

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

## Contenu

[Introduction](#)

[Configuration Steps](#)

[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](#)

[Référence](#)

## 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« .

### Custom and External URL Categories: Add Category

**Edit Custom and External URL Category**

Category Name: Office365

List Order: 1

Category Type: External Live Feed Category

Routing Table: Management

Feed File Location: ?

Cisco Feed Format ?  Office 365 Feed Format ?  Office 365 Web Service ?

Web Service URL: https://endpoints.office.com/enc

Start Test

Checking DNS resolution of feed server...  
Success: Resolved 'endpoints.office.com' address: 138.91.80.132

Retrieving feed content from server...  
Success: Downloaded and Parsed the feed file.

Test completed successfully.

Excluded Sites: ?

Sort URLs  
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced Match specific URLs by regular expressions.

Auto Update the Feed:  Do not auto update  Hourly Every 00:05 (HH:MM)

Cancel Submit

## 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« .

## Identity Profiles: Policy "Office365.ID": Membership by URL Categories

**Advanced Membership Definition: URL Category**

Select any row below to use that URL Category as membership criteria. Leave all rows unselected if membership by URL Category is not desired.

Custom and External URL Categories		
Category	Category Type	
Office365	External Feed	<input type="checkbox"/>

**Add**  
**Select all**  
✓

Le profil d'identification doit maintenant être le suivant :

## Identification Profiles: Office365.ID

**Client / User Identification Profile Settings**

**Enable Identification Profile**

**Name:**   
(e.g. my IT Profile)

**Description:**

**Insert Above:**

**User Identification Method**

**Identification and Authentication:**   
This option may not be valid if any preceding Identification Profile requires authentication on all subnets.

**Membership Definition**

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

**Define Members by Subnet:**   
(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

**Define Members by Protocol:**

- HTTP/HTTPS
- Native FTP

**Advanced**

Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

**Proxy Ports:** None Selected

**URL Categories:** Office365

**User Agents:** None Selected

The Advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories are not applicable for SOCKS transactions or transparent HTTPS (unless decrypted). When Advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.

- 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.

### Decryption Policy: Add Group

**Policy Settings**

**Enable Policy**

Policy Name:  (e.g. my 11 policy)

Description:

Insert Above Policy: 1 (Global Policy) ▾

Policy Expires:  Set Expiration for Policy

On Date:  MM/DD/YYYY

At Time:  :

**Policy Member Definition**

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles ▾

Identification Profile	Authorized Users and Groups	Add Identification Profile
Office365.ID ▾	No authentication required	🗑️

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

▶ [Advanced](#) Define additional group membership criteria.

Cancel
Submit

- 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« .

### Decryption Policies: URL Filtering: Office365.DP

**Custom and External URL Category Filtering**

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop ?	Quota-Based	Time-Based
Office365	External Feed	-	<span style="border: 1px solid red; padding: 2px;">Pass Through 🟢 Select all</span>	Monitor 🟡 Select all	Decrypt 🔴 Select all	Drop ? 🔴 Select all	Quota-Based 🟢 (Unavailable)	Time-Based 🔵 (Unavailable)

Cancel
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](#)