

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

Introduction to external feeds

Starting in AsyncOS 10.5.3-017, you can create custom and external live-feed URL categories that contain specific host names and IP addresses using the Office 365 web service. In addition, you can edit and delete existing URL categories. When you include these custom URL categories in the same Access, Decryption, Identification Policy, or Cisco Data Security Policy group and assign different actions to each category, the action of the higher included custom URL category takes precedence.

Note: For versions earlier than AsyncOS 11.7, you can use no more than five external live feed files, including Cisco live feeds, Office 365 feed format, and Office 365 web service in these URL category definitions, and each file should contain no more than 1000 entries. Increasing the number of external feed entries may cause performance degradation.

Note: WSA version 11.7 adds support for up to 30 feed files with no more than 5000 entries each.

About this document

This document is for Cisco engineers and customers who will deploy Cisco® Web Security using AsyncOS® 10.5.3-0.17 or later. The configuration can be deployed via a Cisco® Security Management Appliance (SMA) or directly on a Cisco® Web Security Appliance (WSA).

This document covers:

- Introduction to external feeds
- Configuration of the Microsoft Office 365 web service
- Configuration of the feed within an access policy

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

Exception list

External feeds, and particularly Office 365 feeds, include commonly used sites fetched as part of third-party integrations (such as dropbox.com, google.com, etc.). Previously, the appliance did not provide any way to exclude such sites from custom feeds. Starting with **AsyncOS 11.8**, a new menu item, **Excluded Sites**, is added under **Custom and External URL Categories**. This option allows an administrator to add the IPv4 address, IPv6 address, host name, or domain name for sites to be excluded.

Before you begin

- Go to Security **Services** > **Acceptable Use Controls** to enable Acceptable Use Controls

External URL category settings

Step 1. Choose **Web Security Manager** > **Custom and External URL Categories**. We will be configuring an Office 365 external feed that consists of IP addresses, domains, and regular expressions that keep track of all Office 365 hosted services.

The screenshot displays the Cisco S300V Web Security Virtual Appliance interface. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The 'Web Security Manager' menu is expanded, showing categories like Authentication, Web Policies, Data Transfer Policies, and Custom Policy Elements. The 'Custom Policy Elements' sub-menu is highlighted, showing 'Custom and External URL Categories'. On the right, a 'System Resource Utilization' table is partially visible, showing metrics like CPU, RAM, and connections.

System Resource Utilization	
Overview > System Resource Utilization	
Last minute: 0	CPU
Last minute: 0	RAM
Last minute: 0	Reporting / logging dis
Connections: 4	
System Status Details	

Contents

About this document

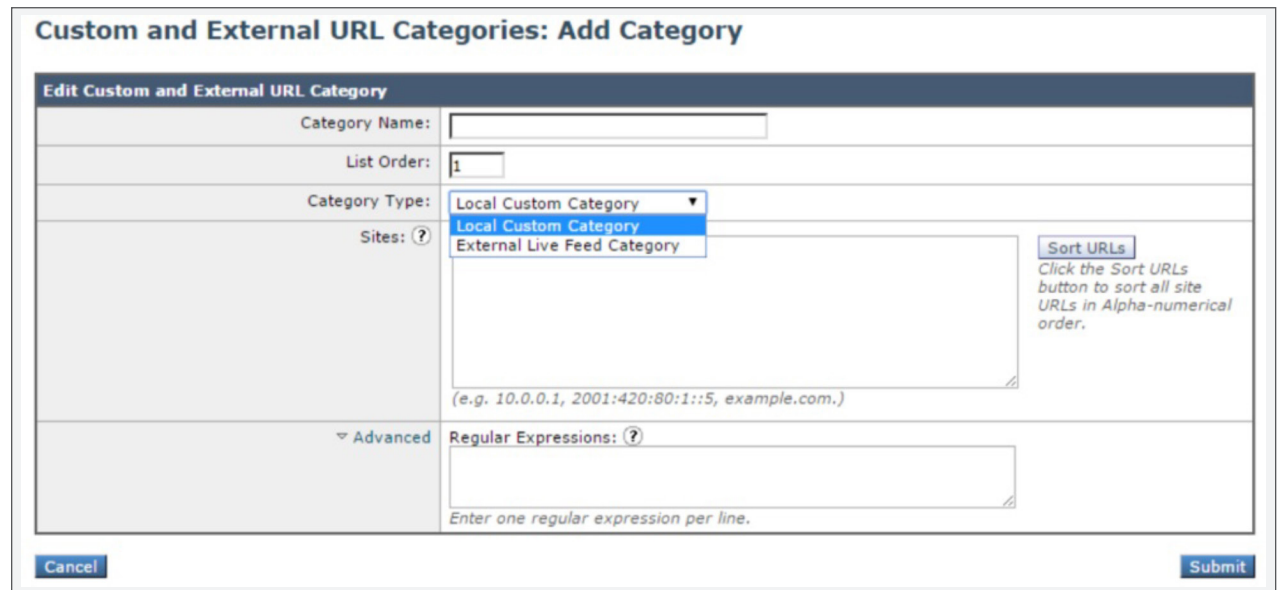
Introduction to external feeds

External URL category settings

External URL categories
in action

Step 2. To create a custom URL category, click **Add Category**. To edit an existing custom URL category, click the name of the URL category.

Step 3. Fill in the Category Name and List Order fields. (The URL filtering engine evaluates a client request against the custom URL categories in the order specified.*) Then select **External Live Feed Category**.



* It is possible to use the same address in multiple custom URL categories, but the order in which the categories are listed is relevant. If you include these categories in the same policy, and define different actions for each, the action defined for the category listed highest in the table of custom URL categories will be the one applied.

Step 4. Select the Office 365 Web Service option and add the feed location provided by Microsoft. When it is added, click **Start Test** to confirm a successful file download, and then click **Submit**.

Reference website: **Office 365 URLs and IP Address Ranges.**

(<https://docs.microsoft.com/en-us/office365/enterprise/office-365-ip-web-service>)

The default feed URL is set to retrieve the list of endpoints for worldwide location:

<https://endpoints.office.com/endpoints/worldwide>

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

With the introduction of the Office 365 web service, administrators can categorize external feeds based on location, service, IPv6, or tenant, as described below.

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	<input type="text" value="Office365worldwide"/>
List Order:	<input type="text" value="4"/>
Category Type:	External Live Feed Category
Routing Table:	Management
Feed File Location: ?	<input type="radio"/> Cisco Feed Format ? <input type="radio"/> Office 365 Feed Format ? <input checked="" type="radio"/> Office 365 Web Service ?
Web Service URL:	<input type="text" value="https://endpoints.office.com/endpoints"/>
	<input type="button" value="Start Test"/>

Note: If the available feed file is different from the currently downloaded file, the newer file will be downloaded and the download time updated. Otherwise, the file is not fetched and a “304 not modified” entry is logged.

Office 365 web service: This is a REST-based web service API by Microsoft Office 365 that offers IP addresses and URLs in the JSON format. The IP addresses and URLs either are trusted by Microsoft Office 365 or are part of their network. The Cisco WSA does not have control over the format of this JSON file.

This web service replaces the old XML format feed and can be accessed directly in a web browser. It supports various parameters as web methods for endpoint retrieval, such as:

Instance: Covers various regions such as Worldwide, China, Germany, USGovDoD, and USGovGCCHigh.

Service Areas: Valid items are Common, Exchange, SharePoint, and Skype.

Tenant Name: Your Office 365 tenant name.

No IPv6: Set this value to true if you want to exclude IPv6.

To apply the various parameters, customize the API URL. The following example extracts a feed file for a worldwide location covering a tenant named Cisco and a SharePoint service with no IPv6 address included.

<https://endpoints.office.com/endpoints/worldwide?ServiceAreas=sharepoint&TenantName=Cisco&NoIPv6=true>

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

To extract the contents of the custom web service URL, browse the link generated with the specific client request ID associated to the API call.

Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name:	<input type="text" value="Office365Cisco"/>
List Order:	<input type="text" value="3"/>
Category Type:	<input type="text" value="External Live Feed Category"/>
Routing Table:	Management
Feed File Location: ?	<input type="radio"/> Cisco Feed Format ? <input type="radio"/> Office 365 Feed Format ? <input checked="" type="radio"/> Office 365 Web Service ?
Web Service URL:	<input type="text" value="https://endpoints.office.com/endpoints"/>
	<input type="button" value="Start Test"/>
	<p>Created URL is, https://endpoints.office.com/endpoints/worldwide?ServiceAreas=sharepoint&TenantName=Cisco&NoIPv6=true&clientrequestid=c77b61e5-15cc-4536-aa84-403f620a95ac</p> <p>Checking DNS resolution of feed server... Success: Resolved 'endpoints.office.com' address: 13.91.37.26</p>

The following screen shot shows the Office 365 web service JSON output for the above example.

```
https://endpoints.office.com/endpoints/worldwide?ServiceAreas=sharepoint&TenantName=Cisco&NoIPv6=true&clientrequestid=c77b61e5-15cc-4536-aa84-403f620a95ac

{
  "id": 31,
  "serviceArea": "SharePoint",
  "serviceAreaDisplayName": "SharePoint Online and OneDrive for Business",
  "uris": [
    "Cisco.sharepoint.com",
    "Cisco-my.sharepoint.com"
  ],
  "ips": [
    "13.107.6.150/31",
    "13.107.6.168/32",
    "13.107.9.150/31",
    "13.107.9.168/32",
    "13.107.136.0/22",
    "40.108.0.0/19",
    "40.108.128.0/17",
    "52.104.0.0/14",
    "104.146.0.0/19",
    "104.146.128.0/17",
    "134.170.200.0/21",
    "134.170.208.0/21",
    "150.171.40.0/22",
    "191.232.0.0/23",
    "191.235.0.0/20"
  ],
  "tcpPorts": "80,443",
  "expressRoute": true,
  "category": "Optimize",
  "required": true
}
```

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

Step 5. To exclude any sites, enter the details in the **Excluded Sites** section.

Excluded Sites: ?	<input type="text" value="accounts.google.com, mail.google.com, www.googleapis.com"/>	<input type="button" value="Sort URLs"/> <i>Click the Sort URLs button to sort all site URLs in Alpha-numerical order.</i>
<i>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</i>		
▼ Advanced	Excluded Regular Expressions: ? <input type="text"/>	
<i>Enter one regular expression per line.</i>		
Auto Update the Feed:	<input checked="" type="radio"/> Do not auto update <input type="radio"/> Hourly <input type="button" value="↓"/> Every <input type="text" value="01:0"/> (HH:MM)	

Multiple entries can be separated with line breaks or commas.

Step 6 (optional). To use regular expressions to specify sites to exclude, expand the Advanced option and add the expressions to the **Excluded Regular Expressions** section.

To view the excluded sites, click the **Feed Content View** option.

Reporting
Web Security Manager
Security Services
Network
System Administration

External Category Content

Custom and External URL Categories

Success — Settings have been saved.

Categories List

Managed by: vsma.lkcol.com - local changes will be overwritten.

Order	Category	Category Type	Last Updated	Feed Content
1	whatsapp	Custom (Local)	N/A	-
2	AlteonCustCat	Custom (Local)	N/A	-
3	feedIIS	External Feed	Never Updated	-
4	Office365Cisco	External Feed	06 Aug 2019 13:33:08 PM	View

Last published from: vsma.lkcol.com 13 Jul 2018 15:12 (GMT +05:30)

wus-www.sway-con.com
 wus-www.sway-extensions.com
 www.acompli.com
 www.bing.com
 www.digicert.com
 www.dropbox.com
 www.evernote.com
 www.google-analytics.com
 www.microsoft.com
 www.office.com
 www.onedrive.com
 www.outlook.com
 www.sway.com
 www.wunderlist.com
 www.youtube.com
 accounts.google.com(excluded)
 mail.google.com(excluded)
 www.googleapis.com(excluded)

Regular Expressions:
 -files.sharepoint.com
 -myfiles.sharepoint.com

The excluded sites are highlighted in **red**.

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

External URL categories in action

Step 1. Choose Web Security Manager > Access Policies.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	Office365 Identification Profile: All Protocols: HTTP, HTTPS, FTP over HTTP, Native FTP, All others	(global policy)	Block: 2 Monitor: 77	(global policy)	(global policy)	Web Reputation: Enabled Advanced Malware Protection: Disabled Anti-Malware Scanning: Enabled	
	Global Policy Identification Profile: All	No blocked items	Monitor: 79	Monitor: 365	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Disabled Anti-Malware Scanning: Enabled	

Step 2. Click the policy that you would like to add to the Office 365 web service.

For this example, we have created a separate policy, Office365CiscoAP. Now click within the URL Filtering cell, as shown below.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	Office365CiscoAP Identification Profile: id1 All identified users	(global policy)	Block: 1 Monitor: 86	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Monitor: 85	Monitor: 356	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

Category	Category Type	Setting Selection
O365GerSp	External Feed	Exclude from policy
O365ChCisEx	External Feed	Exclude from policy
O365WWide	External Feed	Exclude from policy
Office365Cisco	External Feed	Include in policy

Buttons: Cancel, Apply

Step 3. Select **Custom Categories**. A pop-up will display all custom URL categories that have been created.

Step 4. In the example below, we have checked the **Allow** box to set the customer category to Allow. This will place the traffic for Office365Cisco in pass-through mode for HTTP. When it is configured, click **Submit**.

Custom and External URL Category Filtering		Use Global Settings	Override Global Settings				
Category	Category Type		Block	Redirect	Allow	Monitor	Warn
Office365Cisco	External Feed	-	Select all	Select all	Select all	Select all	Select all
Select Custom Categories....					<input checked="" type="checkbox"/>		

Buttons: Cancel

Step 5. Don't forget to commit all changes. Save your configuration.

Step 6. Now select **Web Security Manager > Identification Profiles > Add Identification Profile**.

Select **URL Categories** under the Advanced section, and select **Office365Cisco**.

Note: The external feed was created at the beginning of this guide. The setting below will exempt the Office365Cisco URL from authentication.

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

Identification Profiles: CiscoIdentificationProfile1

Client / User Identification Profile Settings	
<input checked="" type="checkbox"/> Enable Identification Profile	
Name: ?	<input type="text" value="CiscoIdentificationProfile1"/> <small>(e.g. my 11 Profile)</small>
Description:	<input type="text"/>
Insert Above:	1 (Global Profile) ↓

User Identification Method	
Identification and Authentication: ?	<small>For additional options, define an authentication realm (see Network > Authentication) or enable ISE (see Network > Identity Services Engine).</small>

Membership Definition	
<small>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</small>	
Define Members by Subnet:	<input type="text"/> <small>(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)</small>
Define Members by Protocol:	<input checked="" type="checkbox"/> HTTP/HTTPS <input type="checkbox"/> Native FTP
Advanced	<small>Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.</small>
<small>The following advanced membership criteria have been defined:</small>	
Proxy Ports:	None Selected
URL Categories:	Office365Cisco

Step 7. Select **Web Security Manager > Decryption Policies > Add Policy**.

You will need to set the Identification Profile to CiscoIdentificationProfile1, which we created in step 6. When you have selected your identity profile, the URL categories will automatically be populated. The setting below helps Office 365 pass through HTTPS traffic without decrypting the transactions.

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

Decryption Policy: Office365CiscoDP

Policy Settings

Enable Policy

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

Description:

Insert Above 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:

Identification Profile	Authorized Users and Groups	
<input type="text" value="CiscoIdentificationProfile1"/>	No authentication required	<input type="button" value="Add Identification Profile"/>

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

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

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

URL Categories: URL Categories Office365Cisco in Identification Profile CiscoIdentificationProfile1

Step 8. Click Submit.

Contents

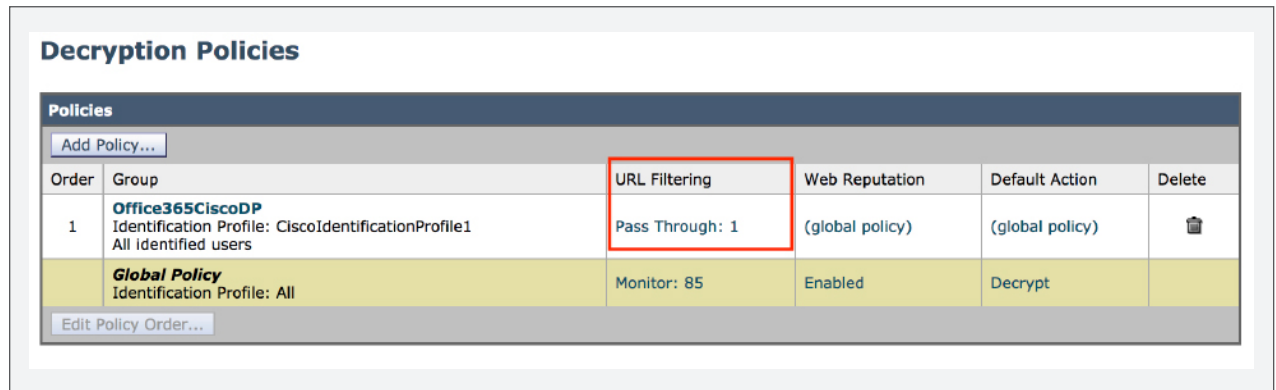
About this document


Introduction to external feeds

External URL category settings

External URL categories
in action

Step 9. Select URL Filter Policy.



Decryption Policies					
Policies					
Add Policy...					
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	Office365CiscoDP Identification Profile: CiscoIdentificationProfile1 All Identified users	Pass Through: 1	(global policy)	(global policy)	
	Global Policy Identification Profile: All	Monitor: 85	Enabled	Decrypt	
Edit Policy Order...					

Step 10. Now, under the Office365CiscoDP policy, select **URL Filtering > Select Custom Categories > Office365Cisco > Include in Policy > Apply and Submit**. Make sure you always commit your changes.

With support for REST-based APIs, the administrators can define different actions for various supported service types, locations, IPv6, and tenants.

In the following example, the worldwide SharePoint traffic is set for **Decrypt** and all other worldwide endpoint traffic is set to **Pass Through**.

Step 1. Choose **Web Security Manager > Custom and External URL Categories**. Add the following categories and URLs as described in the **External URL categories** section.

Name: **SharepointFeedWorldWide**

URL: <https://endpoints.office.com/endpoints/Worldwide?ServiceAreas=sharepoint>

Name: **AllfeedsWorldwide**

URL: <https://endpoints.office.com/endpoints/worldwide>

Step 2. Select **Web Security Manager > Decryption Policies > Add Policy**.

Create a policy **Office365Sharepoint**, and under **Advanced Settings**, add the URL category **SharepointFeedWorldWide** and click **Submit**.

Step 3. Set the URL filtering action for the custom category **SharepointFeedWorldWide** to **Decrypt** (as described in **step 10** of the section **External URL categories in action**).

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

Step 4. Repeat the steps above to create a decryption policy named **Office365WorldWide** for customer category **AllfeedsWorldwide**, and set the URL filtering action to **Pass Through**.

Decryption Policies					
Policies					
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	Office365Sharepoint Identification Profile: All URL Categories: SharepointFeedWorldWide	Decrypt: 1	(global policy)	(global policy)	
2	Office365WorldWide Identification Profile: All URL Categories: AllfeedsWorldwide	Pass Through: 1	(global policy)	(global policy)	

Step 5. Submit and commit changes.

Routing policy configuration (optional)

Administrators can also create routing policies based on the custom URL identification to route to a specific upstream proxy device.

Step 1. Select **Web Security Manager > Routing Policies > Add Policy**. Create a policy named **ToUpstreamWSA**.

Step 2. Expand **Advanced** and click **URL Categories**.

Policy Member Definition

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

<p>Identification Profiles and Users:</p> <p>Select One or More Identification Profiles</p> <p>Identification Profile: Select Identification Profile...</p> <p>Authorized Users and Groups: No Identification Profile selected Add Identification Profile</p>	<p>Advanced</p> <p>Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.</p> <p>The following advanced membership criteria have been defined:</p> <p>Protocols: None Selected</p> <p>Proxy Ports: None Selected</p> <p>Subnets: None Selected</p> <p>Time Range: No Time Range Definitions Available <small>(see Web Security Manager > Defined Time Ranges)</small></p> <p>URL Categories: None Selected</p> <p>User Agents: None Selected</p>
--	--

Step 3. Select the external feed **Office365Cisco** and submit the changes.

Contents

About this document

Introduction to external feeds

External URL category settings

External URL categories
in action

Step 4. Under **Routing Destination**, click **Direct Connection**.

Routing Definitions			
Add Policy...			
Order	Members	Routing Destination	Delete
1	ToUpstreamWSA Identification Profile: CiscoIdentificationProfile1 All identified users	Direct Connection	

Step 5. Select the appropriate upstream proxy from the drop-down option.

In this example we have leveraged a preconfigured upstream proxy named **UpstreamWSA11.7**.

Routing Policies: Add Upstream Proxy Group

Routing Destination Settings

Upstream Proxy Group:

- Use Global Policy Settings
- ✓ Direct Connection
- UpstreamWSA11.7

Cancel

Step 6: Submit and commit the changes.

Contents

About this document


Introduction to external feeds

External URL category settings

External URL categories
in action

Bypass Office 365 traffic

AsyncOS 11.8 adds support for configuring custom and external URL categories in the Proxy Bypass List. This is possible only when the appliance is in transparent mode. The option can be used to bypass any specified Office 365 traffic to be routed normally.



Proxy Bypass	
Proxy Bypass List: ?	All destinations and clients in this list will bypass web proxy policies when the appliance is in transparent mode. 10.0.0.10  (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)
Custom URL Categories: ?	Add custom URL categories to Proxy bypass list. Office365Cisco

Note: The Proxy Bypass List is limited to host names and IP addresses only. Any regular expressions configured in the custom category, or even partial names, are ignored. Both custom and external categories can be used, and for the latter auto-update is honored.