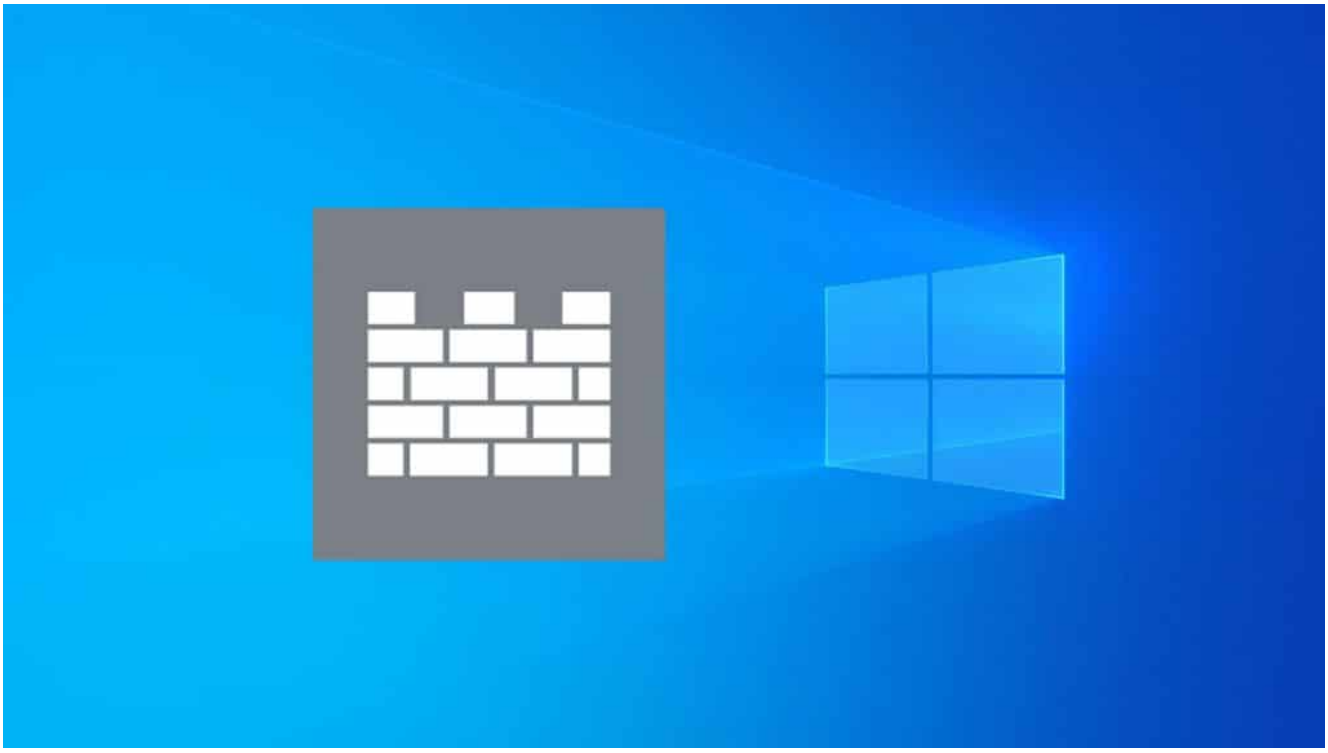
Les réglages avancés de Windows Defender : Tutoriel

Sur Windows 10, **des réglages pour Windows Defender** existent qui ne sont pas accessibles depuis l'interface de ce dernier.
Ce tuto vous explique comment passer ces réglages et donne une liste.
Une sélection de quelques réglages vous sont aussi donnés qui peuvent un peu améliorer **la sécurité de Windows contre les virus**.



Principe

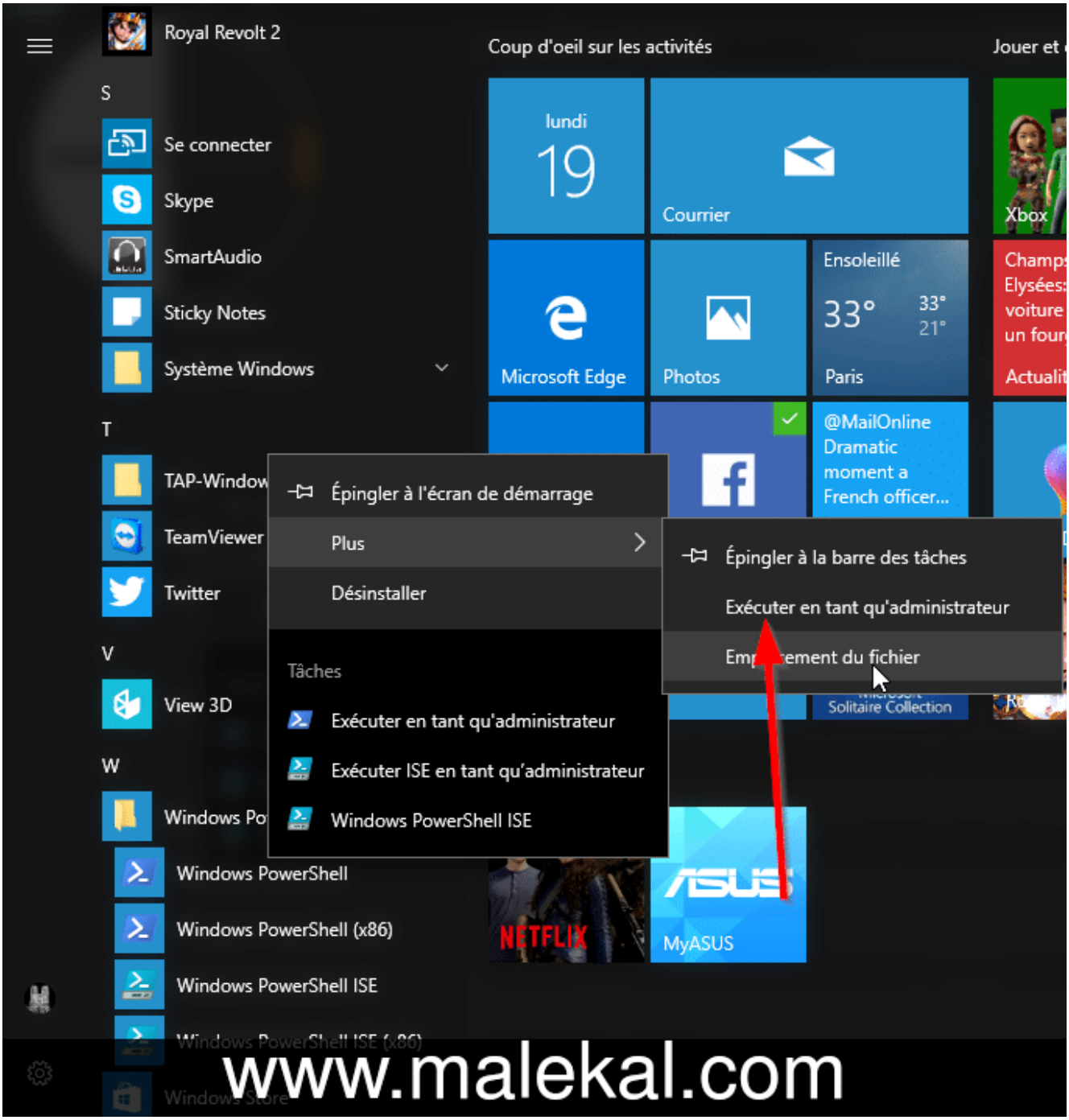
Avant de débuter, je vous rappelle qu'il existe des tutos Windows Defender qui décrivent le fonctionnement général et quelques éléments de configuration qui se limitent à activer/désactiver la protection en temps réel et Cloud et gérer les exclusions.

- Tutoriel et Guide Windows Defender
- Tutoriel Centre de Sécurité Windows Defender (pour la version Creators Update de Windows 10)

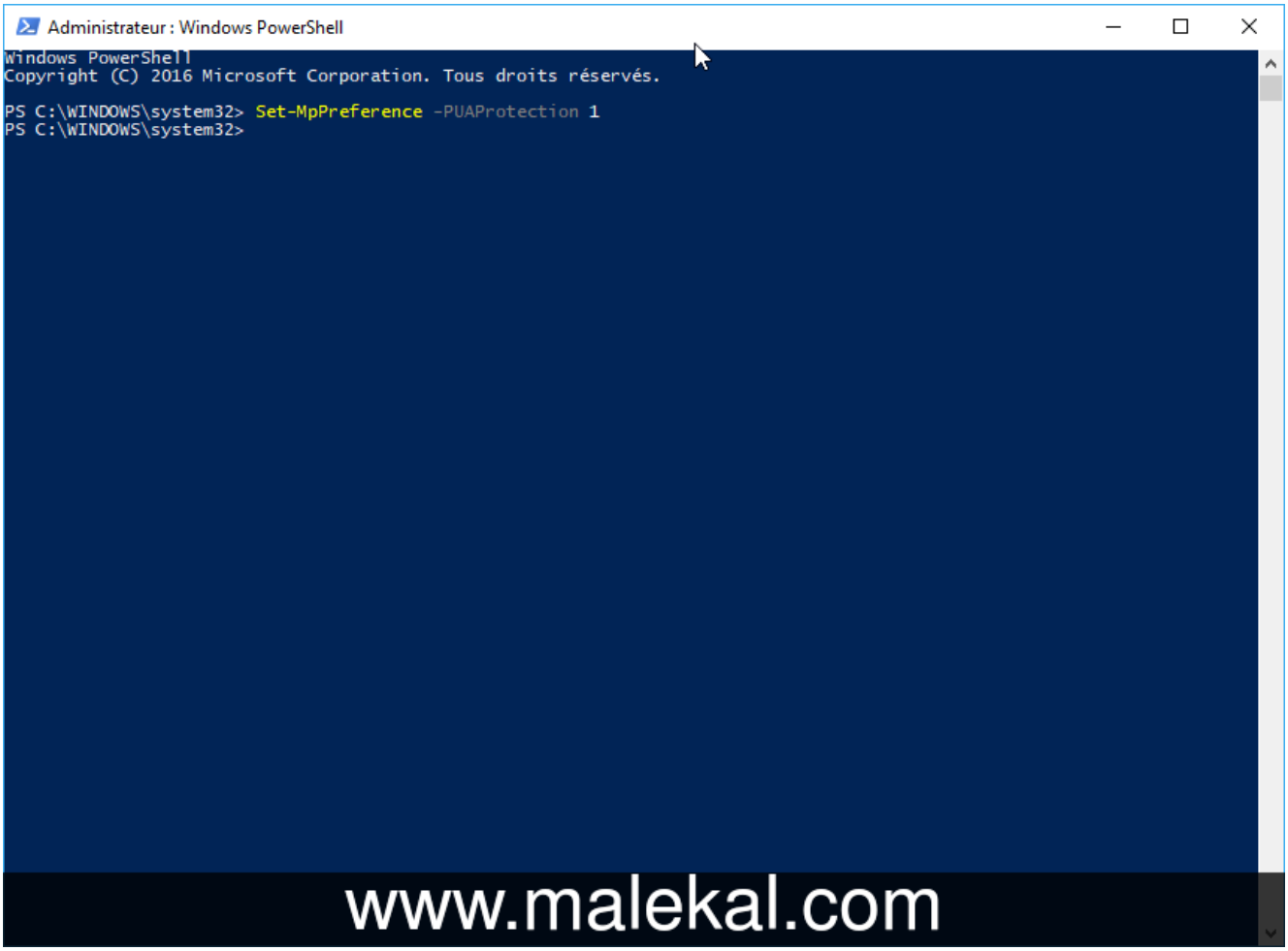
Les réglages avancés de Windows Défender, eux, se font à travers des commandes sur Windows PowerShell.
Notamment, il s'agit d'utiliser la commande *Set-MpPreference* et activer ou désactiver des réglages.

Dans un premier temps, il faut ouvrir PowerShell en administrateur :

- Depuis le menu Démarrer de Windows 10 > Windows PowerShell
- Faites un clic droit sur Windows PowerShell > Plus et Exécuter en tant qu'administrateur



Il ne reste plus qu'à coller la commande *Set-MpPreference* avec l'option que l'on souhaite activer ou désactiver.
Par exemple pour activer la détection PUA/PUP sur Windows Defender, il faudra passer la commande : ***Set-MpPreference -PUAProtection 1***



L'option est *-PUAProtection* que l'on active ou non :

- 1 ou $True active l'option.
- 0 ou $False désactive l'option.

Maintenant, il faut jouer sur les différentes options, vous trouverez donc quelques options et leurs explications pour jouer sur les réglages de Windows Defender.

Les réglages avancés de Windows

Defender

La liste des différents réglages de Windows Defender se trouvent sur la page suivante de Microsoft : https://technet.microsoft.com/fr-fr/library/dn433291.aspx

Parmi les options inintéressantes, on trouve notamment :

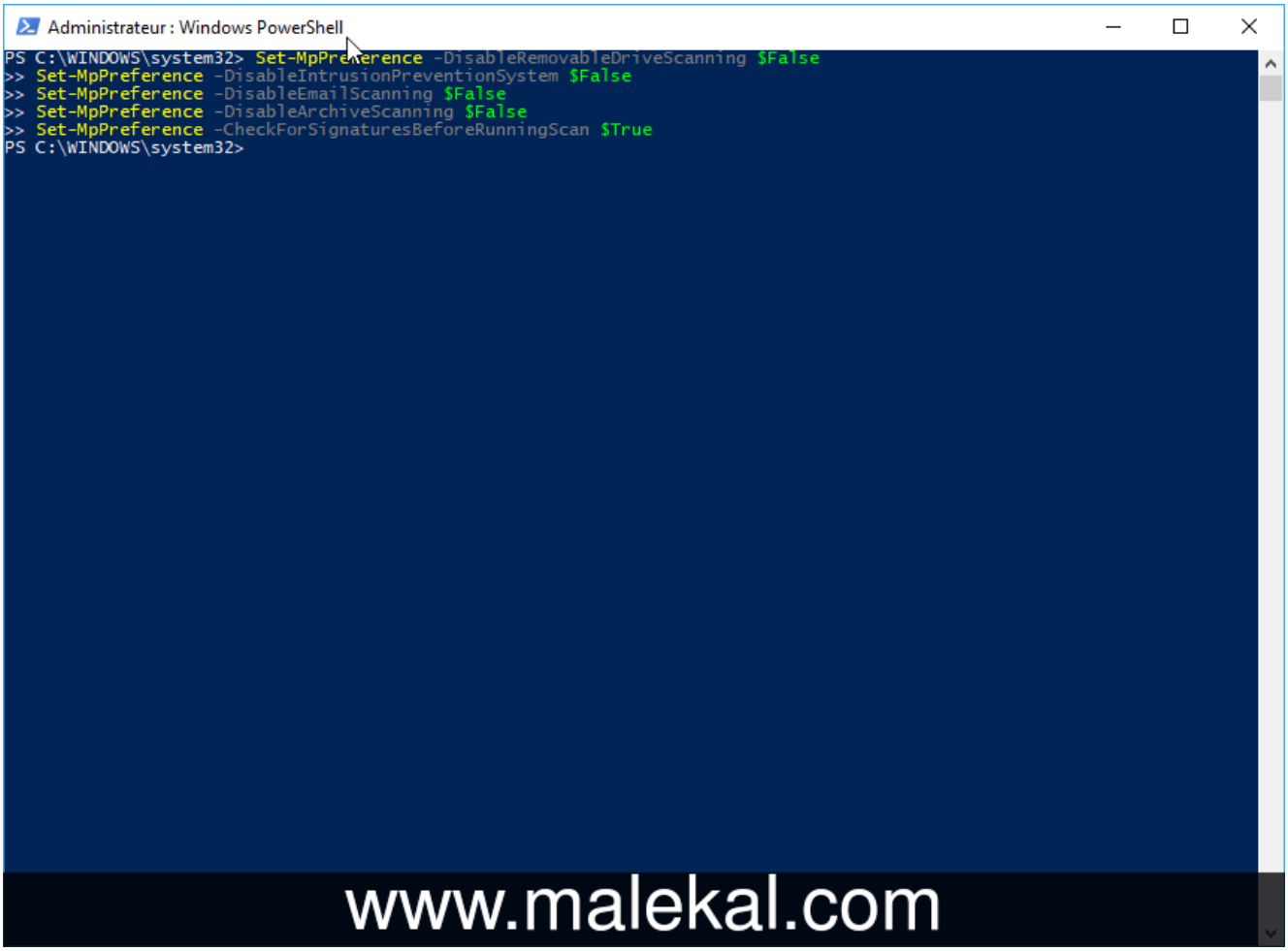
- -CheckForSignaturesBeforeRunningScan qui permet de forcer la mise à jour des définitions virales avant une analyse Windows Defender.
- -DisableArchiveScanning qui permet de forcer l'analyse des archives (zip, etc)
- -DisableEmailScanning forcer le scanne des pièces jointes de mails
- -DisableIntrusionPreventionSystem protège contre les intrusions réseaux
- -DisableRemovableDriveScanning force l'analyse des médias amovibles, très pratique contre les virus par clé USB.

Les clés du registre Windows correspondantes : *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender*

Ainsi, si on veut activer toutes les options, vous pouvez copier/coller, ce qui suit, dans la fenêtre de PowerShell :

```
Set-MpPreference -CheckForSignaturesBeforeRunningScan $True
Set-MpPreference -DisableArchiveScanning $False
Set-MpPreference -DisableEmailScanning $False
Set-MpPreference -DisableIntrusionPreventionSystem $False
```

```
Set-MpPreference -DisableRemovableDriveScanning $False
Set-MpPreference -PUAProtection $True
```



Les protections à activer en ligne de commandes

La plupart des protections peuvent être gérées et activer depuis le centre de sécurité Windows Defender.

Protection anti-ransomware

Les commandes Powershell pour activer la protection de dossiers et fichiers sur Windows Defender.
Plus d'informations : [Comment activer la protection Anti-Ransomware de Windows 10]

- *Set-MpPreference -EnableControlledFolderAccess Enabled*
- *Set-MpPreference -ControlledFolderAccessProtectedFolders C:\demo*

Attack Surface Reduction

Liste de règles à activer contre la protection de scripts et fichiers malveillants.

```
Add-MpPreference -AttackSurfaceReductionRules_Ids BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550 -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EfC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids 3B576869-A4EC-4529-8536-B80A7769E899 -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84 -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids D3E037E1-3EB8-44C8-A917-57927947596D -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids 5BEB7EFE-FD9A-4556-801D-275E5FFC04CC -AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B -AttackSurfaceReductionRules_Actions Enabled
```

```
Add-MpPreference      -AttackSurfaceReductionRules_Ids
D1E49AAC-8F56-4280-B9BA-993A6D77406C                -
AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference      -AttackSurfaceReductionRules_Ids
B2B3F03D-6A65-4F7B-A9C7-1C7EF74A9BA4                -
AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference  -AttackSurfaceReductionRules_Ids  C1DB55AB-
C21A-4637-BB3F-A12568109D35                         -
AttackSurfaceReductionRules_Actions Enabled
Add-MpPreference  -AttackSurfaceReductionRules_Ids  01443614-
CD74-433A-B99E-2ECDC07BFC25                         -
AttackSurfaceReductionRules_Actions Enabled
```

Protection du réseau

La commande pour configurer la protection du réseau.

- *Set-MpPreference -EnableNetworkProtection Enabled*

Les paramètres :

- Enabled = protection et blocage activés (1)
- AuditMode = En mode Audit (2)
- Disabled = Off (0)

Protection contre les exploits

La commande Powershell pour activer la protection contre les exploits.
Cela vous protège durant le surf des exploits kits et autres menaces WEB.

Plus d'informations : les exploits WEB.

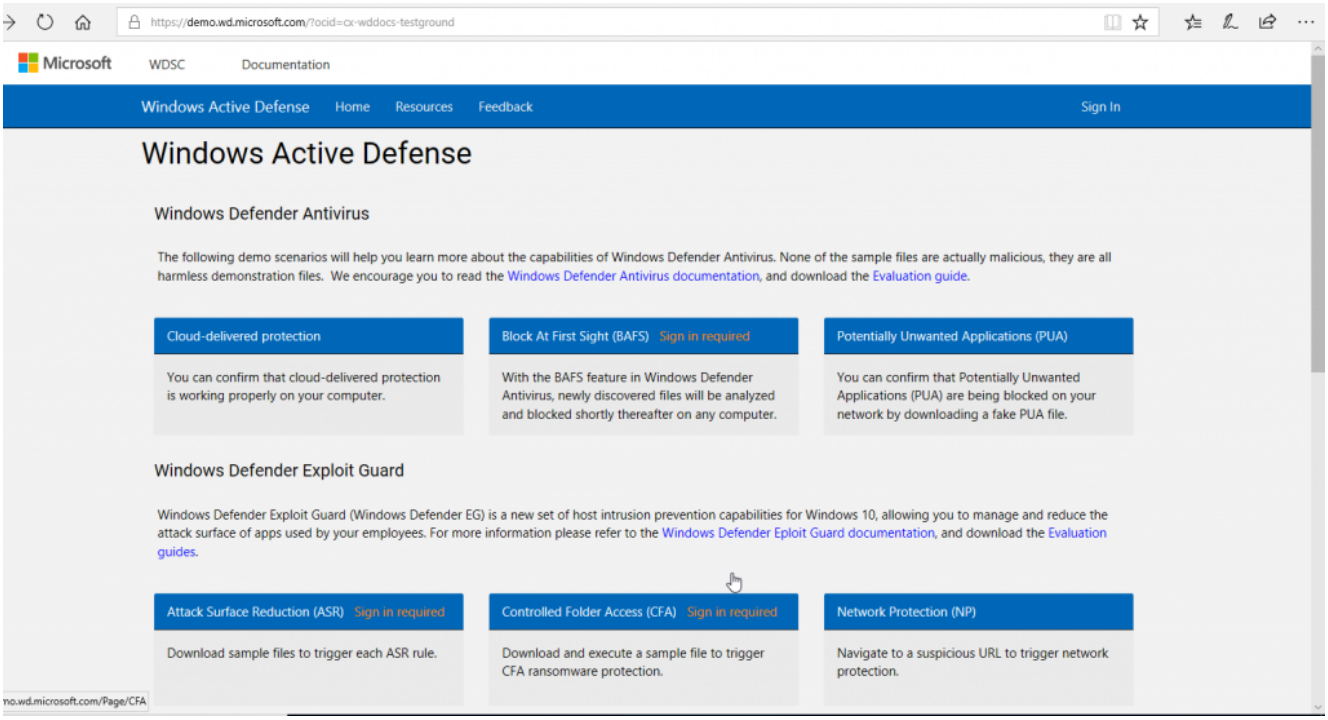
- *Set-ProcessMitigation -PolicyFilePath ProcessMitigation.xml*
- *Set-ProcessMitigation –help*

Activer toutes les protections

Microsoft fournit un script PowerShell qui permet d'activer toutes les protections (ou les désactiver).
Ce script est disponible sur la page : WindowsDefender_InternalEvaluationSettings

Tester les protections Windows Defender

Il existe un site de Microsoft qui regroupe tous les tests de protection Windows Defender et Windows 10.
Ce site est idéal, si vous doutez que les protections de Windows 10 soient bien actives.
Pour tester cela, suivez les indications de notre page : Comment vérifier Windows Defender et protection Windows 10 fonctionnent



Windows Defender Application Guard pour Edge, Firefox et Chrome

Cette fonction permet de faire tourner le navigateur WEB dans un bac à sables.
Cela permet de mieux protéger Windows contre les attaques.

> *Windows Defender Application Guard pour Edge, Firefox et Chrome*

Les tutoriels Windows Defender

Quelques autres tutoriels autour de Windows Defender :

- Tutoriel Centre de Sécurité Windows Defender : il s'agit de la version pour Windows 10
- Tutoriel et Guide Windows Defender avec les versions précédentes pour Windows Vista, Windows 7 et 8.1
- Comment désactiver Windows Defender
- FAQ Windows Defender

D'autres articles sont disponibles depuis le menu Windows Defender : Menu antivirus Windows Defender

Autres liens avec tous les liens de sécurité sur la page : Virus & Sécurité

Et pour sécuriser Windows :

- Comment Sécuriser Windows
- Quelles protections pour Windows 10 ?