Le filtrage des identificateurs de sécurité, *SID Filtering* en anglais, est une mesure de sécurité utilisée dans les environnements Active Directory pour contrôler l'accès aux ressources partagées sur un réseau. Il vise à garantir que seuls les utilisateurs autorisés peuvent accéder à des ressources spécifiques, tout en empêchant les attaques telles que l'usurpation d'identité.

Lorsqu’un utilisateur d’un domaine de confiance accède à des ressources dans un domaine confiant, à travers une relation de confiance (Trust), le jeton d’accès (Access token) de l’utilisateur est transmis au serveur du domaine confiant. La liste des identificateurs de sécurité (SID) contenue dans le jeton d’accès ne devrait contenir que des identificateurs de sécurité provenant du domaine de confiance. Ces identificateurs de sécurité sont utilisés pour donner l’accès à des ressources sur le serveur du domaine confiant.

## Risques

Si un utilisateur falsifie un jeton d’accès en ajoutant des identificateurs de sécurité provenant du domaine confiant, alors l’utilisateur pourrait accéder à des ressources auxquelles il ne devrait pas avoir accès.

Pour réduire ce risque, une fonctionnalité de filtrage des identificateurs de sécurité a été ajouté. Lorsque cette fonctionnalité est activée sur un domaine confiant, les identificateurs de sécurité, présents dans le jeton d’accès d’un utilisateur du domaine de confiance, qui ne proviennent pas du même domaine que l’utilisateur sont ignorés ou supprimés.

À noter que lorsque cette fonctionnalité est activée, d’autres identificateurs de sécurité, comme les identificateurs par défaut d’un domaine, sont également supprimés pour éviter un accès non autorisé aux données du serveur du domaine confiant.