Gérer l’accès aux sites Web Microsoft Defender :

Préambule :

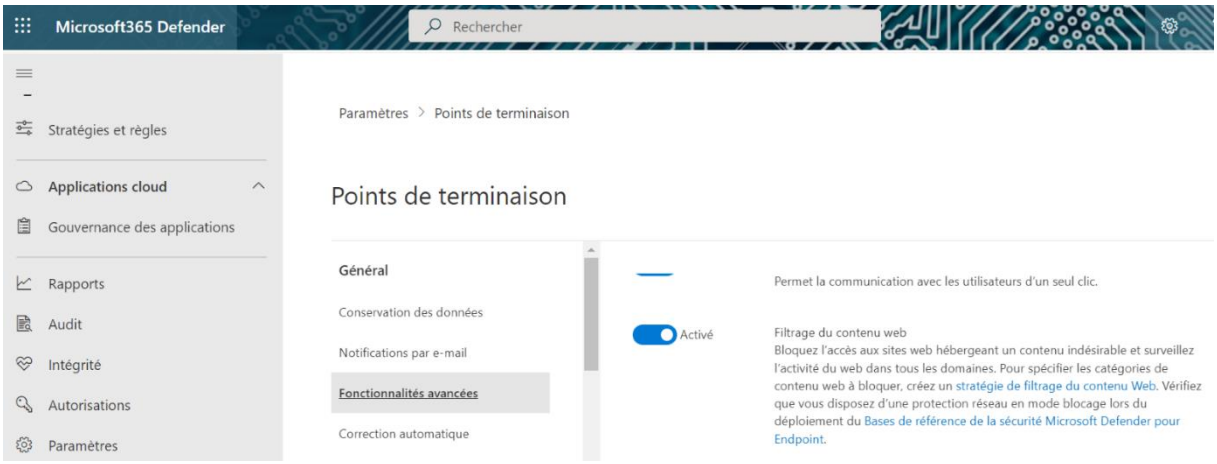
L’EDR Microsoft Defender offre une solution complète de protection pour les utilisateurs et les Endpoint.

Ce document à 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.

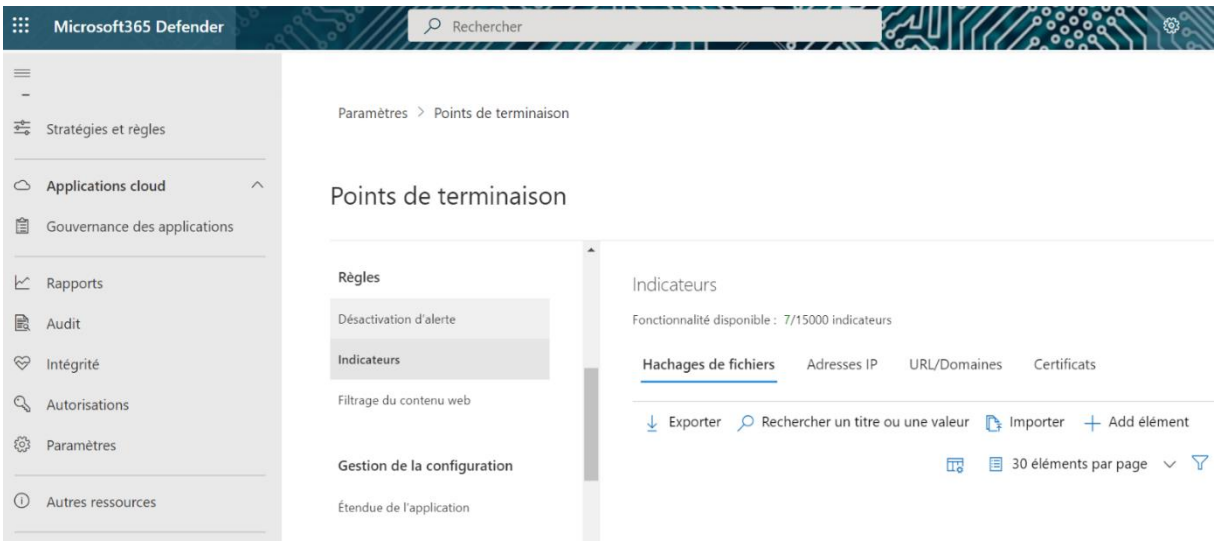
Connexion au panel Microsoft Defender :
https://security.microsoft.com/

I. Activation et configuration du filtrage web :

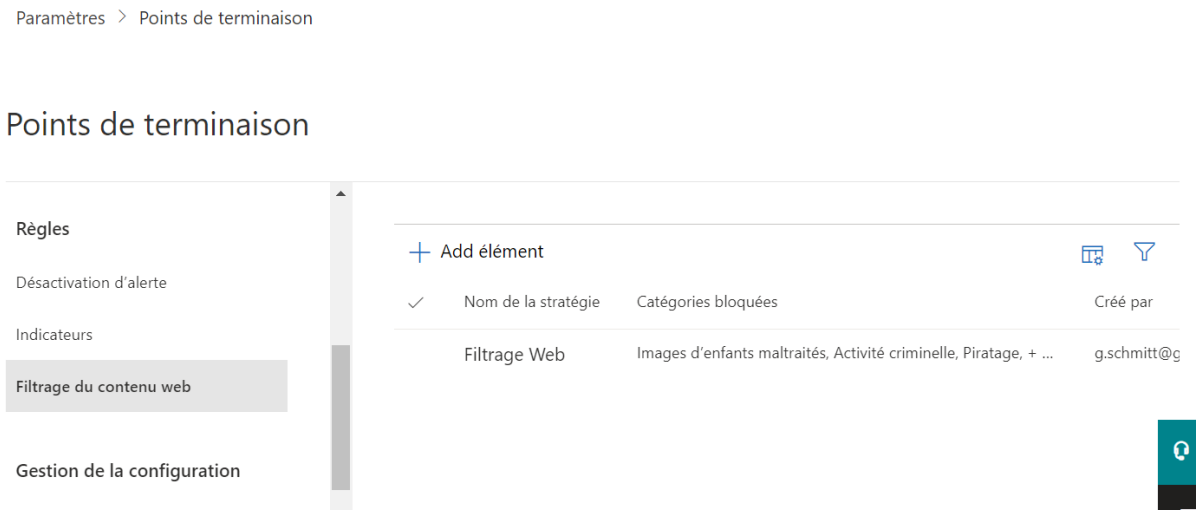
Le filtrage Web est une fonctionnalité avancée de Microsoft Defender, il faut veiller à ce qu’elle soit active dans *Paramètres – Points de terminaisons – Fonctionnalités avancées :*



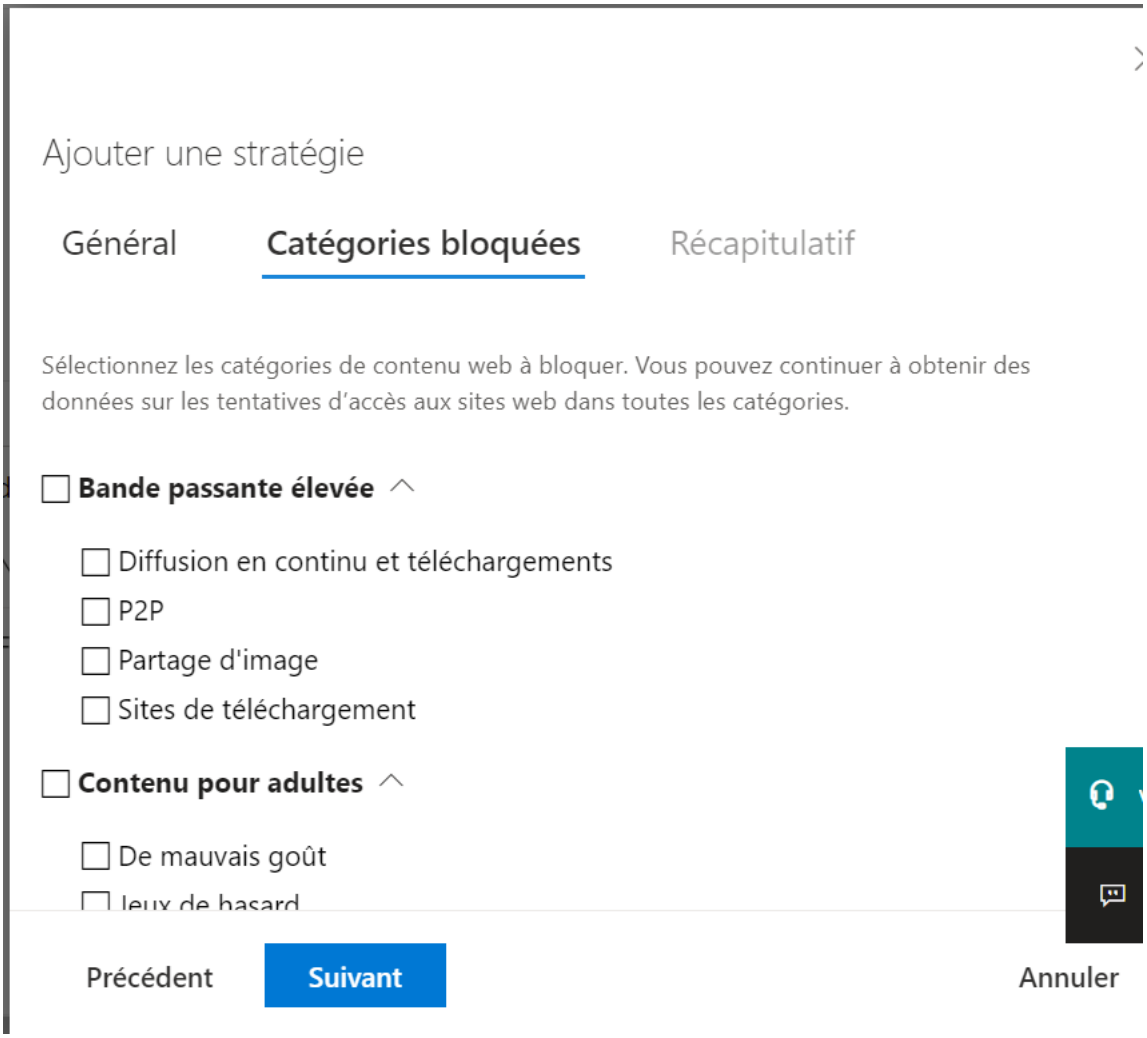
Une fois la fonctionnalité activée, il s’agira pour gérer le filtrage d’aller dans l’onglet *Règle*, *Paramètres – Points de terminaisons – Règles* :



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* :



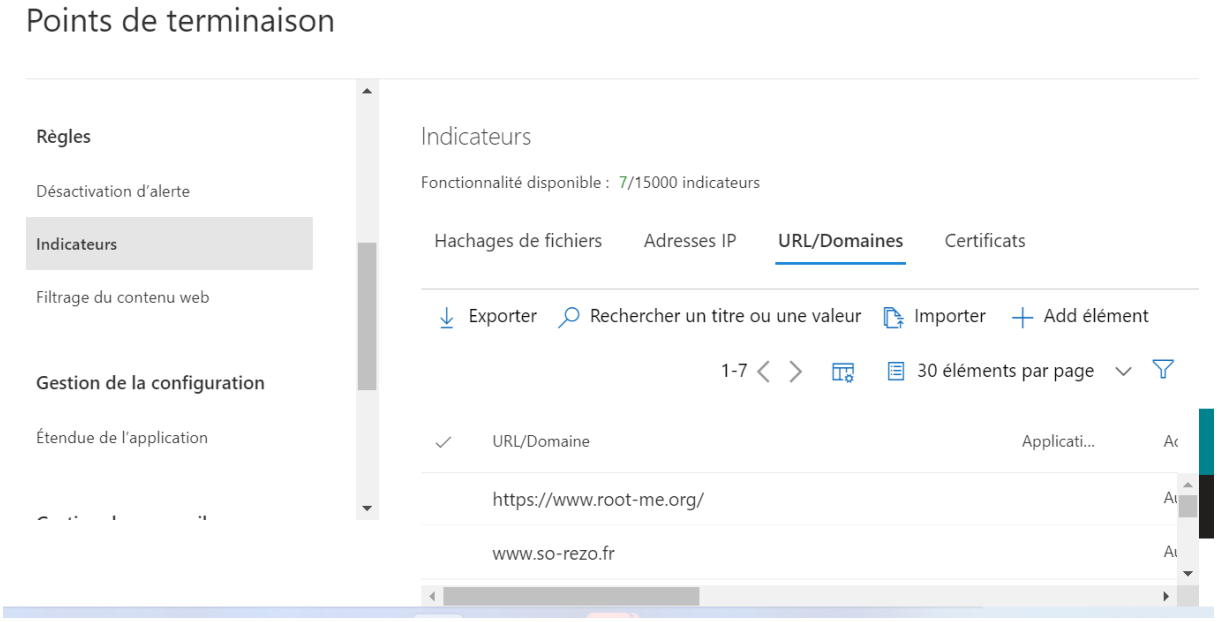
La fonction *Add Element* permet de créer une règle, il suffira de sélectionner les catégories de site à filtrer.



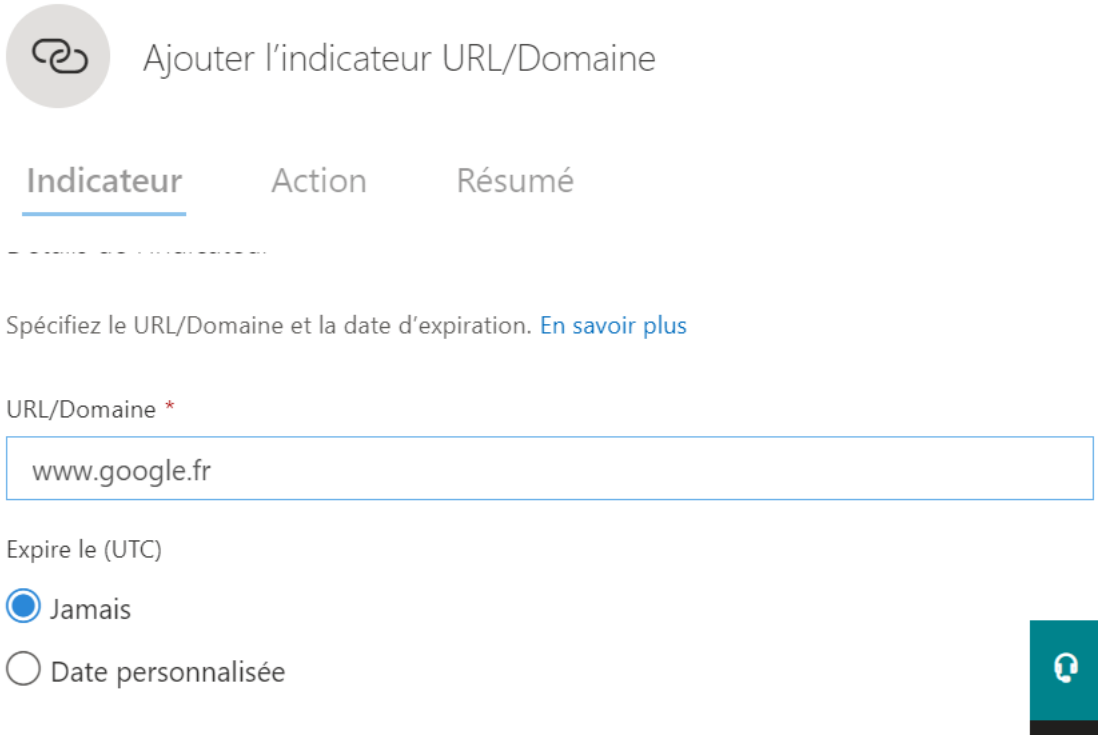
Microsoft s'appui sur une base de données interne constamment remise à jour. Il est bien sur possible de bloquer des sites manuellement.

II.Autoriser / Bloquer un site internet :

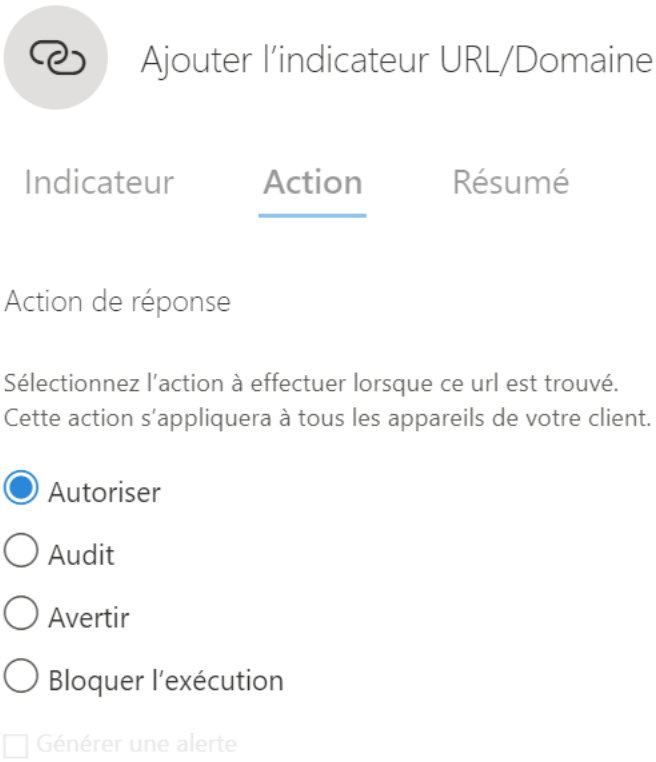
Pour autoriser ou bloquer un site internet, il faudra se rendre dans Paramètres - Points de terminaisons – Indicateurs :



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 :



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



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.