */opt/eset/RemoteAdministrator/<product>/*, exécutable **Diagnostic<produit>** (en un seul mot, par exemple **DiagnosticServer**, **DiagnosticAgent**)

Actions

- **Journaux de vidage** : un dossier de journaux est créé où tous les journaux sont enregistrés.
- **Processus de vidage** : un dossier est créé. Un fichier d'image mémoire de processus est généralement créé en cas de détection de problème. Lorsqu'un problème grave est détecté, un fichier d'image mémoire est créé par le système. Pour le vérifier manuellement, accédez au dossier %temp% (sous Windows) ou au dossier /tmp/ (sous Linux) et insérez un fichier dmp.
  REMARQUE : le service (Agent, Proxy, Server, RD Sensor, FileServer) doit être en cours d'exécution.
- **Informations générales sur l'application** : le dossier GeneralApplicationInformation est créé avec le fichier GeneralApplicationInformation.txt. Ce fichier contient des informations textuelles comprenant le nom et la version du produit actuellement installé.
- **Configuration des actions** : un dossier de configuration est créé dans lequel le fichier storage.lua est enregistré.

6. FAQ

Q : Il y a un champ d'informations personnalisées sur le client dans la version V5. Cela permet à nos MSP de déterminer à qui appartiennent les clients. Cette possibilité existe-t-elle dans la version V6 ?
R : Les groupes dynamiques sont un peu différents (ils sont évalués au niveau de l'agent) et n'autorisent pas la création de « paramètres personnalisés/d'identification ». Vous pouvez cependant générer un rapport pour afficher les données client personnalisées.

Q : Comment résoudre l'erreur « Échec de la connexion, état **"non connecté"** » ?
R : Vérifiez si le service ERA Server ou MS SQL Server est en cours d'exécution. Si ce n'est pas le cas, démarrez-le. S'il fonctionne, relancez le service, actualisez la console Web puis essayez à nouveau de vous connecter.

Q : À quoi sert le groupe « Perdu et trouvé » ?
R : Tous les ordinateurs connectés à ERA Server qui ne sont pas membres d'un groupe statique sont automatiquement affichés dans ce groupe. Vous pouvez travailler avec le groupe et les ordinateurs qui le composent de la même manière qu'avec les ordinateurs appartenant à n'importe quel autre groupe statique. Ce groupe peut être renommé ou déplacé dans un autre groupe, mais il ne peut pas être supprimé.

Q : Comment créer un profil de mise à jour double ?
R : Pour obtenir des instructions détaillées, reportez-vous à cet article de la base de connaissances ESET.

Q : Comment actualiser les informations d'une page ou d'une section de la page sans actualiser l'ensemble de la fenêtre du navigateur ?
R : Cliquez sur **Rafraîchir** dans le menu contextuel situé dans la partie supérieure droite d'une section de la page.

Q : Comment effectuer une installation silencieuse de ERA Agent ?
R : Vous pouvez utiliser un GPO comme script de démarrage à cet effet. À l'heure actuelle, il n'est pas possible d'effectuer une installation silencieuse depuis la console Web.

Q : Rogue Detection Sensor ne détecte pas tous les clients sur le réseau.
R : RD Sensor écoute passivement les communications réseau sur le réseau. Si les PC ne sont pas en communication, ils ne sont pas répertoriés par RD Sensor. Vérifiez vos paramètres DNS pour vous assurer que la communication n'est pas bloquée en raison de problèmes liés à la recherche DNS.

Q : Comment réinitialiser le nombre de menaces actives affichées dans ERA après le nettoyage des menaces ?
R : Pour réinitialiser le nombre de menaces actives, il convient de lancer une analyse complète (approfondie) du ou des ordinateurs cibles à l'aide d'ERA. Si vous avez nettoyé une menace manuellement, vous pouvez mettre l'alerte correspondante en mode silence.

Q : Comment configurer une expression CRON pour l'intervalle de connexion d'ERA Agent ?
R : P_REPLICATION_INTERVAL accepte une expression CRON.
La valeur par défaut est « R R/20 * * * ? * » correspondant à des connexions à des secondes aléatoires (R=0-60) chaque 20e minute aléatoire (par exemple 3, 23, 43 ou 17,37,57). Les valeurs aléatoires doivent être utilisées pour l'équilibrage de la charge dans le temps. Ainsi, chaque ERA Agent se connecte à une heure aléatoire différente. Si un CRON précis est utilisé, par exemple « 0 * * * * ? * », tous les agents ainsi paramétrés se connecteront en même temps (chaque minute à :00 seconde), et il y aura des pics de charge sur le serveur à ce moment.

Q : Comment créer un nouveau groupe dynamique pour un déploiement automatique ?
R : Pour obtenir des instructions détaillées, reportez-vous à cet article de la base de connaissances ESET.

Q : Lorsque j'importe un fichier contenant la liste des ordinateurs à ajouter à ERA, quel format de fichier dois-je utiliser ?
R : Vous devez utiliser un fichier comportant les lignes suivantes :
Tous\Groupe1\GroupeN\Ordinateur1
Tous\Groupe1\GroupeM\OrdinateurX
Tous est le nom requis pour le groupe racine.

Q : Quels certificats tiers peuvent être utilisés pour signer des certificats ERA ?
R : Le certificat doit être un certificat AC (ou AC intermédiaire) muni de l'indicateur 'keyCertSign' de la contrainte 'keyUsage'. Cela signifie que ce certificat peut être utilisé pour signer d'autres certificats.

Q : Comment puis-je **réinitialiser le mot de passe de l'administrateur** pour la console Web (il s'agit du mot de passe saisi pendant la configuration sur les systèmes d'exploitation Windows) ?
R : Il est possible de réinitialiser le mot de passe en exécutant le programme d'installation du serveur et en choisissant **Réparer**. Il est possible que vous ayez besoin du mot de passe de la base de données ERA si vous n'avez pas utilisé l'authentification Windows lors de la création de la base de données.
REMARQUE : vous devez faire attention, car certaines des opérations de réparation peuvent éventuellement entraîner la suppression des données stockées.

Q : Comment puis-je **réinitialiser le mot de passe de l'administrateur** pour la console Web (Linux, saisi pendant la configuration) ?
R : S'il existe un autre utilisateur dans ERA disposant des droits suffisants, vous devriez pouvoir réinitialiser le mot de passe du compte administrateur. Mais si l'administrateur est le seul compte dans le système (il est créé lors de l'installation), vous ne pouvez pas réinitialiser ce mot de passe.
Réinstallez ERA, recherchez l'entrée de la base de données correspondant au compte Administrateur, et mettez l'ancienne base de données à jour selon cette entrée. Généralement, la meilleure solution consiste à sauvegarder les informations d'identification du compte Administrateur dans un endroit sûr et de créer de nouveaux utilisateurs avec le jeu de privilèges souhaité. Dans l'idéal, le compte Administrateur ne doit pas être utilisé à d'autres fins que pour la création d'autres utilisateurs ou la réinitialisation de leurs comptes.

Q : Comment résoudre les problèmes si **RD Sensor** ne détecte rien ?
R : Si votre système d'exploitation est détecté en tant que périphérique réseau, il ne sera pas communiqué à ERA en tant qu'ordinateur. Les périphériques réseau (imprimantes, routeurs) sont exclus. RD Sensor a été compilé avec *libpcap version 1.3.0*, vérifiez que cette version est bien installée sur votre système. La seconde exigence concerne l'existence d'un réseau ponté depuis la machine virtuelle sur laquelle est installé RD Sensor. Si ces exigences sont satisfaites, exécutez nmap avec détection du système d'exploitation (http://nmap.org/book/osdetect-usage.html) pour vérifier si l'OS de votre ordinateur peut être détecté.

7. À propos d'ESET Remote Administrator

Cette fenêtre comporte des informations détaillées sur la version d'ESET Remote Administrator installée, et répertorie les modules du programme installés. La partie supérieure de la fenêtre comporte des informations sur le système d'exploitation et les ressources du système. Vous verrez aussi une licence utilisée par ERA pour télécharger les mises à jour des modules (la même que pour activer ERA).

REMARQUE : Pour obtenir des instructions afin de connaître la version d'un composant ERA, reportez-vous à notre article de la base de connaissances.