Web Reputation score (WBRS) and Web Categorization Engine Frequently Asked Questions (FAQ)

Contents

Web Reputation score (WBRS) and Web Categorization Engine Frequently Asked Questions (FAQ).

This article describes the most frequently asked questions on Web Reputation Score (WBRS) and Categorisation feature with the Cisco Web Security Appliance (WSA).

What Web Reputation Score means?

Web Reputation Filters assigns a Web-Based Reputation Score (WBRS) to a URL to determine the likelihood that it contains URL-based malware. The Web Security appliance uses web reputation scores to identify and stop malware attacks before they occur. You can use Web Reputation Filters with Access,

Decryption, and Cisco Data Security Policies.

What Web Categorization Means?

The internet websites are categories based on the behavior and the purpose of these Websites, in order to make it easier for the Administrators of the proxies, we have added every Website URL to a predefined category, where it can be Identified for security and reporting purposes. the websites that does not belong to one of the predefined categories, are called uncategorized Websites, which can be due to new website creation and lack of enough data/traffic, to determine its category. and this changes by time.

How to find reputation score in access logs?

Every request you are making through the Cisco Web Security Appliance (WSA) should have a Web-Based Reputation Score (WBRS) score and URL category attached to it. and one of the ways to view it is through the access logs, example is below: the Web-Based Reputation Score (WBRS) score is (-1.4), and URL category is: Computers and Internet.

Text reference for the above screenshot.

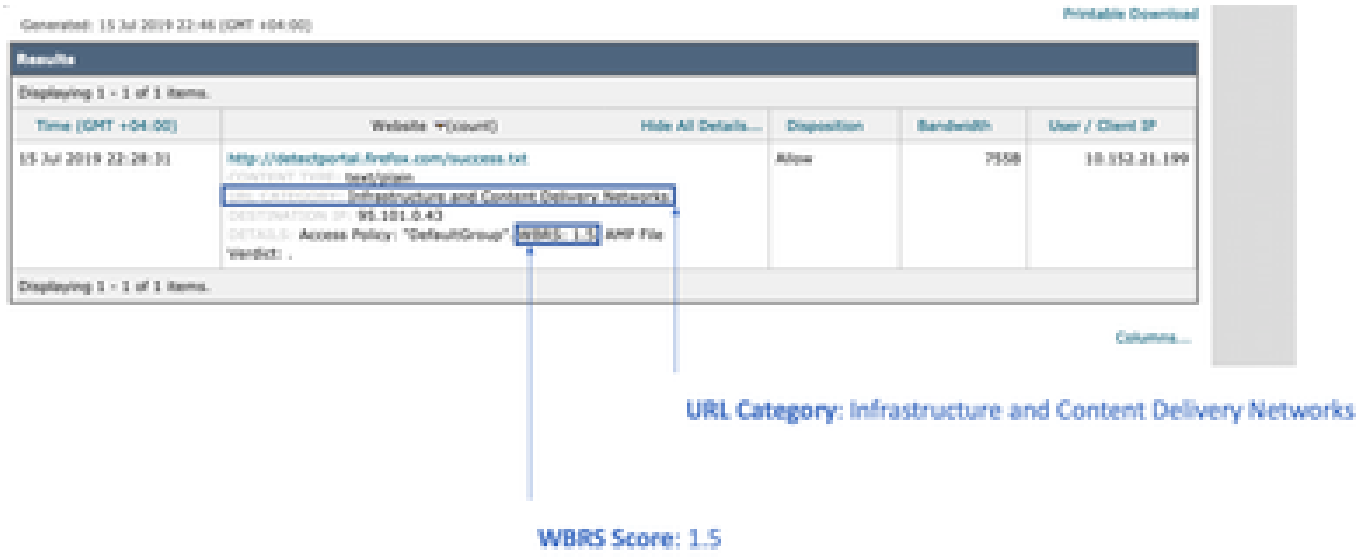
1563214694.033 117 xx.xx.xx.xx TCP_MISS/302 1116 GET https://example.com - DIRECT/example.com text/html DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE

Notes:

- Access logs can be viewed either from Command Line Interface (CLI) or downloaded by connecting using File Transfer Protocol (FTP) method on the management interface IP. (make sure that FTP is enabled on the interface).
- Full list of Categories Abbreviation: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01001.html#con_12

How to find reputation score in my reports?

1. Navigate to Cisco Web Security Appliance (WSA) **GUI** -> **Reporting** -> **Web Tracking**.
2. Search for the **Domain** you are looking for.
3. In the **Results** page, klick on the needed link, and more details will show up as below.



Where do you check the Web-Based Reputation Score (WBRS) updates logs?

Web-Based Reputation Score (WBRS) updates logs can be found under the updater_logs, you can download these logs via File Transfer Protocol (FTP) login to the management interface. or Via Command Line Interface (CLI).

To View Logs using terminal:

1. Open **Terminal**.
2. Type the command **tail**.
3. Chose the **logs number** (it varies depends on the version and the number of logs configured).
4. The logs will be displayed.

```
WSA.local (SERVICE)> tail

Currently configured logs:
1. "xx.xx.xx.xx" Type: "Configuration Logs" Retrieval: FTP Push - Host
xx.xx.xx.xx
2. "Splunk" Type: "Access Logs" Retrieval: FTP Poll
3. "accesslogs" Type: "Access Logs" Retrieval: FTP Push - Host xx.xx.xx.xx
4. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
5. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
....
43. "uds_logs" Type: "UDS Logs" Retrieval: FTP Poll
44. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP
Poll
Enter the number of the log you wish to tail.
[]> 44
```

```
Press Ctrl-C to stop scrolling, then `q` to quit.
Mon Jul 15 19:24:04 2019 Info: mcafee updating the client manifest
Mon Jul 15 19:24:04 2019 Info: mcafee update completed
Mon Jul 15 19:24:04 2019 Info: mcafee waiting for new updates
Mon Jul 15 19:36:43 2019 Info: wbrs preserving wbrs for upgrades
Mon Jul 15 19:36:43 2019 Info: wbrs done with wbrs update
Mon Jul 15 19:36:43 2019 Info: wbrs verifying applied files
Mon Jul 15 19:36:58 2019 Info: wbrs Starting heath monitoring
Mon Jul 15 19:36:58 2019 Info: wbrs Initiating health check
Mon Jul 15 19:36:59 2019 Info: wbrs Healthy
Mon Jul 15 19:37:14 2019 Info: wbrs Initiating health check
Mon Jul 15 19:37:15 2019 Info: wbrs Healthy
Mon Jul 15 19:37:30 2019 Info: wbrs Initiating health check
Mon Jul 15 19:37:31 2019 Info: wbrs Healthy
Mon Jul 15 19:37:46 2019 Info: wbrs Initiating health check
Mon Jul 15 19:37:47 2019 Info: wbrs Healthy
Mon Jul 15 19:38:02 2019 Info: wbrs updating the client manifest
Mon Jul 15 19:38:02 2019 Info: wbrs update completed
Mon Jul 15 19:38:03 2019 Info: wbrs waiting for new updates
Mon Jul 15 20:30:23 2019 Info: Starting scheduled release notification fetch
Mon Jul 15 20:30:24 2019 Info: Scheduled next release notification fetch to occur at Mon Jul 15 23:30:24
Mon Jul 15 23:30:24 2019 Info: Starting scheduled release notification fetch
Mon Jul 15 23:30:25 2019 Info: Scheduled next release notification fetch to occur at Tue Jul 16 02:30:25
```

How do you verify If you have connectivity to Web-Based Reputation Score (WBRS) updates servers?

In order to make sure your Cisco Web Security Appliance (WSA) is able to get the new updates. please verify that you have the connectivity to Cisco update's servers on the following Transmission Control Protocol (TCP) ports 80 and 443:

```
wsa.local (SERVICE)> telnet updates.ironport.com 80
Trying xx.xx.xx.xx...
Connected to updates.ironport.com.
Escape character is '^]'.
```

```
wsa.calo (SERVICE)> telnet upgrades.ironport.com 80
Trying xx.xx.xx.xx...
Connected to upgrades.ironport.com.
Escape character is '^]'.
```

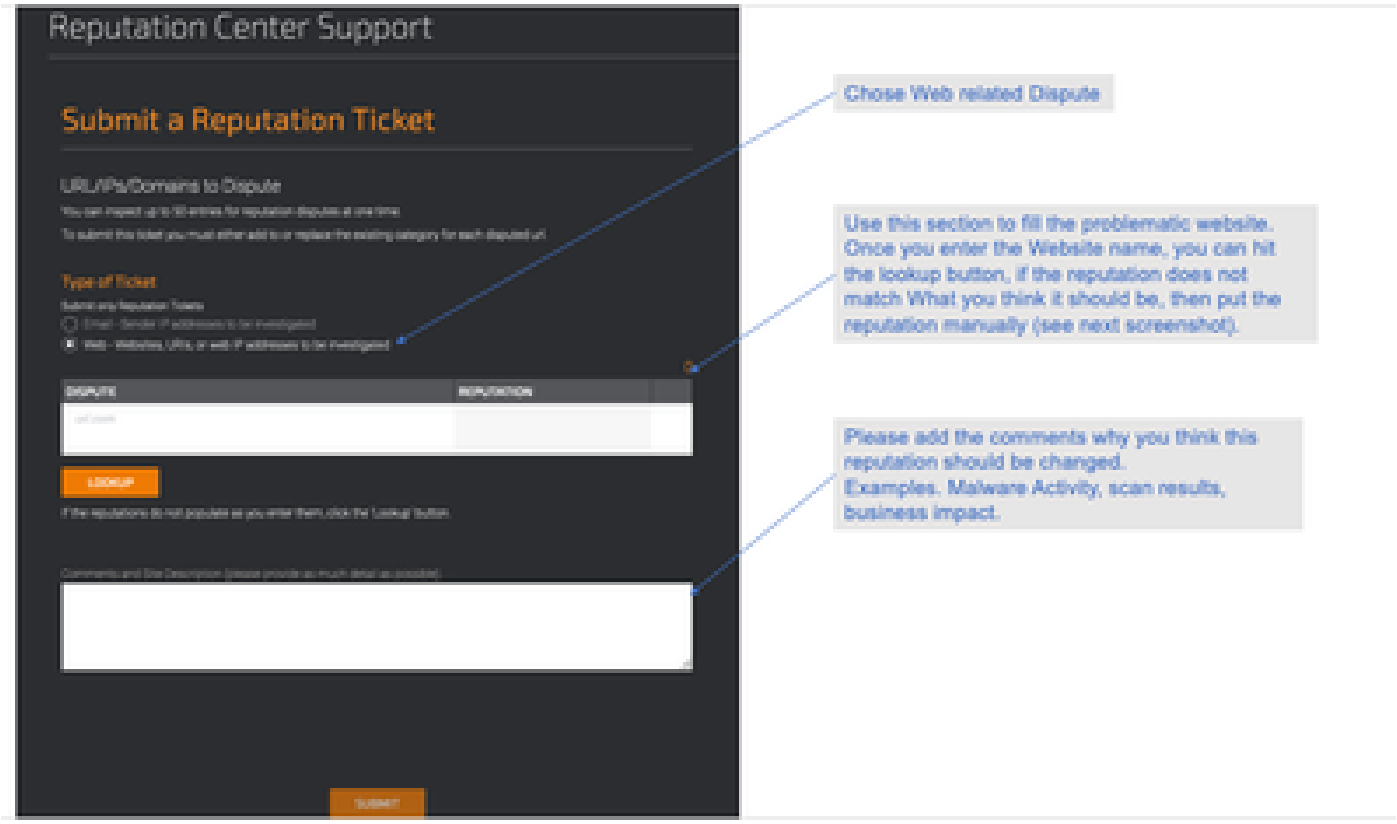
Note: If you have any upstream proxy, do the above tests through your upstream proxy.

How do you file a dispute for Web Categorization?

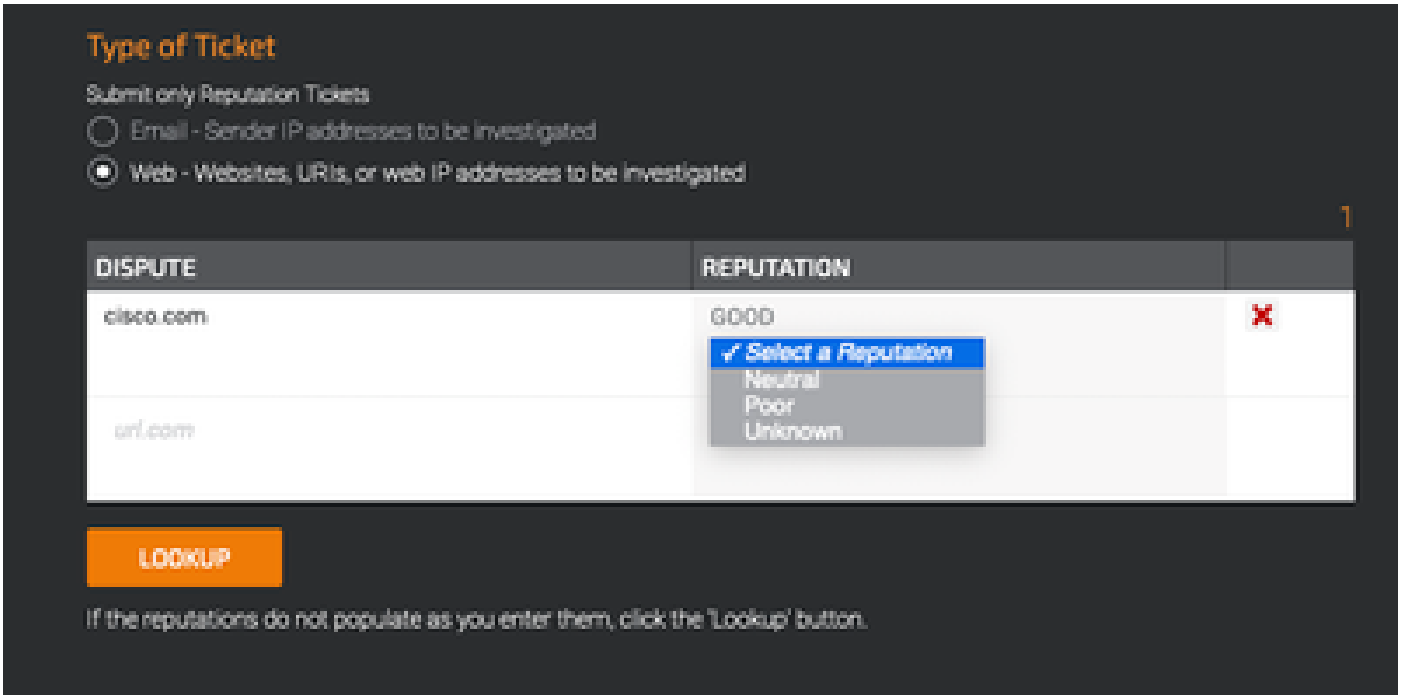
After verifying that both Cisco Web Security Appliance (WSA) and Cisco TALOS having the same reputation score, but you still think this is not a valid result, then this need to be fixed by submitting a dispute with Cisco TALOS team.

This can be done using the following link: https://talosintelligence.com/reputation_center/support

In order to **submit** the **Dispute**, please follow the below instructions.



Results after hitting Lookup and the option to manually change the score.



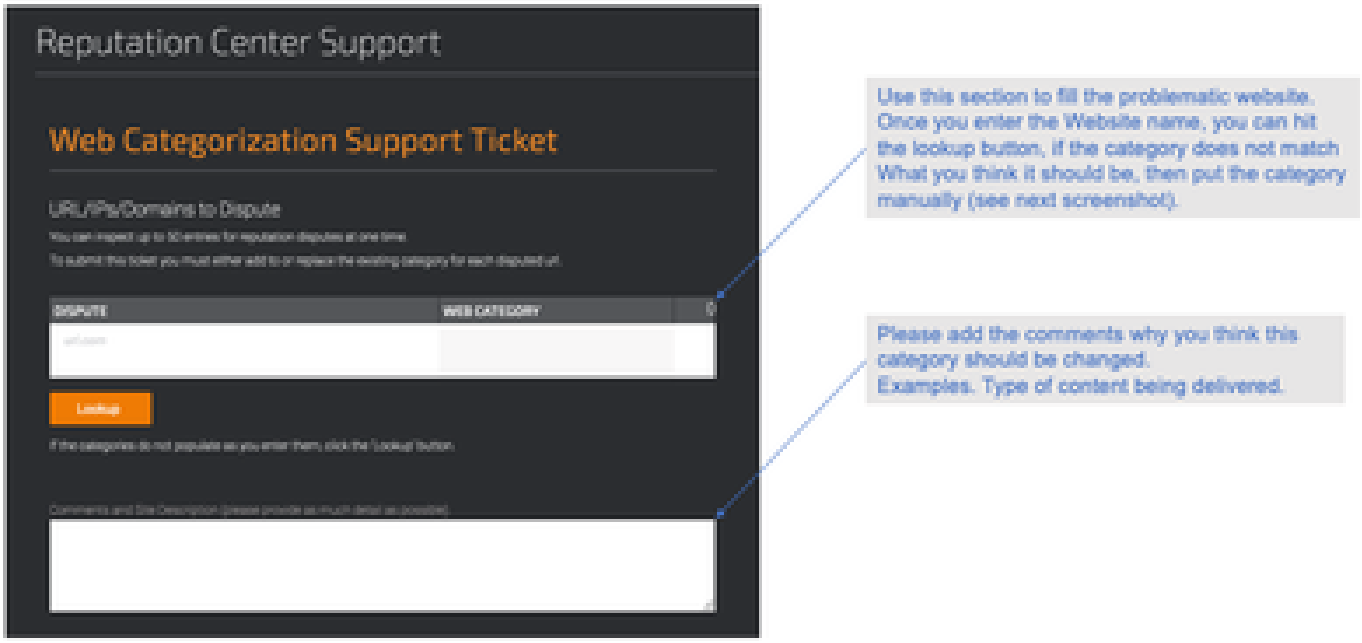
Note: Cisco TALOS submissions might take some time to be reflected on database, if the issue is urgent, you can always create a **WHITELIST** or **BLOCKLIST**, as a work-around till the issue is fixed from Cisco backend. in order to do that, you can check this section (How To Whitelist or BlackList URL).

How do you file dispute for Web Reputation score?

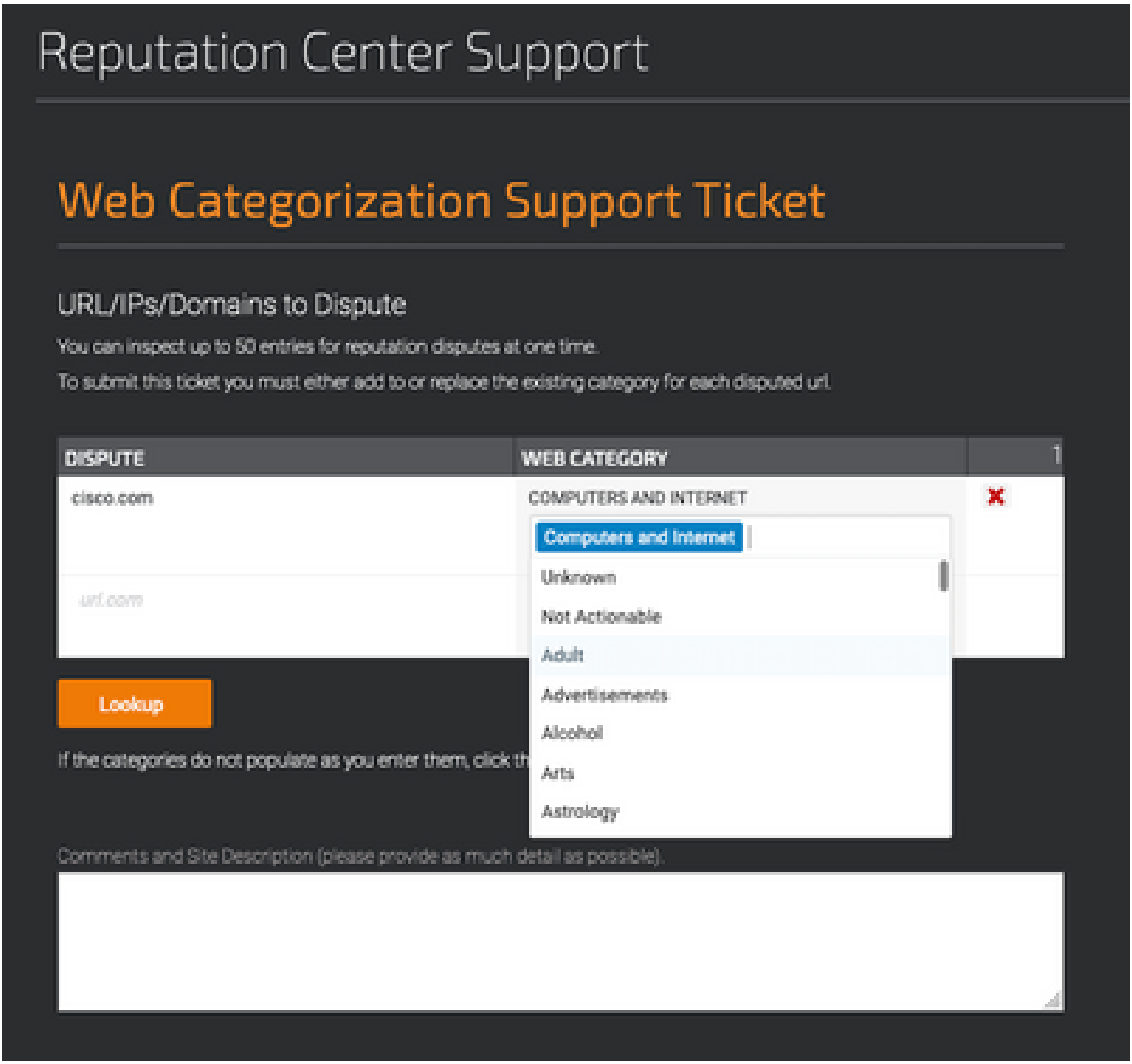
After verifying that both Cisco Web Security Appliance (WSA) and Cisco TALOS having the same Categorization, but you still think this is not a valid result, then this need to be fixed by submitting a dispute with Cisco TALOS team.

Go to the categorization submission page in TALOS website:
https://talosintelligence.com/reputation_center/support#categorization

In order to **submit** the **Dispute**, please follow the below instructions.



To update the Category, chose from the **drop-down** menu what you feel it suits the website better, and make sure you to follow the comments guidelines.



A dispute has been filed but the score or category is not getting updated on Cisco Web Security Appliance (WSA) or Cisco TALOS.

In case you have filed a case with Cisco TALOS and the reputation/score did not get updated within 3-4 days. you can check your updates settings and make sure you have reachability to Cisco update's server. if all these steps were ok, then you can go ahead and open a ticket with Cisco TAC, and Cisco Engineer will assist you in following up with Cisco TALOS team.

Note: you can apply the WHITELIST/BLOCKLIST work-around to apply the needed action till the category/reputation gets updated from Cisco TALOS team.

Cisco Web Security Appliance (WSA) showing different results

than Cisco TALOS, how to fix this?

Database can be out of date on the Cisco Web Security Appliance (WSA) due to multiple reasons, mainly communication with our updates servers, please follow these steps to verify you have correct update servers and connectivity.

1. Verify that you have the connectivity for Cisco update's servers on port 80 and 443:

```
wsa.local (SERVICE)> telnet updates.ironport.com 80
Trying xx.xx.xx.xx...
Connected to updates.ironport.com.
Escape character is '^]'.

wsa.calo (SERVICE)> telnet upgrades.ironport.com 80
Trying xx.xx.xx.xx...
Connected to upgrades.ironport.com.
Escape character is '^]'.
```

2. If you have any upstream proxy, make sure that the upstream proxy makes sure you do the above tests through your upstream proxy.

3. If the connectivity is fine and you still see the difference, then force the updates manually: **updatenow** from the CLI, or from **GUI->Security services -> Malware protection -> updatenow**.

Wait few minutes, and If that does not work please check the next step.

4. At this point you will need to check the updater_logs: open **terminal: CLI->tail-> (chose the number of updater_logs log file.)** this will make the update logs display the new lines only.

Log lines should start with this line "**Received remote command to signal a manual update**":

```
Mon Jul 15 19:14:12 2019 Info: Received remote command to signal a manual update
Mon Jul 15 19:14:12 2019 Info: Starting manual update
Mon Jul 15 19:14:12 2019 Info: Acquired server manifest, starting update 342
Mon Jul 15 19:14:12 2019 Info: wbrs beginning download of remote file "http://updates
Mon Jul 15 19:14:12 2019 Info: wbrs released download lock
Mon Jul 15 19:14:13 2019 Info: wbrs successfully downloaded file "wbrs/3.0.0/ip/defau
Mon Jul 15 19:14:13 2019 Info: wbrs started applying files
Mon Jul 15 19:14:13 2019 Info: wbrs started applying files
Mon Jul 15 19:14:13 2019 Info: wbrs applying component updates
Mon Jul 15 19:14:13 2019 Info: Server manifest specified an update for mcafee
Mon Jul 15 19:14:13 2019 Info: mcafee was signalled to start a new update
Mon Jul 15 19:14:13 2019 Info: mcafee processing files from the server manifest
Mon Jul 15 19:14:13 2019 Info: mcafee started downloading files
Mon Jul 15 19:14:13 2019 Info: mcafee waiting on download lock
```

5. Check for any "**Critical/Warning**" messages, the update logs are very human readable errors, and most likely will guide you where is the problem.

6. If there was no answer then you can go ahead and open a ticket with Cisco support with the results of the above steps, and they will be happy to assist.

How does Web Reputation Scores are being calculated?

Some of the parameters that is being considered when assigning a score to specific website:

- URL categorization data
- Presence of downloadable code
- Presence of long, obfuscated End-User License Agreements (EULAs)
- Global volume and changes in volume
- Network owner information
- History of a URL
- Age of a URL
- Presence on any block lists
- Presence on any allow lists
- URL typos of popular domains
- Domain registrar information
- IP address information

What is the score range for each of the reputation categories (good, neutral, poor)?

Web Reputation Ranges and their associated actions:

Access Policies:

Score	Action	Description	Example
-10 to -6.0 (Poor)	Block	Bad site. The request is blocked, and no further malware scanning occurs.	• URL downloads information without. • user permission. • Sudden spike in URL volume. • URL is a typo of a popular domain.
-5.9 to 5.9 (Neutral)	Scan	Undetermined site. Request is passed to the DVS engine for further malware scanning. The DVS engine scans the request and server response content.	• Recently created URL that has a • dynamic IP address and contains • downloadable content. • Network owner IP address that has a • positive Web Reputation Score.
6.0 to 10.0 (Good)	Allow	Good site. Request is allowed. No malware scanning required.	• URL contains no downloadable content. • Reputable, high-volume domain with long history. • Domain present on several allow lists. • No links to URLs with poor reputations.

Decryption Policies:

Score	Action	Description

-10 to -9.0 (Poor)	Drop	Bad site. The request is dropped with no notice sent to the end user. Use this setting with caution.
-8.9 to 5.9 (Neutral)	Decrypt	Undetermined site. Request is allowed, but the connection is decrypted and Access Policies are applied to the decrypted traffic.
6.0 to 10.0 (Good)	Pass through	Good site. Request is passed through with no inspection or decryption.

Cisco Data Security Policies:

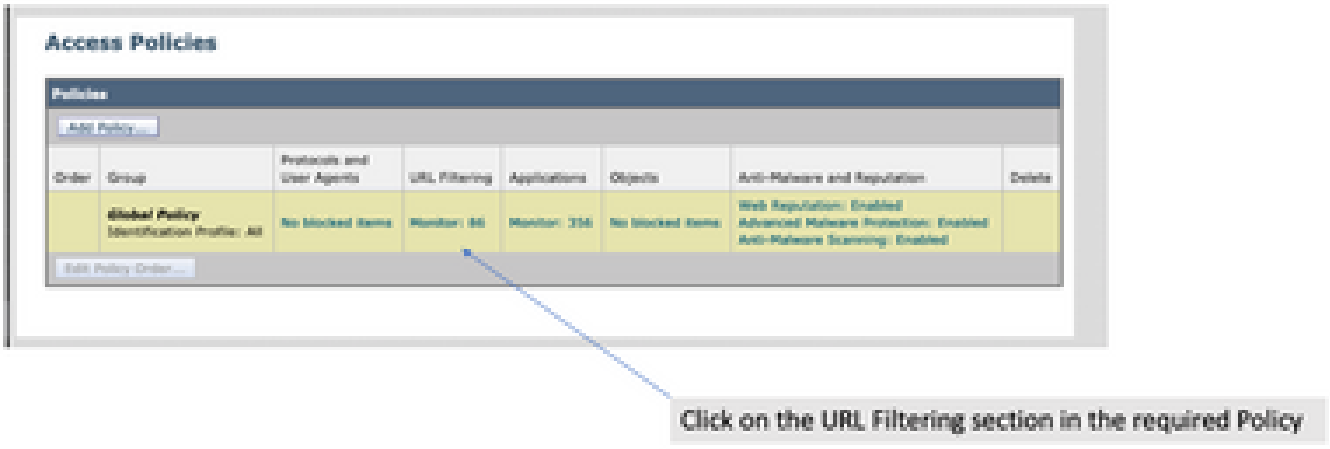
Score	Action	Description
-10 to -6.0 (Poor)	Block	Bad site. The transaction is blocked, and no further scanning occurs.
-5.9 to 0.0 (Neutral)	Monitor	The transaction will not be blocked based on Web Reputation, and will proceed to content checks (file type and size). Note Sites with no score are monitored.

What does uncategorized website mean?

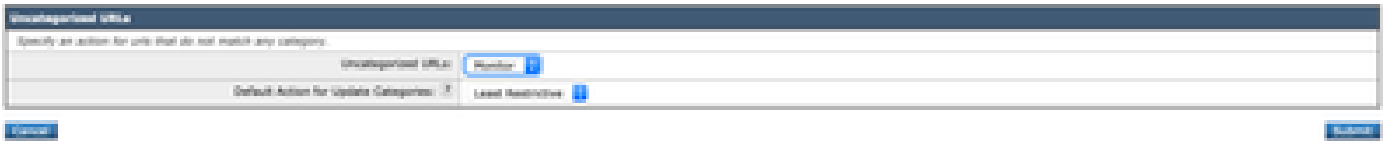
Uncategorized URLS are the ones that Cisco Database does not have enough information about to confirm their category. usually newly created websites.

How do you block uncategorized URLS?

1. Go to the desired Access Policy: **Web Security Manager -> Access Policies**.



2. Scroll down to the Uncategorized URLs section.



3. Chose one of the desired actions, **Monitor**, **Block**, or **Warn**.

4. **Submit** and **Commit** changes.

How frequent the database gets updated?

The updates check frequency can be updated either using the following command from CLI: **updateconfig**

<#root>

```
WSA.local (SERVICE)> updateconfig

Service (images): Update URL:

-------------------------------------------------------------------------------
Webroot Cisco Servers
Web Reputation Filters Cisco Servers
L4 Traffic Monitor Cisco Servers
Cisco Web Usage Controls Cisco Servers
McAfee Cisco Servers
Sophos Anti-Virus definitions Cisco Servers
Timezone rules Cisco Servers
HTTPS Proxy Certificate Lists Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Service (list): Update URL:

-------------------------------------------------------------------------------
Webroot Cisco Servers
Web Reputation Filters Cisco Servers
L4 Traffic Monitor Cisco Servers
Cisco Web Usage Controls Cisco Servers
McAfee Cisco Servers
Sophos Anti-Virus definitions Cisco Servers
Timezone rules Cisco Servers
HTTPS Proxy Certificate Lists Cisco Servers
Cisco AsyncOS upgrades Cisco Servers
```

Update interval for Web Reputation and Categorization: 12h

Update interval for all other services: 12h

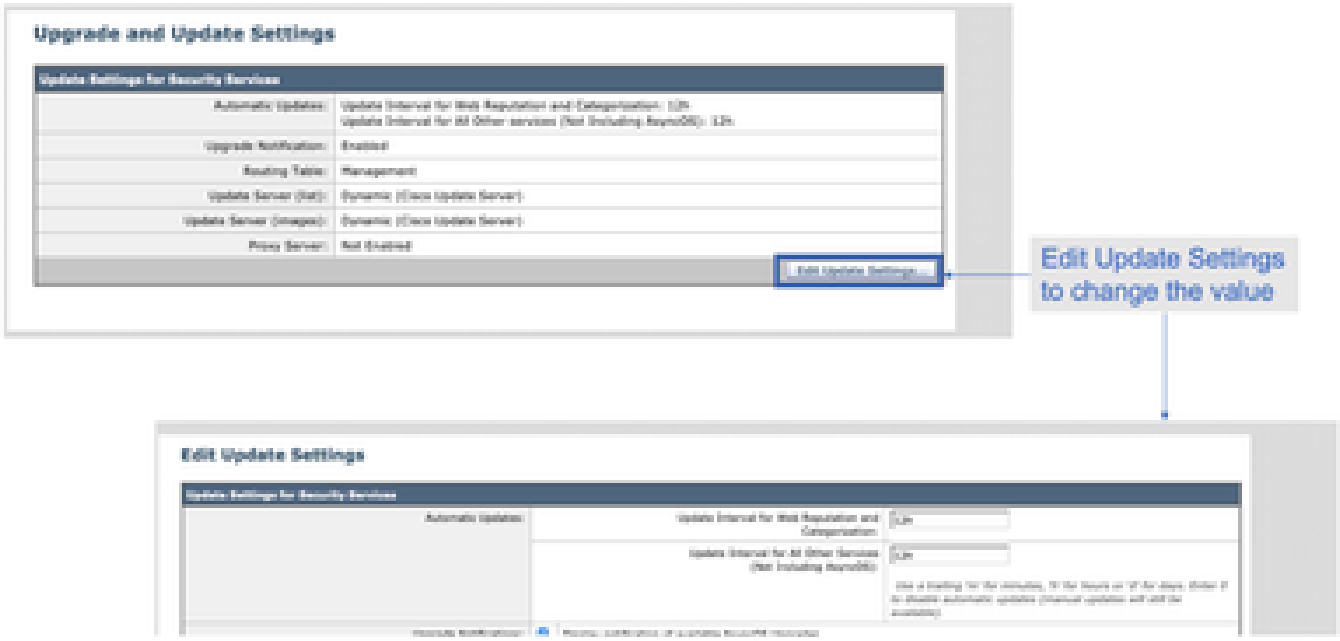
```
Proxy server: not enabled
HTTPS Proxy server: not enabled
Routing table for updates: Management
The following services will use this routing table:
- Webroot
- Web Reputation Filters
- L4 Traffic Monitor
- Cisco Web Usage Controls
- McAfee
- Sophos Anti-Virus definitions
- Timezone rules
- HTTPS Proxy Certificate Lists
- Cisco AsyncOS upgrades

Upgrade notification: enabled
```

```
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

Note: the above value shows how frequent we check for updates, but not how frequent we release new updates for the reputation and other services. the updates can be available at any point of time.

OR from GUI: **System Administration -> Upgrade and updates settings.**



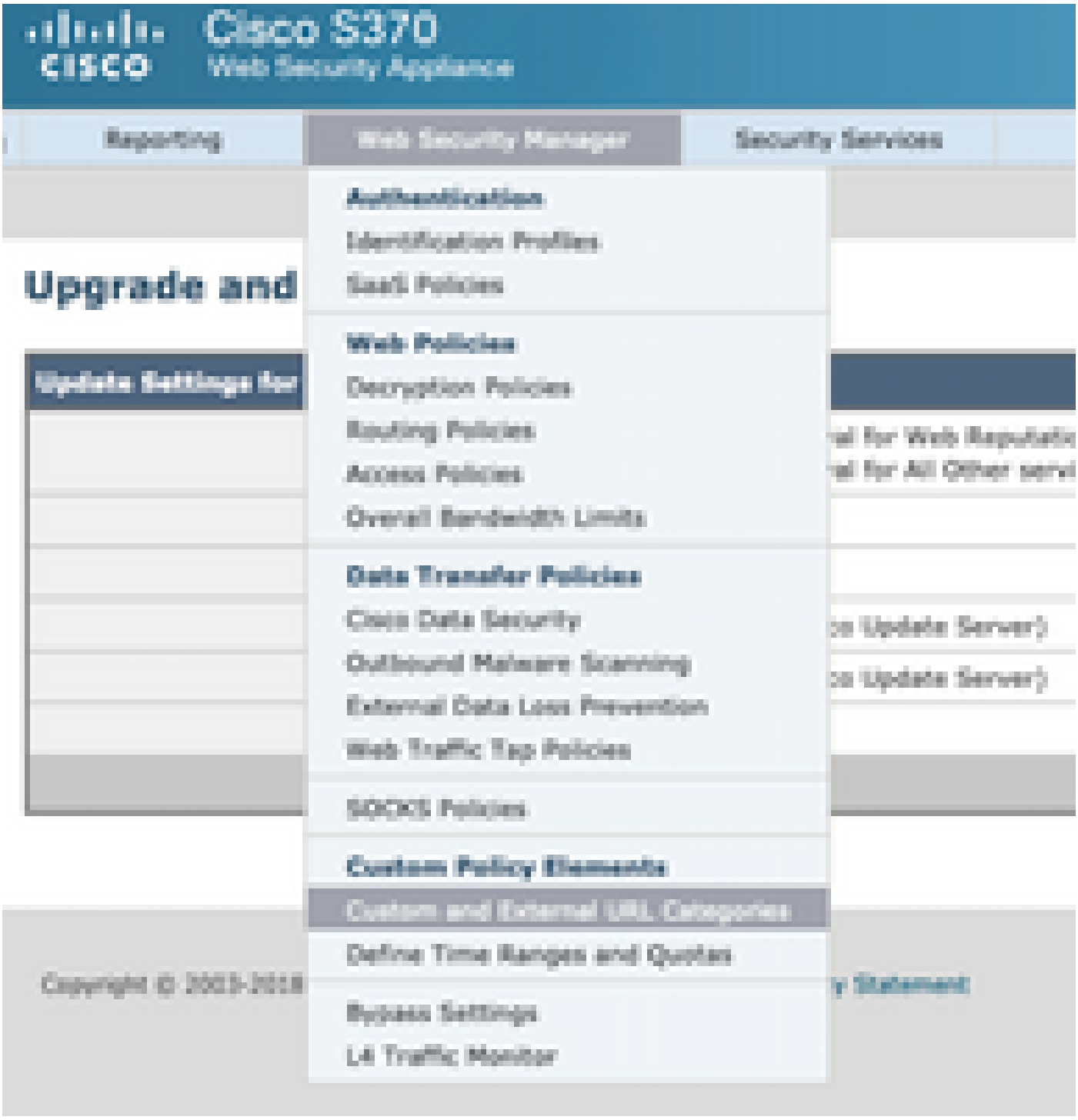
How to whitelist/blacklist a URL?

Sometimes the updates for URLs from Cisco TALOS takes time, either due to lack of enough information. or there's no way to change the reputation as the website still did not prove the change in the malicious behavior. at this point you can add this URL to a custom URL category that is allow/block on your Access policies or passed-through/drop on your Decryption Policy, and that will guarantee the URL gets deliver without scanning or URL filtering check by the Cisco Web Security Appliance (WSA) or block.

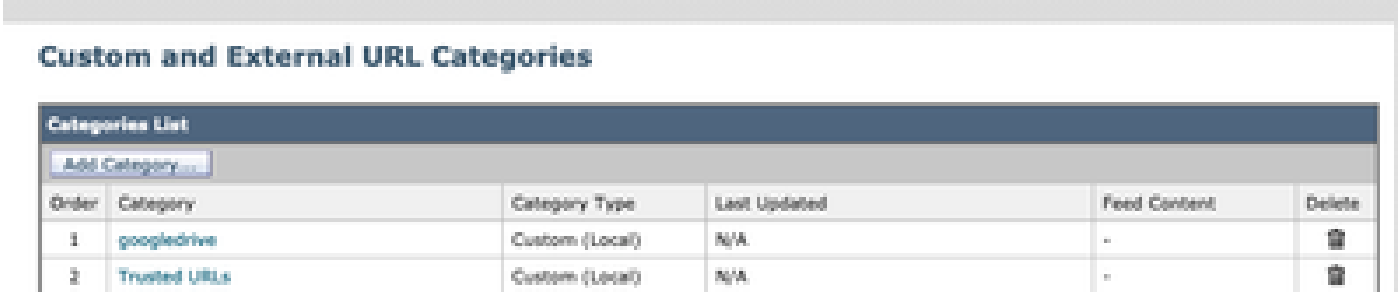
in order to Whitelist/Blacklist a URL please follow the following steps:

1**.** Add URL in custom URL category.

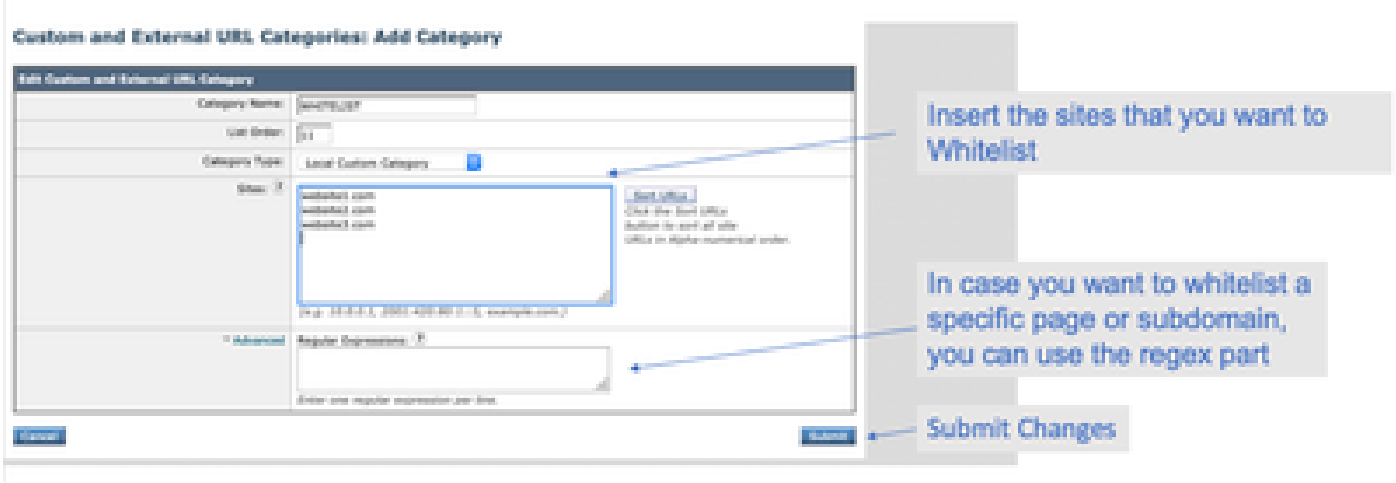
From the GUI go to **Web Security Manager** -> **Custom and External URL Category**.



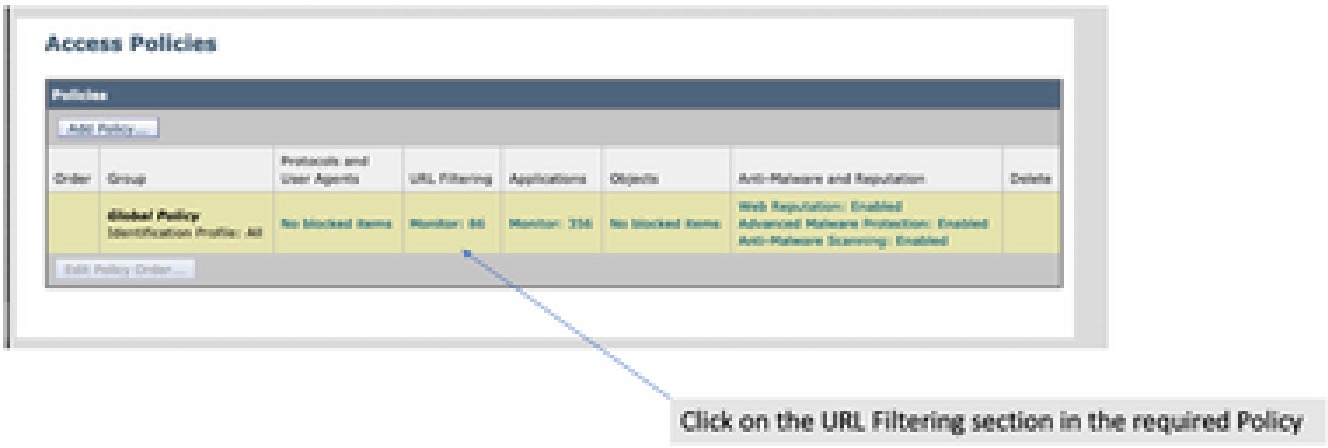
2. Click on **Add Category**:



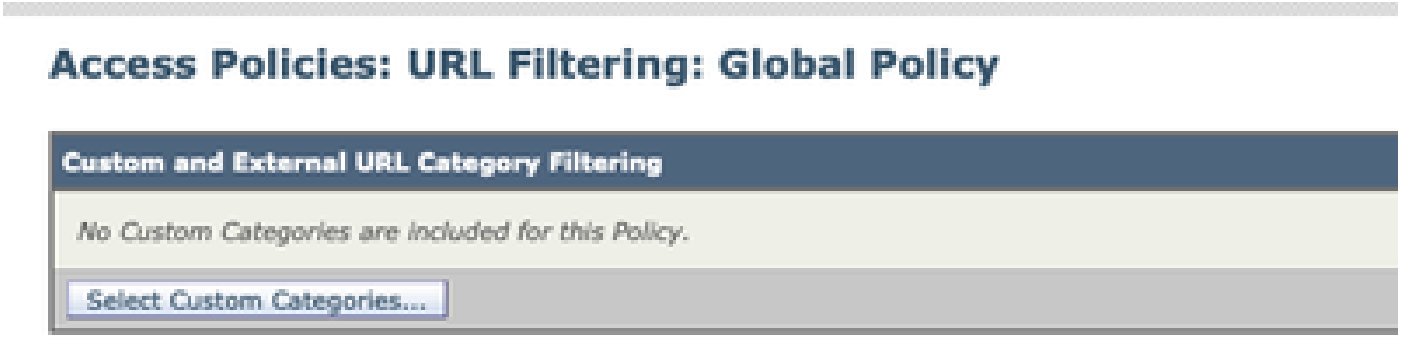
3. Add the websites similar to the screenshots below:



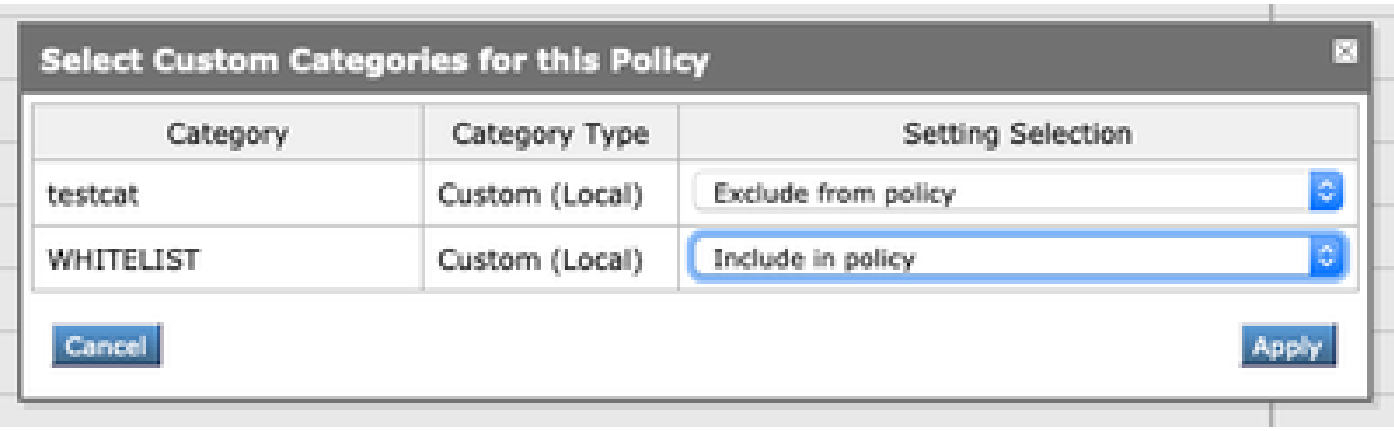
4. Go to the URL filtering in the required Access policy (**Web Security Manager -> Access Policies -> URL Filtering**).



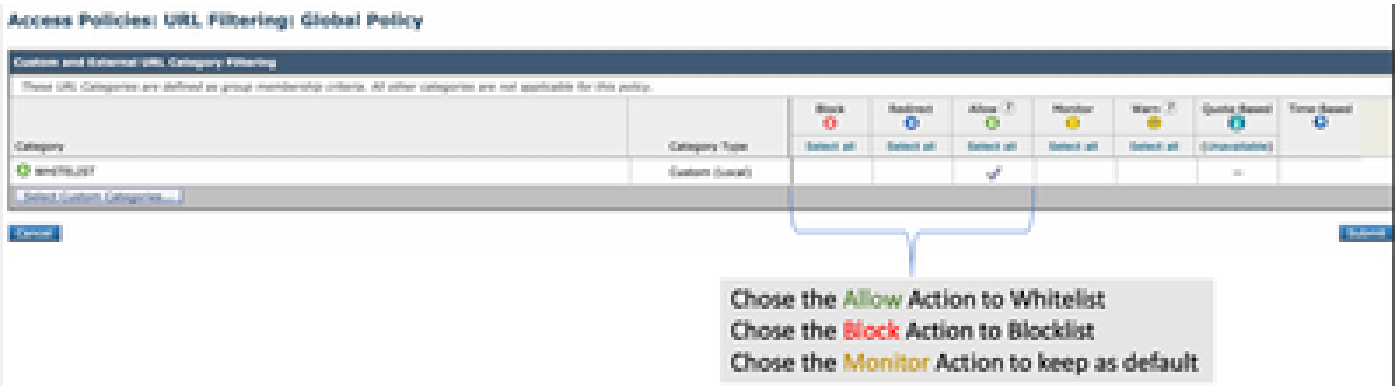
5. Select the **WHITELIST or BLACKLIST** that we just created and include it in the policy.



6. Include the Policy Category in the Policy URL filtering settings as below.



7. Define the action, Block to Blocklist, Allow to Whitelist. and if you wish the URL to go through the scanning engines keep the Action as Monitor.



8. **Submit** and **Commit** Changes.