ivanti

Neuf façons de limiter les utilisateurs disposant de privilèges d'administrateur Windows

Table des matières

Introduction

Combien de comptes Administrateur Windows existe-t-il dans votre entreprise ? Si la réponse est « beaucoup », il est probable qu'un grand nombre de ces comptes à privilèges soient utilisés par des personnes qui n'ont pas besoin d'un tel niveau d'accès dans le cadre de leur rôle, ou qui nécessitent un accès avec privilèges uniquement pour une ou deux tâches.

L'attribution de droits Admin complets à des utilisateurs qui ne sont pas formés à être administrateur IT, augmente les risques de sécurité, les coûts de gestion et complique la mise en conformité. Ce livre blanc présente neuf restrictions simples que vous pouvez mettre en place immédiatement avec Ivanti® Security Controls. Combinées, elles offrent les avantages suivants :

- Réduire la probabilité qu'une personne modifie par inadvertance des paramètres d'administration et n'ait besoin de l'aide du département IT pour les corriger.
- Rendre plus difficile pour une personne de modifier ou de désactiver certaines protections sur vos postes clients.

Pour renforcer la protection, votre objectif à long terme doit être de remplacer les comptes administrateurs inutiles par des comptes utilisateurs standards, et d'adopter l'approche des moindres privilèges. Vous pouvez pour ce faire utiliser Ivanti Security Controls, mais ce n'est pas le sujet de ce livre blanc.

Les fonctions de restriction des administrateurs qui n'en sont pas réellement, font partie du module Privilege Management d'Application Control, lequel est un module d'Ivanti Security Controls. Le moteur Application Control qui fait partie de l'agent Security Controls, s'exécute sur chaque poste de travail. Ce moteur applique un ensemble de règles définies dans une configuration, et détermine le comportement d'Application Control. Les captures d'écran de ce livre blanc montrent la configuration requise pour chacune des restrictions.

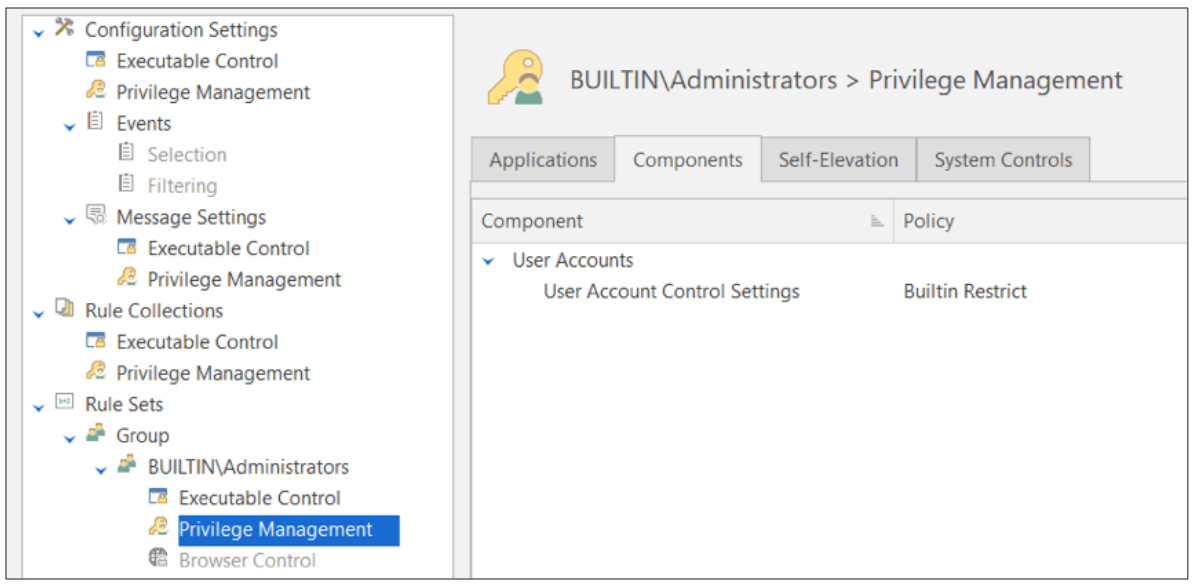
Restriction 1 – Interdire aux utilisateurs de modifier les paramètres de Contrôle de Compte d'Utilisateur (UAC)

Ivanti recommande que tous vos utilisateurs, y compris ceux dotés de comptes Admin, activent le contrôle de compte d'utilisateur. Sur son site Web, Microsoft explique :

> *Le contrôle de compte d'utilisateur (UAC) empêche les programmes malveillants d'endommager un ordinateur et aide les organisations à déployer des postes de travail mieux gérés. Avec le contrôle de compte d'utilisateur, les applications et les tâches s'exécutent toujours dans le contexte de sécurité d'un compte non-administrateur, sauf si un administrateur autorise expressément un accès de niveau administrateur au système. Le contrôle de compte d'utilisateur peut bloquer l'installation automatique d'applications non autorisées et empêcher les modifications accidentelles de paramètres système.*

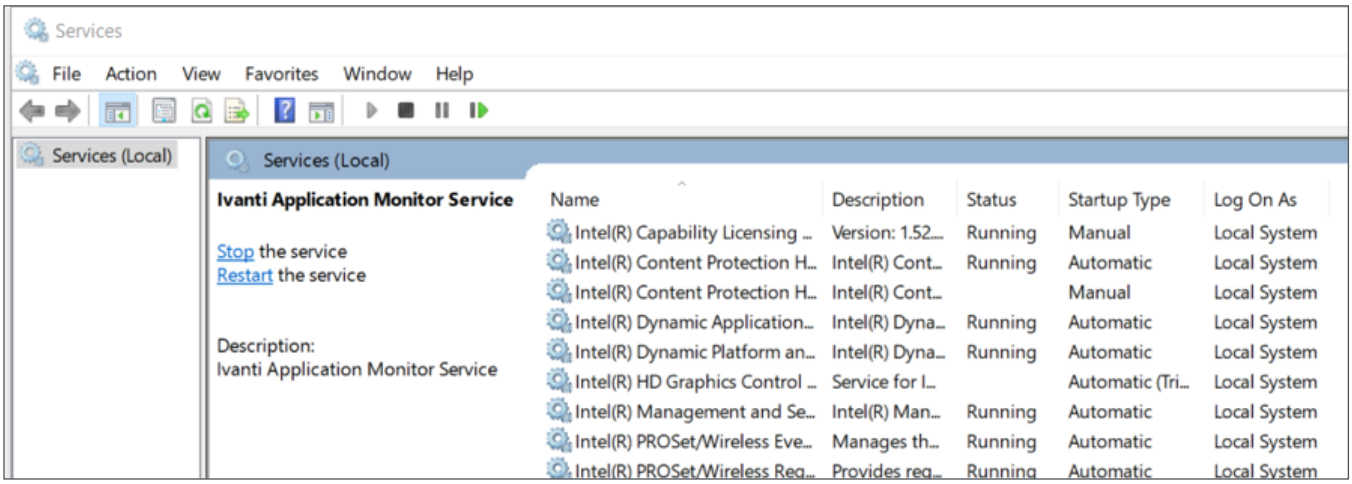
Il est conseillé d'activer le contrôle de compte d'utilisateur sur toutes les machines et de sélectionner le paramètre « Toujours m'avertir ». Vous activez cette fonction à l'aide d'une stratégie de groupe (GPO). Ivanti Security Controls peut empêcher les administrateurs de désactiver le contrôle de compte d'utilisateur.

Dans l'éditeur de configuration illustré ci-après, naviguez jusqu'à l'onglet « Composants » et sélectionnez le composant Windows « Paramètres de contrôle de compte d'utilisateur ». Définissez ensuite la stratégie de l'élément de règle sur « Restriction intégrée ».



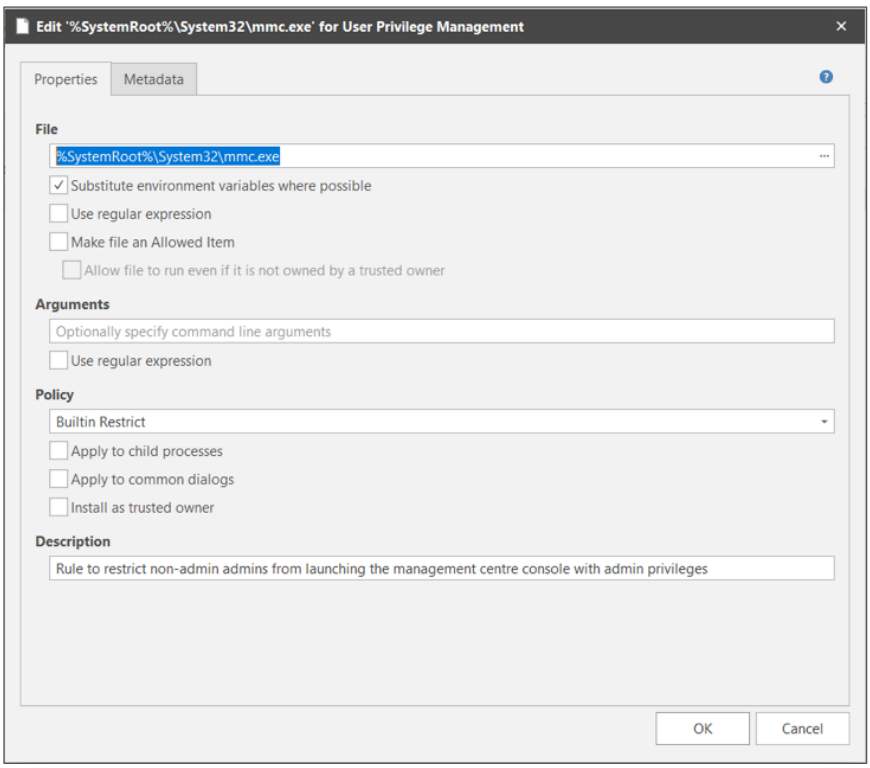
Restriction 2 – Interdire aux utilisateurs d'exécuter la console MMC avec des privilèges Admin

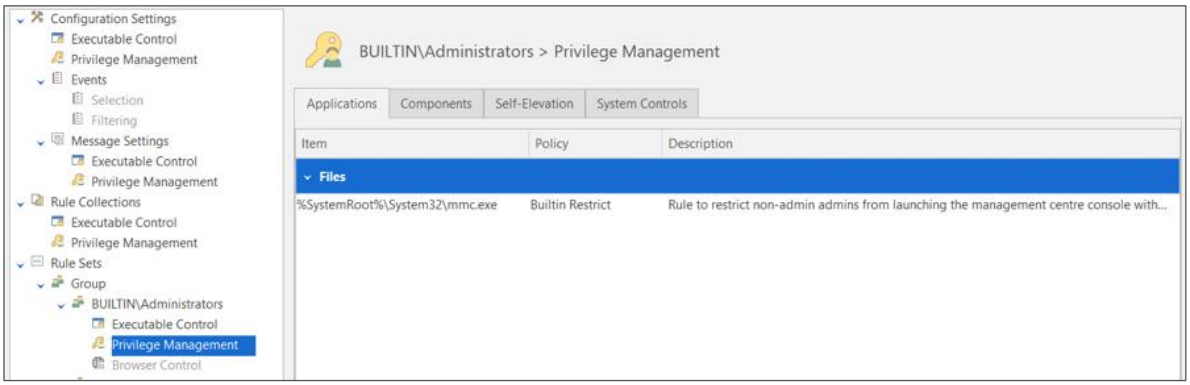
La console MMC (Microsoft Management Console) est une structure qui fournit aux utilisateurs une interface pour la gestion et la configuration du système d'exploitation. Elle permet à l'utilisateur de charger des composants logiciels enfichables. Chacun d'entre eux est un outil servant à gérer une fonction Windows spécifique. Par exemple, le logiciel enfichable « Services » fournit un outil pour gérer les services Windows.



Ces outils peuvent être très puissants. Par exemple, dans le logiciel enfichable « Services », un utilisateur doté de privilèges peut arrêter des services. Si l'un des services arrêtés fait partie de votre système antivirus, cela peut désactiver l'analyse antivirus des téléchargements et augmenter les risques de malware.

Avec Ivanti Security Controls, vous pouvez empêcher les utilisateurs dotés d'un compte Admin d'exécuter la console MMC avec des privilèges Admin. Dans l'éditeur de configuration, créez une règle de fichier dans l'onglet « Applications ». Définissez ensuite la stratégie de l'élément de règle sur « Restriction intégrée ».



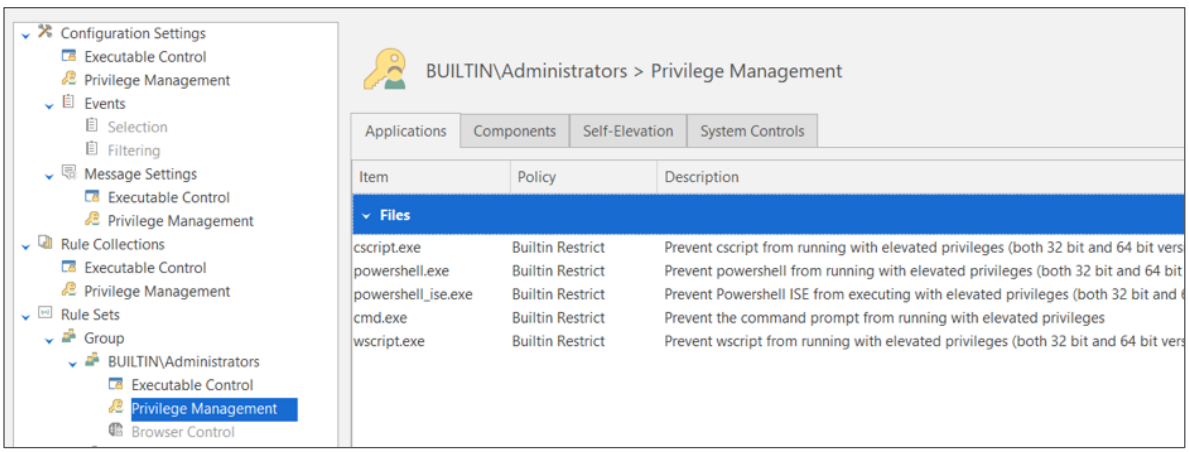


Restriction 3 – Interdire aux utilisateurs d'exécuter des commandes ou des scripts avec des privilèges Admin

Windows prend en charge des méthodes alternatives pour interagir avec le système d'exploitation à l'aide de commandes spécifiques émises via des interpréteurs de ligne de commande ou l'exécution de scripts. La première méthode est généralement utilisée pour la gestion et la seconde, pour l'automatisation. Les interfaces de ligne de commande fournies avec Windows sont l'invite de commande et Windows PowerShell. Le système d'exploitation inclut également WSH (Windows Script Host), qui peut servir à exécuter des scripts dans différents langages de script.

Toute personne dotée de privilèges Administrateur peut exécuter des commandes ou des scripts, ce qui constitue une méthode alternative, dans de nombreux cas, pour contourner les restrictions fondées sur le GUI présentées dans ce document. Pour cette raison, restreignez les interpréteurs de ligne de commande et Windows Script Host.

Application Control peut vous y aider. Pour configurer cette restriction, créez une règle de fichier pour chaque interpréteur de ligne de commande, ainsi que pour les versions Windows et console de Windows Script Host. Créez chaque élément de règle dans l'onglet « Applications » et définissez sa stratégie sur « Restriction intégrée ».

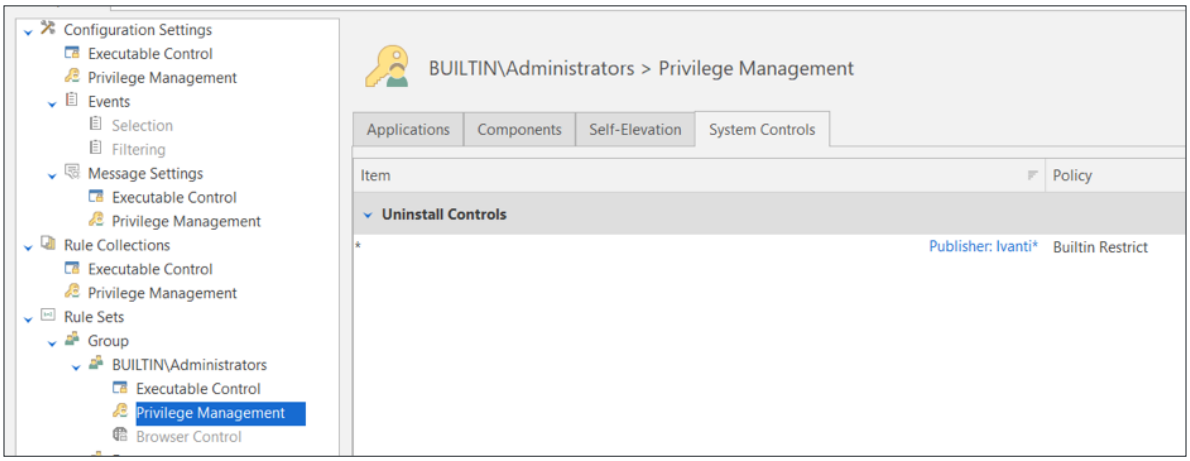


S'il est nécessaire d'exécuter un script avec des privilèges élevés, Application Control peut également être configuré pour autoriser l'opération uniquement pour ce script.

Restriction 4 – Interdire aux utilisateurs de désinstaller les logiciels tiers qui protègent votre système

Ivanti Security Controls fonctionne avec un agent, installé sur vos postes clients pour les protéger. Cet agent peut être désinstallé par un utilisateur doté de privilèges Admin et vous perdez alors cette protection. Pour éviter cela, configurez une règle de désinstallation dans l'onglet Contrôles Système. Il est possible de cibler la règle de désinstallation sur une version spécifique d'une application ou d'utiliser des caractères génériques pour que la règle s'applique plus largement.

Dans la capture d'écran ci-après, seul l'éditeur est défini. Aucune application correspondant à l'éditeur ne peut être désinstallée par un utilisateur avec des privilèges Admin.

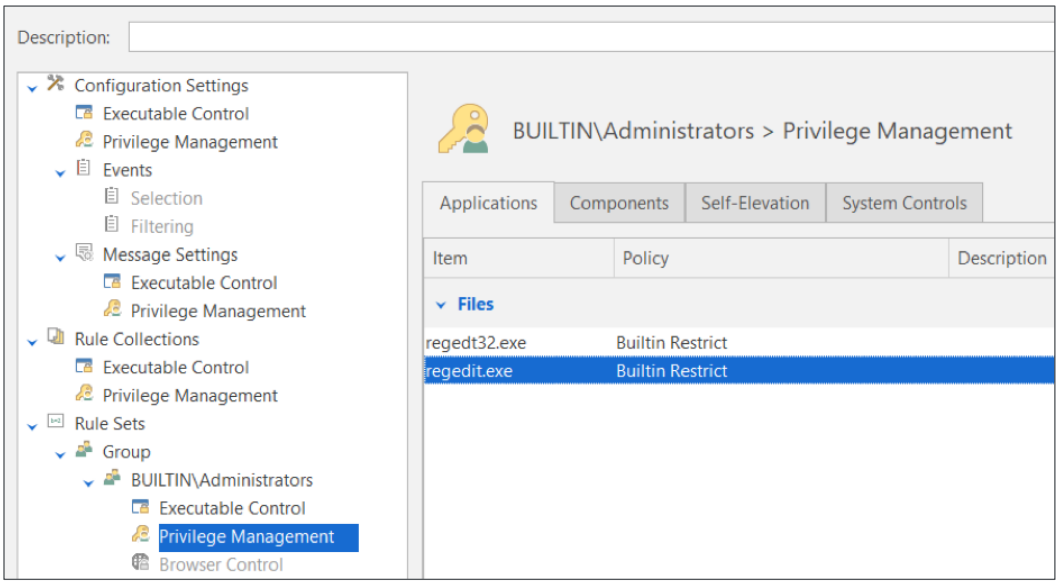


Vous pouvez également utiliser Ivanti Security Controls pour interdire la désinstallation d'autres logiciels tiers en créant des règles similaires.

Restriction 5 – Interdire aux utilisateurs de modifier les paramètres système dans le registre

Le registre Windows est important parce qu'il stocke des informations vitales concernant un poste client Windows et sa configuration, ainsi que des données sur tous les programmes installés. En leur donnant la possibilité d'accéder directement aux clés de registre et de les modifier, les privilèges administrateurs permettent aux utilisateurs de naviguer dans les stratégies de gestion centralisée chaque fois qu'ils le souhaitent et de modifier les paramètres. Cet accès représente une autre méthode qui permet aux utilisateurs de contourner un grand nombre des protections décrites dans le présent document.

Il faut au minimum restreindre l'accès avec privilèges au registre. Dans Ivanti Security Controls, vous configurez cette restriction en créant des règles de fichier dans l'onglet « Applications » pour chaque application qui modifie le registre, et en configurant leur stratégie sur « Restriction intégrée ».

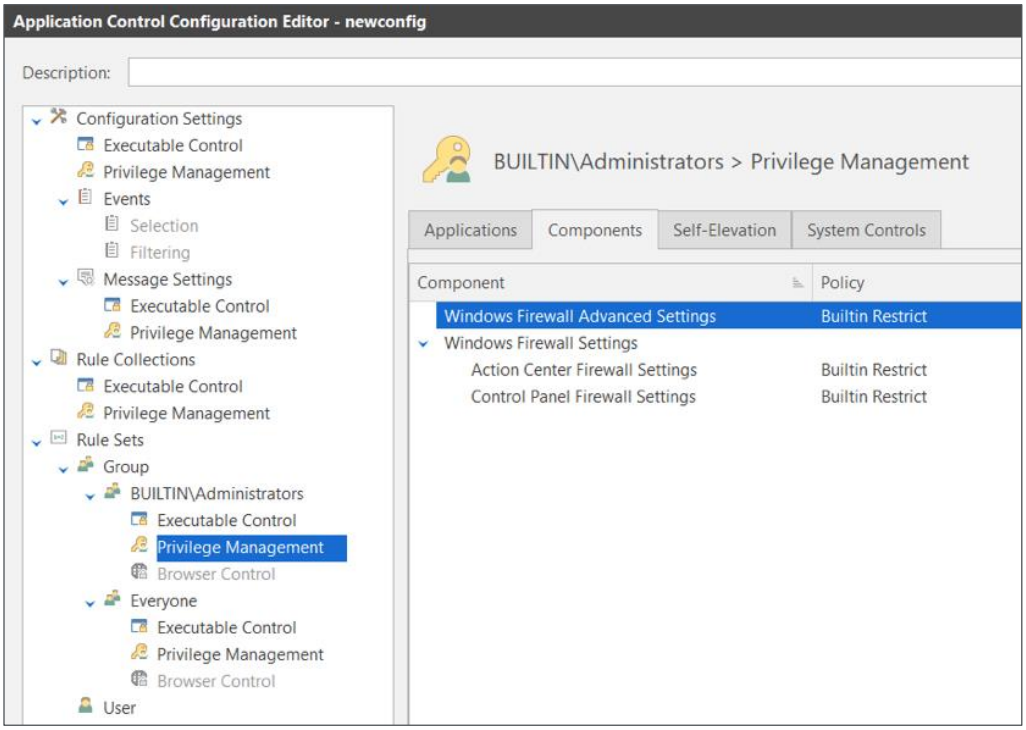


Si l'on va plus loin, Ivanti Security Controls peut même interdire à un utilisateur (avec ou sans droits Admin) tout accès à l'application utilisée pour modifier le registre.

Restriction 6 – Interdire aux utilisateurs de désactiver ou de modifier les paramètres de pare-feu des postes clients

Un pare-feu est un dispositif de sécurité réseau qui surveille le trafic vers ou depuis votre réseau, et autorise ou bloque ce trafic en fonction de l'ensemble des règles de sécurité définies. Avec les pare-feux, il est plus difficile pour les logiciels malveillants de se propager sur un réseau.

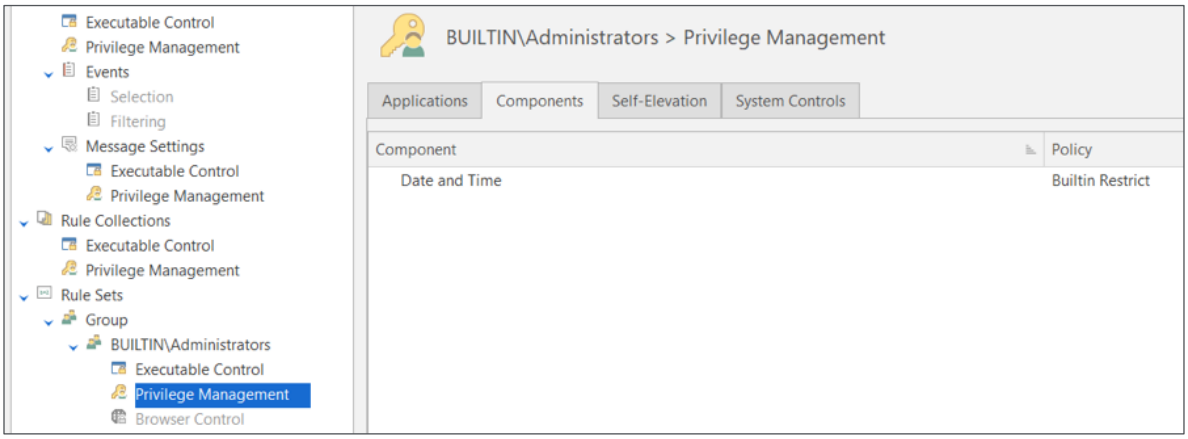
Si vous utilisez le pare-feu Windows Defender, nous vous recommandons d'interdire la désactivation de cette fonction. Pour ce faire, sélectionnez les composants Windows suivants sous le nœud « Gestion des privilèges » et définissez la stratégie de chacun d'eux sur « Restriction intégrée ».



Restriction 7 – Interdire aux utilisateurs de changer la date et l'heure

Les administrateurs non Admin peuvent changer la date et l'heure. Cela peut paraître insignifiant, mais l'opération peut avoir un profond impact. Si la date ou l'heure est incorrecte, de nombreuses applications peuvent avoir un comportement inattendu. De plus, les journaux portent alors des horodatages incorrects, ce qui peut, potentiellement, invalider l'audit et compliquer le dépannage. Autre raison pour cette restriction : certaines personnes peuvent tenter d'utiliser cette méthode pour contourner les restrictions de licence et reculer l'horloge pour continuer à utiliser sans cesse la même licence d'évaluation.

Ivanti Security Controls peut empêcher les administrateurs de changer la date et l'heure. Sélectionnez le composant « Date et heure » dans l'onglet « Composants Windows ». Définissez ensuite la stratégie du composant sur « Restriction intégrée ».



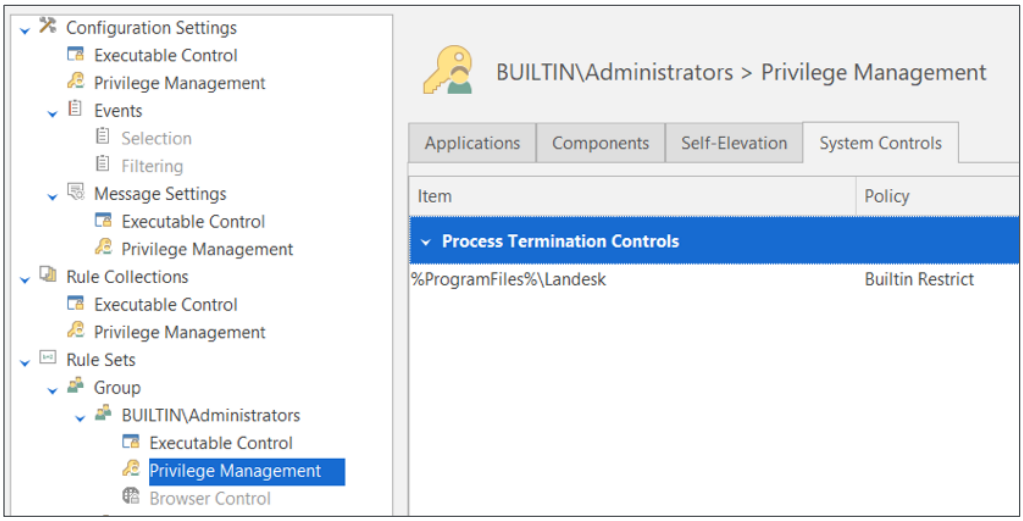
Il est également possible de changer la date et l'heure via une ligne de commande élevée, à l'aide de commandes de date et d'heure. Pour vous protéger de ce comportement, appliquez la restriction 3.

Restriction 8 – Interdire aux utilisateurs d'arrêter des processus

Les utilisateurs dotés de privilèges Admin peuvent arrêter des processus en cours d'exécution. Par exemple : 1) utilisation du Gestionnaire de tâches et clic sur « Fin de tâche », ou 2) exécution de l'Explorateur de processus et sélection de l'option « Arrêter le

processus ». Ces méthodes sont des alternatives qui permettent aux utilisateurs de désactiver les logiciels de protection exécutés sur leur système et, par conséquent, d'augmenter les risques de sécurité.

Pour éviter l'arrêt du logiciel d'agent Ivanti Security Controls, ajoutez à la configuration une règle de dossier « Contrôle Arrêt de processus », dans l'onglet « Contrôles système ». La règle doit spécifier le dossier où réside le logiciel à protéger (dans ce cas, %ProgramFiles%\Landesk). Sa stratégie doit être définie sur « Restriction intégrée ».



Vous pouvez également ajouter d'autres règles à la configuration AC pour interdire l'arrêt d'autres logiciels.

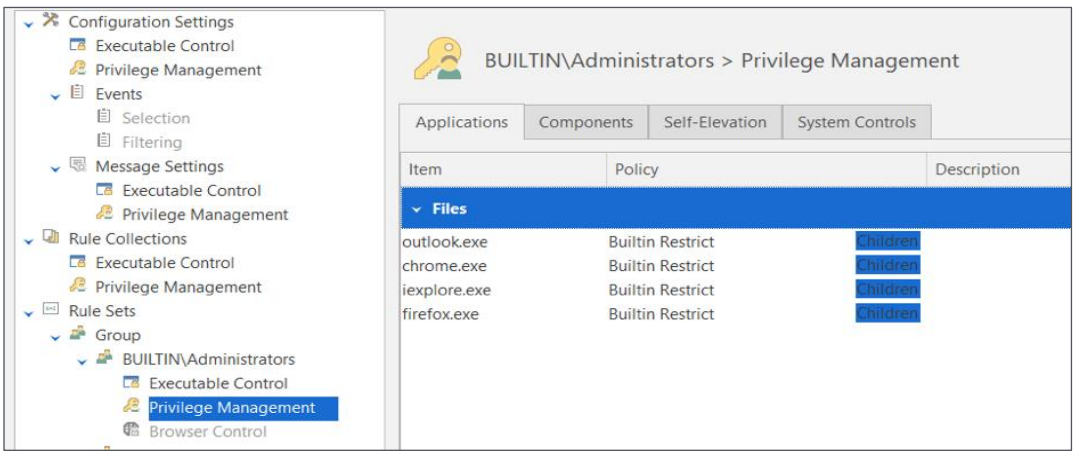
Notez que cette restriction empêche l'arrêt des processus par certaines applications d'interface utilisateur (GUI) mais que l'arrêt peut également passer par une invite de commande élevée, par exemple avec la commande « taskkill ». La restriction 3 permet de l'interdire.

Restriction 9 – Interdire aux utilisateurs d'élever des applications susceptibles d'introduire des malwares

Les utilisateurs dotés de privilèges Admin peuvent lancer n'importe quelle application avec des privilèges élevés. Certaines de ces applications (comme l'e-mail et le navigateur) peuvent introduire un malware sur le poste client. En général, ces applications ne s'exécutent pas avec des droits élevés, sauf si un utilisateur doté de privilèges Admin les élève volontairement. Cette restriction les en empêche.

Si l'une de ces applications s'exécute avec des privilèges Admin, tous les processus enfants générés dynamiquement qui contiennent un malware s'exécutent également avec des droits Admin. Par conséquent, il faut restreindre ces applications pour qu'elles ne puissent s'exécuter qu'avec des privilèges standards.

Dans Ivanti Security Controls, vous configurez cette restriction en créant des règles de fichier dans l'onglet « Applications » pour chaque application d'e-mail ou de navigateur, et en configurant leur stratégie sur « Restriction intégrée ». De plus, vous devez sélectionner l'option d'application aux processus enfants pour chacun de ces éléments. La capture d'écran ci-dessous montre les plus courants :



Et ensuite ?

Ceci complète la présentation des restrictions utilisées pour : 1) limiter les risques de voir des utilisateurs Admin qui ne sont pas réellement administrateurs changer par inadvertance des paramètres d'administration et demander l'aide du département IT pour corriger le problème, ou 2) rendre plus difficile pour les utilisateurs non administrateurs la modification ou la désactivation de certaines protections sur vos postes clients.

Vous voulez découvrir par vous-même comment Application Control peut vous aider ? Demandez une démo.

En savoir plus **www.ivanti.fr** **+33 (0)1 49 03 77 80** **contact@ivanti.fr**