Comment exempter le trafic Office 365 de l'authentification et du déchiffrement sur l'appareil de sécurité Web Cisco (WSA)

Contenu

Introduction

Cet article décrit le processus nécessaire pour exempter le trafic Office 365 de l'authentification et du déchiffrement sur l'appareil de sécurité Web (WSA). Il existe plusieurs problèmes de compatibilité connus avec Office 365 et les proxys, et l'exemption de l'authentification et du déchiffrement du trafic Office 365 peut aider à résoudre certains de ces problèmes.

> **Note**: Il ne s'agit pas d'un contournement complet du proxy Web et exempter le trafic du déchiffrement empêche le WSA d'inspecter le trafic HTTPS chiffré généré par les clients Office 365.

Configuration Steps

Aperçu:

1. Créer une **catégorie d'URL personnalisée** à l'aide du flux externe Office365
2. Créer un **profil d'identification** pour le trafic Office 365
3. Exempter le trafic Office 365 de la **stratégie de déchiffrement**

> **Note**: Ce processus nécessite l'utilisation du flux JSON externe Office 365 à mise à jour dynamique qui contient toutes les URL/adresses IP associées à Office 365.

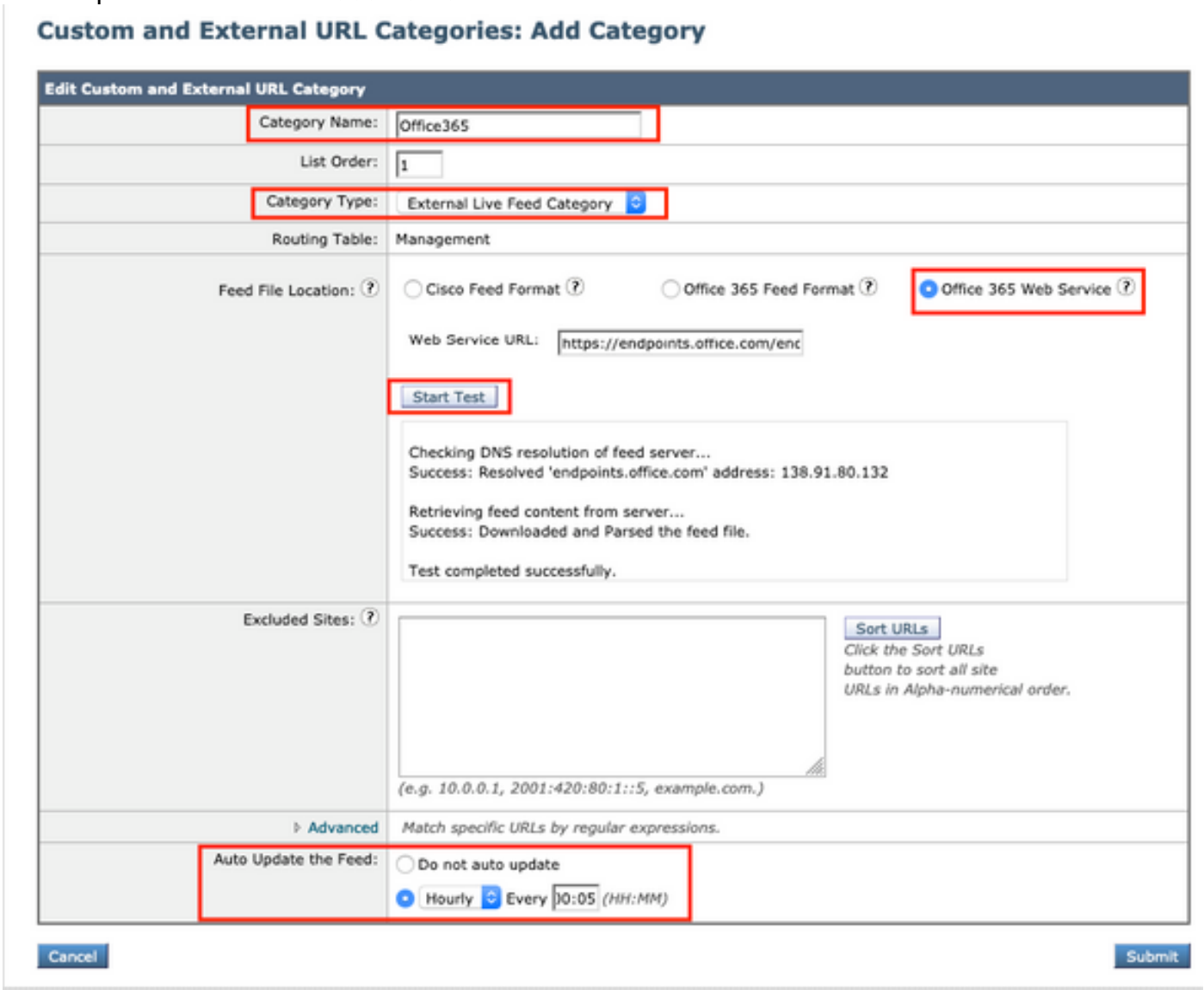
> **Note**: La prise en charge de ce flux est présente dans AsyncOS version 10.5.3 et ultérieures et 11.5 versions ultérieures.

1. Créer une catégorie d'URL personnalisée à l'aide du flux externe Office365

- Accédez à **Web Security Manager->Catégories d'URL personnalisées et externes**
- Cliquez sur "**Ajouter une catégorie**"
- Attribuez un nom à la catégorie, sélectionnez le type de catégorie "**Catégorie de flux**

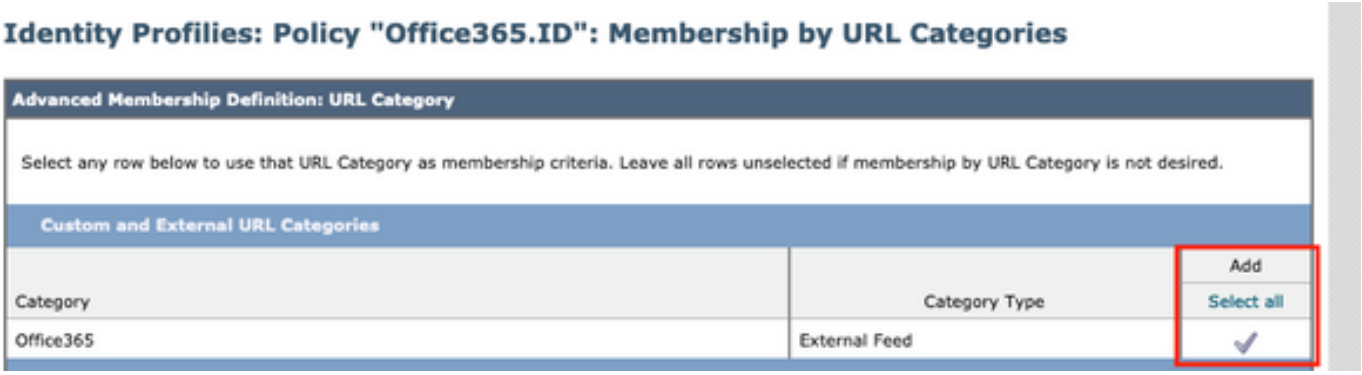
dynamique externe" et sélectionnez "**Service Web Office 365**« .

- Cliquez sur "**Démarrer le test »** si vous souhaitez tester la capacité de WSA à télécharger le flux de Notation d'objet JavaScript Office 365 (JSON).
- En bas, définissez l'option "**Mise à jour automatique du flux**" sur "**Heure**" avec un intervalle de 00:05 (toutes les 5 minutes)
- Cliquez sur le bouton "**Soumettre**« .

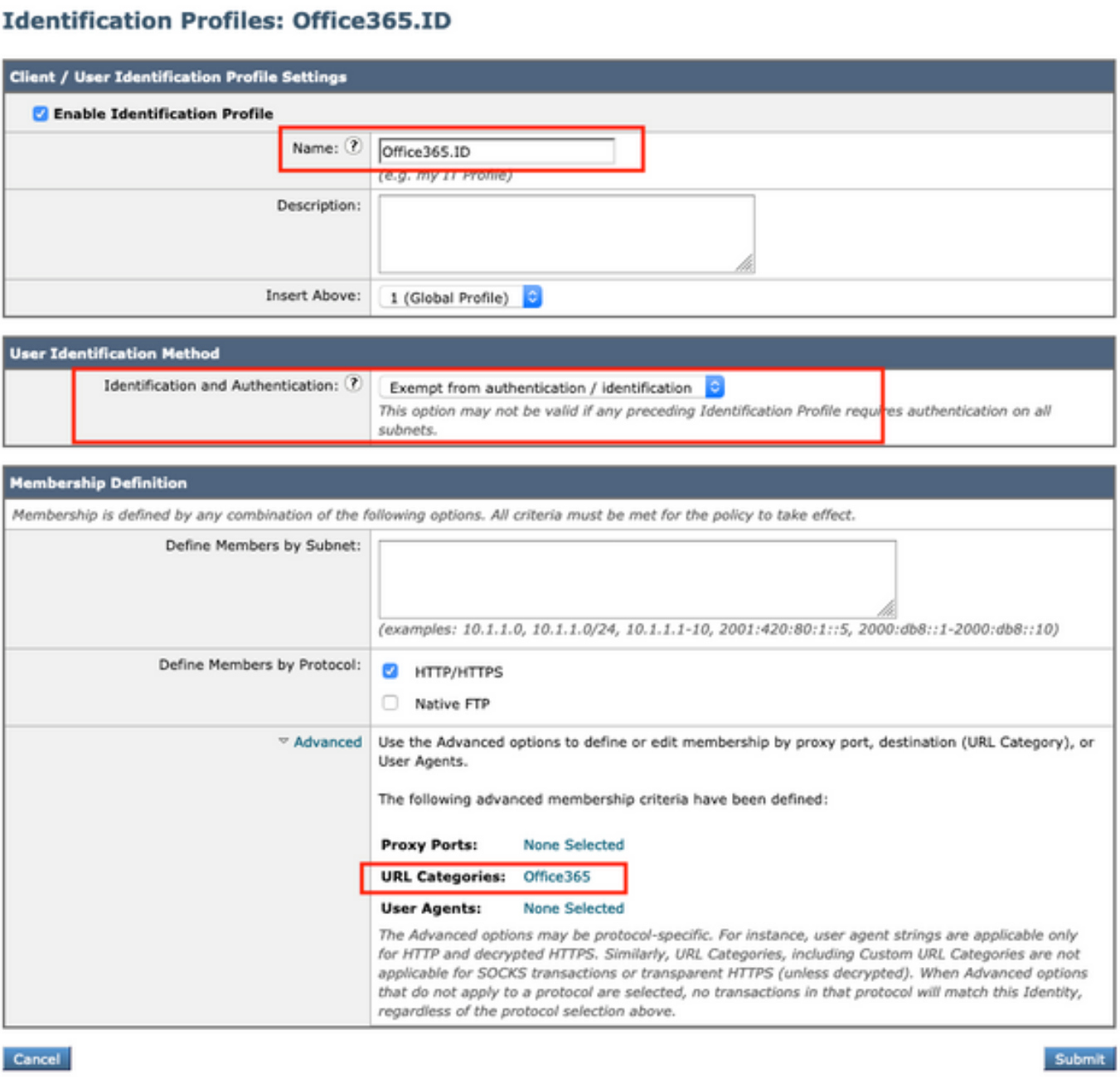


2. Créer un profil d'identification pour le trafic Office 365

- Accédez à **Web Security Manager->Profils d'identification**
- Cliquez sur "**Ajouter un profil d'identification**"
- Attribuez un nom, définissez "**Identification et Authentification**" sur "**Exempt de l'authentification/identification**« .
- Cliquez sur le bouton "**Avancé**« , puis cliquez sur le lien en regard de "**Catégories d'URL**"
- Recherchez la catégorie que vous avez créée à l'étape précédente, sélectionnez-la, puis faites défiler la page jusqu'en bas et cliquez sur le bouton "**Terminé**« .



Le profil d'identification doit maintenant être le suivant :

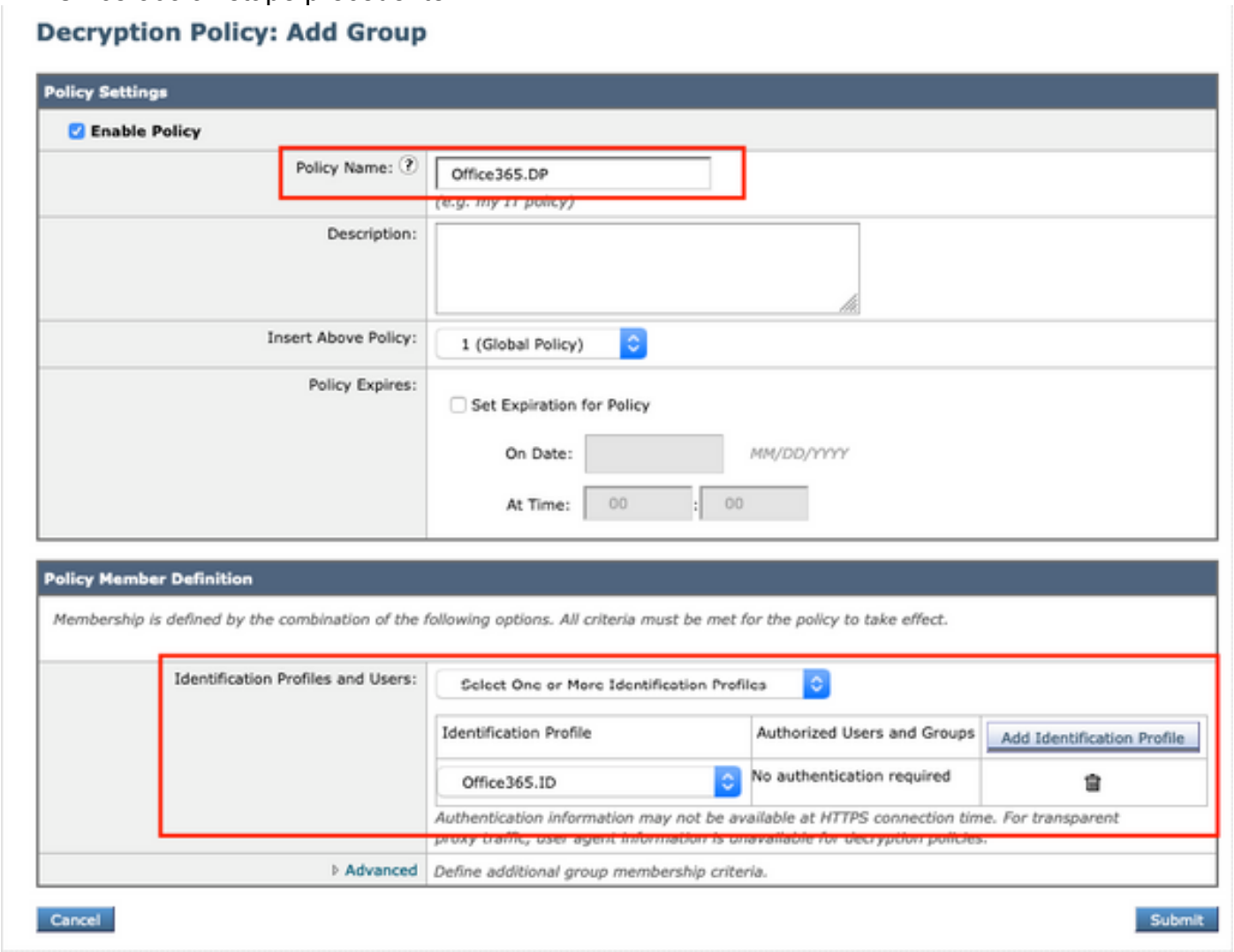


- Cliquez sur le bouton "**Soumettre**" en bas de l'écran.

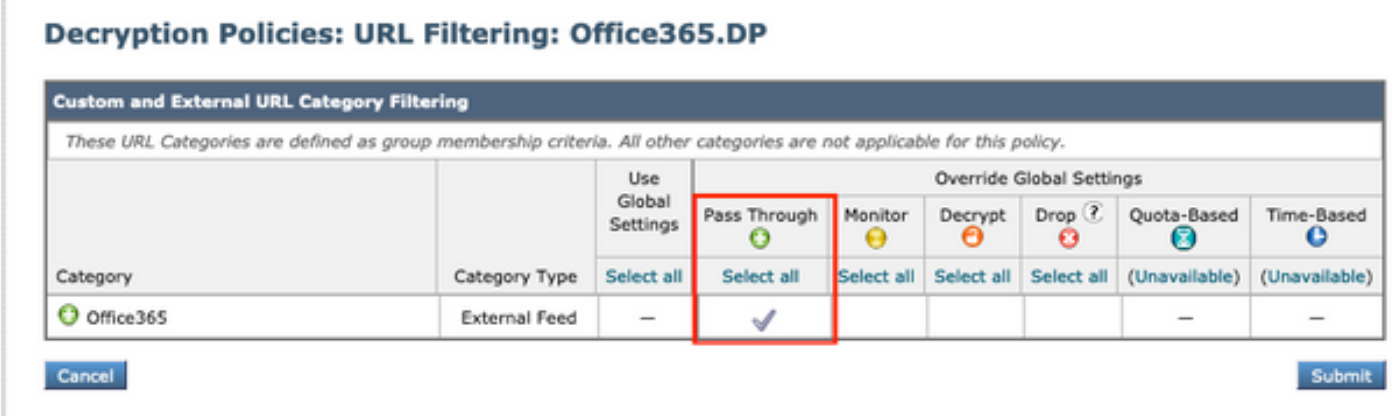
3. Exempter le trafic Office 365 de la stratégie de déchiffrement

- Accédez à **Web Security Manager->Decryption Policies**

- Cliquez sur "**Ajouter une stratégie**"
- Attribuez un nom, puis dans le champ "**Profils d'identification et utilisateurs**« , choisissez l'option "**Sélectionner un ou plusieurs profils d'identification**" et sélectionnez votre identité Office 365 à l'étape précédente.



- Cliquez sur le bouton "**Soumettre**« .
- Cliquez sur le lien sous "**Filtrage d'URL**" qui dit "**Surveillance : 1**"
- Définissez la catégorie Office 365 sur "**Passthrough**" et cliquez sur le bouton "**Submit**« .



- Enfin, confirmez vos modifications en cliquant sur le bouton jaune "**Valider les modifications**" situé dans le coin supérieur droit de l'interface utilisateur graphique.

Référence

Documentation officielle de Cisco sur **comment activer les flux externes Office 365** et **comment exempter Office 365 de la stratégie de déchiffrement** dans WSA :

Comment activer les flux externes Office 365 dans AsyncOS pour Cisco Web Security