### Intégration au service Microsoft Defender ATP

10/04/2020 • 8 minutes de lecture • 🏘 📑

#### Dans cet article

Intégration à l'aide du gestionnaire de configuration de point de terminaison Microsoft Détection et réponse au point de terminaison Protection nouvelle génération Réduction de la surface d'attaque

### 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 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.

 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.

Create De	vice Collection Wiza	ard
Specify details for	this collection	
Nama	Endouint Protection	for Windows 10
Comment:		
Limiting collection:	All Systems	Browse
Last update		Last membership change
	Specify details for Name: Comment: Select a collection to us that you can add to this Umiting collection:	Specify details for this collection         Name:       Endpoint Protection         Comment:

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

2	Create Device Colle	ction Wizard		
Membership R	bules			
General Membership Rules	Define membership rules for	or this collection		
Progress Completion	Membership rules determine the resou can use membership rules to add a sp membership can also include or exclur objects that are members of the limiting	rces that are included in the c eofic object or a set of object de other collections. Membersi g collection.	ollection when s from a query hip rules can i	n it updates. You , The collection add only those
	Membership rules:	Time	Collect	tion Id
	There as	e no items to show in this view	Ψ.	>
		Add Rule 💌	Edt	Delete
	Use incremental updates for this	Direct Rule		
	An incremental update periodic to this collection. This option do	Query Rule Device Category Rule Include Collections Exclude Collections	sdds re tate fo	sources that qualify this collection.
	<ul> <li>Schedule a full update on this-w Occurs every 7 days effective 9/24/2</li> </ul>	2019 4:18 AM		Schedule
	< Previo	ous Next >	Summary	Cancel

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

ieneral		Query Rule Properties	
lembership Rules ummary rogress	General Name:	0	when it updates. You
ompletion		Import Query Statement	suery. The collection can add only those
	Resource class:	System Resource V	
		Edit Query Statement	
	Query Statement:	Select * from SMS_R_System	
	Configuration Man Instrumentation (W database.	ager uses the Windows Management MI) Query Language (WQL) to query the site	ds resources that qual te for this collection.
		OK Cancel	Schedule

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

General	Query Statement Properties	
Membership Rules Summary Progress Completion	General Oteria Joins You can specify citeria to narrow the query and limit the results that are returned. Criteria:	when it updates. You uery. The collection can add only those
		offection Id
		is resources that qualify e for this collection.
	Show Query Language OK Cancel	

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.

1.1		Criterion Prope	ties	×
Membership Rules Summary Progress Completion	General	Properties		when it updates. You usry. The collection
	Criterion Type:	Simple value	*	
	Where:	Operating System - E	uild Number	
			Select	
	Operator:	is equal to	v	ollection Id
	Value:	10240		
		Type: Sting	Value	1
		.,,,	Vaue	Delete
				Is resources that qua e for this collection.
			OK Cancel	Schedule

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

2	Create Device	e Collection Wizard		
Membership	Rules			
General Membership Rules Summary Progress Completing	Define membership n Membership rules determine t	rules for this collection	the collection when biects from a query	t updates. You The collection
Completion	membership can also include objects that are members of t Membership rules:	or exclude other collections. Men he limiting collection.	bership rules can a	dd only those
	Windows 10	Guery	Not An	olicable
	<			>
		Add Rule	Edt	Delete
	Use incremental updates An incremental update pe to this collection. This opt	for this collection modically evaluates new resource ion does not require you to sched on this collection re 9/24/2019 4:18 AM	s and then adds res ule a full update for S	ources that qualify this collection.
		< Previous Next >	Summary	Cancel

9. Sélectionnez **Suivant**.

General • Collection Name • Comment: Membership Rules • (Direct) WIN10-0	: Windows 10 - WDA 12	TP	

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 <u>paramètres, puis sur intégration</u>.
- Sous méthode de déploiement, sélectionnez la version prise en charge de \* \* Microsoft Endpoint Configuration Manager \* \*.

Settings		
General	Select operating system to start onboarding process:	
Data retention	Windows 10 $\checkmark$	
Alert notifications		
Power BI reports	1. Onboard a machine	
Advanced features	First machine onboarded: Completed Ø	
Permissions Roles Machine groups	preparation instructions, read Onboard and set up. Deployment method	ration packa
	Configuration Manager V	
APIs	Configuration Manager v Local Script (for up to 10 machines)	
APIs SIEM	Configuration Manager V Local Script (for up to 10 machines) Group Policy	
APIs SIEM	Configuration Manager  Configuration Manager Configuration Manager (current branch)	5
APIs SIEM Rules	Configuration Manager  Local Script (for up to 10 machines) Group Policy Configuration Manager (current branch) Configuration Manager 2012 / 2012 R2 / 1511 / 1602 / 1606	3
APIs SIEM Rules Custom detections	Configuration Manager  Configuration Manager (our pto 10 machines) Group Policy Configuration Manager (current branch) Configuration Manager 2012 / 2012 R2 / 1511 / 1602 / 1606 Mobile Device Management / Microsoft Intune	3 N
APIs SIEM Rules Custom detections Alert suppression	Configuration Manager  Local Script (for up to 10 machines) Group Policy Configuration Manager (current branch) Configuration Manager 2012 / 2012 R2 / 1511 / 1602 / 1606 Mobile Device Management / Microsoft intune VDI onboarding scripts for non-persistent machines	3

3. Sélectionnez Télécharger le package.



- 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**.

Name:	
WDATP Win 10 Policy	
Description:	
Windows Defender ATP Windows 10 Policy	^
olicy type: Onboarding - Add devices to the online service and start sendir Offboarding - Remove devices from the online service (for exam longer managed)	ng threat data for analysis

- 8. Cliquez sur Parcourir.
- 9. Accédez à l'emplacement du fichier téléchargé à partir de l'étape 4 cidessus.

pecify which file samples are shared for nalysis by the Windows Defender ATP online ervice:	All file types e	
Telemetry reporting frequency:	Normal	~

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

pecify which file samples are shared for nalysis by the Windows Defender ATP online ervice:	All file types	~
Telemetry reporting frequency:	Normal	~

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

General     Name: WDAT     Description: W	P Win 10 Policy	TP Windows 1	Policy	
Configuration • Policy Type: C	nboarding			
Organization 1  Agent Configuratio     Sample Sharir     Telemetry Rep	n ng: All file types porting Frequency: I	4a/6-01/a-0/8 Normal	000621068	
	an aliak Presiona	To apply the est	tions, click Next	

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

<ul> <li>Success: Gen</li> <li>Name: WDA</li> <li>Description: \</li> </ul>	eral 'P Win 10 Policy Vindows Defender ATP	Windows 10 Polic	у	
<ul> <li>Success: Cont</li> <li>Policy Type:</li> <li>Organization</li> </ul>	guration Onboarding ID: 66cd81a1-3836-4a7	6-h17a-078heh82	1b8a	
Success: Ager • Sample Shar • Telemetry Re	t Configuration ng: All file types porting Frequency: Norr	nal		
exit the wizard, cli	ck Close.			

- 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**.

Device Collections		
Device Collections	Filter	
Root	Name	Member Count
	All Desktop and Server Clients	0
	All Mobile Devices	0
	Systems All Systems	3
	All Unknown Computers	0
	Endpoint Protection for Windows 10	0

### 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.

- 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. Configure connection

Configure the agents to connect using the following workspace information:

Workspace ID

Workspace key

Copy
Copy
Copy

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:



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



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 <u>mise à jour pour</u> <u>l'expérimentation des clients et la télémétrie de diagnostic</u> 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 <u>KB4074598</u>
- Installez <u>.NET Framework 4,5</u> (ou une version ultérieure ) ou <u>KB3154518</u>.
   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 .

Specify info	rmation about this package
Enter a name an Application Cata	d other details for the new package. To take full a log, use an application instead.
Name:	WDATP Onboarding Down-Level Systems
Description:	

5. Option vérifier le programme standard sélectionnée

Choose the program type that you want to create
Standard program
Create a program for a client computer.

6. Cliquez sur **Suivant**.

Name:	WDATP Install MMA CMD Script	
Command line:	installMMA.cmd	
Startup folder:		
Run:	Hidden	
Program can run:	Whether or not a user is logged or	
Run mode:	Run with administrative rights	
Allow users to view	and interact with the program installation	
Drive mode:	Runs with UNC name	
Beconnect to distrib	n tion point at log on	

- 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.

All Windows RT	
All Windows RT 8.1	
All Windows 10 (32-bit)	
All Windows 10 (64-bit)	
All Windows 7 (64-bit)	
All Windows 8 (64-bit)	
All Windows 8.1 (64-bit)	
Windows Embedded 8 Industry (64-bit)	
Windows Embedded 8 Standard (64-bit)	)
Windows Embedded 8.1 Industry (64-bit	t)
timated disk space:	Unknown
avimum allowed run time (minutes):	720
windin allowed full time (minutes).	/20

14. Vérifiez la configuration, puis cliquez sur suivant.

eneral:	10
<ul> <li>Name: WDATP Onboarding Down-Lev</li> <li>Description:</li> </ul>	vel Systems
Version:	
Publisher:	
Language:	
rogram Type: Standard Program	
rogram:	
<ul> <li>Name: WDATP Install MMA CMD Scri</li> </ul>	pt
Command line: InstallMMA.cmd     Start in:	
Run: Hidden	
· Run mode: Run with administrative rig	hts
<ul> <li>Program can run: Whether or not a use</li> </ul>	er is logged on
Drive mode: Runs with UNC name	
equirements:	
<ul> <li>Platforms supported: Any</li> </ul>	
<ul> <li>Maximum allowed runtime(minutes): 7</li> </ul>	20

To change these settings, click Previous. To apply the settings, click Next.

#### 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.

 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.

	Create Antimalware Policy
General Scheduled scans Scan settings Default actions Real-time protection Exclusion settings Advanced Threat overrides Cloud Protection Service Security Intelligence updates	
	OK Cancel

 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.

	Next Generation Protection	X
General Scheduled scans Scan settings Default actions Real-time protection Exclusion settings Advanced Threat overrides Cloud Protection Service Security Intelligence updates Security	Scheduled scans         Image: The settings that you specify in this policy apple Custom policies override the default policy.         Specify scheduled scan settings         Image: The settings that you specify in this policy apple Custom policies override the default policy.         Specify scheduled scan settings         Image: Scan type:         Scan type:         Scan type:         Scan time:         Run a daily quick scan on client computers:         Daily quick scan schedule time:         Check for the latest security intelligence updates before running a scan:         Start a scheduled scan only when the computer is offline during two or more scheduled scans:         Limit CPU usage during scans to (%):	y to all Endpoint Protection clients in the hierarchy. Yes ▼ Quick Scan ▼ Daily ▼ 12:00 PM ↓ Yes ▼ No ▼ Yes ▼ No ▼ Yes ▼ 50 ▼
		OK Cancel

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 <u>sécurité Windows</u>

	Next Generation Protection	n	X
General Scheduled scans Scan settings Default actions Real-time protection Exclusion settings Advanced Threat overrides Cloud Protection Service Security Intelligence updates Security	Scan settings         Image: Specify scan settings         Second settings         Scan remail and email attachments:         Scan remail and email attachments:         Scan removable storage devices such as USB drives:         Scan network files:         Scan archived files:         Allow users to configure CPU usage during scans:         User control of scheduled scans:	poply to all Endpoint Protection clients in the hierarchy. Yes ↓ No ↓ Yes ↓ No ↓ Yes ↓ No ↓ No ↓ No ↓	
		OK Cancel	

	Next Generatio	on Protection		X
General Scheduled scans Scan settings Default actions Real-time protection Exclusion settings Advanced Threat overrides Cloud Protection Service Security Intelligence updates Security	Next Generations          Default actions         Image: The settings that you specify custom policies override the custom policies override the specify how Endpoint Protection represented response for each the specify default actions         Specify default actions         Severe:         High:         Medium:         Low:	on Protection y in this policy apply to all Endpoint P default policy.  sponds to threats classified accordin reat is specified in the security intellig  Quarantine Quarantine Quarantine Allow	Protection clients in the g to the following all gence files.	et levels. The
			01/	
		[	ОК	Cancel

1	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	Next Generation Protection         Image: Comparison of the settings that you specify in this policy apply to Custom policies override the default policy.         Specify real-time protection settings         Image: Comparison of the setting protection of the setting protection:         Monitor file and program activity on your computer:         Scan system files:         Scan all downloaded files and enable exploit protection for Internet Explorer:         Enable behavior monitoring:         Enable protection against network-based exploits:         Allow users on client computers to configure real-time protection against Potentially Unwanted Applications at download and prior to installation:	all Endpoint Protection clients in the hierarchy.
		OK Cancel

	Next Generation Pro	otection		X
General Scheduled scans Scan settings Default actions Real-time protection Exclusion settings Advanced Threat overrides Cloud Protection Service Security Intelligence updates Security	Specify excluded files and folders:         Excluded file synces:	s policy apply to all Endpoint Protection <b>, file types, and processes</b> %windir%\Softwa (none) (none)	on clients in the hierarchy.	x
			OK Cancel	
			Cancel	

General         Scheduled scans         Scan settings         Default actions         Real-time protection         Exclusion settings         Advanced         Threat overrides         Cloud Protection Service         Security Intelligence updates         Scourity         Orable the client user interface:         No< ∨         Underwiden the user interface:         Scourity         Delate the client user interface:         Now vertices         Scourity         Allow users to configure the setting for quarantimed file deleton::         Now vertices to configure the setting for quarantimed file deleton::         Allow users to configure the setting for intelligence update stat times (within 30)         Allow users to nodify auto sample file autorisation to help Microsoft delemine whether certain decleted.         Randomize scheduled scan and security intelligence update stat times (within 30)         Microsoft determine whether certain decleted.         Microsoft determine wheth	1	Next Generation Protection	
Exclusion settings         Advanced         Threat overrides         Cloud Protection Service         Security Intelligence updates         Scurity         Computer when the user needs to nu a full scan, update security intelligence, or nu Windows Defender Offline.         Delete quarantine files after (days):         30         Allow users to configure the setting for quarantine file after (days):         Allow users to configure the setting for quarantine file deletion:         Allow users to view the full History results:         No         Enable reparse point scanning:         Randomize scheduled scan and security intelligence update start times (within 30 minutes):         Brable auto sample file submission to help Microsoft determine whether certain detected items are Malcious:         Allow is sent to modify auto sample file         Allow is sent to modify auto sample file	General Scheduled scans Scan settings Default actions	Advanced The settings that you specify in this policy apply Custom policies override the default policy.	r to all Endpoint Protection clients in the hierarchy.
Advanced         Threat overrides         Cloud Protection Service         Security Intelligence updates         Security Intelligence updates         Security Intelligence updates         Security         Security         Outer when the user needs to up a full scan, update security intelligence, or run Windows Defender Offline.         Delete quarantined files after (days):         Allow users to configure the setting for quarantined files after (days):         Allow users to exclude files and folders, file types, and processes:         Allow all users to view the full History results:         No         Enable treparse point scanning:         No         Security intelligence update start times (within 30 minutes):         Enable reparse point scanning:         No         Security intelligence update start times (within 30 minutes):         Enable users to mortify auto sample file submission to help Microsoft determine whether certain detected terms are Malicious:         Allow users to mortify auto sample file         Submission settings:	Exclusion settings		
Threat overrides         Cloud Protection Service         Security Intelligence updates         Security         Security         Cloud Protection Service         Security         Cloud Protection Service         Security         Cloud Protection Service         Security         Cloud Protection Service         Security         Security         Delete quarantined file safter (days):         Allow users to configure the setting for quarantined file deleton:         Allow users to view the full History results:         No         Chade a sample file submission to help Microsoft determine whether certain detected tens are Malcious:         Allow users to modify auto sample file submission settings:	Advanced	Specify advanced settings	
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       Image: Client C	Threat overrides Cloud Protection Service Security Intelligence updates	Create a system restore point before computers are cleaned: Disable the client user interface:	No v No v
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 atto sample file submission to help Microsoft determine whether certain detected items are Malicious:       No       ∨         Allow users to modify auto sample file       No       ∨	Security	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 v
Allow users to configure the setting for quarantined file deletion:       No <ul> <li>Allow users to exclude files and folders, file types, and processes:</li> <li>Allow all users to view the full History results:</li> <li>No</li> <li>Enable reparse point scanning:</li> <li>No</li> <li>Randomize scheduled start times (within 30 minutes):</li> <li>Enable auto sample file submission to help Microsoft determine whether certain detected items are Malicious:</li> <li>Allow users to modify auto sample file submission settings:</li> </ul> No <ul> <li>No</li> <li>Carced</li> </ul>		Delete quarantined files after (days):	30 🗘
Allow users to exclude files and folders, file       No       ✓         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       No       ✓       ✓		Allow users to configure the setting for quarantined file deletion:	No ¥
Alow 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       ✓		Allow users to exclude files and folders, file types, and processes:	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       ~		Allow all users to view the full History results:	No v
Randomize scheduled scan and security intelligence update start times (within 30 minutes):       No <ul> <li>Enable auto sample file submission to help Microsoft determine whether certain detected items are Malicious:</li> <li>Allow users to modify auto sample file submission settings:</li> </ul> No <ul> <li>OK</li> <li>Carcel</li> </ul>		Enable reparse point scanning:	No Y
Enable auto sample file submission to help No V Microsoft determine whether certain detected items are Malicious: Allow users to modify auto sample file No V submission settings:		Randomize scheduled scan and security intelligence update start times (within 30 minutes):	No Y
Allow users to modify auto sample file No V		Enable auto sample file submission to help Microsoft determine whether certain detected items are Malicious:	No Y
		Allow users to modify auto sample file submission settings:	Nov
			OK Cancel

	Next Generation Protection	X
General         Scheduled scans         Scan settings         Default actions         Real-time protection         Exclusion settings         Advanced         Threat overrides         Cloud Protection Service         Security Intelligence updates         Security	Threat overrides         Image: 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://co.unicrosoft.com/fwlink/?LinkID=223866).         Specify the threat override settings         Image: Threat name and override action:       (none)         Set	
	OK Cancel	

Next Generation Protection			
General Scheduled scans Scan settings Default actions Real-time protection Exclusion settings	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.		
Advanced	Specify Cloud Protection Service settings		
Threat overrides	Cloud Protection Service membership Advanced membership		
Cloud Protection Service	Allow users to modify Cloud Protection		
Security Intelligence updates	Service settings:		
Security	Level for blocking suspicious files: Normal V Allow extended cloud check to block and scan suspicious files for up to (seconds):		
	OK Cancel		

	Next Generation Protection	x
General Scheduled scans Scan settings Default actions Real-time protection Exclusion settings Advanced Threat overrides Cloud Protection Ser Security Intelligence	Avext Generation Protection         Security Intelligence updates         Image: Configure how Endpoint Protection clients will receive security intelligence updates         Configure how Endpoint Protection clients will receive security intelligence updates         Image: Check for Endpoint Protection clients will receive security intelligence updates         Image: Check for Endpoint Protection clients will receive security intelligence updates         Image: Check for Endpoint Protection security intelligence updates         Image: Check for Endpoint Protection security intelligence updates         Image: Check for Endpoint Protection security intelligence update if interval (hours);         Image: Check for Endpoint Protection security intelligence update if the client computer is offline for more than two consecutive scheduled updates:         Image: Set sources and order for Endpoint Protection security intelligence updates is         If Configuration Manager is used as a source for security intelligence update from atemative sources of security intelligence is older from security intelligence update from atemative sources of security intelligence update from atemative sources of security intelligence update from atemative sources of security intelligence updates	×
	If UNC file shares are selected as a security intelligence update source, (none) specify the UNC 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**.

evice Collections	✓ Filter	
Root	Name	Member Count
	💞 All Desktop and Server Clients	0
	Sector All Mobile Devices	0
	Systems 41 Systems	3
	Sector All Unknown Computers	0
	Endpoint Protection for Windows 10	0

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:

 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 protectioncontre les attaques.



- 2. Sélectionnez réduction surface Attack.
- 3. Définissez règles à **auditer**, puis cliquez sur **suivant**.

•-	Create Windows Defender Exploit Guard Policy		x
Attack Surface Re	duction		
General Attack Surface Reduction Controlled Folder Access	Configure Attack Surface Reduction		
Network Protection Summary Progress Completion	Attack Surface Reduction helps prevent actions that malware explo Learn more about Attack Surface Reduction Files and folders to exclude from Attack Surface Reduction rules:	it to infect devices.	
	Email threats: Block executable content from email client and webmail: Office threats: Block Office applications from creating child processes: Block Office applications from creating executable content: Block Office applications from injecting code into other processes: Block Win32 API calls from Office macros: Scripting threats: Block JavaScript or VBScript from launching downloaded	Audit        Audit        Audit        Audit        Audit        Audit	
	Block execution of potentially obfuscated scripts:	Audit v	~

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**.

		Select Collection	X
Device Collections	~	Filter	Q
I Boot		Name	Member Count
		🗳 All Desktop and Server Clients	0
		🗳 All Mobile Devices	0
		🗳 All Systems	3
		🗳 All Unknown Computers	0
		Findpoint Protection for Windows 10	0
			OK Cancel

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)

- À partir d'un navigateur Web, <u>https://securitycenter.windows.com</u>accédez 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 II affiche la vue d'ensemble de la configuration des règles ASR et l'état des règles ASR sur chaque appareil.

Reports > Attack surface re	duction rules			
Detections Configuration Add exclusions				
Identify and fix devices with limited protection d	lue to missing prerequisites	or misconfigured rules. Lea	arn about prerequisites	
Device configuration overview			Configure devices	
Blocking Auditing only Off/Unknown 0 2 0			Create or edit an attack surface red protection for the	endpoint protection policy for luction (ASR) to increase e devices below.
			Get started	
Device	Overall configuration	Rules in block mode	Rules in audit mode	Rules turned off
mdatp-pc02.catjp.com	Rules in audit mode	0	11	3
mdatp-pc01.catjp.com	Rules in audit mode	0	11	3

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

### mdatp-pc02.catjp.com

Configuration details of attack surface reduction rules on this device



Pour plus d'informations, reportez-vous à <u>optimiser le déploiement et les</u> <u>détections de la règle ASR</u>.

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

 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 protectioncontre les attaques.



- 2. Sélectionnez protection du réseau.
- 3. Définissez le paramètre sur audit, puis cliquez sur suivant.

•	Create Windows Defender Exploit Guard Policy
Network Protection	n
General Attack Surface Reduction Controlled Folder Access	Configure Network protection
Network Protection Summary Progress	Network protection helps minimize the attack surface on devices from internet-based attacks. The service restricts access to suspicious domains that might host phishing scams, exploits, and malicious content.
Completion	Learn more about Network protection           Configure Network protection:   Audit
	( Dention ) Netty Commercial Count
< III >	< Previous INEXT > Summary Cancel

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**.

		Select Collection	
Device Collections	~	Filter	P
E Root		Name	Member Count
		🗳 All Desktop and Server Clients	0
		🗳 All Mobile Devices	0
		🗳 All Systems	3
		💕 All Unknown Computers	0
		Findpoint Protection for Windows 10	0
			OK Cancel

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:

 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 protectioncontre les attaques.



- 2. Sélectionnez accès contrôlé au dossier.
- 3. Définissez la configuration à auditer, puis cliquez sur suivant.

•-	Create Windows Defender Exploit Guard Policy	X
Controlled Folde	er Access	
General Attack Surface Reduction	Configure Controlled folder access	
Network Protection Summary Progress	Controlled folder access blocks malicious or suspicious apps from changing files in protected folders. Protected folders include common system folders. You can specify additional protected folders below.	
Completion	Learn more about Controlled folder access         Configure Controlled folder access:         Allow apps through Controlled folder access:         Additional protected folders:	<ul><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>▶</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li><li>&gt;</li></ul> <li>&gt;</li> <li>&gt;</li>
	< Previous Next > Summary Canc	el

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**.

		Select Collection	2
Device Collections	~	Filter	P
T Root		Name	Member Count
		🗳 All Desktop and Server Clients	0
		All Mobile Devices	0
		Systems	3
		All Unknown Computers	0
		Findpoint Protection for Windows 10	0
			OK Cancel

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