

Gérer l'accès aux sites Web Microsoft Defender :

Préambule :

L'EDR Microsoft Defender offre une solution complète de protection pour les utilisateurs et les Endpoint.

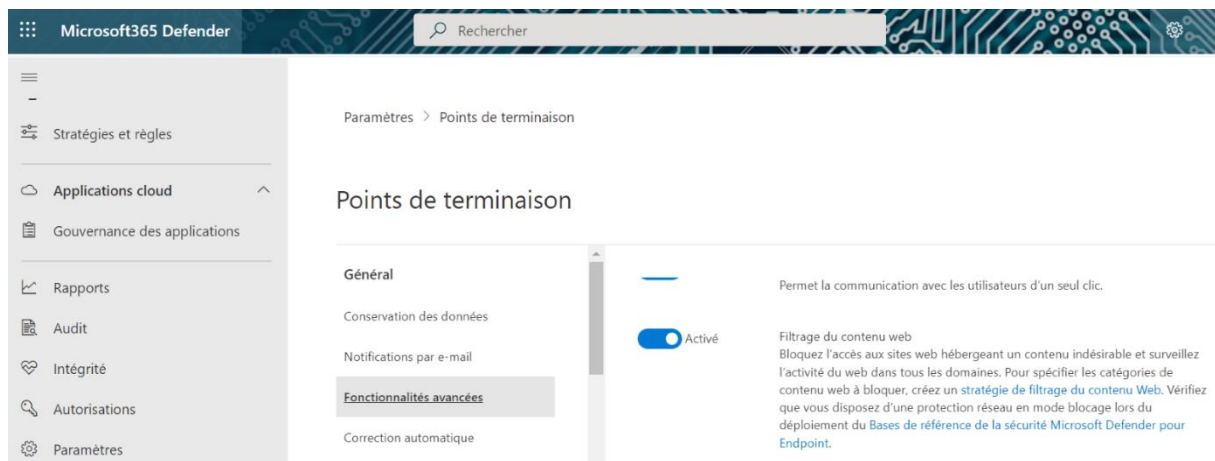
Ce document a pour objectif de décrire la gestion du filtrage Web afin de sécuriser les accès au Web que ce soit dans les locaux de l'entreprise ou en télétravail.

Connexion au panel Microsoft Defender :

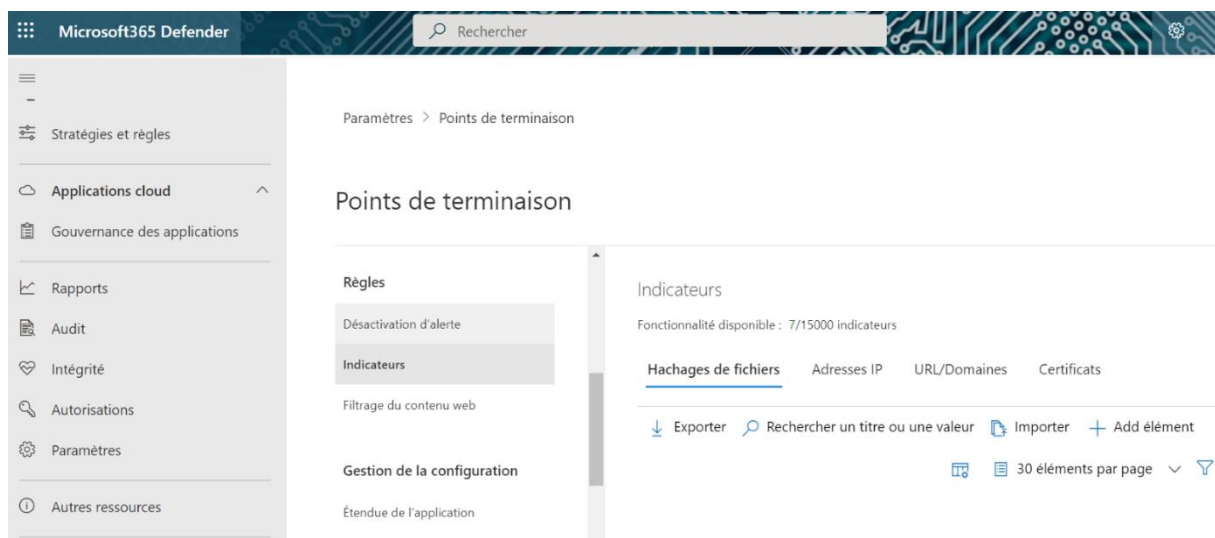
<https://security.microsoft.com/>

I.Activation et configuration du filtrage web :

Le filtrage Web est une fonctionnalité avancée de Microsoft Defender, il faut veiller à ce qu'elle soit active dans *Paramètres – Points de terminaison – Fonctionnalités avancées* :



Une fois la fonctionnalité activée, il s'agira pour gérer le filtrage d'aller dans l'onglet *Règle, Paramètres – Points de terminaisons – Règles* :



Afin que ce dernier soit fonctionnel, il s'agira de mettre en place une Stratégie de filtrage Web, pour ce faire, il faut aller dans la partie *Filtrage du contenu Web* :

Points de terminaison

Nom de la stratégie	Catégories bloquées	Créé par
Filtrage Web	Images d'enfants maltraités, Activité criminelle, Piratage, + ...	g.schmitt@g

La fonction *Add Element* permet de créer une règle, il suffira de sélectionner les catégories de site à filtrer.

Ajouter une stratégie

Général **Catégories bloquées** Récapitulatif

Sélectionnez les catégories de contenu web à bloquer. Vous pouvez continuer à obtenir des données sur les tentatives d'accès aux sites web dans toutes les catégories.

☐ **Bande passante élevée** ^

- ☐ Diffusion en continu et téléchargements
- ☐ P2P
- ☐ Partage d'image
- ☐ Sites de téléchargement

☐ **Contenu pour adultes** ^

- ☐ De mauvais goût
- ☐ Jeux de hasard

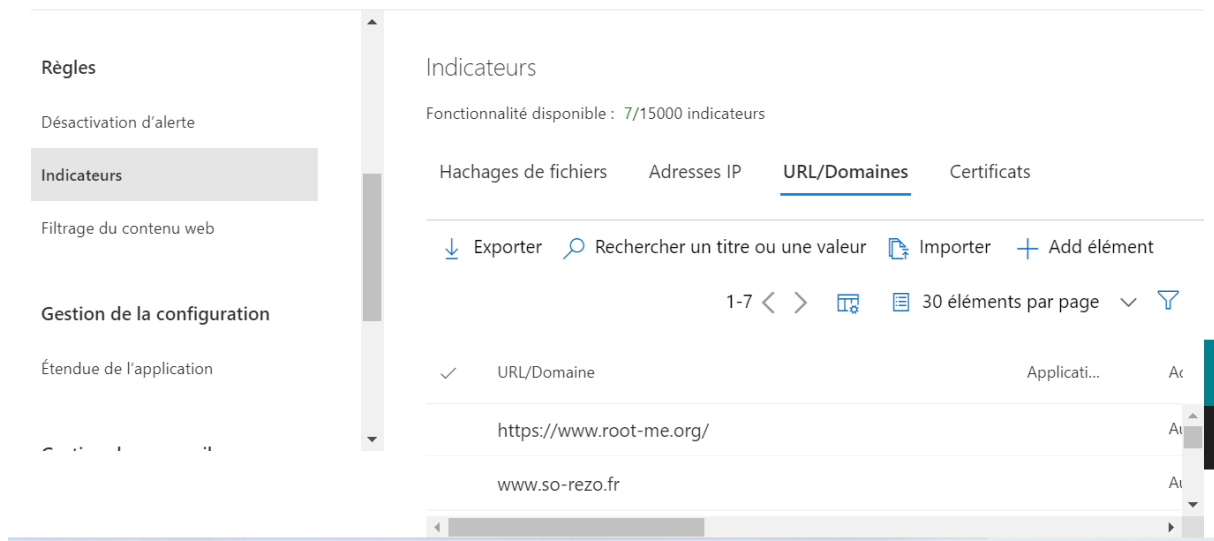
Précédent **Suivant** Annuler

Microsoft s'appuie sur une base de données interne constamment remise à jour. Il est bien sûr possible de bloquer des sites manuellement.

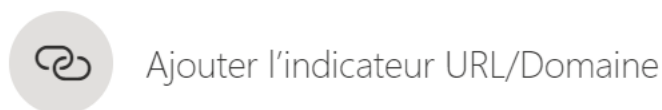
II. Autoriser / Bloquer un site internet :

Pour autoriser ou bloquer un site internet, il faudra se rendre dans Paramètres - Points de terminaison - Indicateurs :

Points de terminaison



Il existe plusieurs types de filtrages, les deux cas qui nous intéressent sont URL/Domaines et Adresses IP. Cliquer sur un des types de filtrages, dans ce cas-ci URL/Domaines et Add Element :



Ajouter l'indicateur URL/Domaine

Indicateur

Action

Résumé

Spécifiez le URL/Domaine et la date d'expiration. [En savoir plus](#)

URL/Domaine *

www.google.fr

Expire le (UTC)

☒ Jamais

☐ Date personnalisée



Indiquer l'URL puis la périodicité, il est possible de choisir un deadline puis *Suivant* :



Ajouter l'indicateur URL/Domaine

Indicateur

Action

Résumé

Action de réponse

Sélectionnez l'action à effectuer lorsque ce url est trouvé.
Cette action s'appliquera à tous les appareils de votre client.

- ☒ Autoriser
- ☐ Audit
- ☐ Avertir
- ☐ Bloquer l'exécution

☐ Générer une alerte

Choisir l'action à effectuer, il est possible d'auditer le site (combien de connexion à ce site au sein de domaine etc), d'avertir l'utilisateur d'une potentielle faille, de bloquer le site ou de l'autoriser dans le cas d'un faux positif.

Passer les différentes étapes, et enregistrer la règle.

A savoir :

Le temps de propagation des règles de filtrage annoncé par Microsoft peut prendre jusqu'à 120 minutes.