How To Exempt Office 365 Traffic From Authentication and Decryption on Cisco Web Security Appliance (WSA)

Contents

Introduction

This article describes the process involved to exempt Office 365 traffic from authentication and decryption on the Web Security Appliance (WSA). There are several known compatibility issues with Office 365 and proxies, and exempting Office 365 traffic authentication and decryption can help with some of these issues.

> **Note**: This is not a full bypass from web proxy, and exempting traffic from decryption prevents the WSA from inspecting the encrypted HTTPS traffic generated by Office 365 clients.

Configuration Steps

Overview:

1. Create a **Custom URL Category** using the Office365 External Feed
2. Create an **Identification Profile** for the Office 365 traffic
3. Exempt the Office 365 traffic from **Decryption Policy**

> **Note**: This process requires use of the dynamically updating Office 365 external JSON feed which contains all the URLs/IP addresses associated to Office 365.

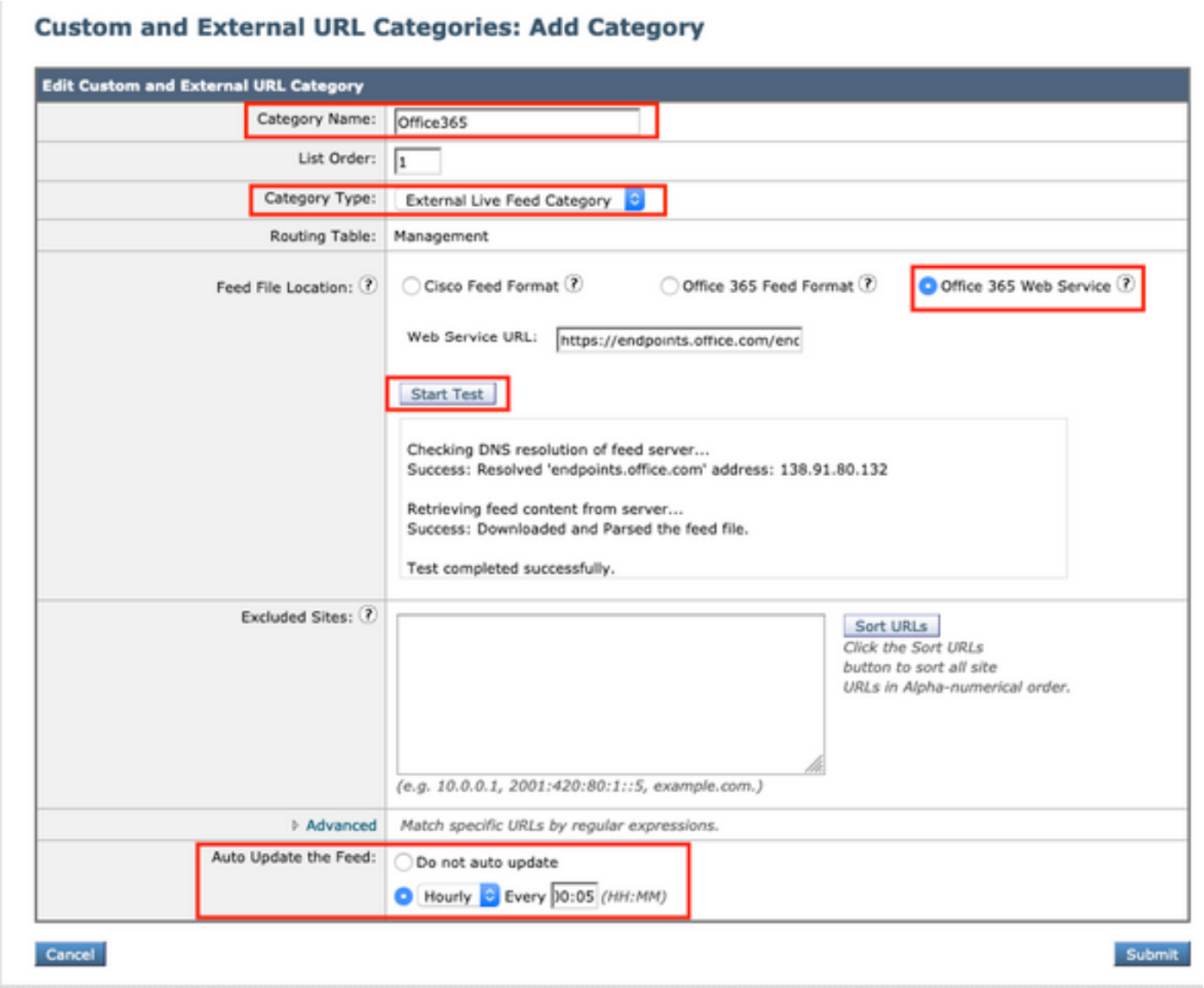
> **Note**: Support for this feed is present in AsyncOS version 10.5.3 onwards and 11.5 onwards versions.

1. Create a Custom URL Category using the Office365 External Feed

- Navigate to **Web Security Manager->Custom and External URL Categories**
- Click "**Add Category**"
- Assign a name to the category, select the category type as "**External Live Feed Category**",

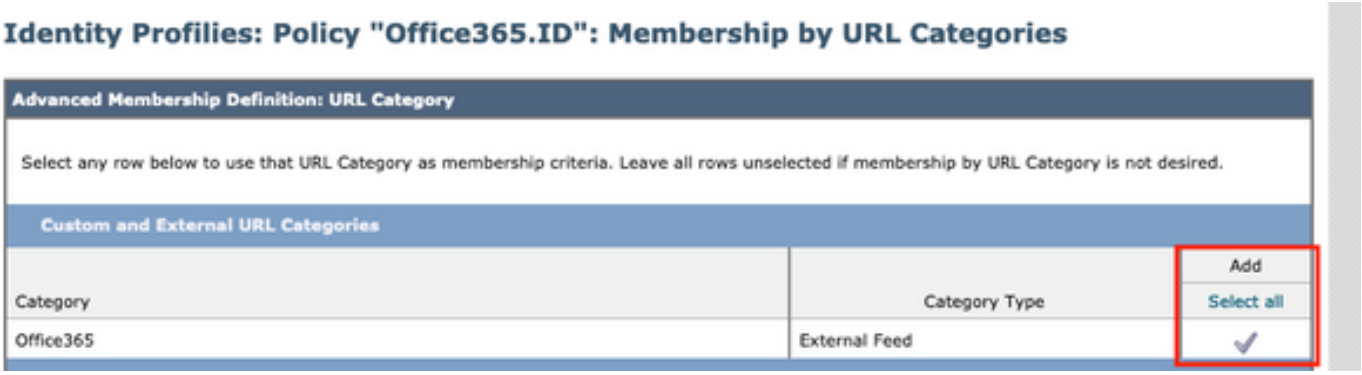
and select the "**Office 365 Web Service**" option.

- Click "**Start Test"** if you would like to test the WSA's ability to download the Office 365 JavaScript Object Notation (JSON) feed.
- At the bottom, set the "**Auto Update the Feed**" option to "**Hourly**" with an interval of 00:05 (every 5 minutes)
- Click the "**Submit**" button.

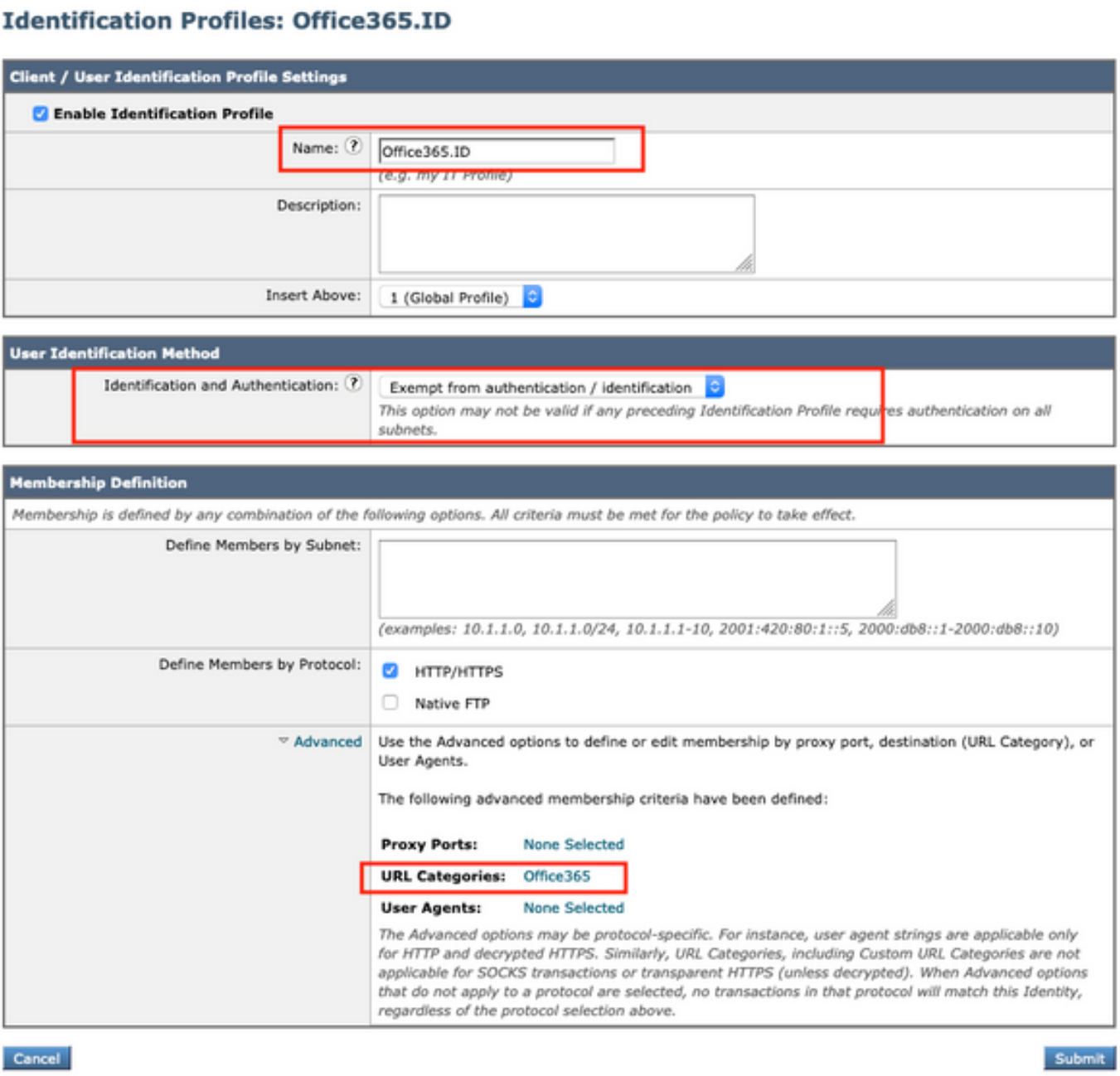


2. Create an Identification Profile for the Office 365 traffic

- Navigate to **Web Security Manager->Identitifcation Profiles**
- Click "**Add Identification Profile**"
- Assign a name, set "**Identification and Authentication**" to "**Exempt from authentication/identification**".
- Click the "**Advanced**" button, and click the link next to "**URL Categories**"
- Find the category you created in the previous step, and select that category, and then scroll to the bottom of the page and click the "**Done**" button.



The Identification Profile should now look as follows:

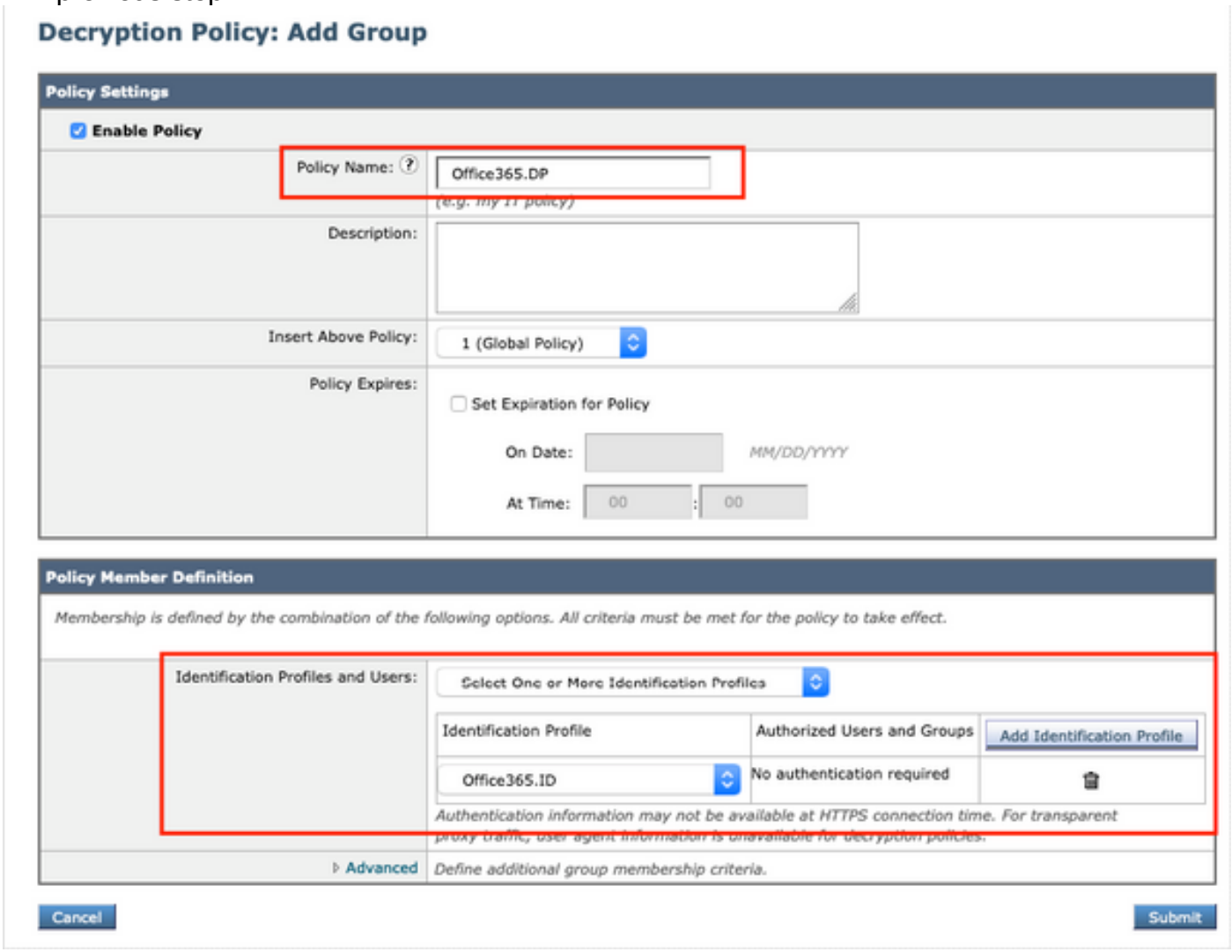


- Click the "**Submit**" button at the bottom of the screen.

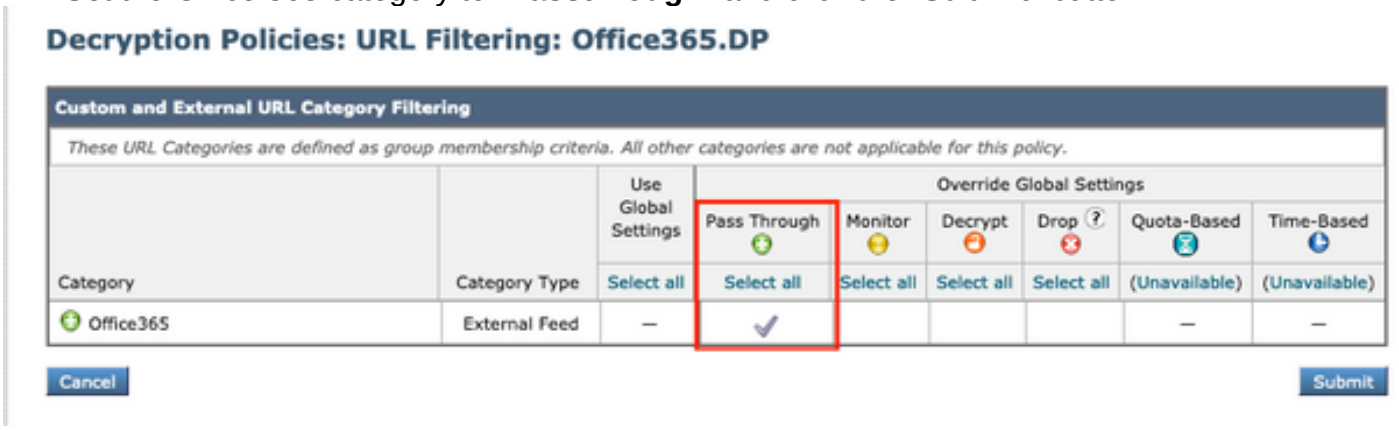
3. Exempt the Office 365 traffic from Decryption Policy

- Navigate to **Web Security Manager->Decryption Policies**

- Click "**Add Policy**"
- Assign a name, and then in the "**Identification Profiles and Users**" field, choose the "**Select One or More Identification Profiles**" option and select your Office 365 identity from the previous step.



- Click on the "**Submit**" button.
- Click on the link under "**URL Filtering**" that says "**Monitor: 1**"
- Set the Office 365 category to "**Passthrough**" and click the "**Submit**" button.



- Finally, commit your changes by clicking the yellow "**Commit Changes**" button at the top right-hand corner of the GUI.

Reference

More official Cisco documentation on **How to enable Office 365 External Feeds** and **How to exempt Office 365 from Decryption Policy** in WSA:

How to Enable Office 365 External Feeds in AsyncOS for Cisco Web Security