

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

Contents

[Introduction](#)

[Configuration Steps](#)

[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](#)

[Reference](#)

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.

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. Create an Identification Profile for the Office 365 traffic

- Navigate to **Web Security Manager->Identification 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.

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"/>

The Identification Profile should now look as follows:

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.

- 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.

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

- 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.

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
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Office365	External Feed	-	<input checked="" type="checkbox"/>					

Cancel
Submit

- 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](#)