Intégration au service Microsoft Defender ATP

10/04/2020 • 8 minutes de lecture •

Dans cet article

S'applique à:

- Microsoft Defender– Protection avancée contre les menaces (MicrosoftDefender ATP)

Le déploiement de Microsoft Defender ATP est un processus en trois étapes:

Phase 1: préparation

Phase 2: configuration

Étape 3: intégration

Vous êtes actuellement dans la phase d'intégration.

Pour déployer Microsoft Defender ATP, vous devez utiliser des appareils intégrés au service. Selon l'architecture de votre environnement, vous devez utiliser l'outil de gestion approprié qui répond à vos besoins.

Le Guide de déploiement utilise le Microsoft Endpoint Configuration Manager comme outil de gestion pour illustrer un déploiement de bout en bout.

Cet article vous guidera:

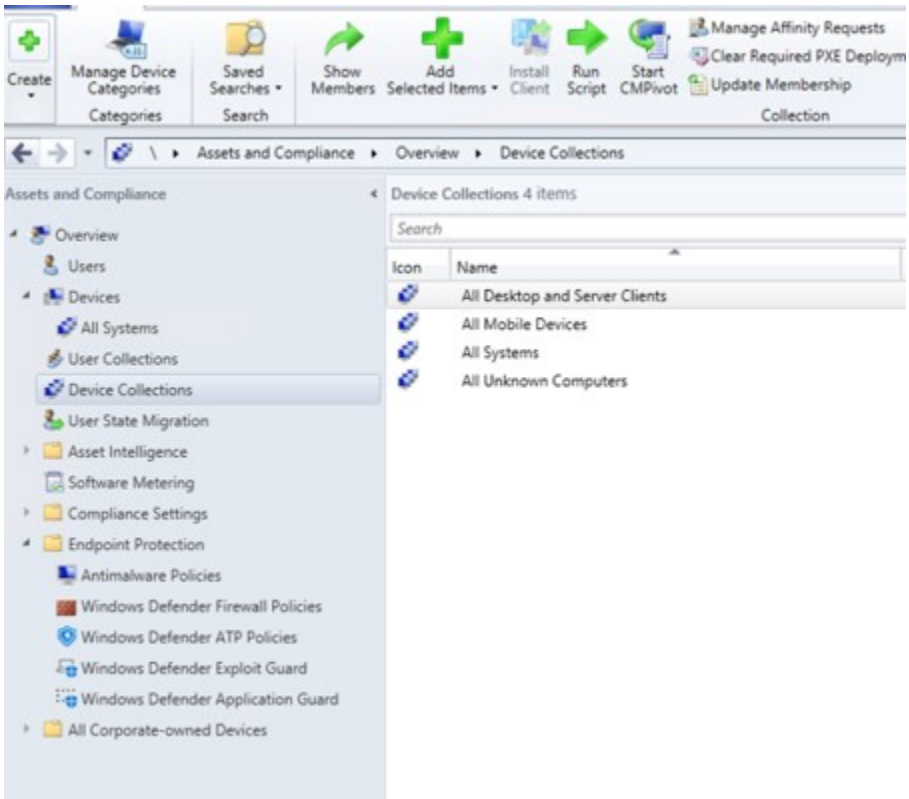
- Configuration de Microsoft Endpoint Configuration Manager
- Détection de point de terminaison et configuration de réponse
- Configuration de la protection de nouvelle génération
- Configuration de la réduction de surface d'attaque

Intégration à l'aide du gestionnaire de configuration de point de terminaison Microsoft

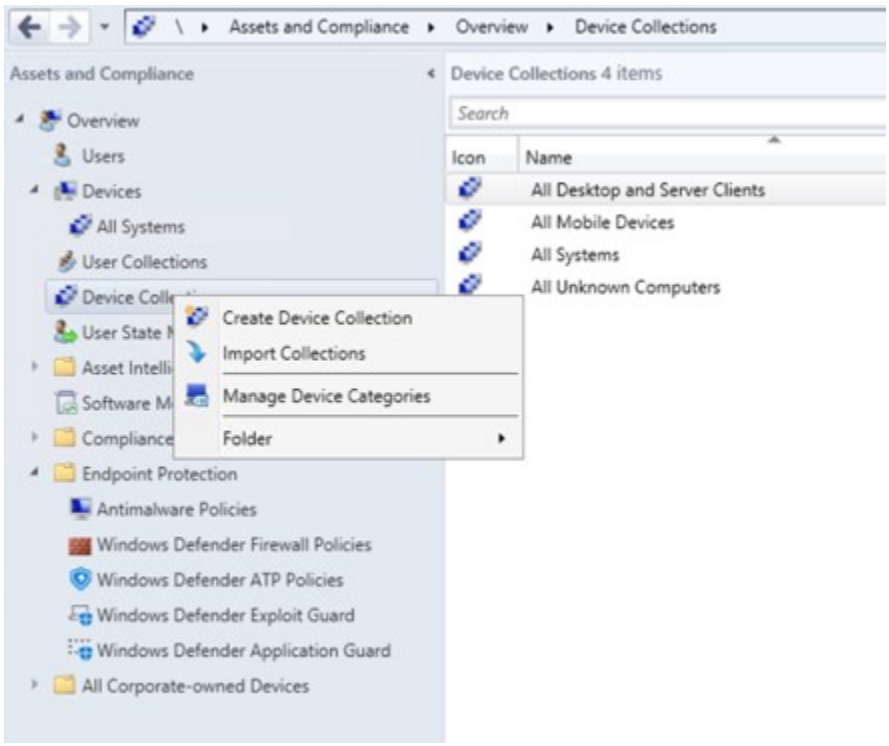
Création de collection

Pour embarquer les appareils Windows 10 avec Microsoft Endpoint Configuration Manager, le déploiement peut cibler une collection ou une collection existante ou une nouvelle collection peut être créée à des fins de test. La stratégie de groupe, telle que la stratégie de groupe ou la méthode manuelle, n'installe pas d'agent sur le système. Dans la console Configuration Manager, le processus d'intégration est configuré dans le cadre des paramètres de conformité de la console. Tout système qui reçoit cette configuration requise conserve cette configuration tant que le client Configuration Manager continue de recevoir cette stratégie à partir du point de gestion. Suivez les étapes décrites ci-dessous pour les systèmes intégrés avec Configuration Manager.

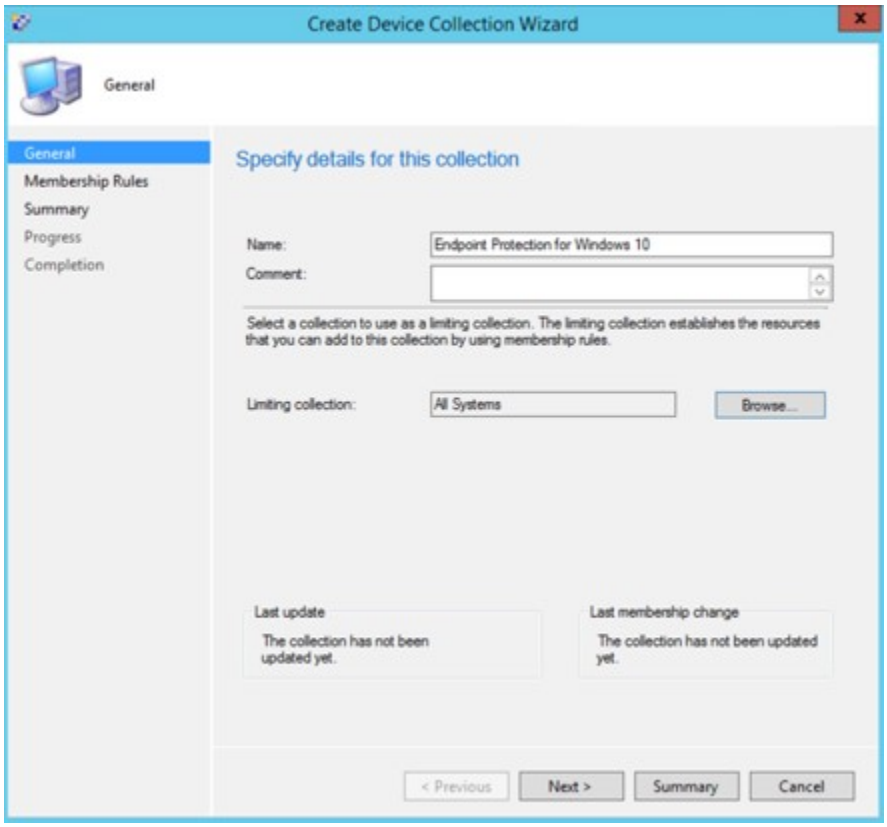
1. Dans la console Microsoft Endpoint Manager, accédez à **ressources et conformité \ > vue d'ensemble \ > collections de périphériques**.



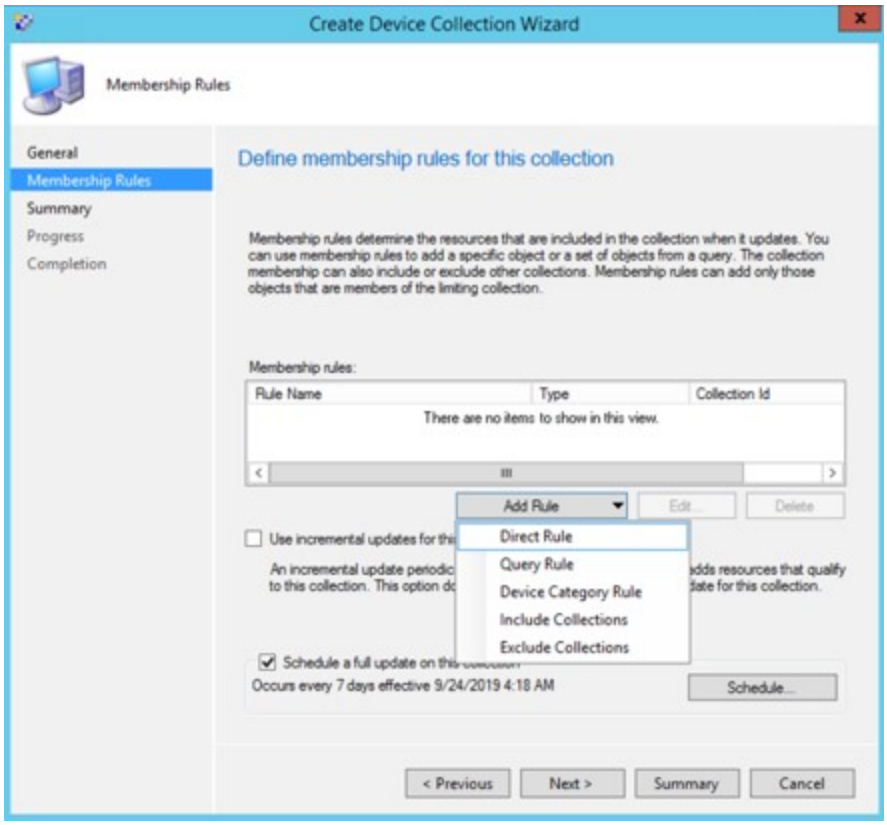
2. Cliquez avec le bouton droit sur **collection d'appareils** et sélectionnez créer une **collection d'appareils**.



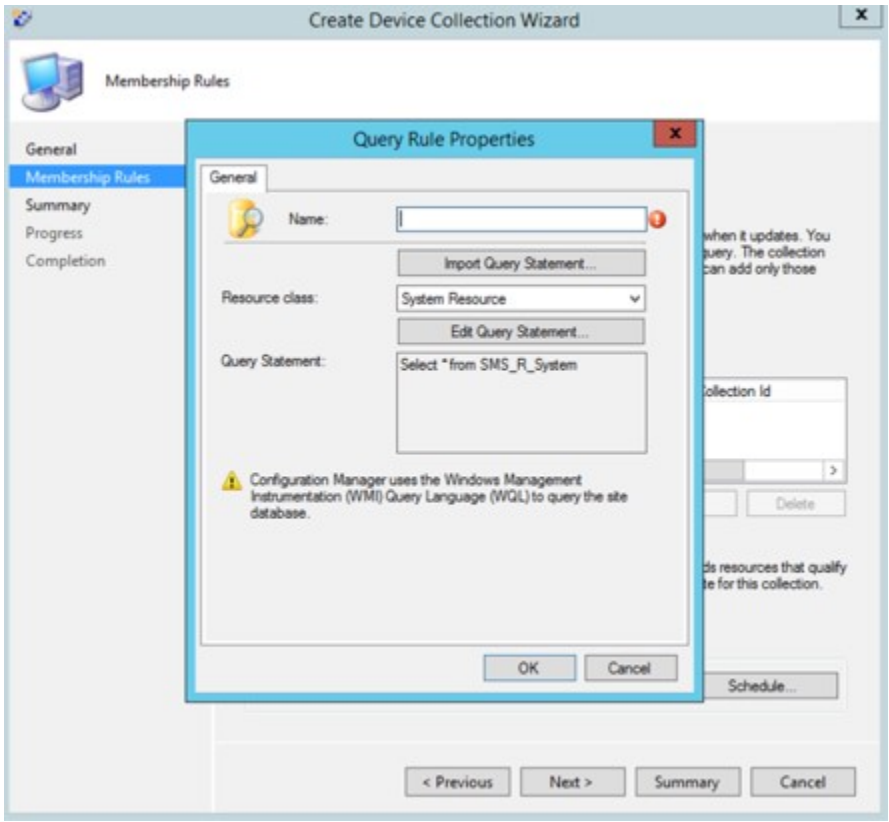
3. Indiquez un **nom** et une **collection limitative**, puis sélectionnez **suivant**.



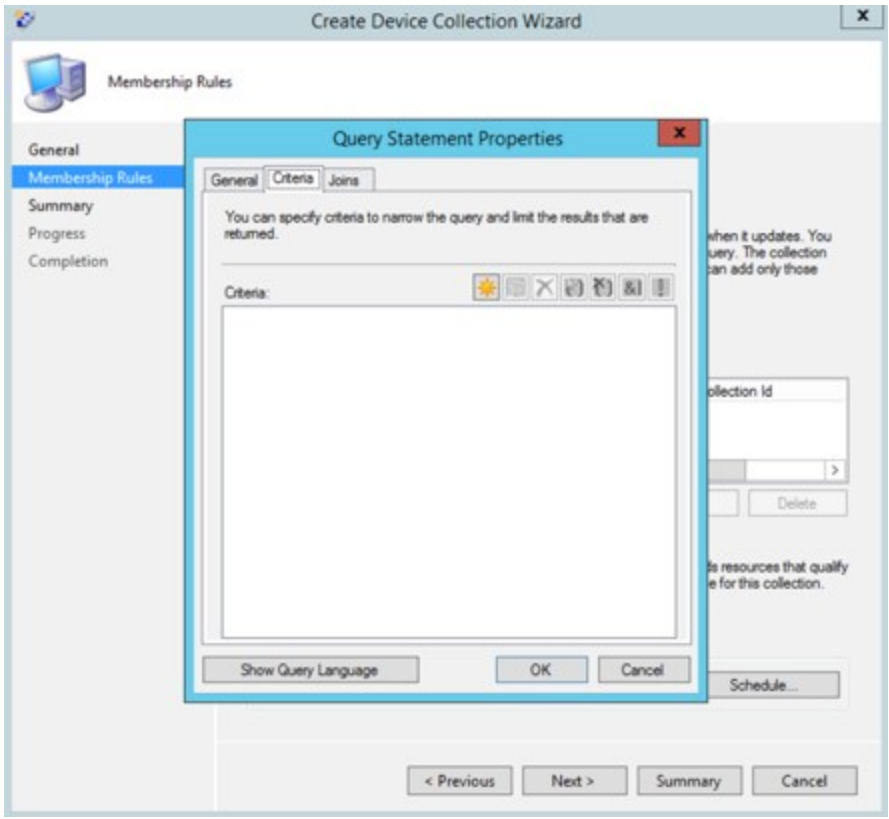
4. Sélectionnez **Ajouter une règle** , puis sélectionnez **règle de requête**.



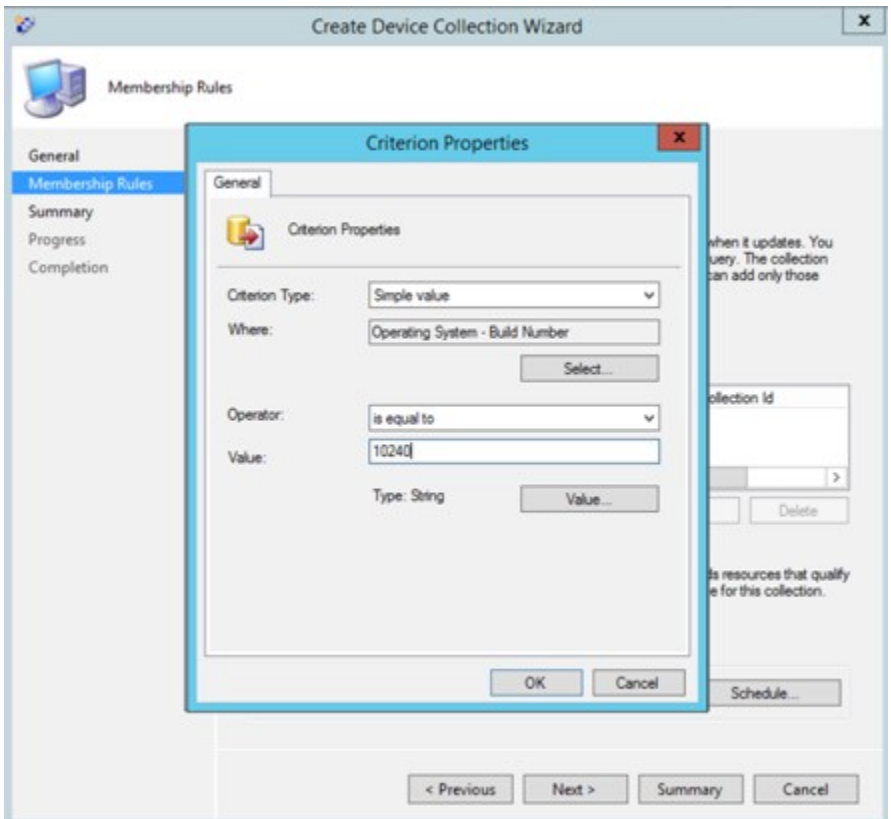
5. Cliquez sur **suivant** dans l' **Assistant adhésion directe** et cliquez sur modifier l'instruction de **requête**.



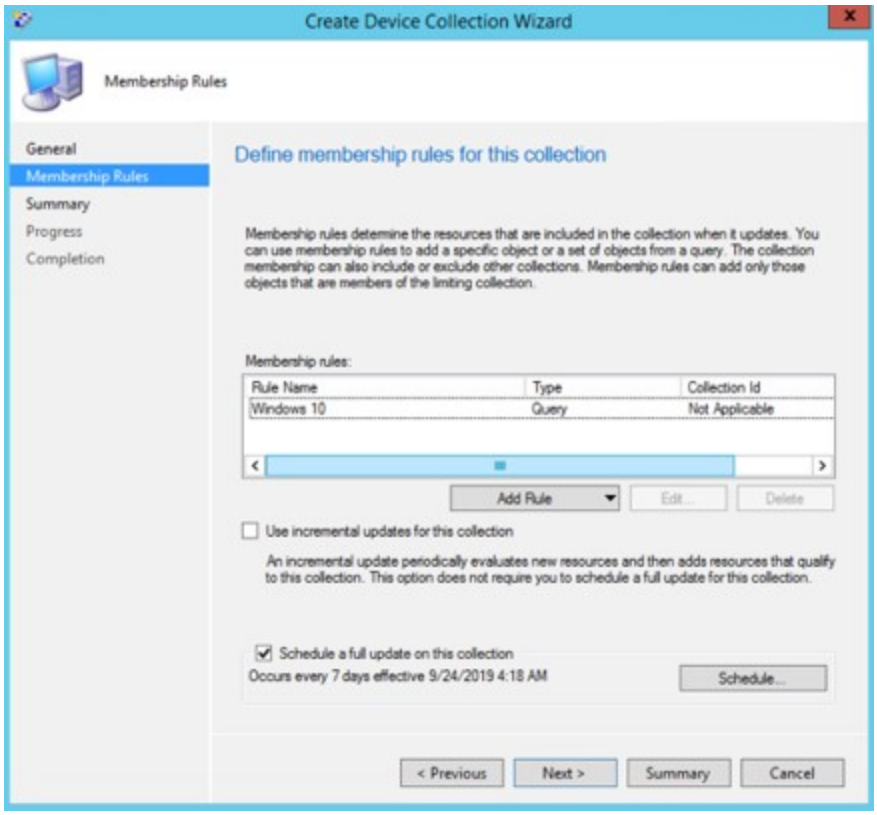
6. Sélectionnez **critères** , puis sélectionnez l'icône en étoile.



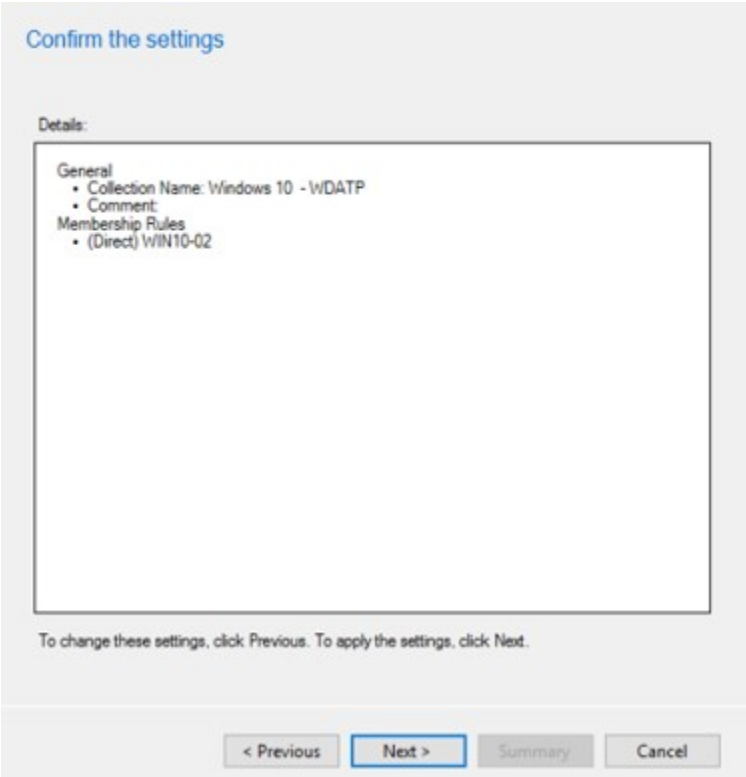
7. Conserver le type de critère comme **valeur simple**, choisissez l'emplacement comme **système d'exploitation-numéro de build**, l'opérateur as **est égal à** et la valeur **10240** , puis cliquez sur **OK**.



8. Sélectionnez **suivant** , puis **Fermer**.



9. Sélectionnez **Suivant**.



À l'issue de cette tâche, vous disposez maintenant d'une collection de périphériques avec tous les points de terminaison Windows 10 dans l'environnement.

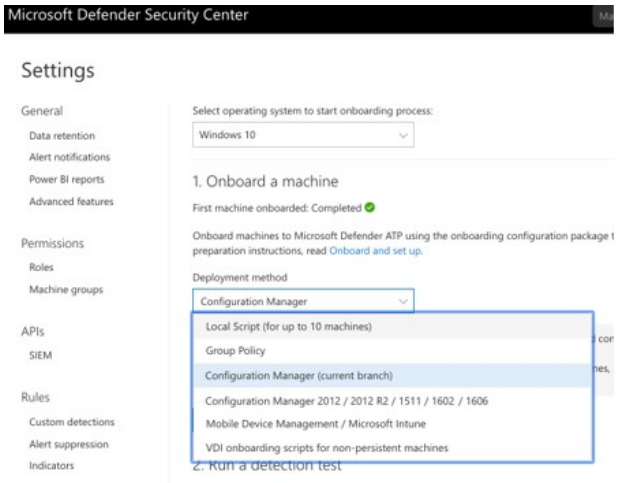
Détection et réponse au point de terminaison

Windows 10

À partir du centre de sécurité Microsoft Defender, il est possible de télécharger la stratégie «. Onboard» qui peut être utilisée pour créer la stratégie dans System Center Configuration Manager et déployer cette stratégie sur les appareils Windows 10.

1. À partir d'un portail du centre de sécurité Microsoft Defender, cliquez sur paramètres, puis sur intégration.

2. Sous méthode de déploiement, sélectionnez la version prise en charge de * * Microsoft Endpoint Configuration Manager * *.



3. Sélectionnez **Télécharger le package**.

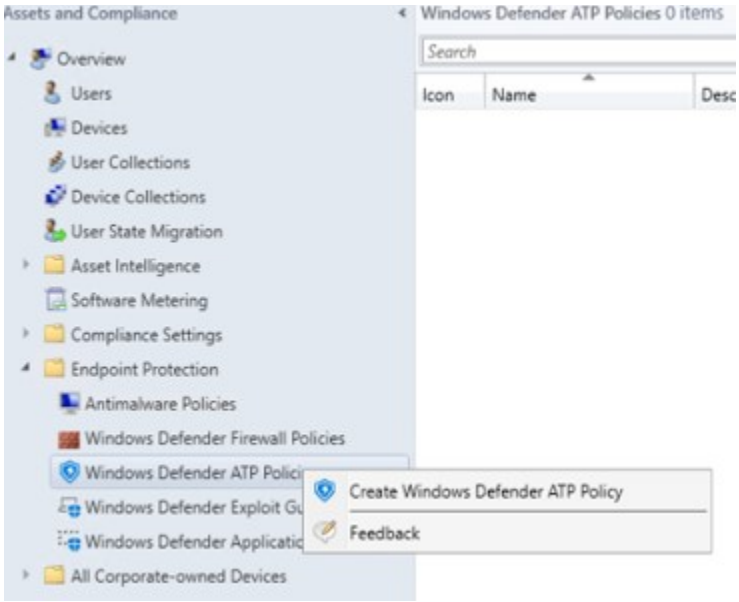
Copier

```
![Image de l'Assistant intégration de Microsoft Defender ATP]
(images/mdatp-download-package.png)
```

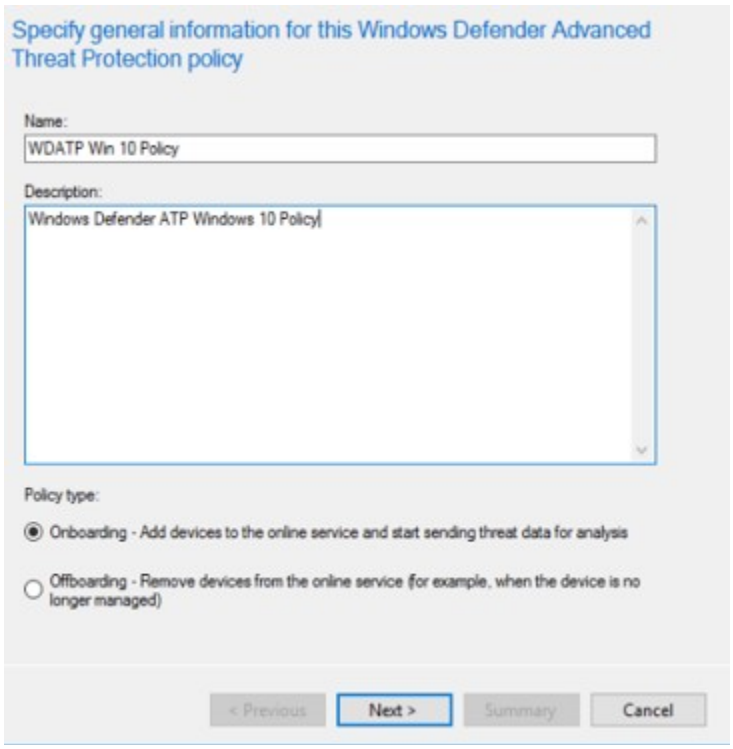
4. Enregistrez le package à un emplacement accessible.

5. Dans le gestionnaire de configuration de points de terminaison de Microsoft, accédez à: **ressources et conformité > vue d'ensemble > Endpoint Protection > stratégies ATP de Microsoft Defender**.

6. Cliquez avec le bouton droit sur **stratégies Microsoft Defender ATP** et sélectionnez **créer une stratégie Microsoft Defender ATP**.

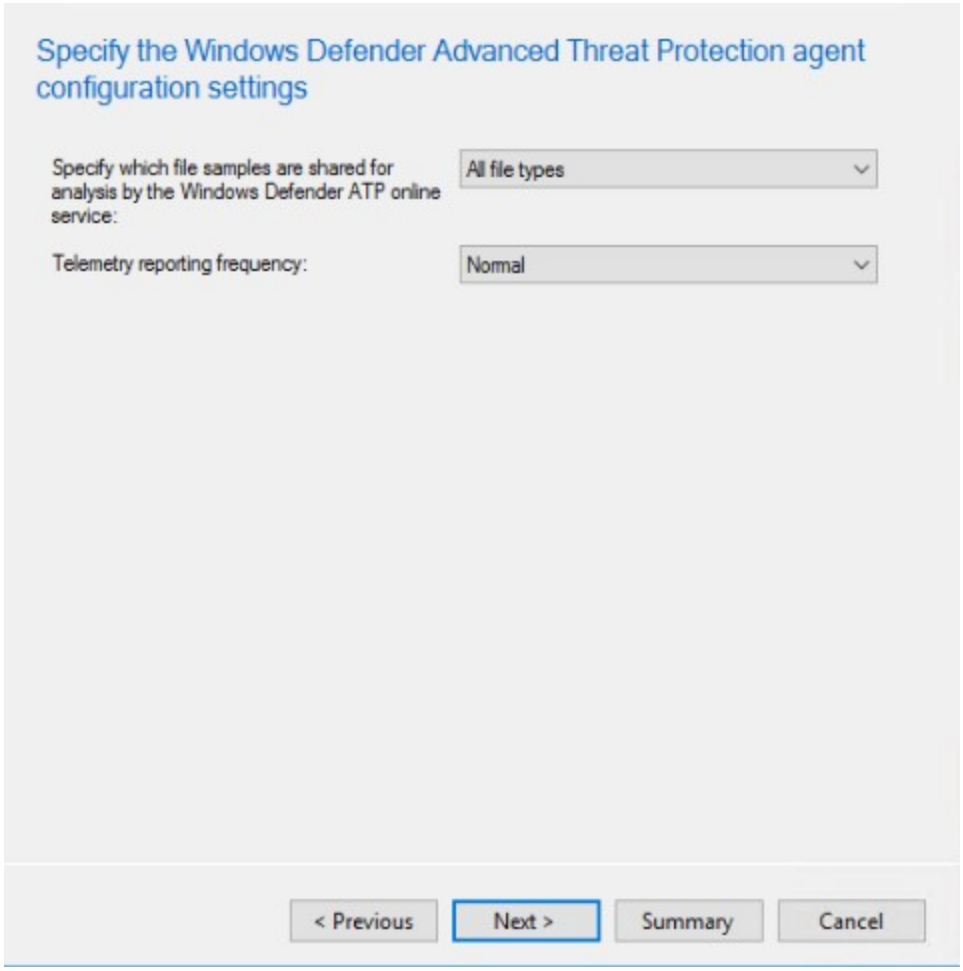


7. Entrez le nom et la description, vérifiez que l'option **intégration** est activée, puis sélectionnez **suivant**.

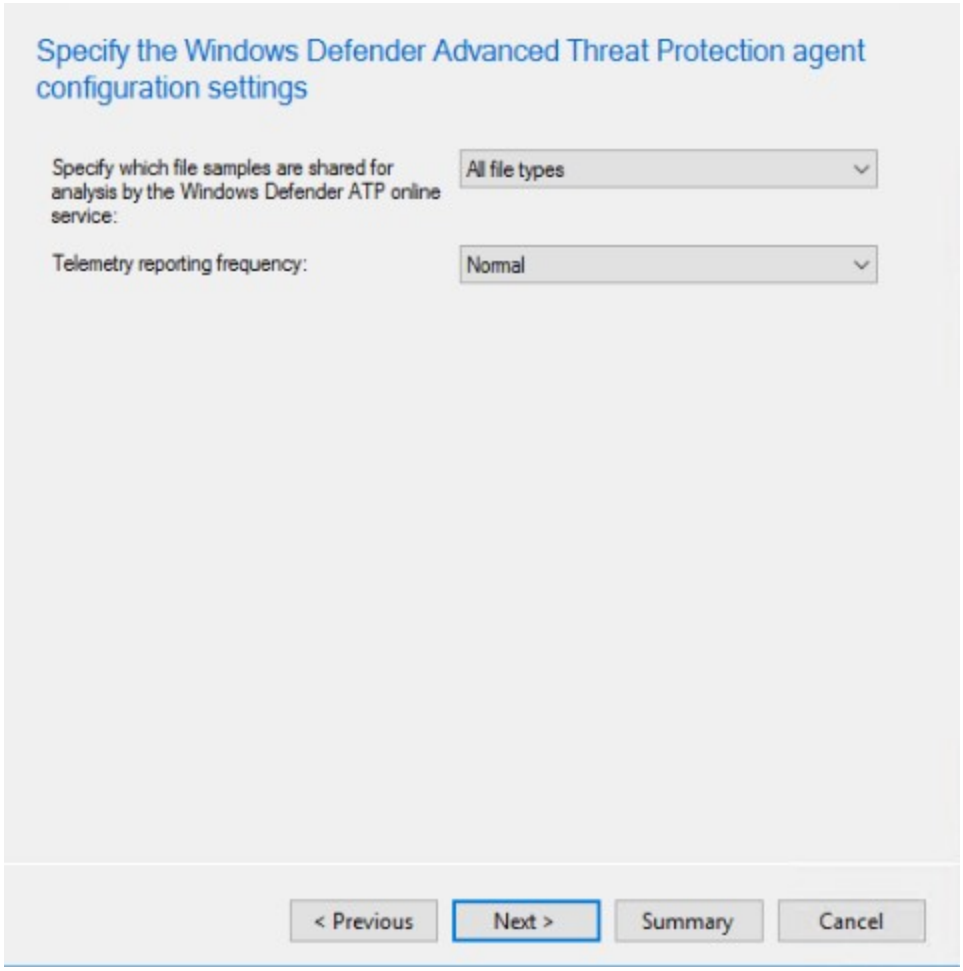


8. Cliquez sur **Parcourir**.

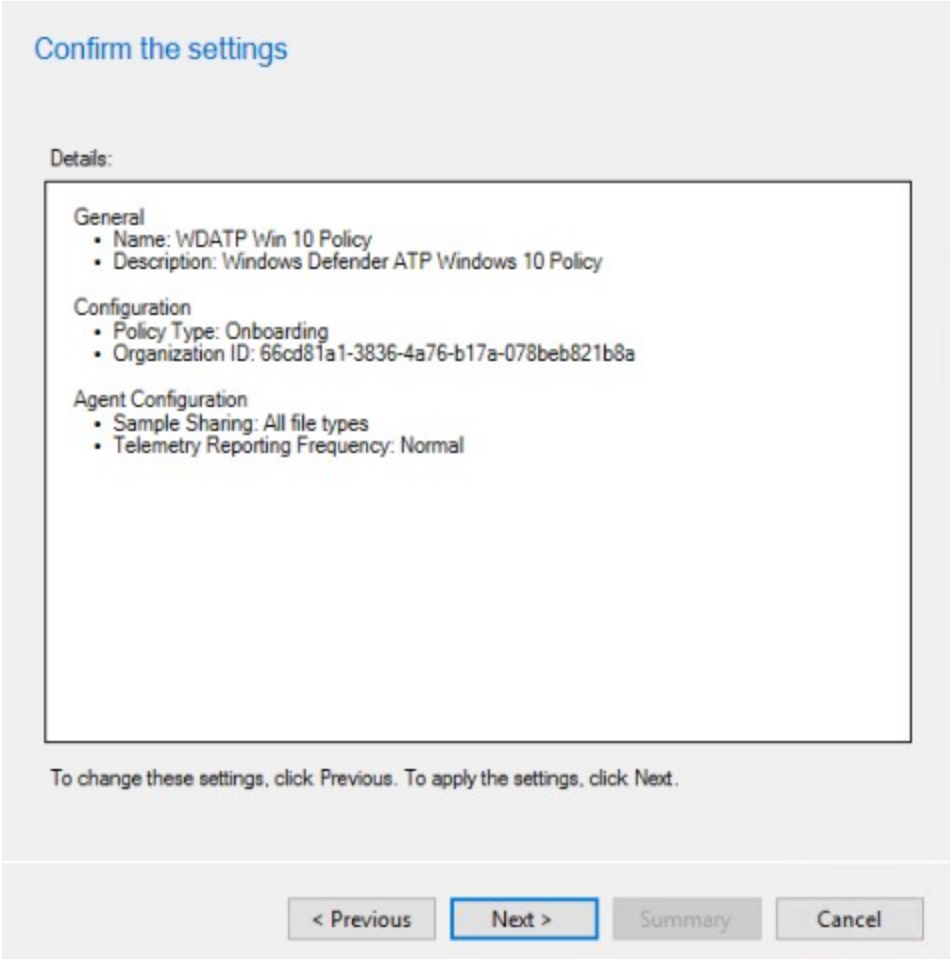
9. Accédez à l'emplacement du fichier téléchargé à partir de l'étape 4 ci-dessus.



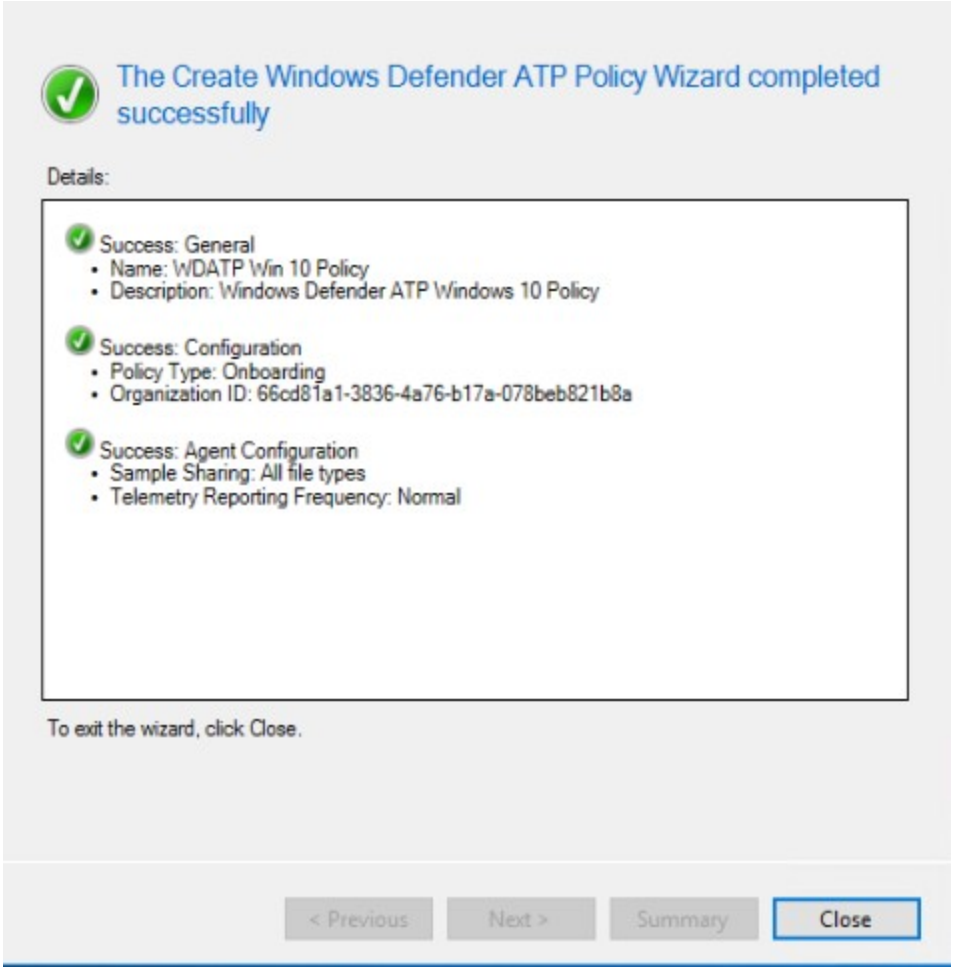
10. Cliquez sur **Suivant**.
11. Configurez l'agent avec les exemples appropriés (**aucun** ou **tous les types de fichiers**).



12. Sélectionnez le télémétrie approprié (**normal** ou **Expedited**), puis cliquez sur **suivant**.

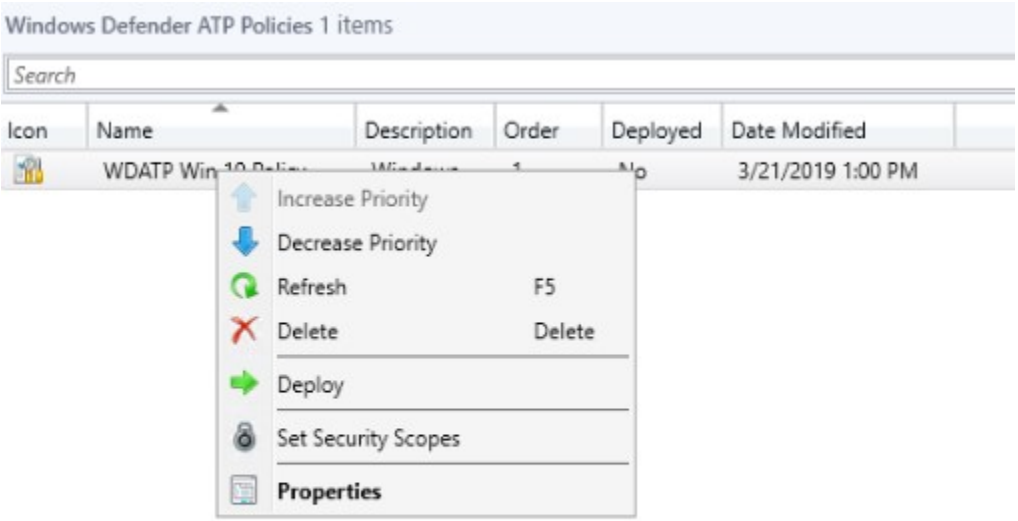


13. Vérifiez la configuration, puis cliquez sur **suivant**.

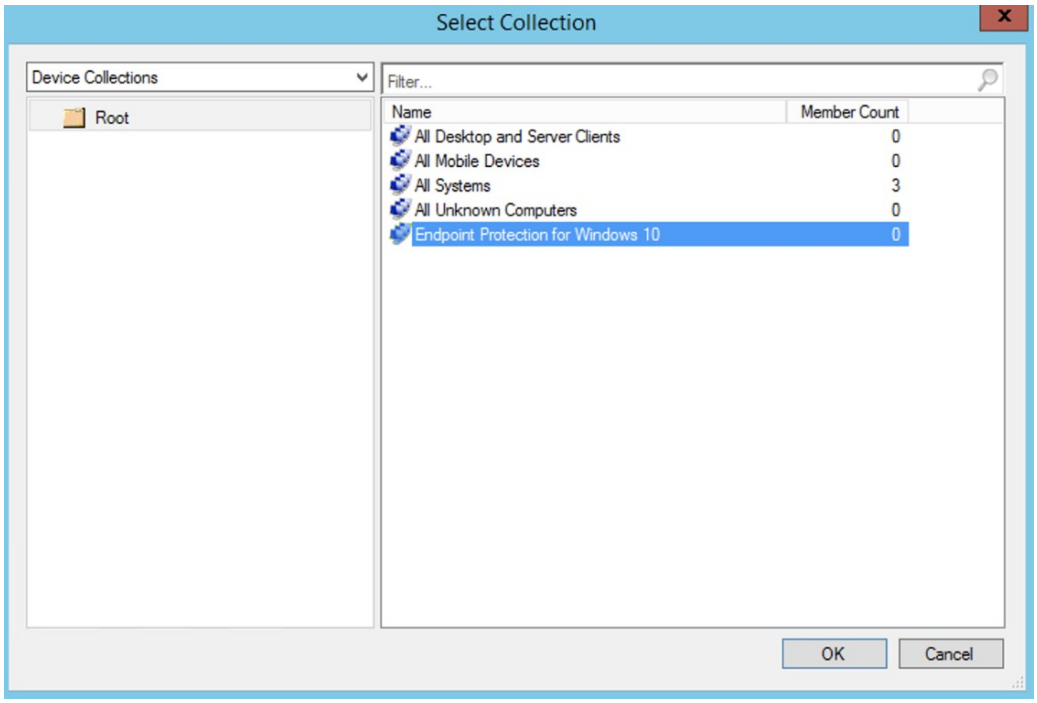


14. Cliquez sur **Fermer** à la fin de l'Assistant.

15. Dans la console Microsoft Endpoint Manager, cliquez avec le bouton droit sur la politique Microsoft Defender ATP que vous venez de créer, puis sélectionnez **déployer**.



16. Dans le panneau de droite, sélectionnez la collection précédemment créée, puis cliquez sur **OK**.

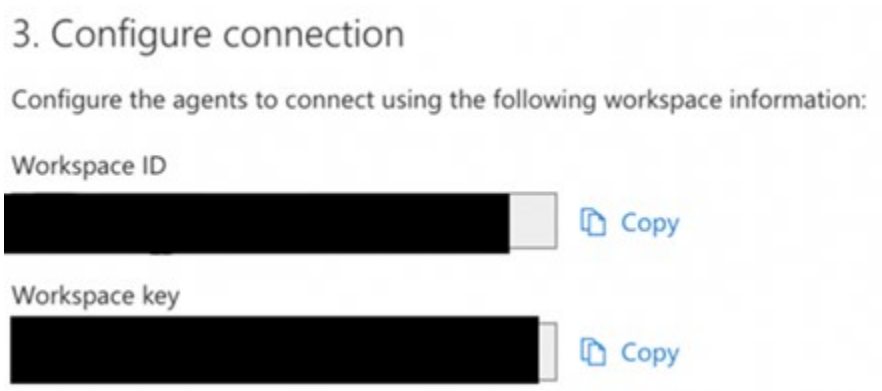


Versions précédentes du client Windows (Windows 7 et Windows 8,1)

Suivez les étapes décrites ci-dessous pour identifier l'ID de l'espace de travail et la clé de l'espace de travail Microsoft Defender ATP qui seront nécessaires pour l'intégration de versions précédentes de Windows.

1. À partir d'un portail du centre de sécurité Microsoft Defender, sélectionnez **paramètres > l'intégration**.

2. Sous système d'exploitation **, choisissez Windows 7 SP1 et 8,1**.



3. Copiez l' **ID d’espace de travail** et la **clé de l’espace de travail** , puis enregistrez-les. Il sera utilisé plus tard dans le processus.

Pour que les systèmes puissent être intégrés dans l’espace de travail, vous devez mettre à jour les scripts de déploiement pour qu’ils contiennent les informations correctes. Dans le cas contraire, les systèmes ne seront pas correctement intégrés. Selon la méthode de déploiement, cette étape est susceptible d’avoir déjà été effectuée.

Modifiez InstallMMA. cmd à l’aide d’un éditeur de texte, tel que le bloc-notes, et mettez à jour les lignes suivantes, puis enregistrez le fichier:

Copier

```
![Image of onboarding](images/a22081b675da83e8f62a046ae6922b0d.png)
```

Modifiez le ConfiguerOMSAgent. vbs avec un éditeur de texte tel que le bloc-notes, puis mettez à jour les lignes suivantes et enregistrez le fichier:

Copier

```
![Image of onboarding](images/09833d16df7f37eda97ea1d5009b651a.png)
```

L’agent de surveillance Microsoft (MMA) est actuellement (en janvier 2019) pris en charge sur les systèmes d’exploitation Windows suivants:

- Références serveur: Windows Server 2008 SP1 ou une version ultérieure
- Références clientes: Windows 7 SP1 et versions ultérieures

L’agent MMA doit être installé sur les appareils Windows. Pour installer l’agent, certains systèmes doivent télécharger la mise à jour pour l’expérimentation des clients et la télémétrie de diagnostic afin de recueillir les données auprès de MMA. Les versions suivantes de ce système peuvent être limitées aux éléments suivants:

- Windows 8.1
- Windows7
- Windows Server2016

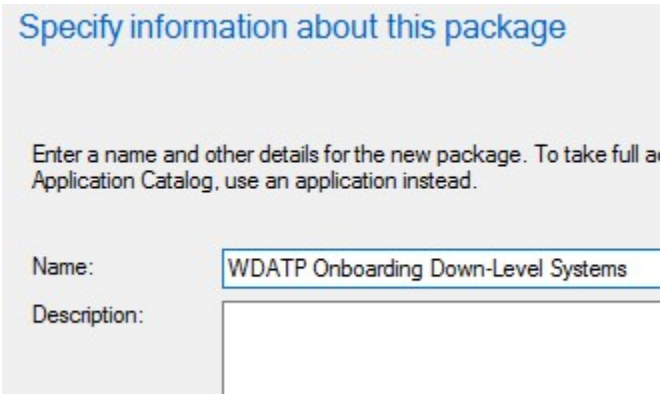
- WindowsServer2012R2
- Windows Server2008R2

Plus précisément, pour Windows 7 SP1, les correctifs suivants doivent être installés:

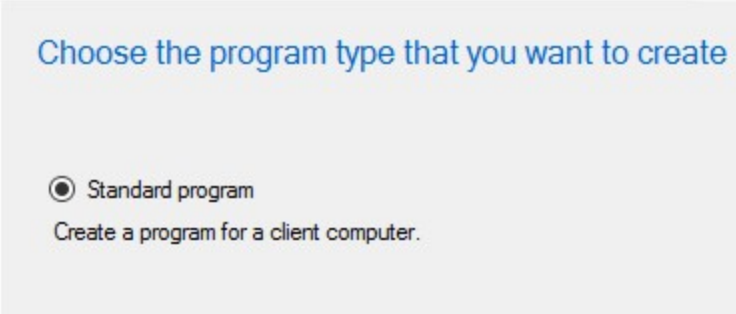
- Installation de KB4074598
- Installez .NET Framework 4,5 (ou une version ultérieure **) ou** KB3154518. Ne procédez pas à l'installation sur le même système.

Pour déployer le fichier MMA avec Microsoft Endpoint Configuration Manager, suivez les étapes ci-dessous pour utiliser les fichiers de commandes fournis dans l'intégration des systèmes. Le fichier CMD en cas d'exécution nécessite que le système copie les fichiers à partir d'un partage réseau par le système, le système installe les fichiers MMA, installe le DependencyAgent et configure le rapport MMA pour l'inscription dans l'espace de travail.

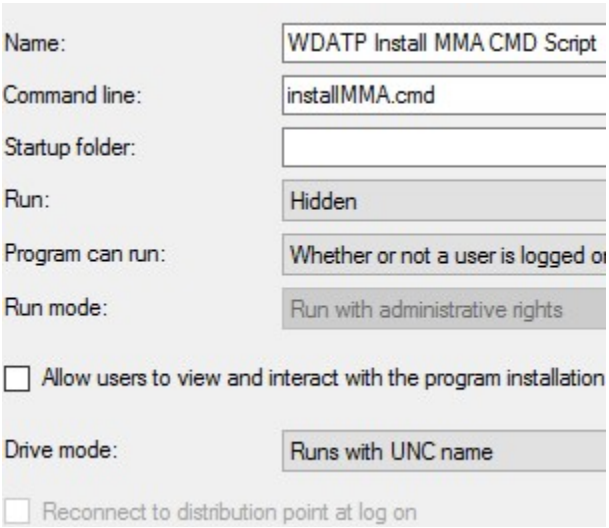
1. Dans la console Microsoft Endpoint Manager, accédez à la **bibliothèque de logiciels**.
2. Développez **gestion des applications**.
3. Cliquez avec le bouton droit sur **packages** , puis sélectionnez **créer un package**.
4. Donnez un nom au package, puis cliquez sur **suivant** .



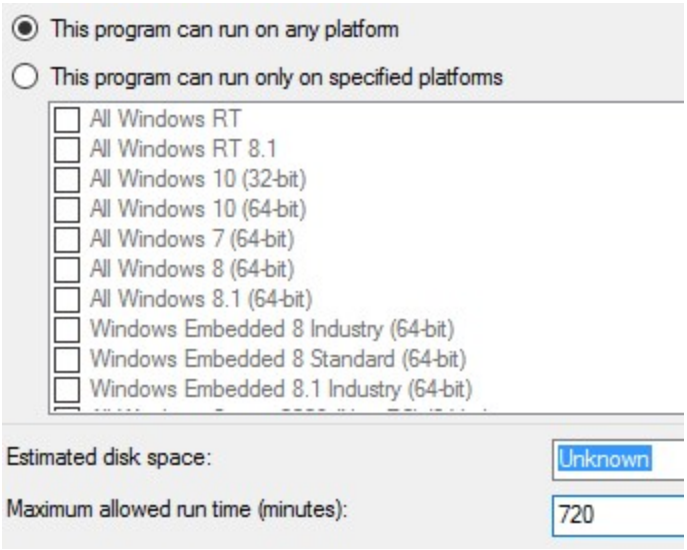
5. Option vérifier le **programme standard** sélectionnée



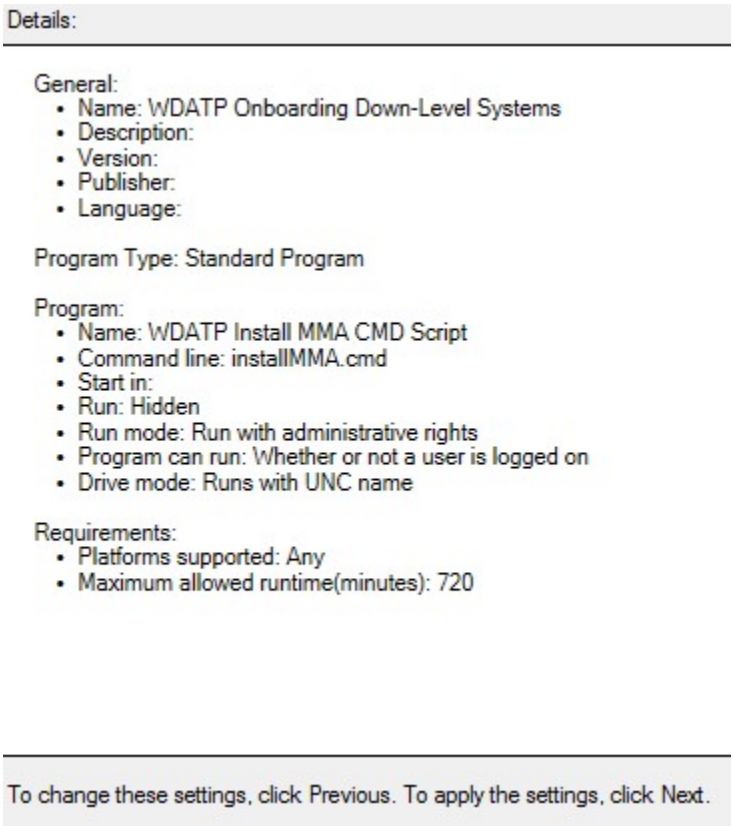
6. Cliquez sur **Suivant**.



7. Entrez le nom d'un programme.
8. Naviguez jusqu'à l'emplacement du InstallMMA. cmd.
9. Définissez exécuter sur **caché**.
10. Le **programme Set peut s'exécuter** sur l'état de **connexion d'un utilisateur**.
11. Cliquez sur **Suivant**.
12. Définissez le **délai d'exécution maximal autorisé** sur 720.
13. Cliquez sur **Suivant**.



14. Vérifiez la configuration, puis cliquez sur **suivant**.



15. Cliquez sur **Suivant**.

16. Cliquez sur **Fermer**.

17. Dans la console Microsoft Endpoint Manager, cliquez avec le bouton droit sur le package d'intégration de Microsoft Defender disponible, que vous venez de créer, puis sélectionnez **déployer**.

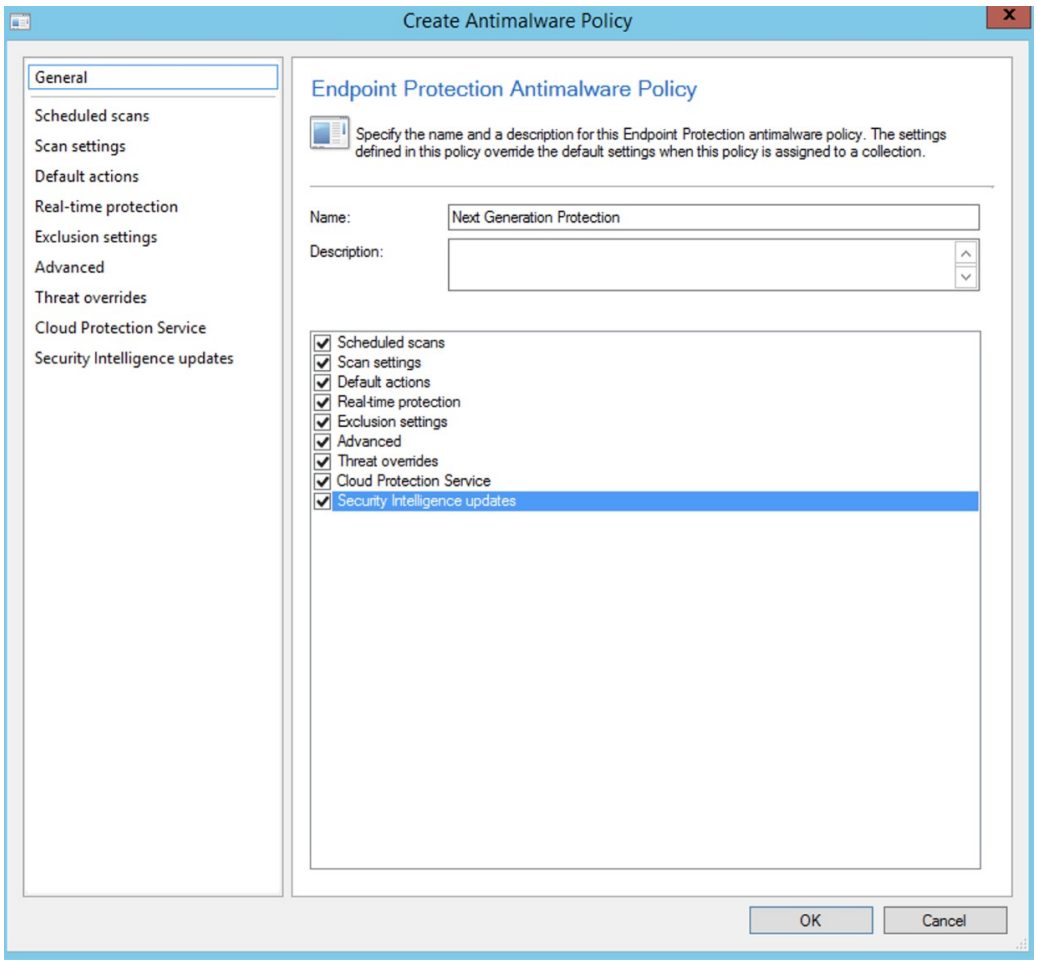
18. Dans le panneau de droite, sélectionnez la collection appropriée.

19. Cliquez sur **OK**.

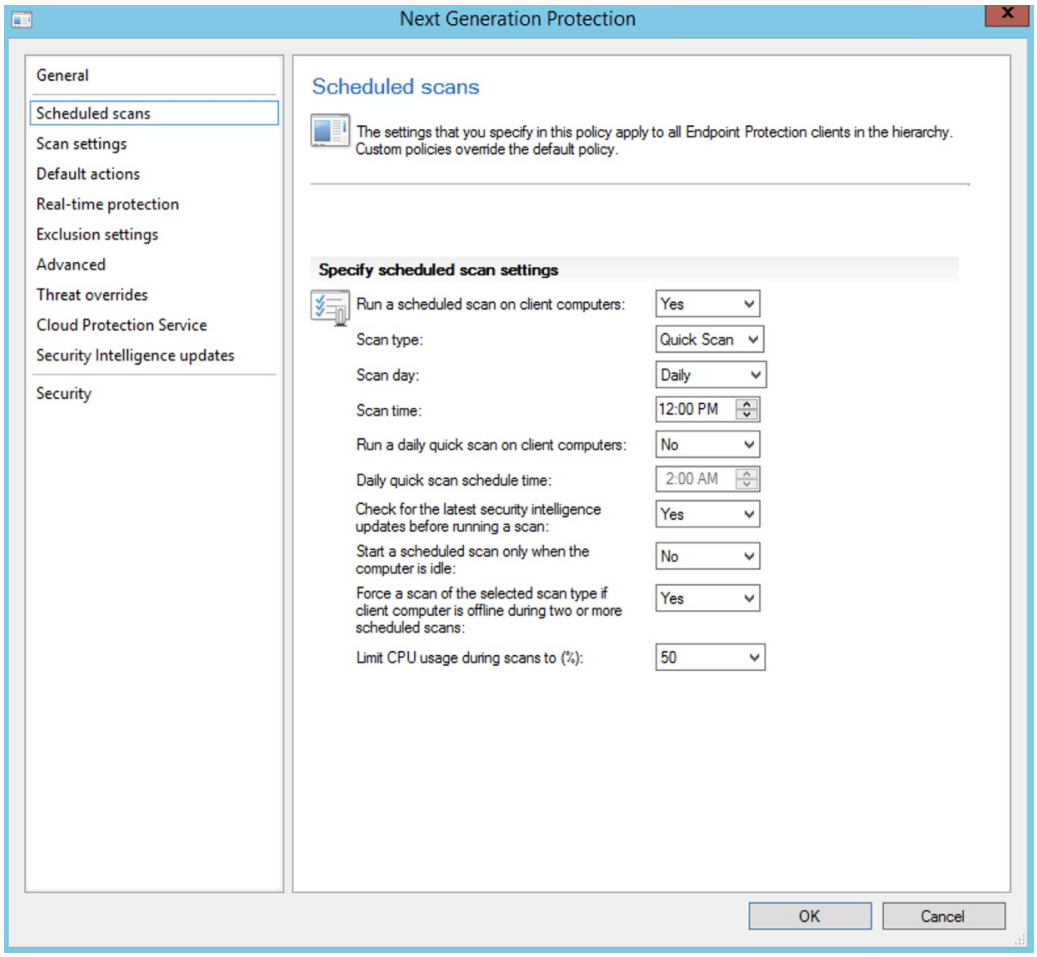
Protection nouvelle génération

L'antivirus Microsoft Defender est une solution anti-programme malveillant prédéfinie qui fournit une nouvelle génération de protection pour les postes de travail, les ordinateurs portables et les serveurs.

1. Dans la console Microsoft Endpoint Manager, accédez à **ressources et conformité \ > vue d'ensemble \ > points de terminaison \ > des politiques de protection des logiciels malveillants** et sélectionnez **créer une stratégie anti-programme malveillant**.



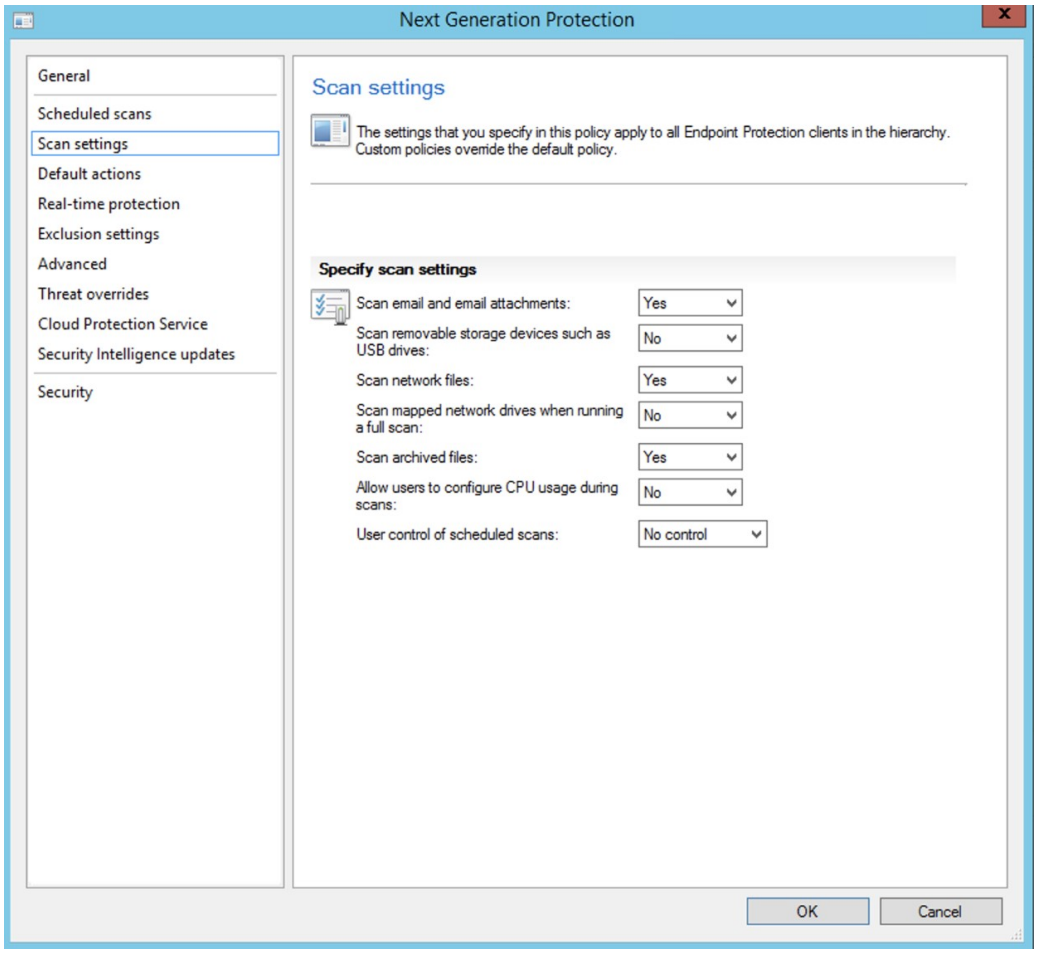
2. Sélectionnez **analyses planifiées**, **paramètres de numérisation**, **actions par défaut**, **protection en temps réel**, **paramètres d'exclusion**, **Options avancées**, **remplacements de menaces**, service de **protection Cloud** et **mises à jour d'intelligence de sécurité** , puis sélectionnez **OK**.

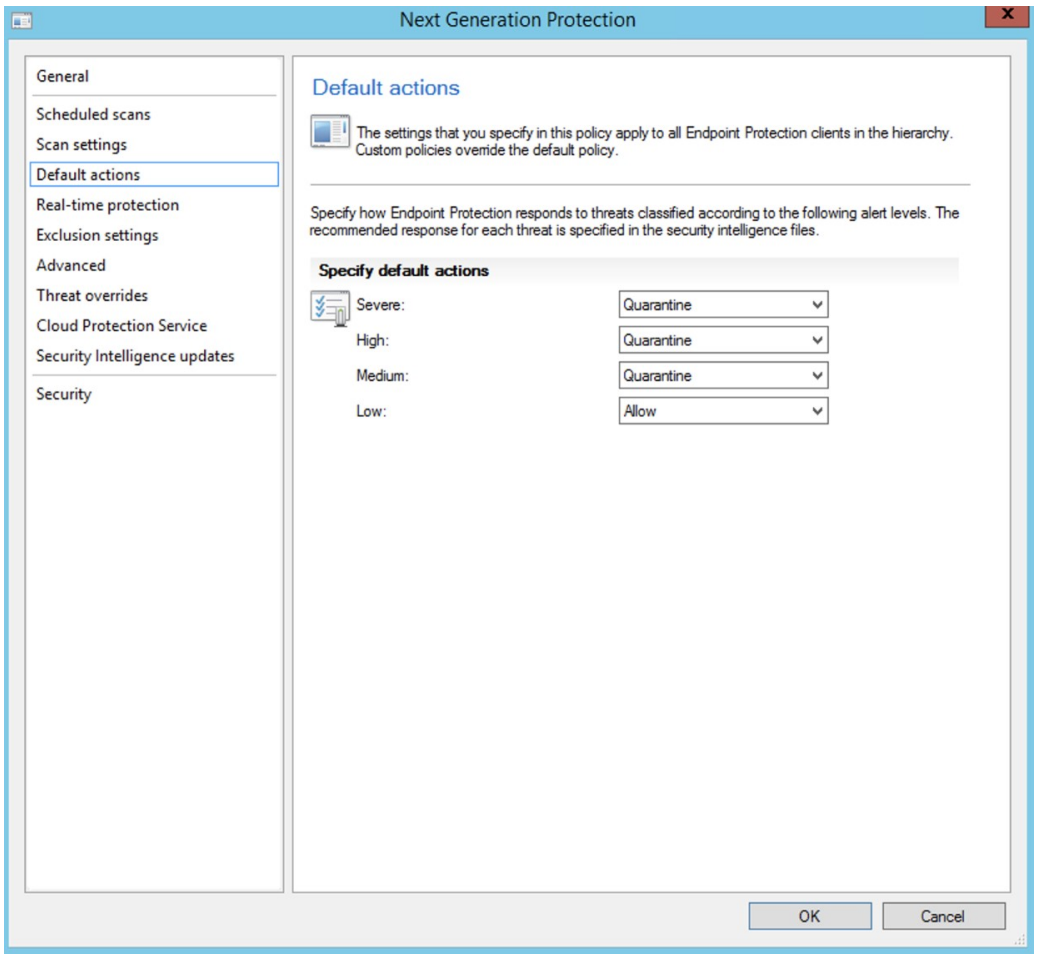


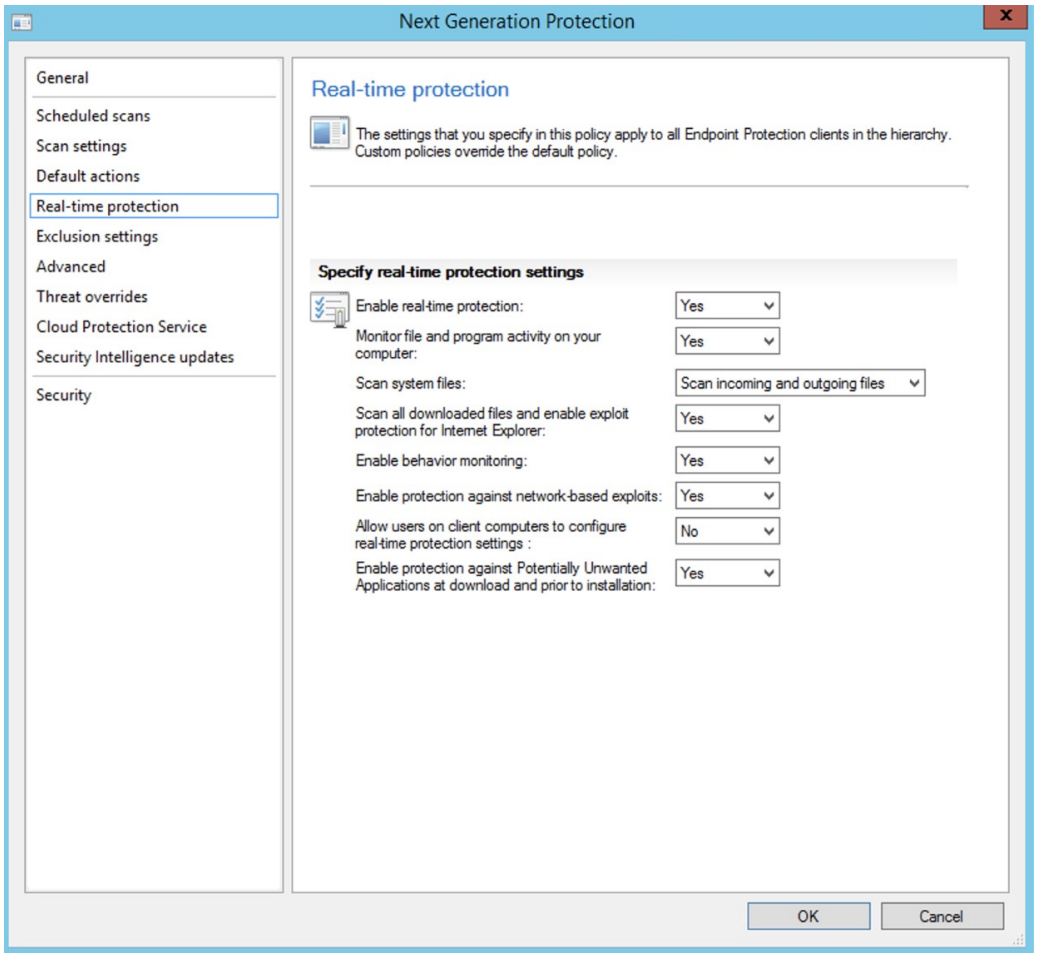
Dans certains secteurs d'entreprise, certains clients d'entreprise peuvent avoir besoin d'un certain nombre de fois que le logiciel antivirus est configuré.

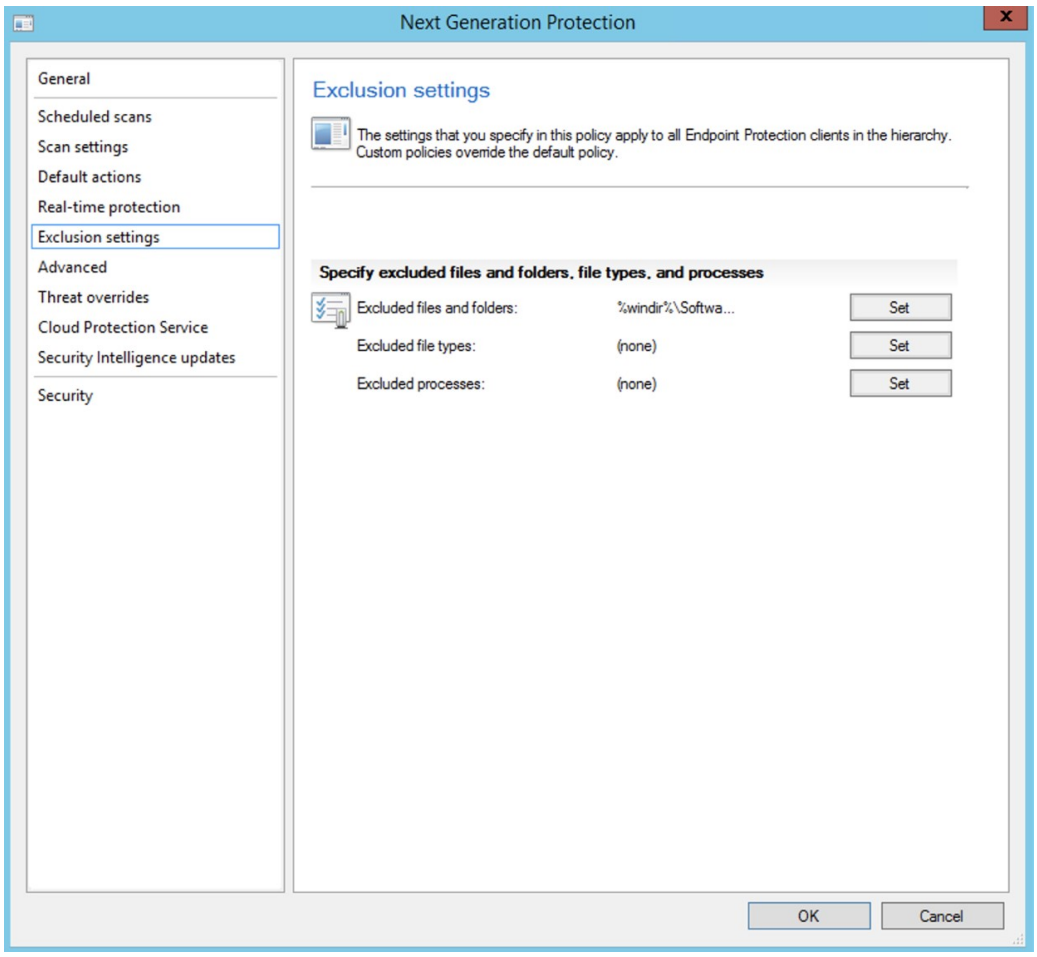
Analyse rapide et analyse complète et analyse personnalisée

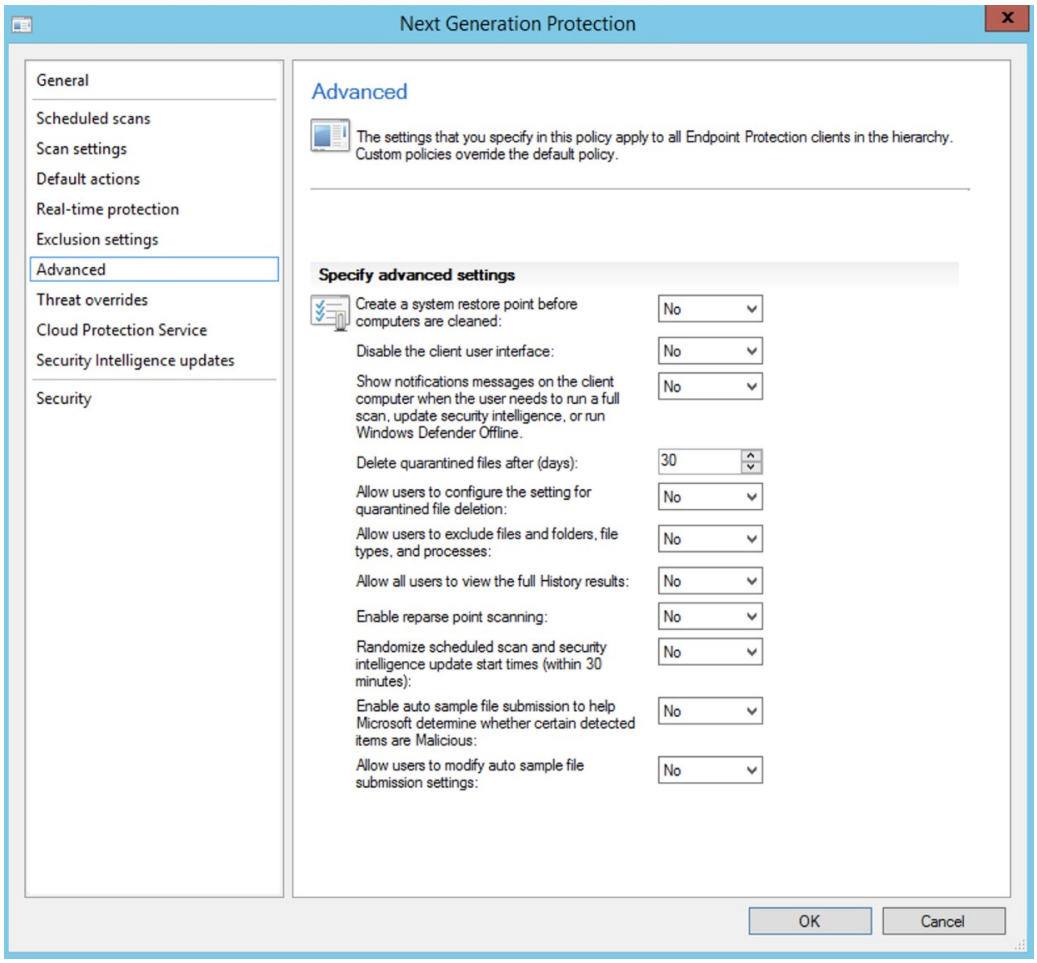
Pour plus d'informations, voir infrastructure de configuration de la sécurité Windows

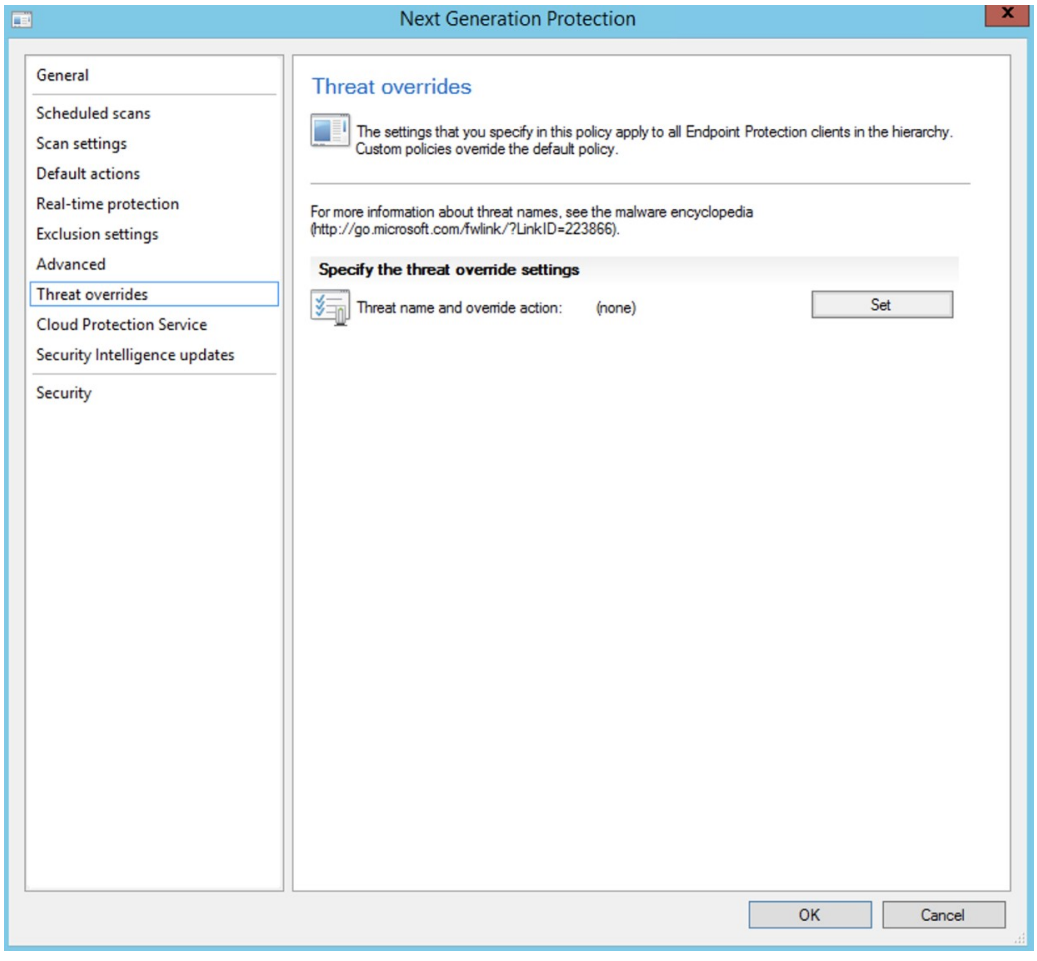

Next Generation Protection
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Cloud Protection Service
Security Intelligence updates
Security
Scan settings
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Specify scan settings
Scan email and email attachments: Yes
Scan removable storage devices such as USB drives: No
Scan network files: Yes
Scan mapped network drives when running a full scan: No
Scan archived files: Yes
Allow users to configure CPU usage during scans: No
User control of scheduled scans: No control
OK
Cancel

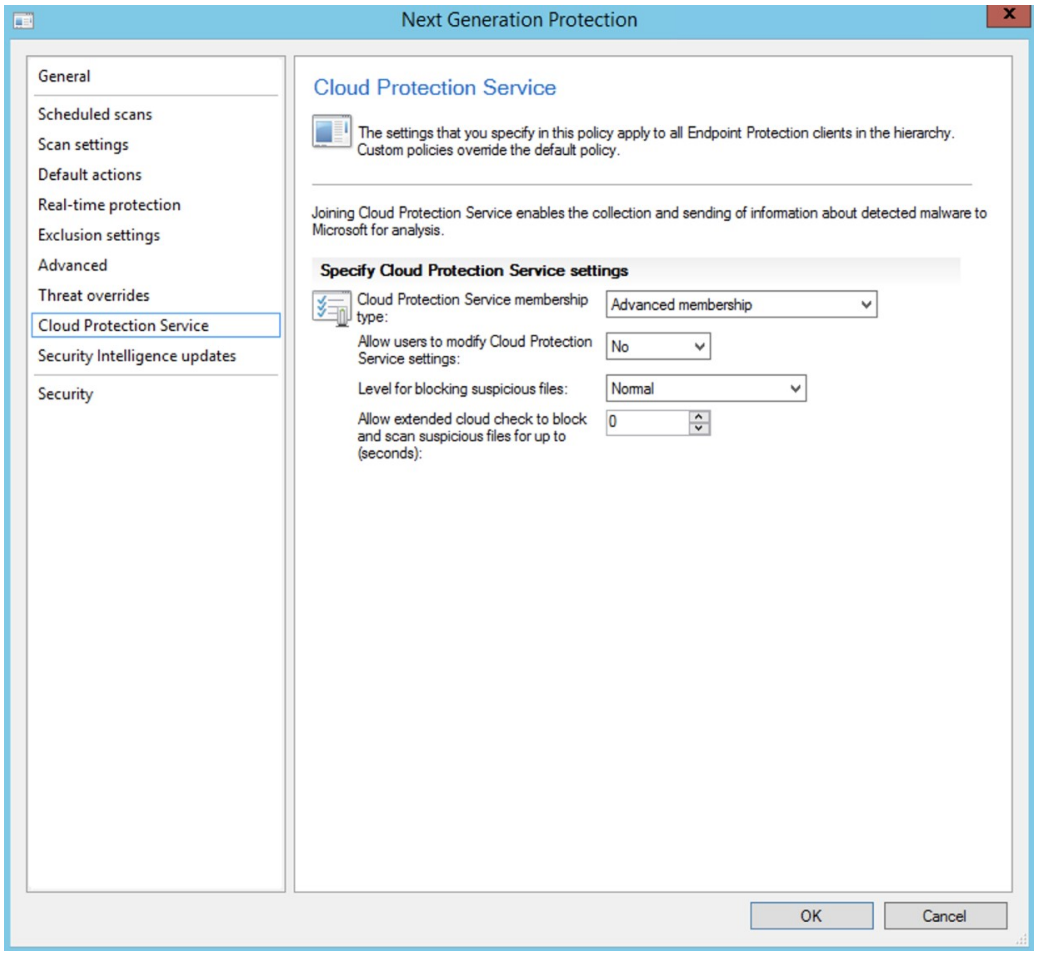

Next Generation Protection
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Cloud Protection Service
Security Intelligence updates
Security
Default actions
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Specify how Endpoint Protection responds to threats classified according to the following alert levels. The recommended response for each threat is specified in the security intelligence files.
Specify default actions
Severe: Quarantine
High: Quarantine
Medium: Quarantine
Low: Allow
OK
Cancel

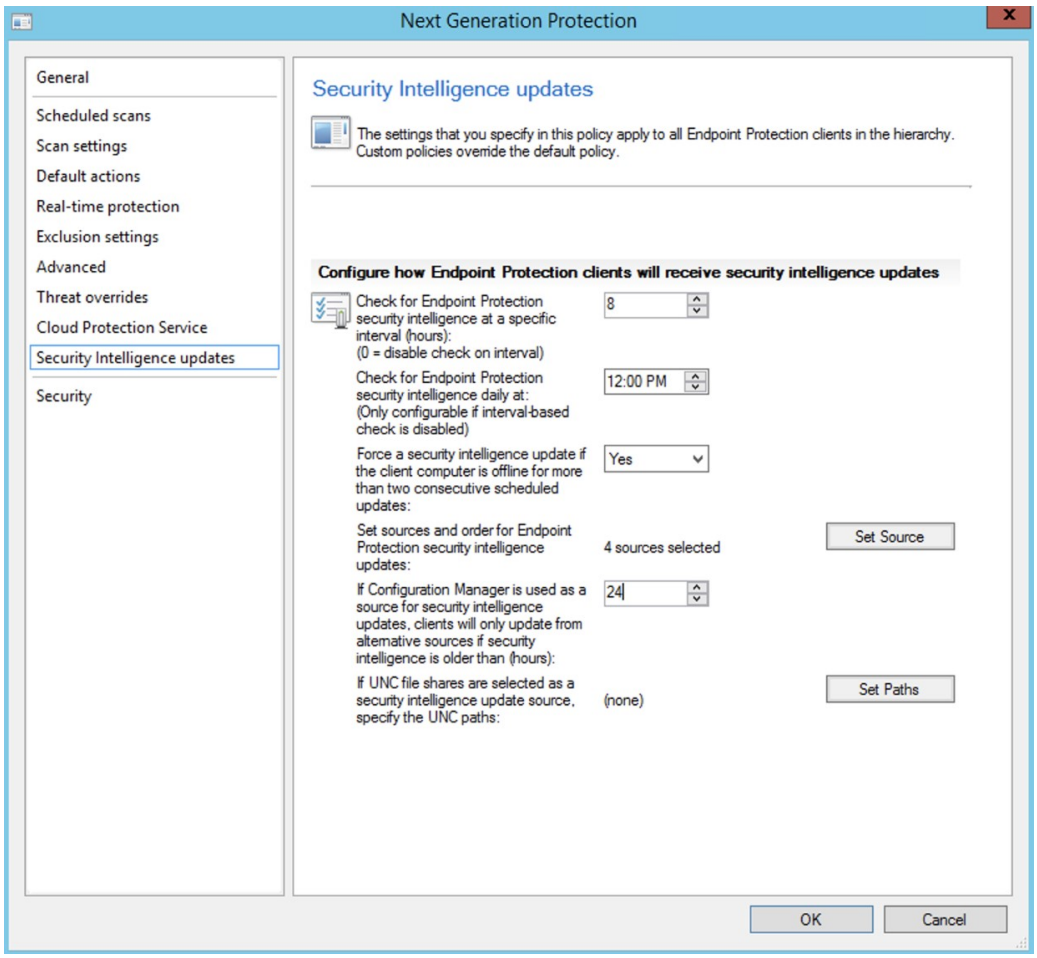

Next Generation Protection
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Cloud Protection Service
Security Intelligence updates
Security
Real-time protection
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Specify real-time protection settings
Enable real-time protection: Yes
Monitor file and program activity on your computer: Yes
Scan system files: Scan incoming and outgoing files
Scan all downloaded files and enable exploit protection for Internet Explorer: Yes
Enable behavior monitoring: Yes
Enable protection against network-based exploits: Yes
Allow users on client computers to configure real-time protection settings : No
Enable protection against Potentially Unwanted Applications at download and prior to installation: Yes
OK
Cancel


Next Generation Protection
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Cloud Protection Service
Security Intelligence updates
Security
Exclusion settings
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Specify excluded files and folders, file types, and processes
Excluded files and folders: %windir%\Softwa... Set
Excluded file types: (none) Set
Excluded processes: (none) Set
OK
Cancel

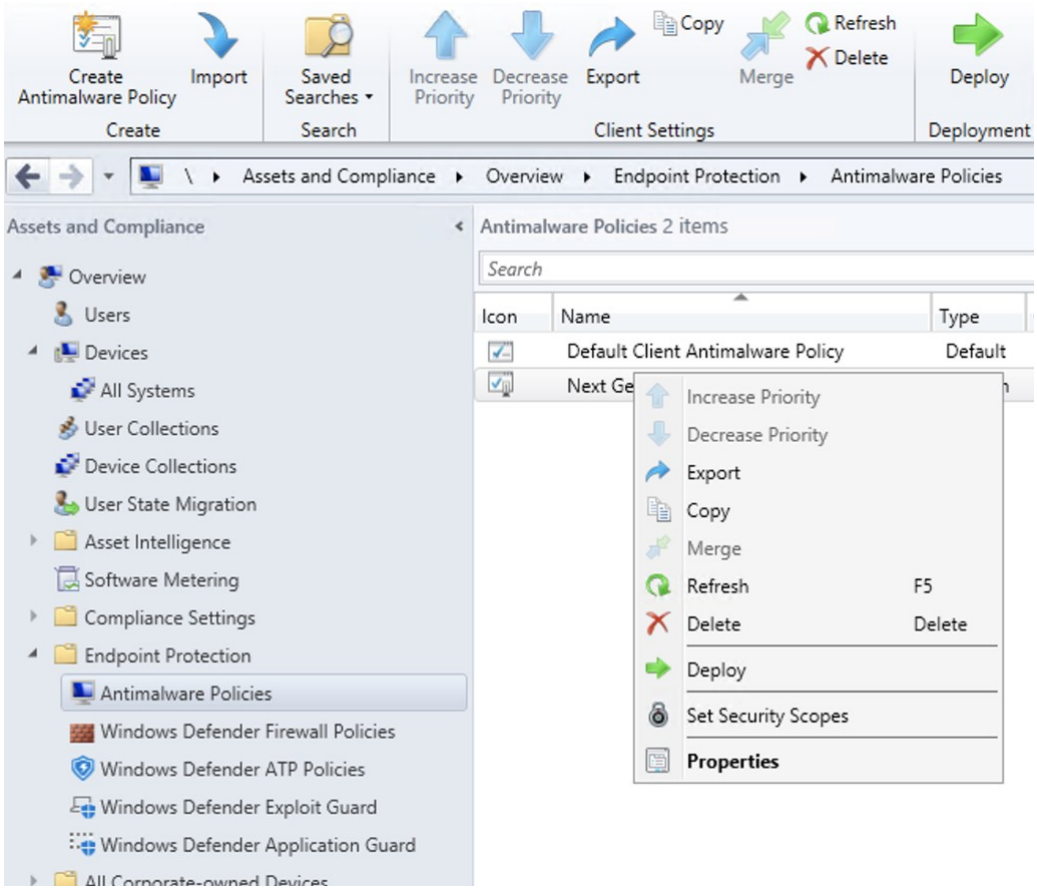

Next Generation Protection
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Cloud Protection Service
Security Intelligence updates
Security
Advanced
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Specify advanced settings
Create a system restore point before computers are cleaned: No
Disable the client user interface: No
Show notifications messages on the client computer when the user needs to run a full scan, update security intelligence, or run Windows Defender Offline. No
Delete quarantined files after (days): 30
Allow users to configure the setting for quarantined file deletion: No
Allow users to exclude files and folders, file types, and processes: No
Allow all users to view the full History results: No
Enable reparse point scanning: No
Randomize scheduled scan and security intelligence update start times (within 30 minutes): No
Enable auto sample file submission to help Microsoft determine whether certain detected items are Malicious: No
Allow users to modify auto sample file submission settings: No
OK
Cancel


Next Generation Protection
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Cloud Protection Service
Security Intelligence updates
Security
Threat overrides
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
For more information about threat names, see the malware encyclopedia (http://go.microsoft.com/fwlink/?LinkID=223866).
Specify the threat override settings
Threat name and override action: (none)
Set
OK
Cancel

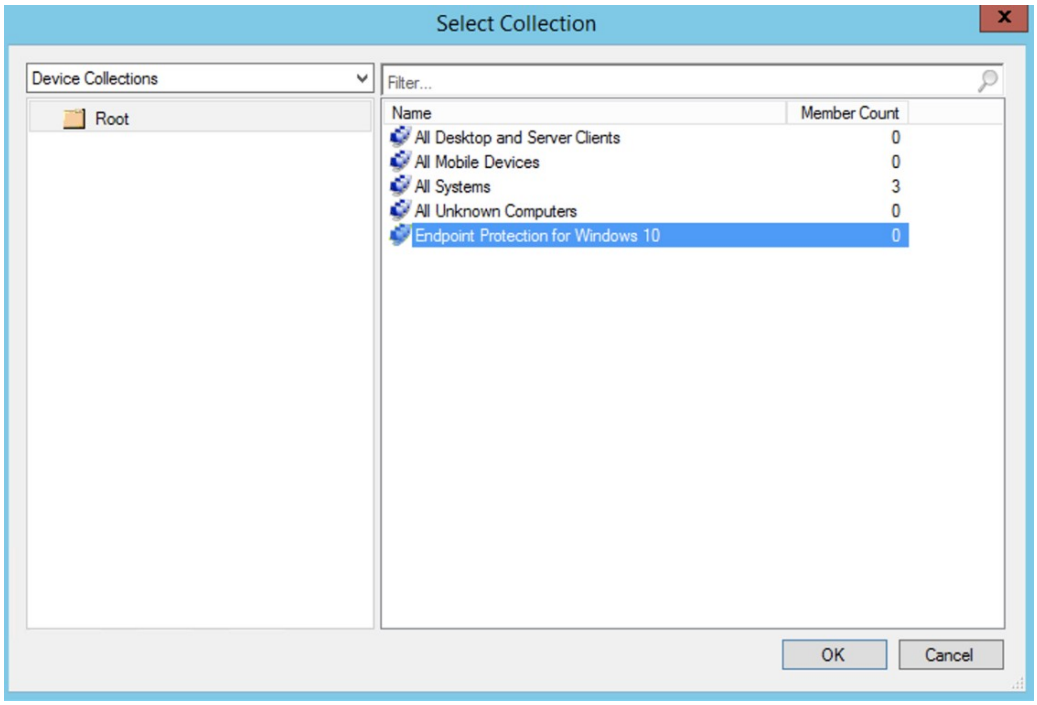

Next Generation Protection
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Cloud Protection Service
Security Intelligence updates
Security
Cloud Protection Service
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Joining Cloud Protection Service enables the collection and sending of information about detected malware to Microsoft for analysis.
Specify Cloud Protection Service settings
Cloud Protection Service membership type:
Advanced membership
Allow users to modify Cloud Protection Service settings:
No
Level for blocking suspicious files:
Normal
Allow extended cloud check to block and scan suspicious files for up to (seconds):
0
OK
Cancel


Next Generation Protection
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Cloud Protection Service
Security Intelligence updates
Security
Security Intelligence updates
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Configure how Endpoint Protection clients will receive security intelligence updates
Check for Endpoint Protection security intelligence at a specific interval (hours): (0 = disable check on interval)
8
Check for Endpoint Protection security intelligence daily at: (Only configurable if interval-based check is disabled)
12:00 PM
Force a security intelligence update if the client computer is offline for more than two consecutive scheduled updates:
Yes
Set sources and order for Endpoint Protection security intelligence updates:
4 sources selected
Set Source
If Configuration Manager is used as a source for security intelligence updates, clients will only update from alternative sources if security intelligence is older than (hours):
24
If UNC file shares are selected as a security intelligence update source, specify the UNC paths:
(none)
Set Paths
OK
Cancel

3. Cliquez avec le bouton droit sur la nouvelle stratégie anti-malware créée et sélectionnez **déployer**.



4. Ciblez la nouvelle stratégie anti-programme malveillant sur votre collection Windows 10, puis cliquez sur **OK**.



À l'issue de cette tâche, vous avez correctement configuré l'antivirus Windows Defender.

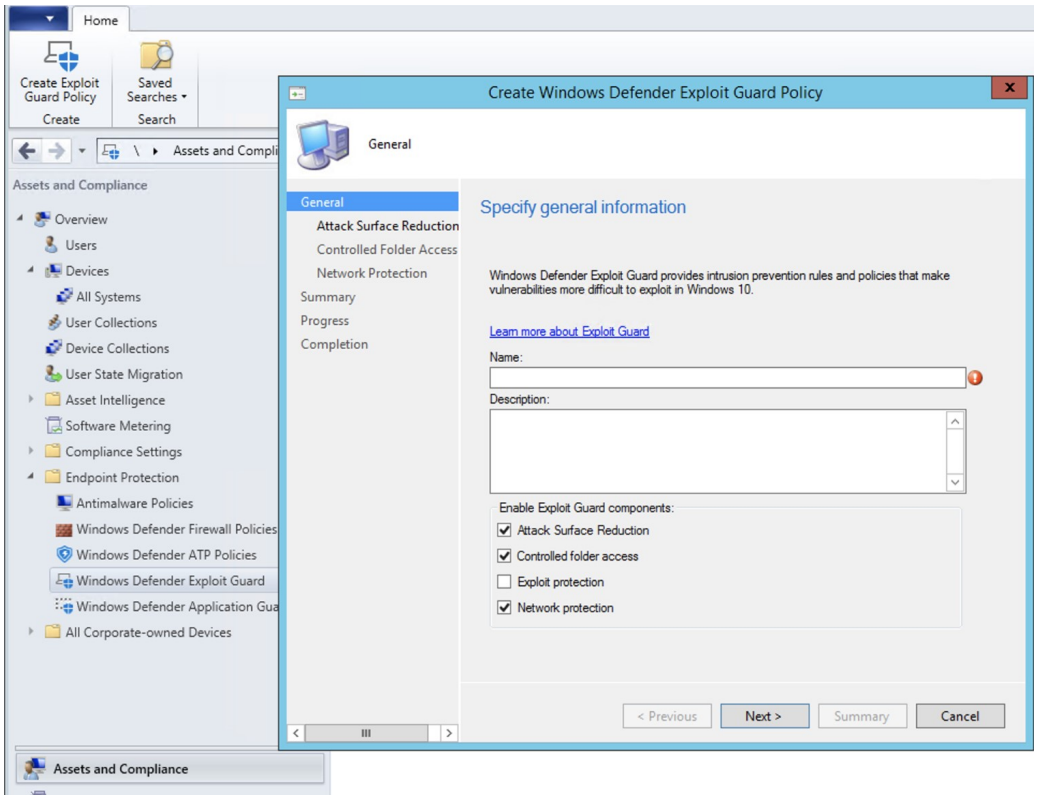
Réduction de la surface d'attaque

Le fondement de la réduction de surface d'attaque de Microsoft Defender ATP inclut l'ensemble des fonctionnalités disponibles sous exploit Guard. Les règles de réduction de surface d'attaque (ASR), l'accès contrôlé aux dossiers, la protection du réseau et la protection contre les attaques.

Toutes ces fonctionnalités fournissent un mode de vérification et un mode de blocage. En mode audit, il n'y a aucun impact sur l'utilisateur final. Tout cela consiste à collecter une télémétrie supplémentaire et à la rendre disponible dans le centre de sécurité Microsoft Defender. L'objectif d'un déploiement consiste à déplacer les contrôles de sécurité détaillés en mode bloc.

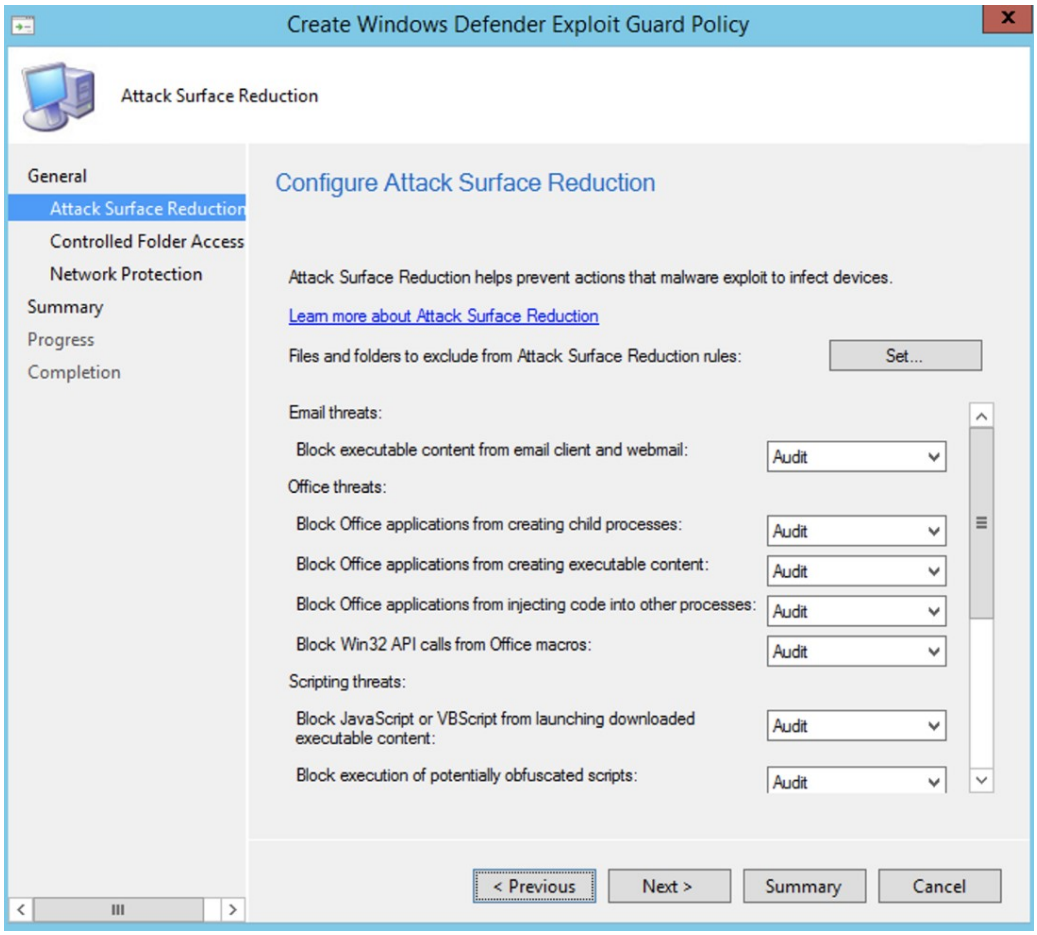
Pour définir les règles de ASR en mode d'audit:

1. Dans la console Microsoft Endpoint Configuration Manager, accédez à **ressources et conformité \ > vue d'ensemble \ > Endpoint Protection \ > Windows Defender exploit Guard** et sélectionnez **créer une stratégie de protection**contre les attaques.

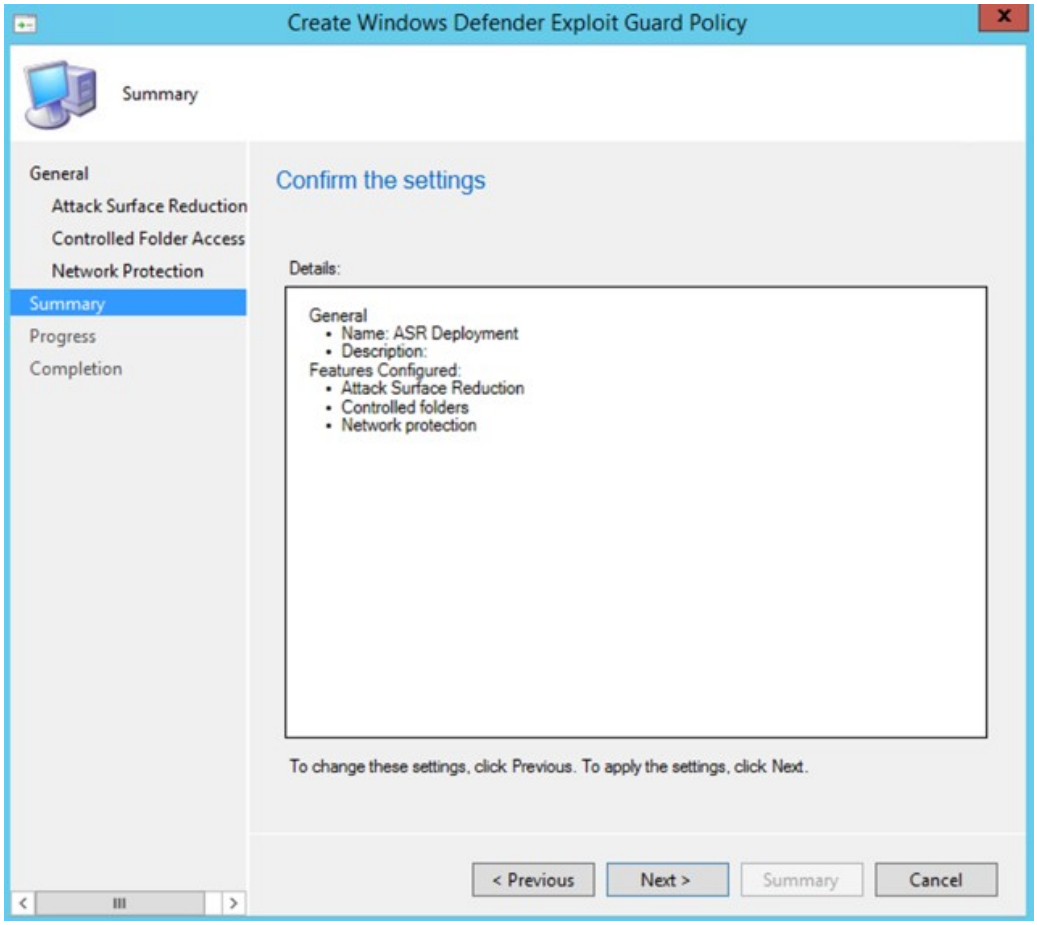


2. Sélectionnez **réduction surface Attack**.

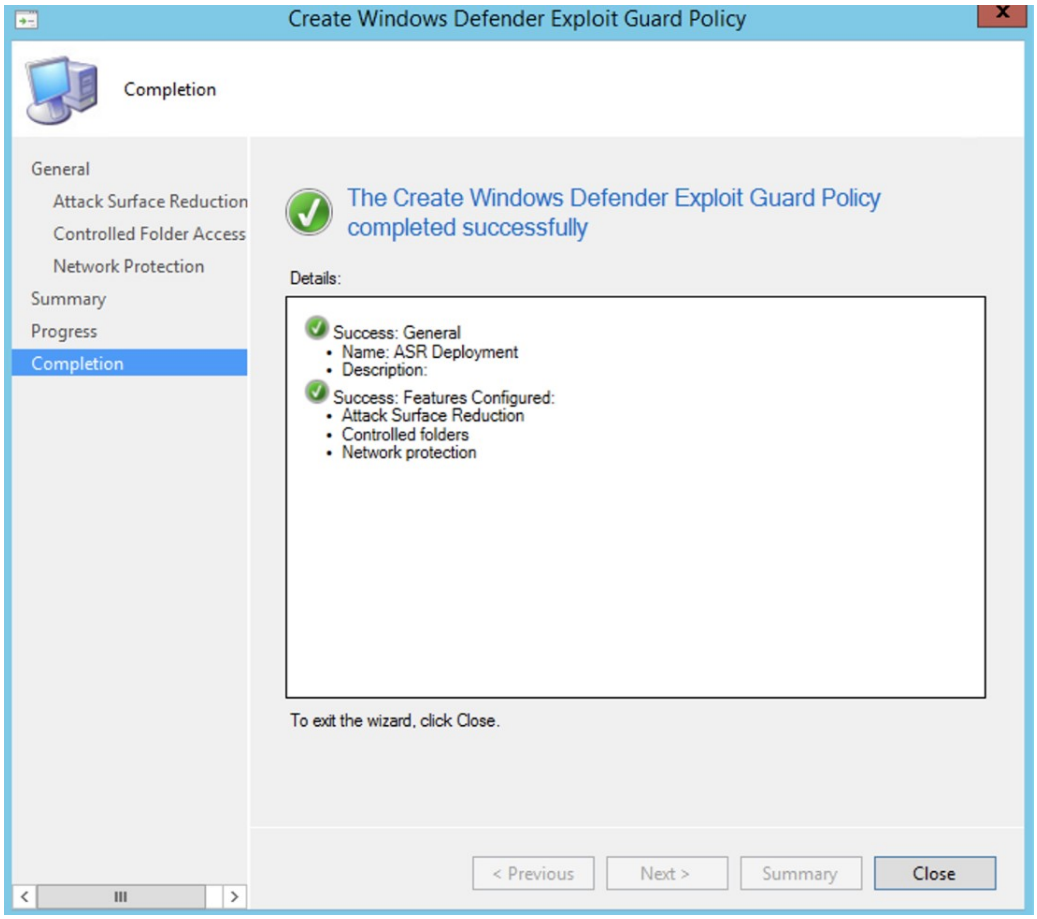
3. Définissez règles à **auditer** , puis cliquez sur **suivant**.



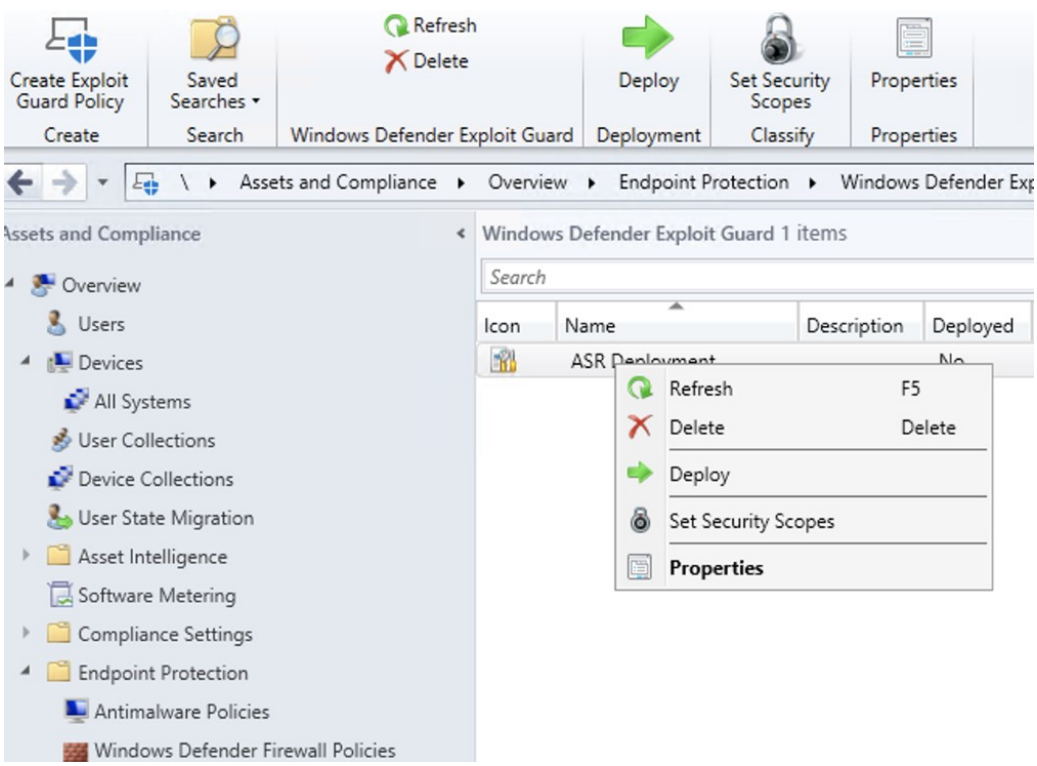
4. Confirmez la nouvelle stratégie d'exploitation du protecteur en cliquant sur **suivant**.



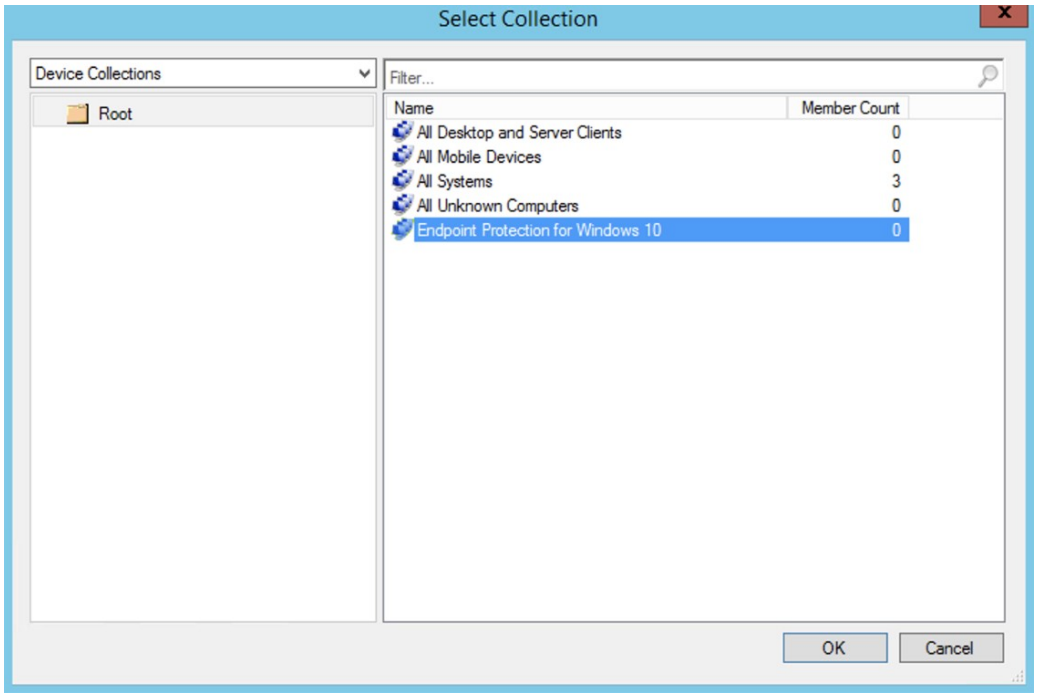
5. Une fois la stratégie créée, cliquez sur **Fermer**.



6. Cliquez avec le bouton droit sur la stratégie que vous venez de créer, puis sélectionnez **déployer**.



7. Ciblez la stratégie pour la collection Windows 10 que vous venez de créer, puis cliquez sur **OK**.

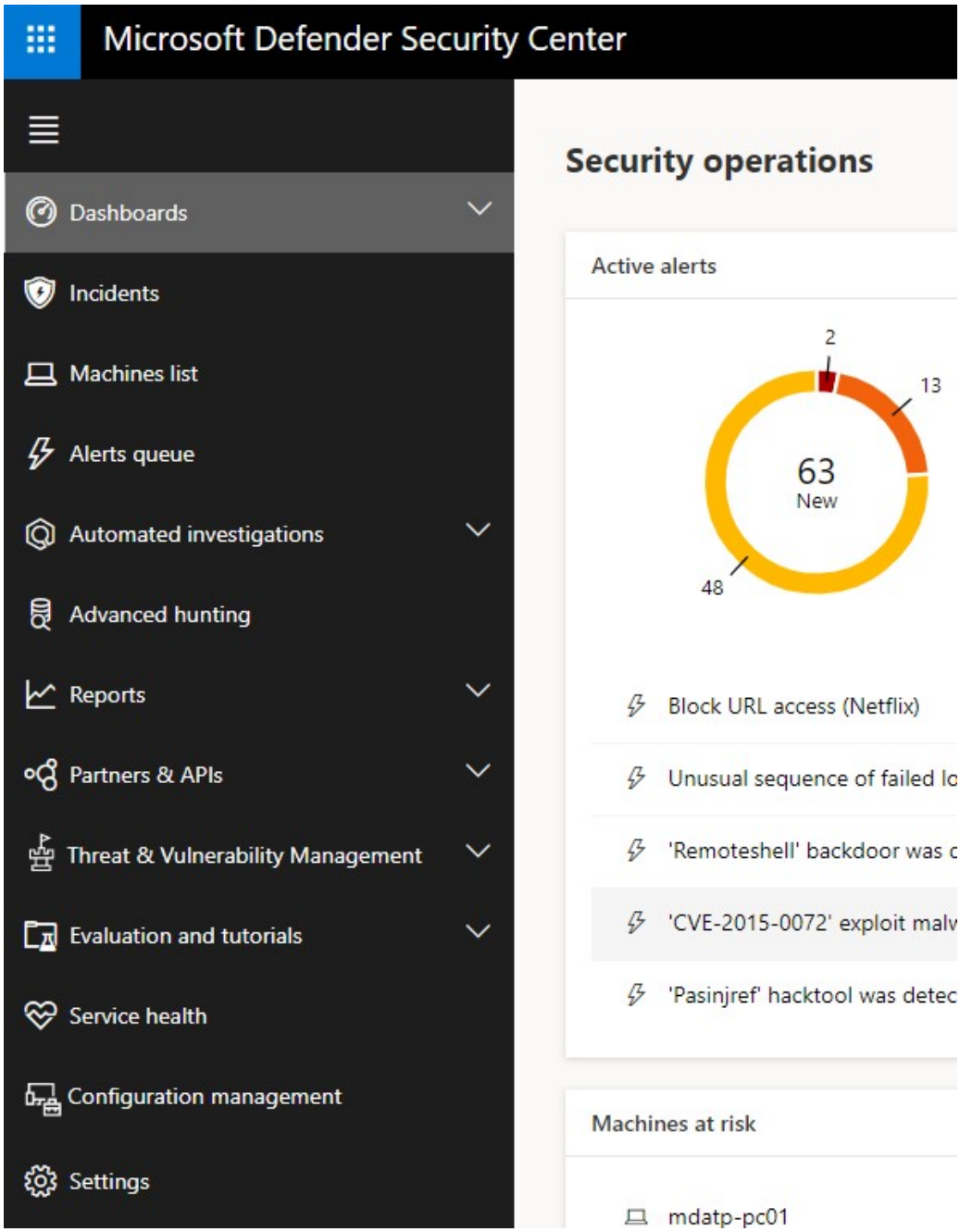


À l'issue de cette tâche, vous avez configuré correctement les règles de récupération automatique du mode audit.

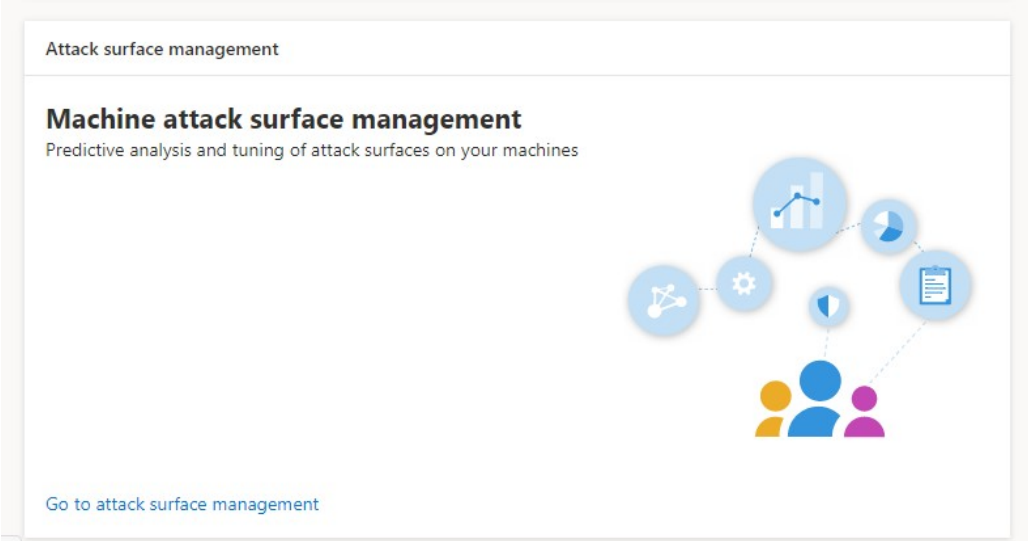
Vous trouverez ci-dessous des étapes supplémentaires permettant de vérifier si les règles ASR sont appliquées correctement aux points de terminaison. (Cela risque de durer quelques minutes)

1. À partir d'un navigateur Web, https://securitycenter.windows.comaccédez à.

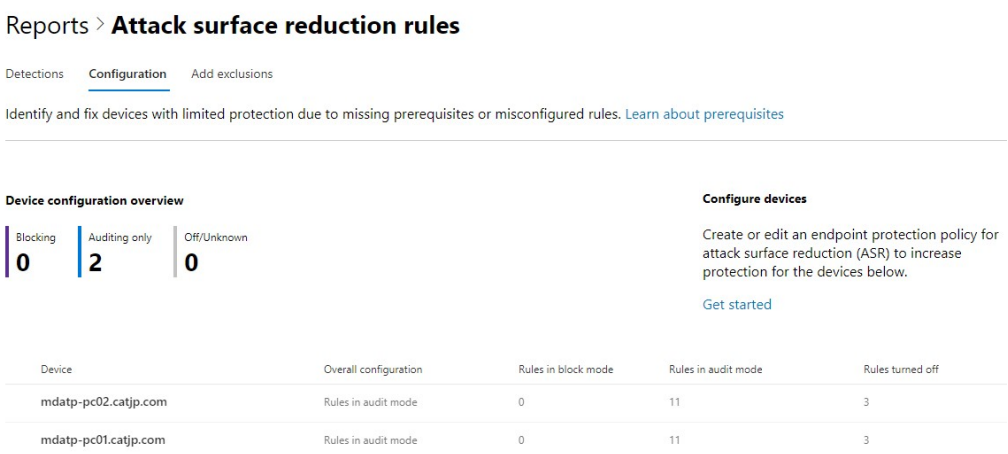
2. Sélectionnez **configuration** de la gestion dans le menu de gauche.



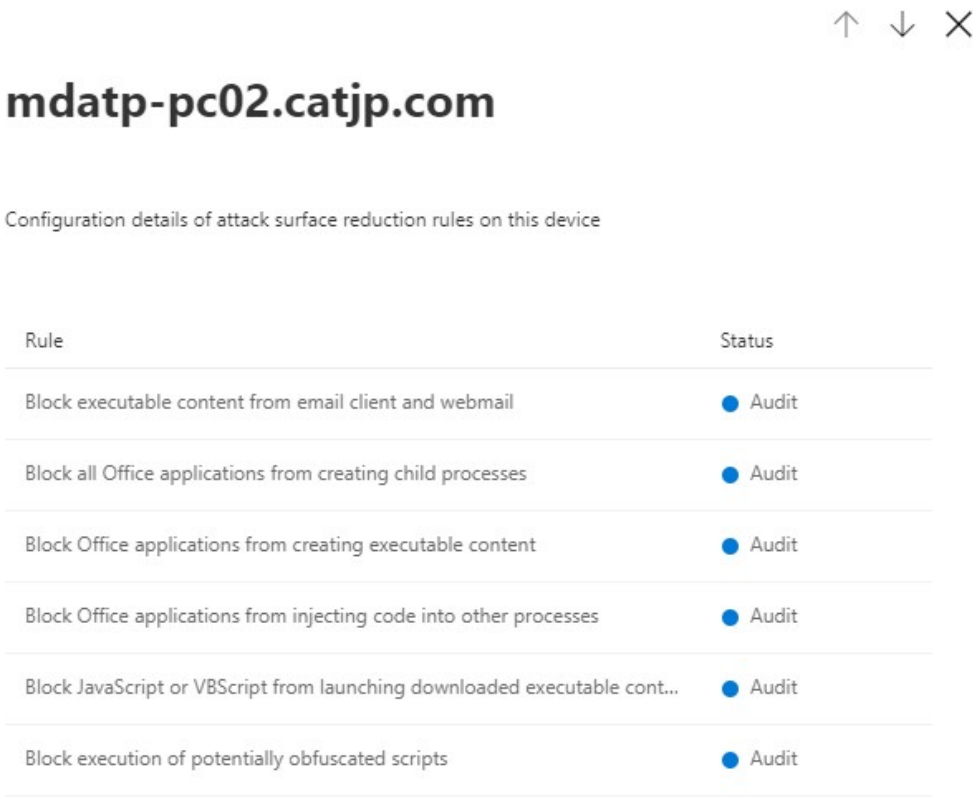
3. Cliquez sur **aller à la gestion** de la surface d'attaque dans le volet de gestion des surfaces d'attaque.



4. Cliquez sur l'onglet **configuration** dans rapports sur les règles de réduction de surface Il affiche la vue d'ensemble de la configuration des règles ASR et l'état des règles ASR sur chaque appareil.



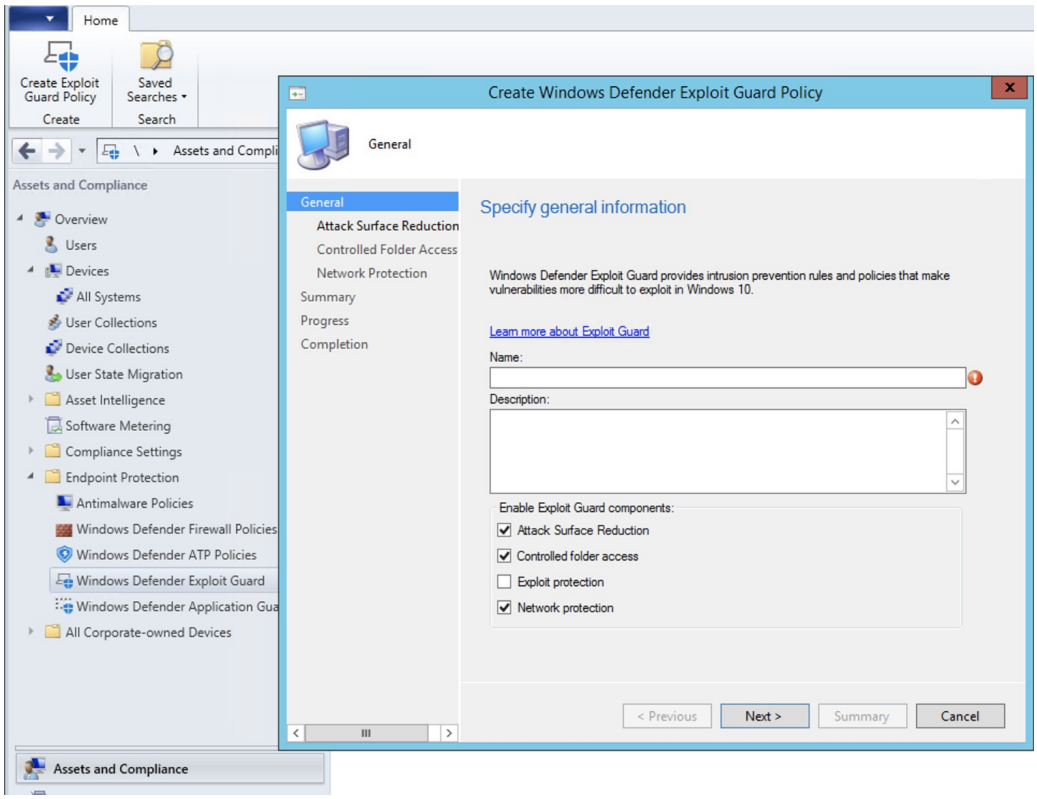
5. Cliquez sur chaque appareil pour afficher les détails de la configuration des règles de récupération automatique.



Pour plus d'informations, reportez-vous à [optimiser le déploiement et les détections de la règle ASR] .

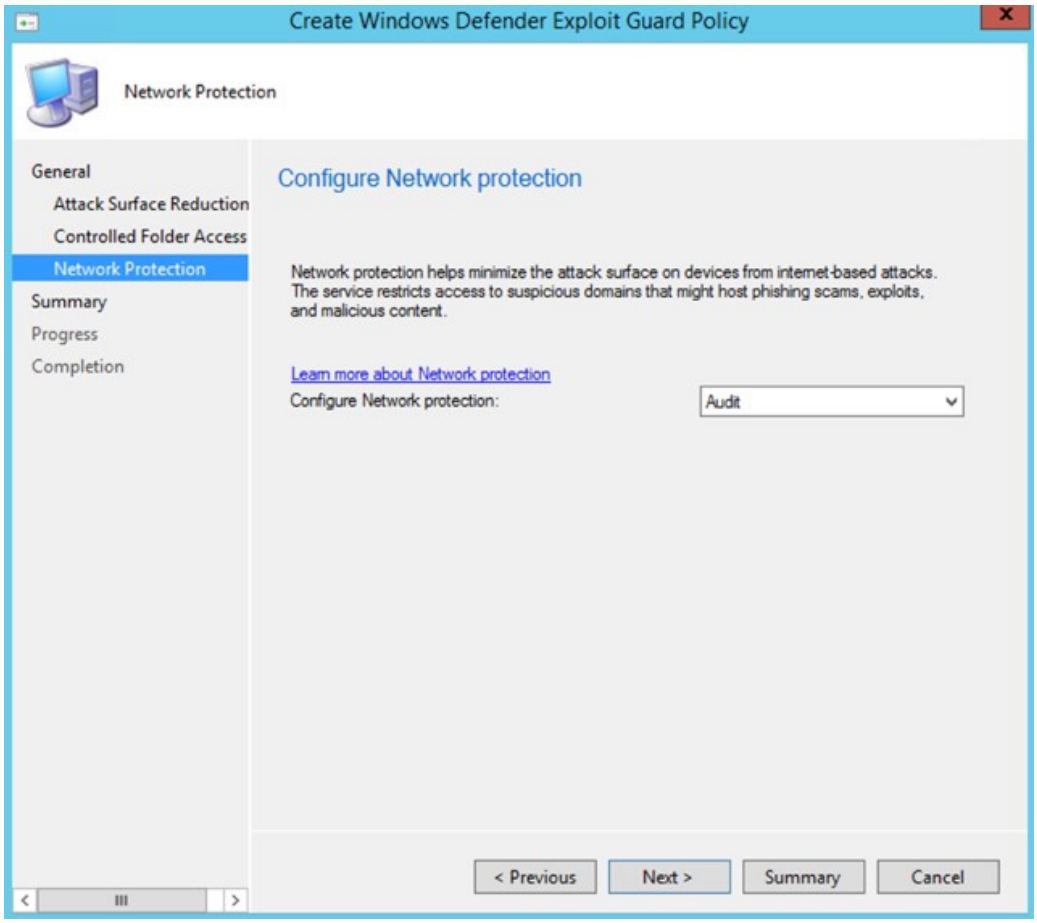
Pour définir des règles de protection du réseau en mode d'audit:

1. Dans la console Microsoft Endpoint Configuration Manager, accédez à **ressources et conformité \ > vue d'ensemble \ > Endpoint Protection \ > Windows Defender exploit Guard** et sélectionnez **créer une stratégie de protection**contre les attaques.

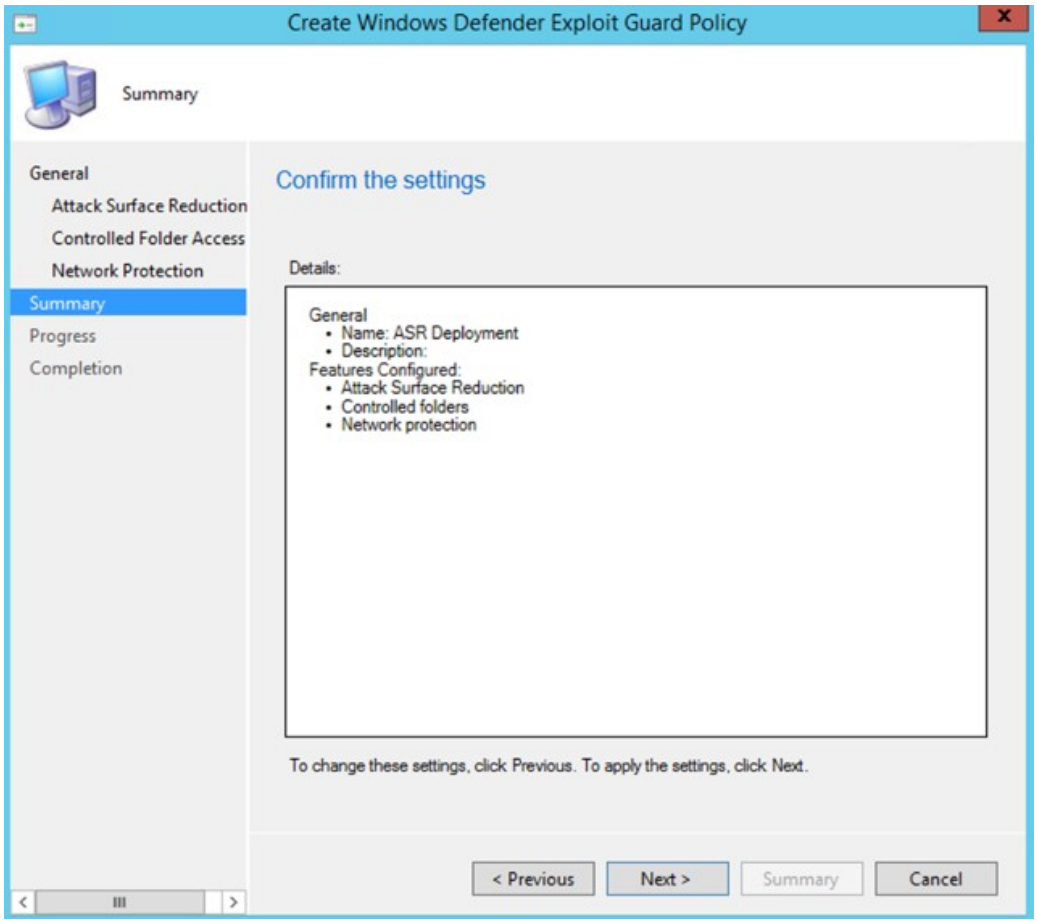


2. Sélectionnez **protection du réseau**.

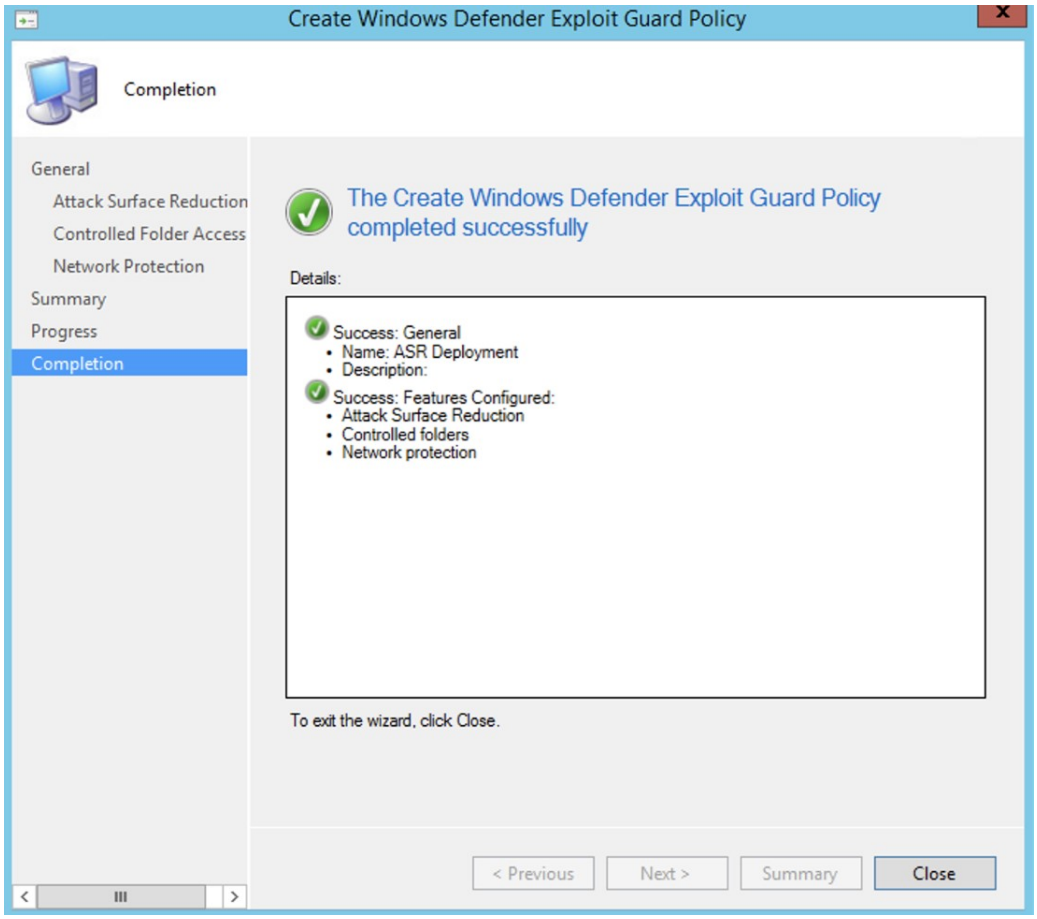
3. Définissez le paramètre sur **audit** , puis cliquez sur **suivant**.



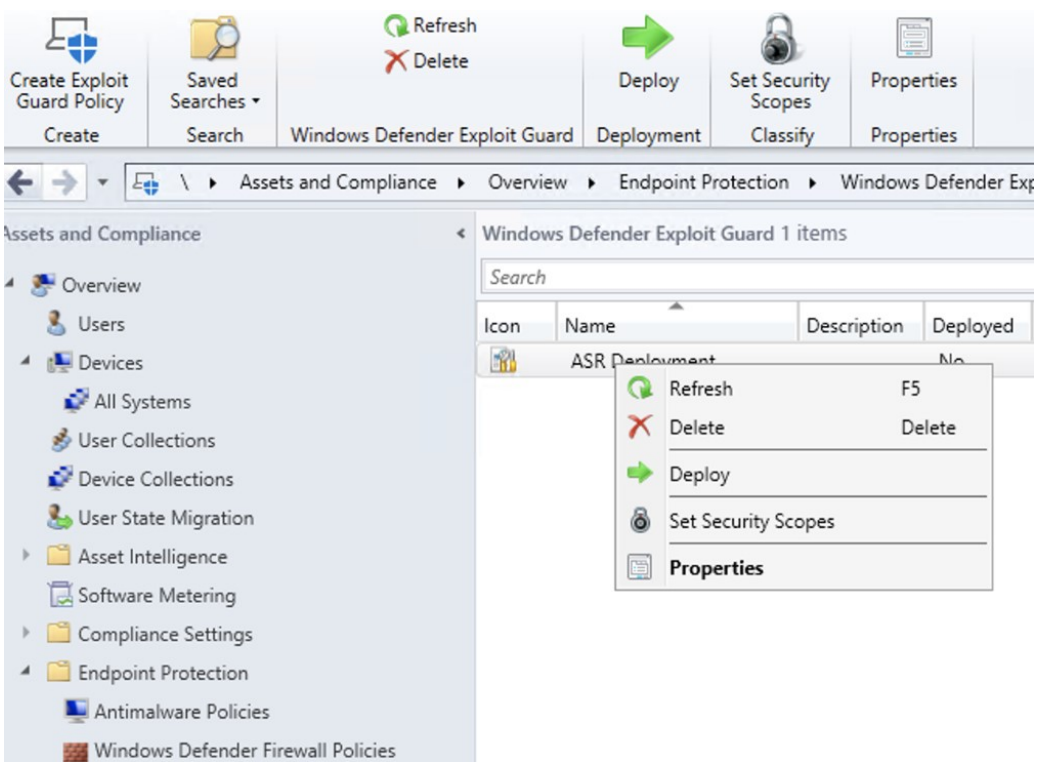
4. Confirmez la nouvelle stratégie d'exploitation du protecteur en cliquant sur **suivant**.



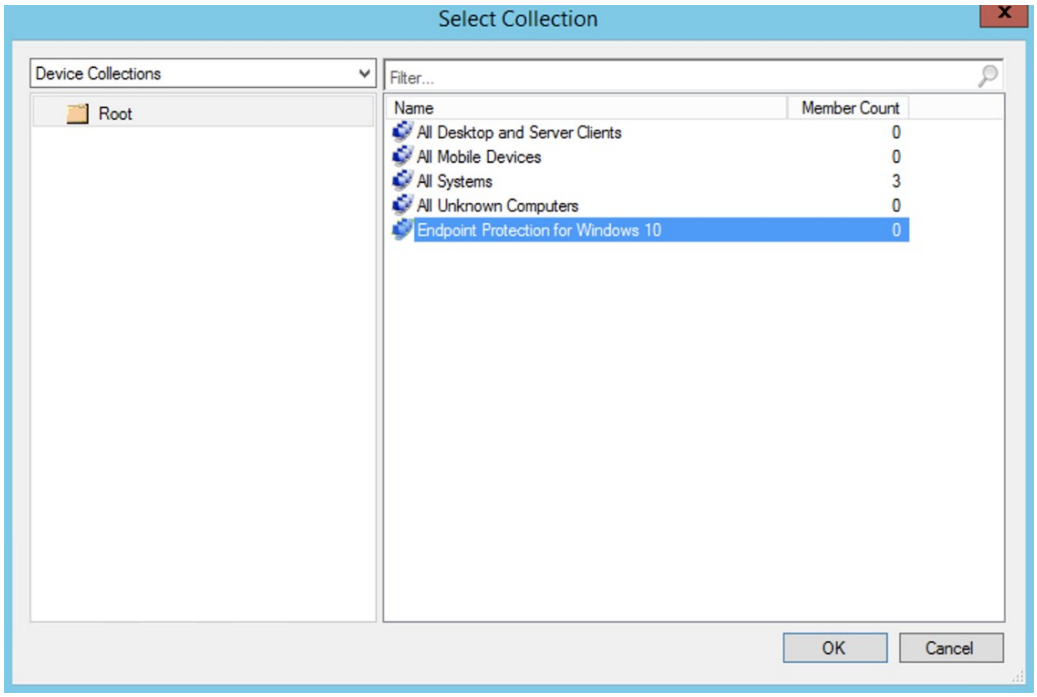
5. Une fois la stratégie créée, cliquez sur **Fermer**.



6. Cliquez avec le bouton droit sur la stratégie que vous venez de créer, puis sélectionnez **déployer**.



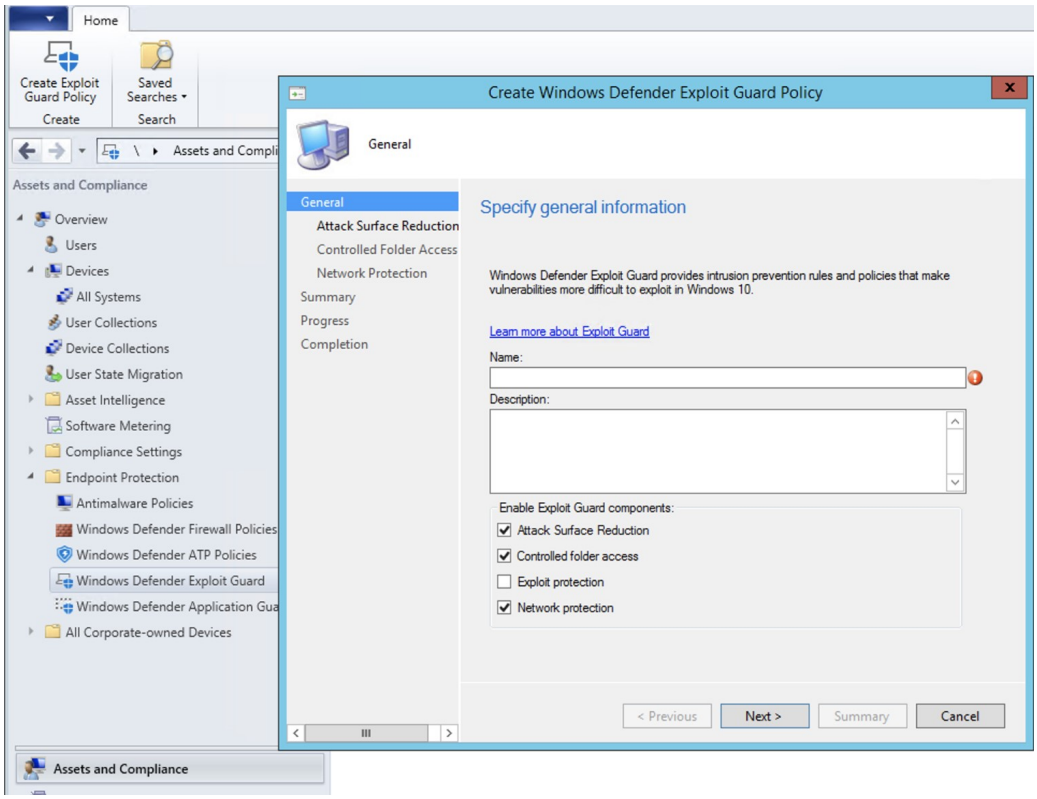
7. Sélectionnez la stratégie pour la collection Windows 10 que vous venez de créer, puis cliquez sur **OK**.



À l'issue de cette tâche, vous avez correctement configuré la protection réseau en mode d'audit.

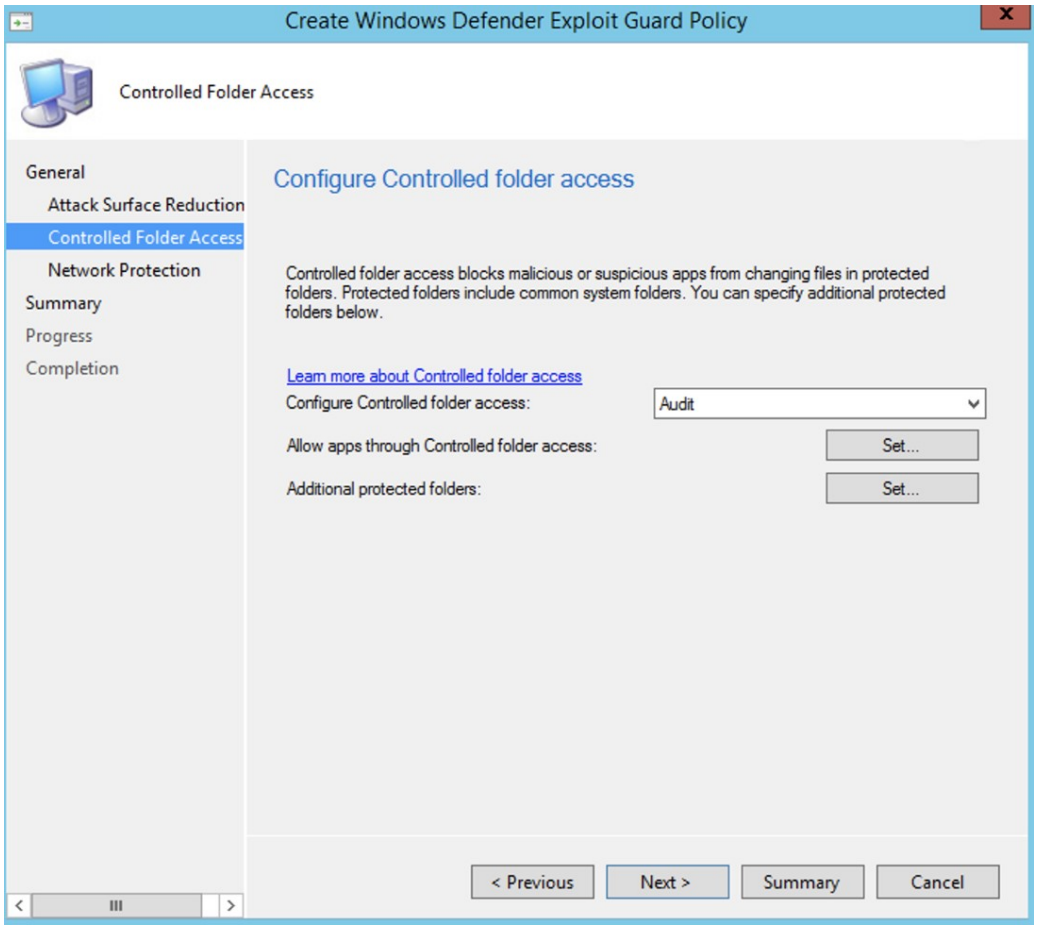
Pour définir des règles d'accès aux dossiers contrôlés en mode d'audit:

1. Dans la console Microsoft Endpoint Configuration Manager, accédez à **ressources et conformité \ > vue d'ensemble \ > Endpoint Protection \ > Windows Defender exploit Guard** et sélectionnez **créer une stratégie de protection**contre les attaques.

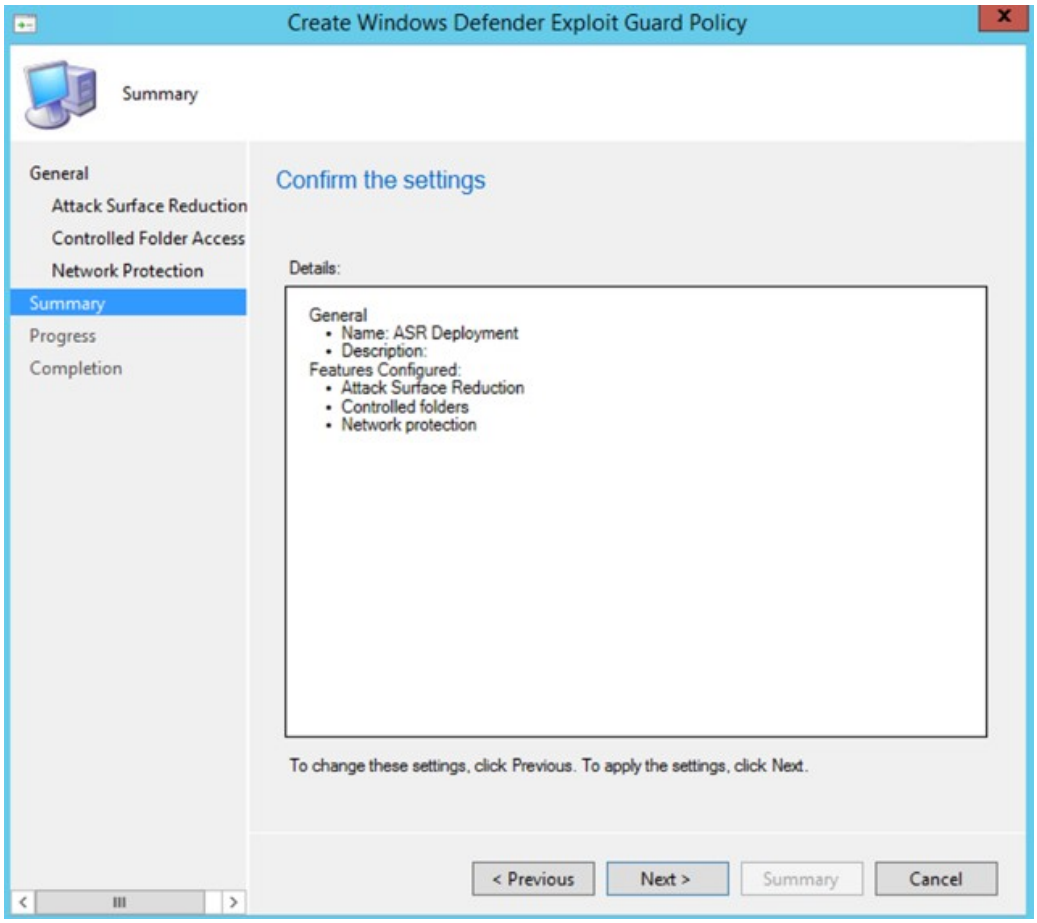


2. Sélectionnez **accès contrôlé au dossier**.

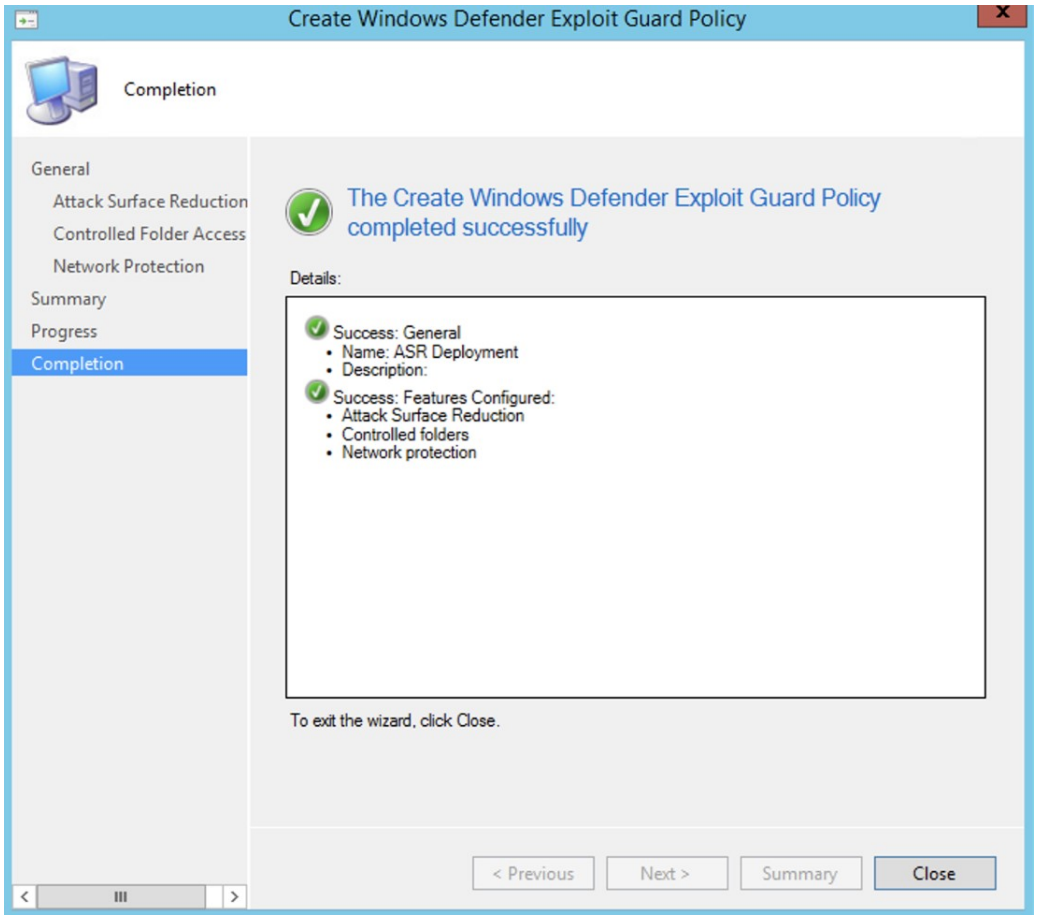
3. Définissez la configuration à **auditer** , puis cliquez sur **suivant**.



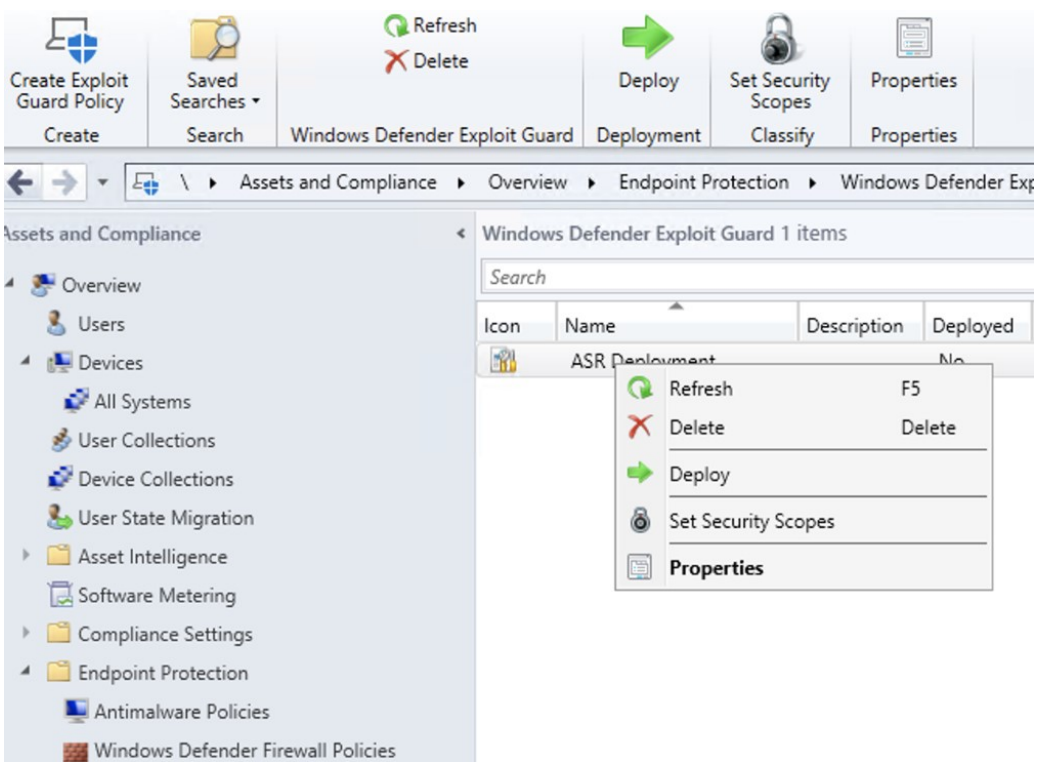
4. Confirmez la nouvelle stratégie d'exploitation du protecteur en cliquant sur **suivant**.



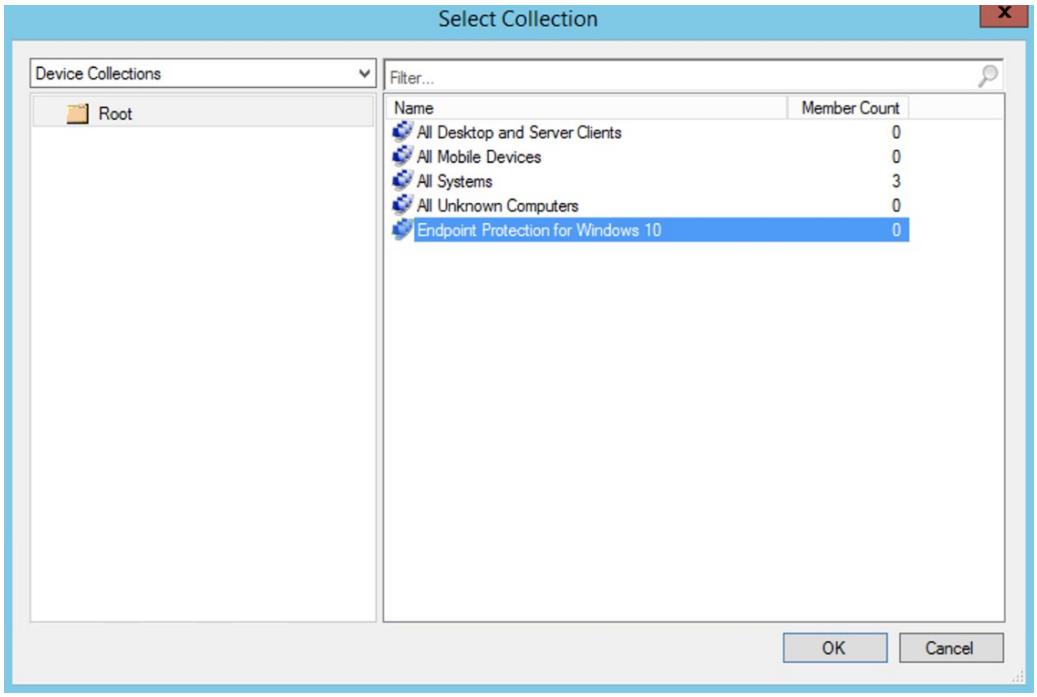
5. Une fois la stratégie créée, cliquez sur **Fermer**.



6. Cliquez avec le bouton droit sur la stratégie que vous venez de créer, puis sélectionnez **déployer**.



7. Ciblez la stratégie pour la collection Windows 10 que vous venez de créer, puis cliquez sur **OK**.



À l'issue de cette tâche, vous avez désormais configuré avec succès l'accès contrôlé aux dossiers en mode d'audit.

Cette page est-elle utile ?

Yes No
