Web聲譽得分(WBRS)和Web分類引擎常見問題(FAQ)

目錄

Web(WBRS)Web(FAQ)

本文描述有關思科網路安全裝置(WSA)的網路信譽得分(WBRS)和分類功能的最常見問題。

Web聲譽得分意味著什麼？

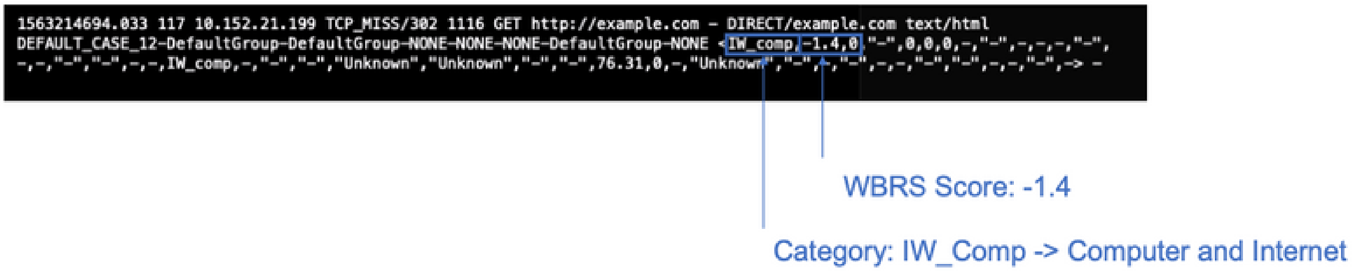
Web聲譽過濾器將基於Web的聲譽分數(WBRS)分配給URL，以確定它包含基於URL的惡意軟體的可能性。網路安全裝置使用Web信譽得分來識別和阻止惡意軟體攻擊。您可以將網路信譽過濾器與訪問、解密和思科資料安全策略配合使用。

Web分類意味著什麼？

Internet網站是根據這些網站的行為和用途進行分類，為了方便代理的管理員，我們已將每個網站URL新增到預定義類別中，該類別可出於安全和報告目的進行標識。不屬於預定義類別的網站稱為未分類網站，可能是因為新網站建立以及缺乏足夠的資料/流量來確定其類別。這種狀況會隨著時間而改變。

如何在訪問日誌中查詢信譽分數？

您通過思科網路安全裝置(WSA)提出的每個請求都應附加基於網路的聲譽得分(WBRS)和URL類別。檢視它的方法之一是通過訪問日誌，示例如下：網路型信譽得分(WBRS)為(-1.4),URL類別為：電腦和網際網路。



```
1563214694.033 117 10.152.21.199 TCP_MISS/302 1116 GET http://example.com - DIRECT/example.com text/html
DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup-NONE <IW_comp,-1.4,0,"-",0,0,0,-,"-",-,-,-,"-",
-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",76.31,0,-,"Unknown","-",-,"-",-,-,"-","-",-,-,"-",-> -
```

WBRS Score: -1.4

Category: IW_Comp -> Computer and Internet

以上螢幕截圖的文本參考。

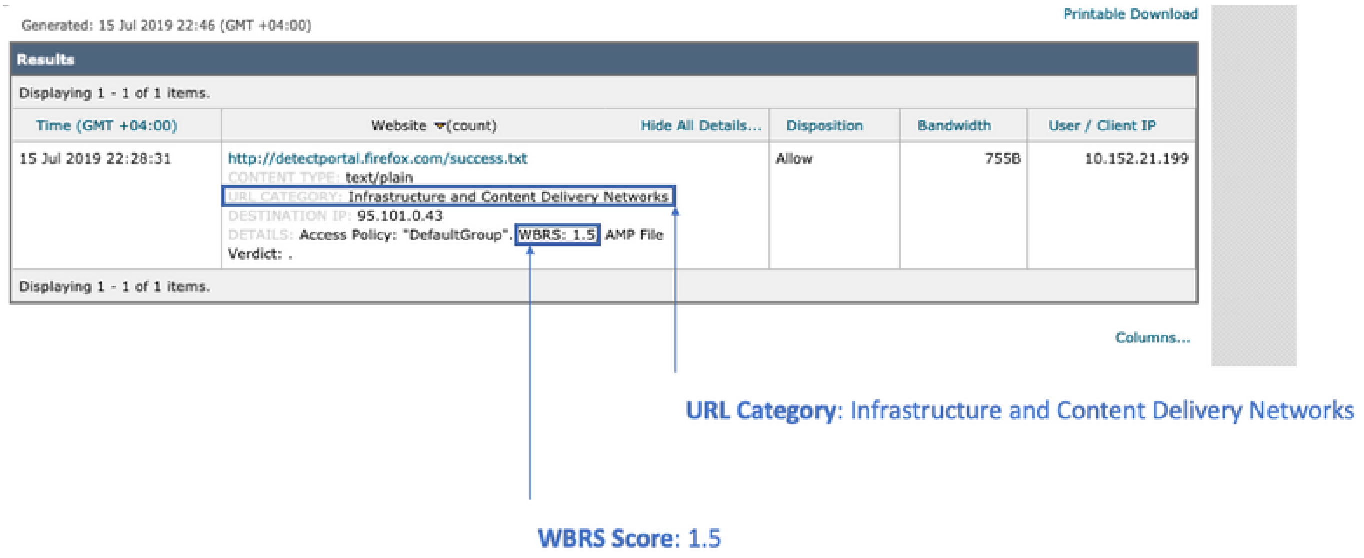
1563214694.033 117 xx.xx.xx.xx TCP_MISS/302 1116 GET https://example.com - DIRECT/example.com text/html DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup-NONE ,0,"-",0,0,0,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",76.31,0,-,"Unknown","-",-,"-",-,-,"-","-",-,-,"-",-> -

附註：

- 可以從命令列介面(CLI)檢視訪問日誌，也可以通過在管理介面IP上使用檔案傳輸協定(FTP)方法連線來下載訪問日誌。（確保在該介面上啟用FTP）。
- 類別縮寫完整清單：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_1208638

如何在我的報表中查詢信譽分數？

1. Cisco Web Security Appliance(WSA)**GUI** -> **Reporting** -> **Web Tracking**
2.
3. **Results**



Generated: 15 Jul 2019 22:46 (GMT +04:00)

Results

Displaying 1 - 1 of 1 items.

Time (GMT +04:00)	Website ▾(count) Hide All Details...	Disposition	Bandwidth	User / Client IP
15 Jul 2019 22:28:31	http://detectportal.firefox.com/success.txt CONTENT TYPE: text/plain URL CATEGORY: Infrastructure and Content Delivery Networks DESTINATION IP: 95.101.0.43 DETAILS: Access Policy: "DefaultGroup". WBRS: 1.5 AMP File Verdict: .	Allow	755B	10.152.21.199

Displaying 1 - 1 of 1 items.

URL Category: Infrastructure and Content Delivery Networks

WBRS Score: 1.5

在哪裡檢查基於Web的信譽得分(WBRS)更新日誌？

Web型信譽得分(WBRS)更新日誌可在updater_logs下找到，您可以通過檔案傳輸協定(FTP)登入管理介面下載這些日誌。或Command Line Interface(CLI)。

要使用終端檢視日誌：

1. 開啟**Terminal**。
2. 鍵入命令**tail**。
3. 選擇**logs number**（具體取決於配置的日誌版本和數量）。
4. 將顯示日誌。

```
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 2019
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 2019
```

如何驗證您是否連線到 網路型信譽評分(WBRS) 是否更新伺服器？

為了確保您的思科網路安全裝置(WSA)能夠獲得新的更新。請驗證您與以下傳輸控制協定(TCP)埠80和443上的思科更新伺服器的連線：

```
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 '^]'.
```

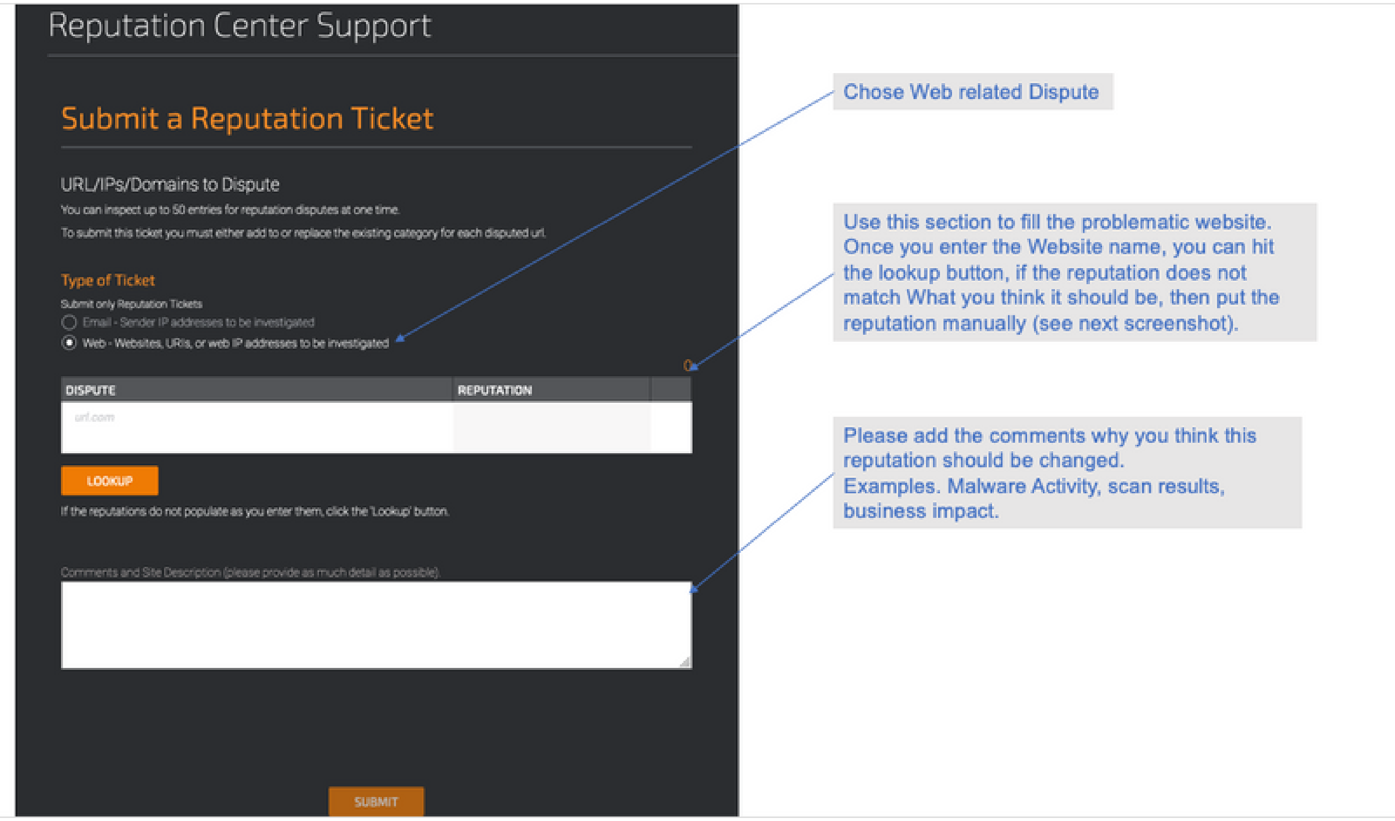
附註：如果您有任何上游代理，請通過上游代理執行上述測試。

如何提交網路分類爭議？

在驗證思科網路安全裝置(WSA)和思科TALOS具有相同的信譽得分後，您仍認為該結果無效，則需要通過與思科TALOS團隊提交爭議來解決此問題。

可以使用以下連結完成此操作：https://talosintelligence.com/reputation_center/support

為了提交**爭議**，請按照以下說明操作。



Reputation Center Support

Submit a Reputation Ticket

URL/IPs/Domains to Dispute

You can inspect up to 50 entries for reputation disputes at one time.

To submit this ticket you must either add to or replace the existing category for each disputed url.

Type of Ticket

Submit only Reputation Tickets

○ Email - Sender IP addresses to be investigated

● Web - Websites, URIs, or web IP addresses to be investigated

0

DISPUTE	REPUTATION	
url.com		

LOOKUP

If the reputations do not populate as you enter them, click the 'Lookup' button.

Comments and Site Description (please provide as much detail as possible).

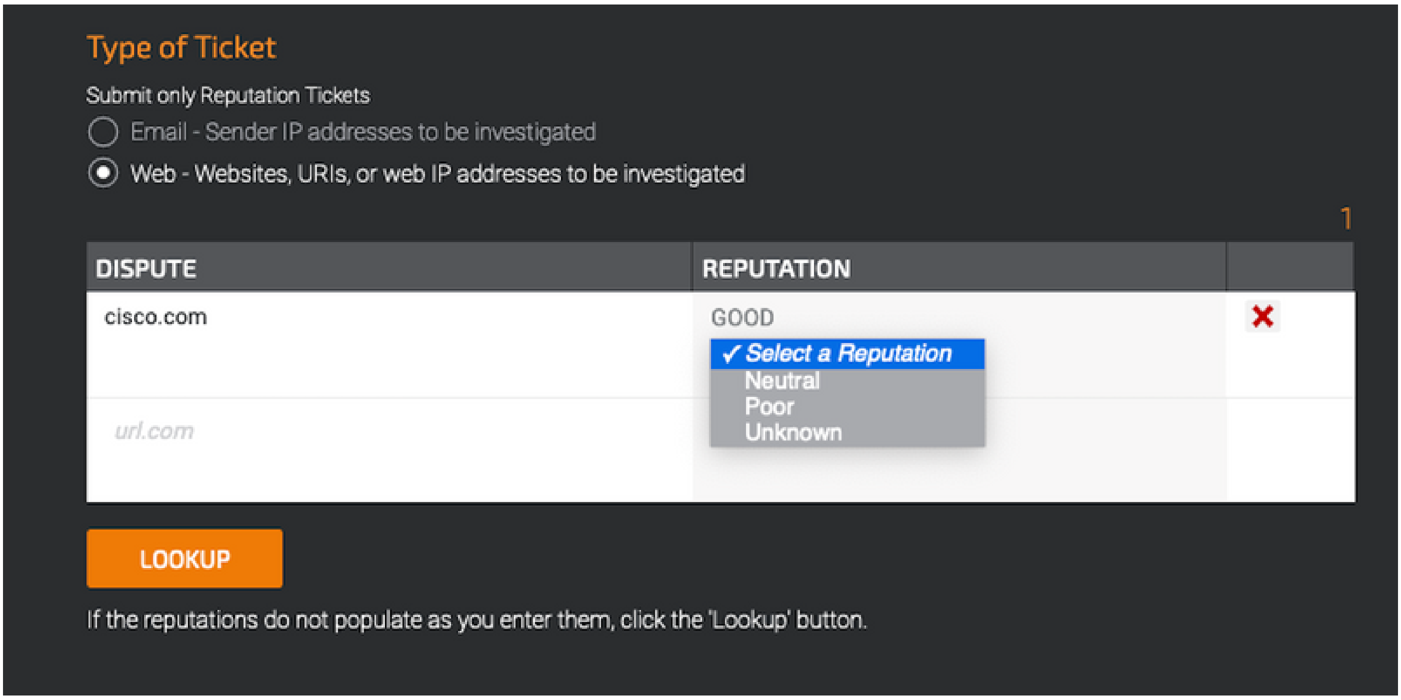
SUBMIT

Chose Web related Dispute

Use this section to fill the problematic website. Once you enter the Website name, you can hit the lookup button, if the reputation does not match What you think it should be, then put the reputation manually (see next screenshot).

Please add the comments why you think this reputation should be changed. Examples. Malware Activity, scan results, business impact.

按下「查詢」按鈕和手動更改得分的選項後的結果。



Type of Ticket

Submit only Reputation Tickets

○ Email - Sender IP addresses to be investigated

● Web - Websites, URIs, or web IP addresses to be investigated

1

DISPUTE	REPUTATION	
cisco.com	GOOD	✕
url.com		

LOOKUP

If the reputations do not populate as you enter them, click the 'Lookup' button.

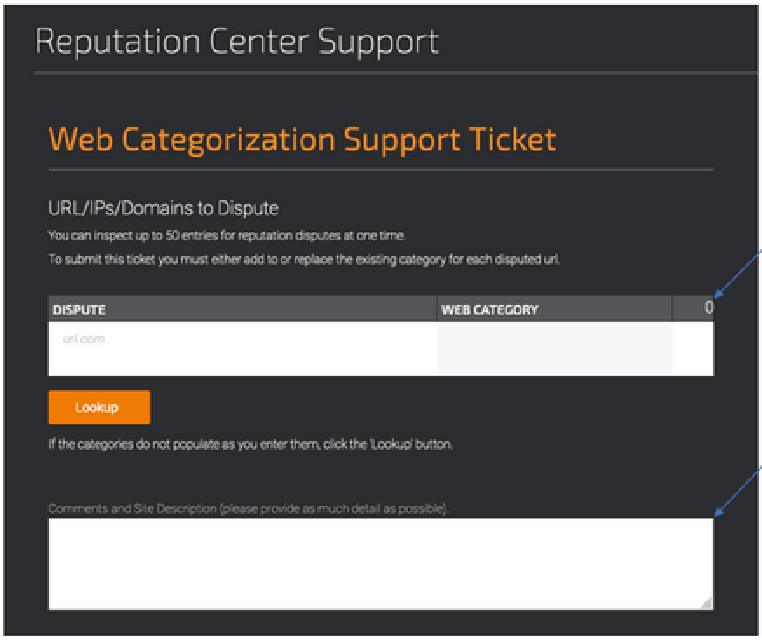
附註：Cisco TALOS提交可能需要一段時間才能反映在資料庫中，如果問題緊急，您可以始終建立**WHITELIST**或**BLOCKLIST**，作為從思科後端修復問題之前的解決方法。為此，您可以檢查此部分（如何列入白名單或黑名單URL）。

如何為Web聲譽得分提交爭議？

在驗證思科網路安全裝置(WSA)和思科TALOS具有相同的分類後，您仍認為這不是有效的結果，則需要通過與思科TALOS團隊提交爭議來解決此問題。

轉到TALOS網站中的分類提交頁面
：https://talosintelligence.com/reputation_center/support#categorization

為了提交**爭議**，請按照以下說明操作。



Reputation Center Support

Web Categorization Support Ticket

URL/IPs/Domains to Dispute

You can inspect up to 50 entries for reputation disputes at one time.

To submit this ticket you must either add to or replace the existing category for each disputed url.

DISPUTE	WEB CATEGORY	0
url.com		

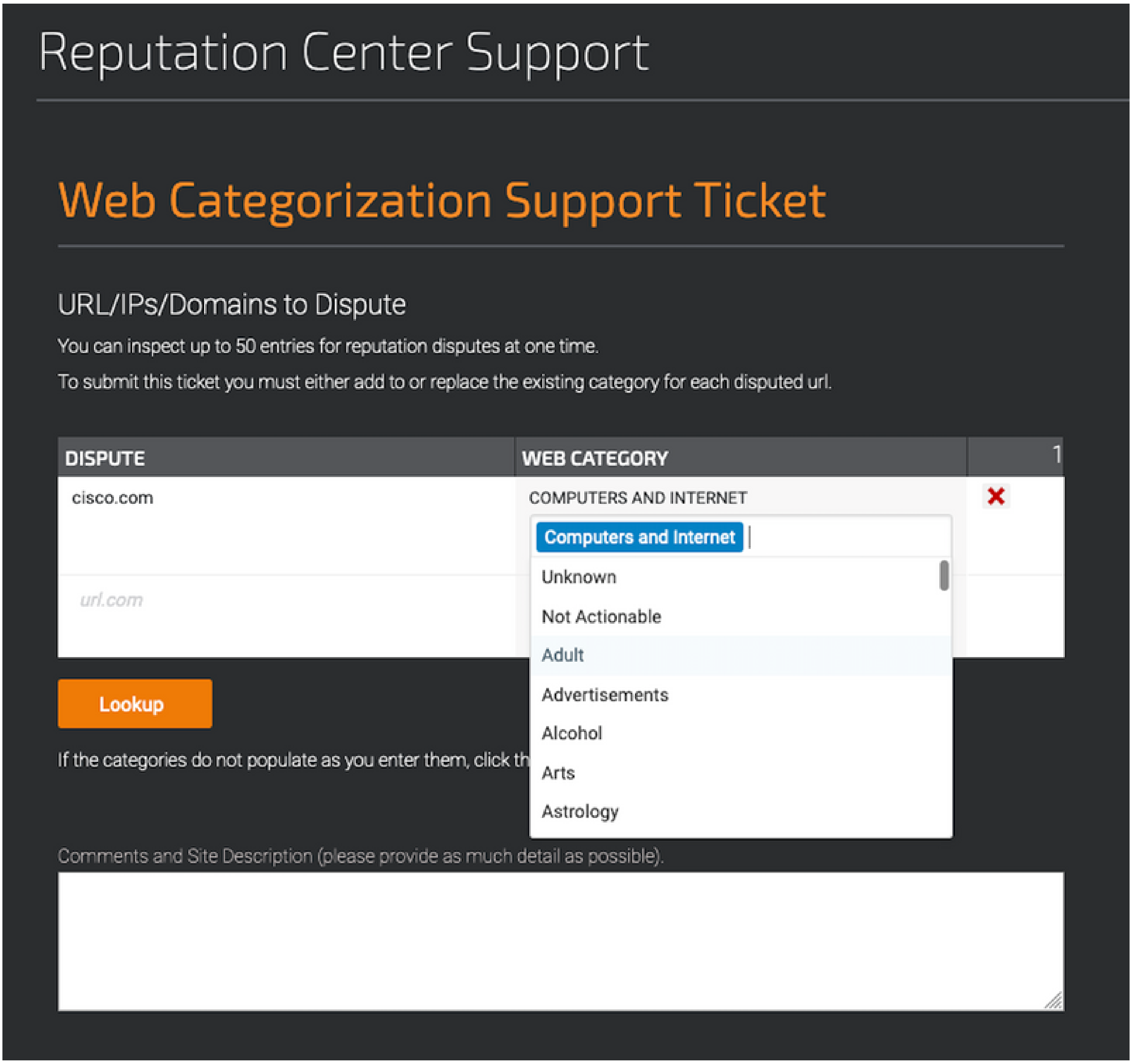
If the categories do not populate as you enter them, click the 'Lookup' button.

Comments and Site Description (please provide as much detail as possible)

Use this section to fill the problematic website. Once you enter the Website name, you can hit the lookup button, if the category does not match What you think it should be, then put the category manually (see next screenshot).

Please add the comments why you think this category should be changed.
Examples. Type of content being delivered.

若要更新類別，請從下拉選單中選擇**您認為更適合網站的內容，並確保您遵循評論准則。**



Reputation Center Support

Web Categorization Support Ticket

URL/IPs/Domains to Dispute

You can inspect up to 50 entries for reputation disputes at one time.

To submit this ticket you must either add to or replace the existing category for each disputed url.

DISPUTE	WEB CATEGORY
cisco.com	COMPUTERS AND INTERNET Computers and Internet
url.com	

If the categories do not populate as you enter them, click th

Comments and Site Description (please provide as much detail as possible).

已提交爭議，但在思科網路安全裝置(WSA)或思科TALOS上未更新分數或類別。

如果您向Cisco TALOS提交案例，且信譽/評分在3到4天內未更新。您可以檢查更新設定並確保可以訪問Cisco更新的伺服器。如果所有這些步驟都正常，則您可以繼續使用Cisco TAC開啟票證，思科工程師將幫助您跟進Cisco TALOS團隊。

> **附註**：您可以應用WHITELIST/BLOCKLIST解決方法應用所需的操作，直到類別/信譽從Cisco TALOS團隊獲得更新。

思科網路安全裝置(WSA) 顯示與Cisco TALOS不同的結果，如何修復此問題？

由於多種原因（主要是與我們的更新伺服器通訊），思科網路安全裝置(WSA)上的資料庫可能過期

，請按照以下步驟驗證您是否具有正確的更新伺服器和連線。

1.驗證埠80和443上思科更新的伺服器是否連通：

```
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.如果您有任何上游代理，請確保上游代理確保您通過上游代理執行上述測試。

3.如果連線正常，但您仍然看到差異，則手動強制更新：**從**CLI或GUI更新**->安全服務 — >惡意軟體防護 — >更新。**

請等待幾分鐘，如果此操作無效，請檢查下一步。

4.此時，您需要檢查updater_logs:open **terminal:CLI->tail->(選擇updater_logs日誌檔案的數**量。)這將使更新日誌僅顯示新行。

日誌行應以「Received remote command **to signal a manual update」行開頭：**

```
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.ironport.com/wbrs/3.0.0/ip/default/1563201291.inc"
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/default/1563201291.inc"
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.檢查是否有任何「**嚴重/警告**」消息，更新日誌是非常容易讀取的錯誤，並且極有可能引導您找出問題的原因。

6.如果沒有答案，則您可以利用上述步驟的結果，在思科的支援下開啟一張票證，他們樂意提供幫助。

如何計算Web聲譽分數？

為特定網站分配得分時考慮的一些引數：

- URL分類資料
- 存在可下載代碼

- 存在長期、模糊的終端使用者許可協定(EULA)
- 全域性卷和卷更改
- 網路所有者資訊
- URL歷史記錄
- URL的期限
- 出現在任何阻止清單中
- 任何允許清單中的存在
- 常用域的URL錯誤
- 域註冊器資訊
- IP地址資訊

每個信譽類別（良好、中性、差）的分數範圍是多少？

Web聲譽範圍及其相關操作：

訪問策略：

-10–6.0			• URL • • URL • URL.
-5.95.9		DVS DVS	• URL • 動態IP地址並包含 • 可下載內容。 • IP • 正面Web信譽得分。
6.0 - 10.0			• URL • • • URL

解密策略：

-10–9.0	drop	
-8.95.9		
6.0 - 10.0		

思科資料安全策略：

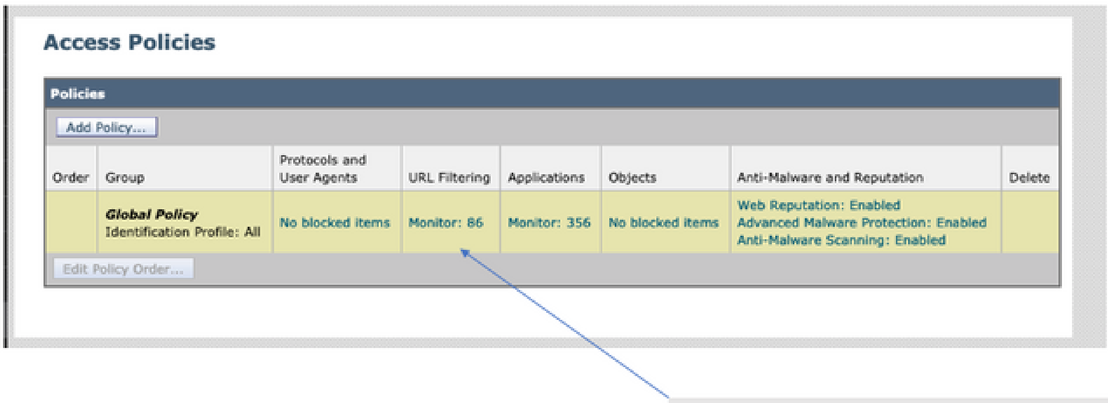
-10–6.0		
-5.90.0		Web

未分類網站意味著什麼？

未分類的URL是Cisco資料庫沒有足夠資訊來確認其類別的。通常是新建立的網站。

如何阻止未分類的URL?

1.轉到所需的訪問策略：**網路安全管理器 — >訪問策略。**



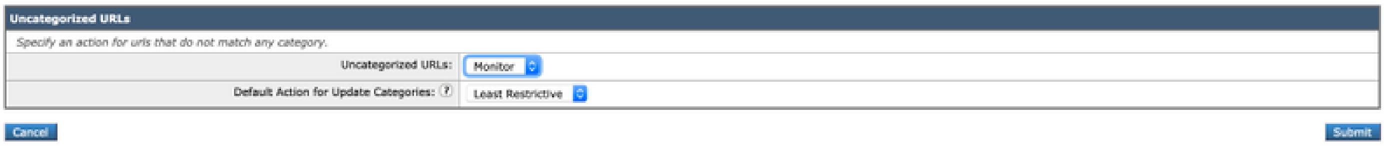
Access Policies

Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
	Global Policy Identification Profile: All	No blocked items	Monitor: 86	Monitor: 356	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	

Click on the URL Filtering section in the required Policy

2.向下滾動至「未分類的URL」部分。



Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs: Monitor

Default Action for Update Categories: Least Restrictive

3.選擇所需操作之一，即**Monitor**、**Block**或**Warn**。

4. **Submit**和**Commit**更改。

資料庫更新的頻率如何？

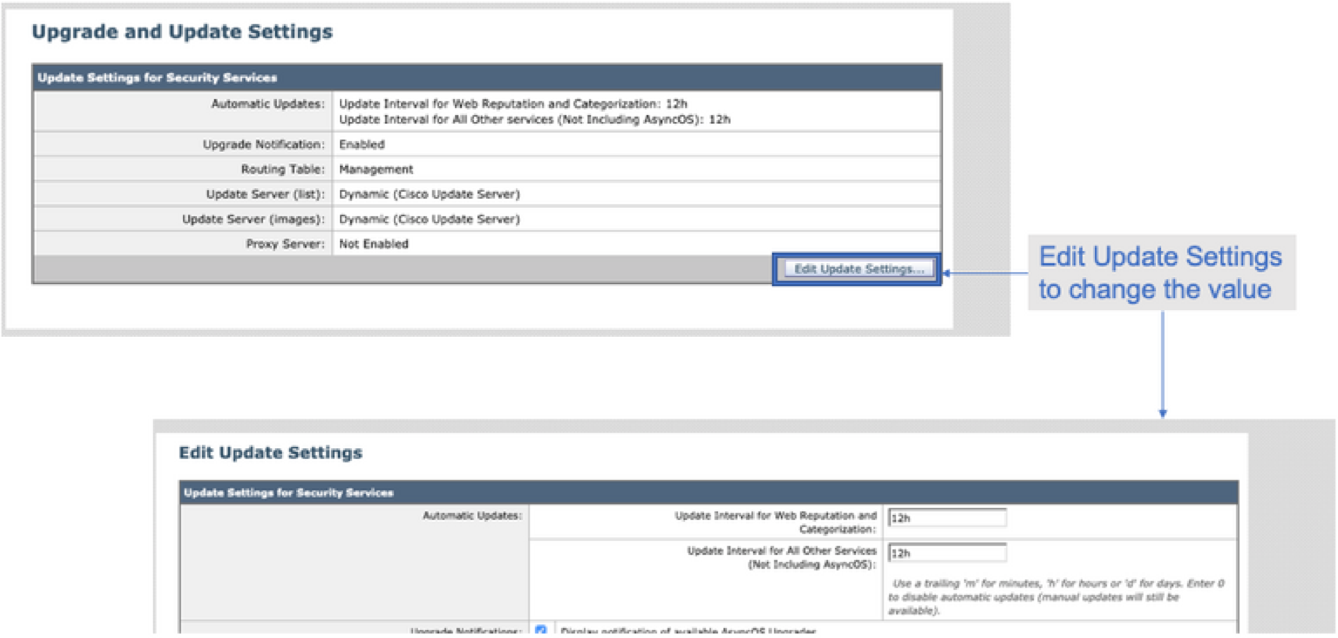
可以在CLI中使用以下命令更新檢查頻率：**updateconfig**

```
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
[]>
```

> **附註**：上面的值顯示我們檢查更新的頻率，但不顯示我們發佈信譽和其他服務的新更新的頻率。可在任何時間點獲得更新。

或在GUI上：**系統管理 — >升級和更新設定。**



Upgrade and Update Settings

Update Settings for Security Services	
Automatic Updates:	Update Interval for Web Reputation and Categorization: 12h Update Interval for All Other services (Not Including AsyncOS): 12h
Upgrade Notification:	Enabled
Routing Table:	Management
Update Server (list):	Dynamic (Cisco Update Server)
Update Server (images):	Dynamic (Cisco Update Server)
Proxy Server:	Not Enabled

Edit Update Settings to change the value

Edit Update Settings

Update Settings for Security Services		
Automatic Updates:	Update Interval for Web Reputation and Categorization:	12h
	Update Interval for All Other Services (Not Including AsyncOS):	12h *Use a trailing 'm' for minutes, 'h' for hours or 'd' for days. Enter 0 to disable automatic updates (manual updates will still be available).*
Upgrade Notifications:	☑ Display notification of available AsyncOS Upgrades	

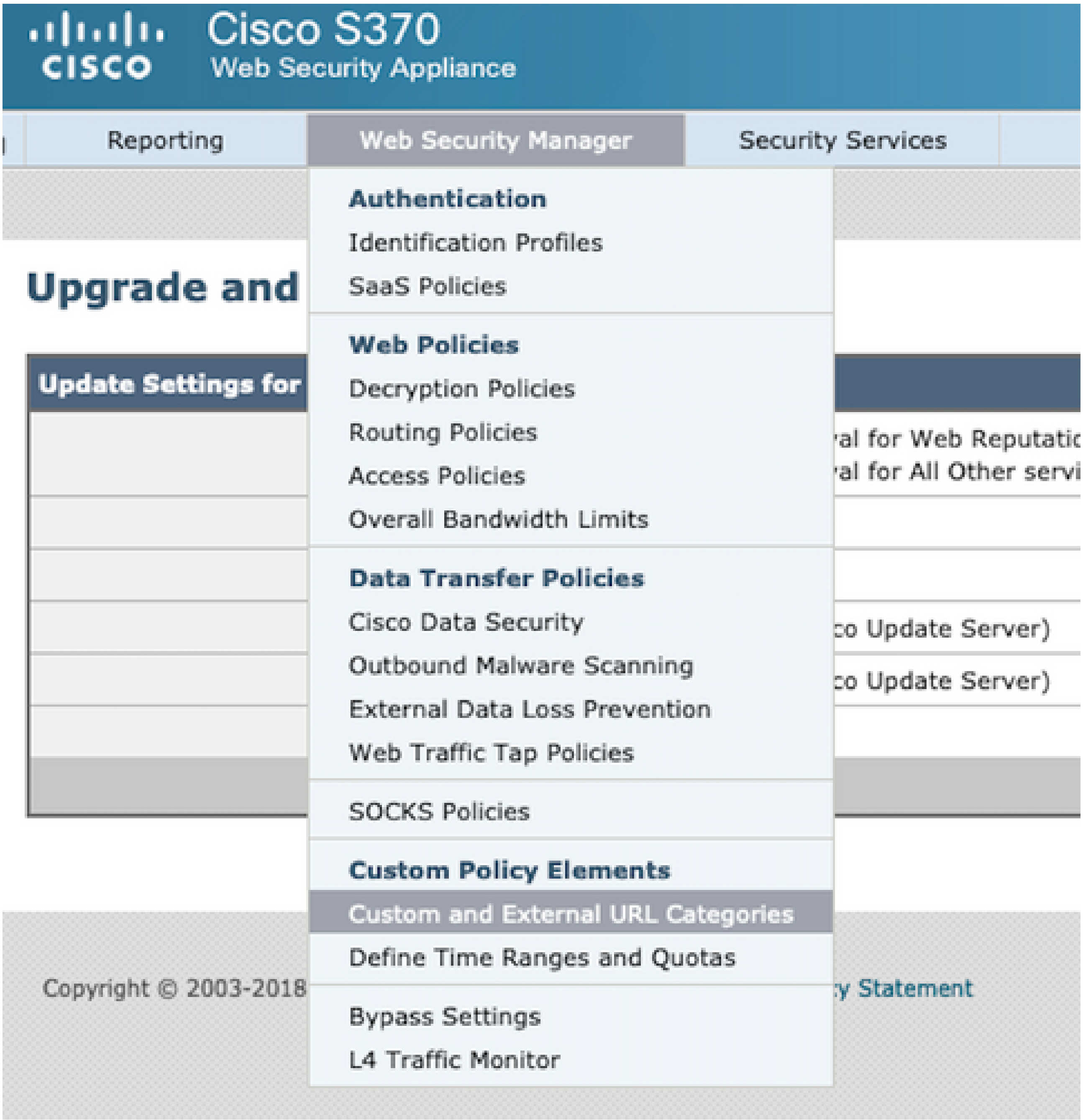
如何將URL列入白名單/黑名單？

有時，由於缺少足夠的資訊，Cisco TALOS的URL更新需要時間。或者無法改變聲譽因為網站仍然無法證明惡意行為的改變。此時，您可以將此URL新增到自定義URL類別，該類別在您的訪問策略上允許/阻止或在解密策略上傳遞/丟棄，並且可保證URL在未經思科網路安全裝置(WSA)或阻止掃描或URL過濾檢查的情況下被傳送。

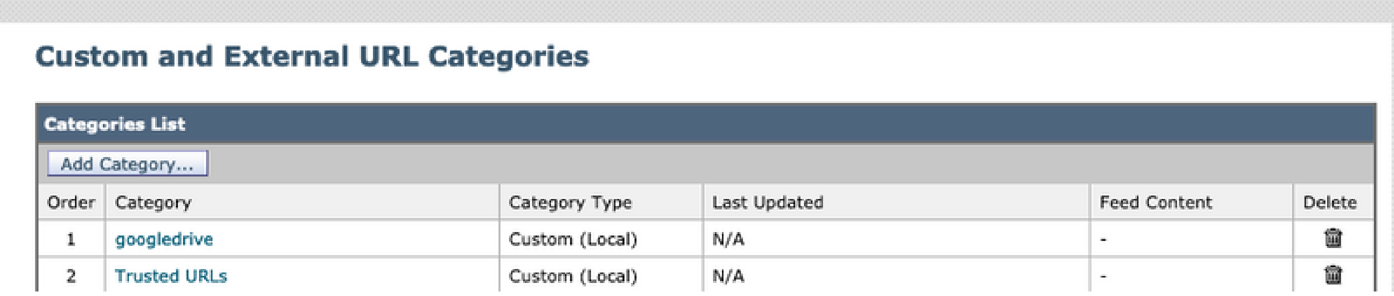
要將URL列入白名單/黑名單，請執行以下步驟：

1. 在自定義URL類別中新增URL。

在GUI中，前往**Web Security Manager** -> **Custom and External URL Category**。



2.**Add Category**:



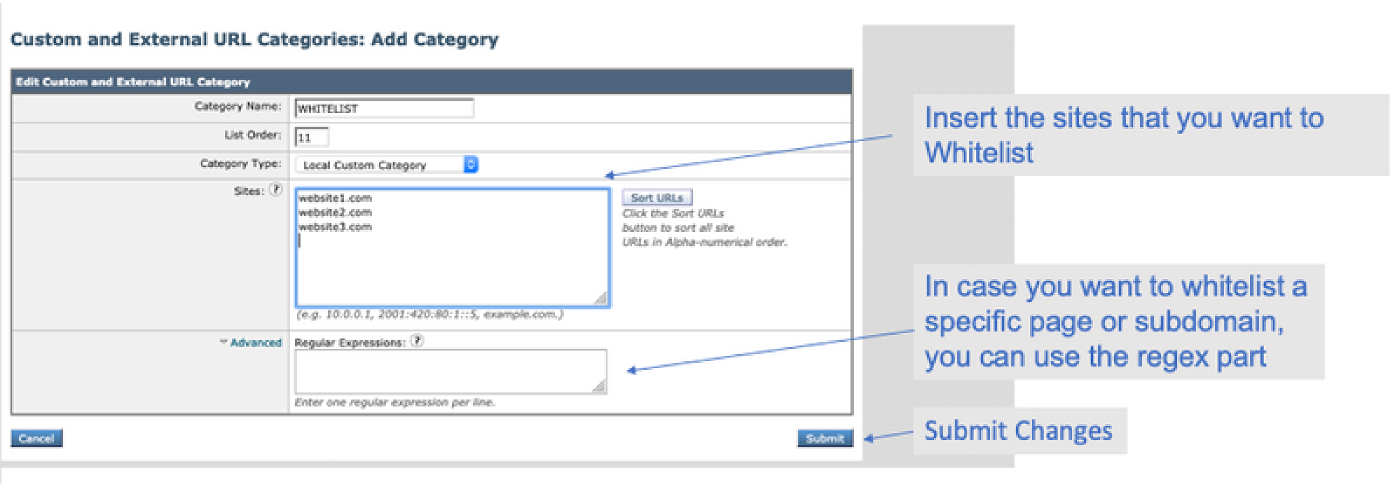
Custom and External URL Categories

Categories List

Add Category...

Order	Category	Category Type	Last Updated	Feed Content	Delete
1	googledrive	Custom (Local)	N/A	-	🗑
2	Trusted URLs	Custom (Local)	N/A	-	🗑

3.



Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name: WHITELIST

List Order: 11

Category Type: Local Custom Category

Sites: website1.com
website2.com
website3.com

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

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

Regular Expressions:

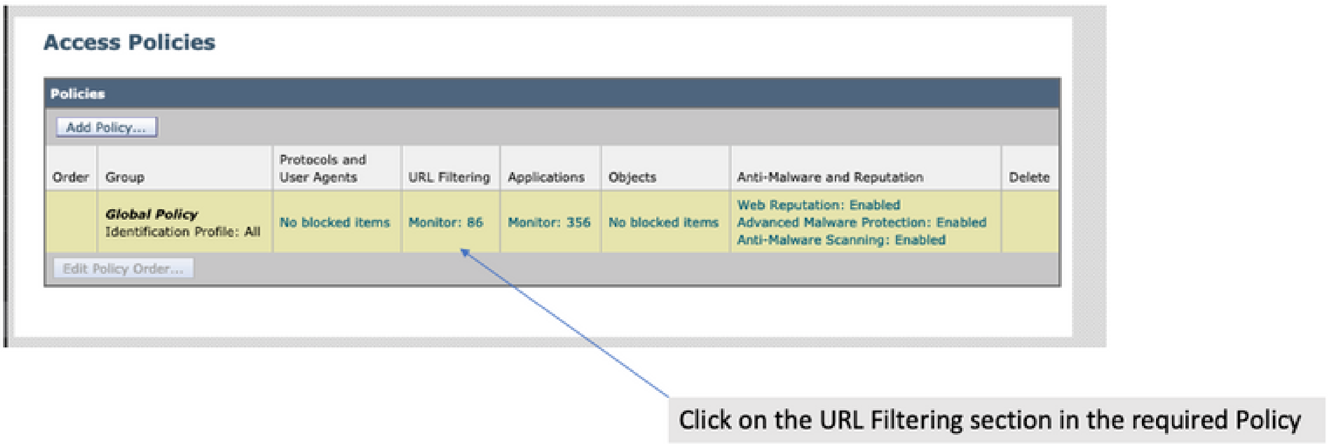
Enter one regular expression per line.

Insert the sites that you want to Whitelist

In case you want to whitelist a specific page or subdomain, you can use the regex part

Submit Changes

4.URL(**— > — > URL**)



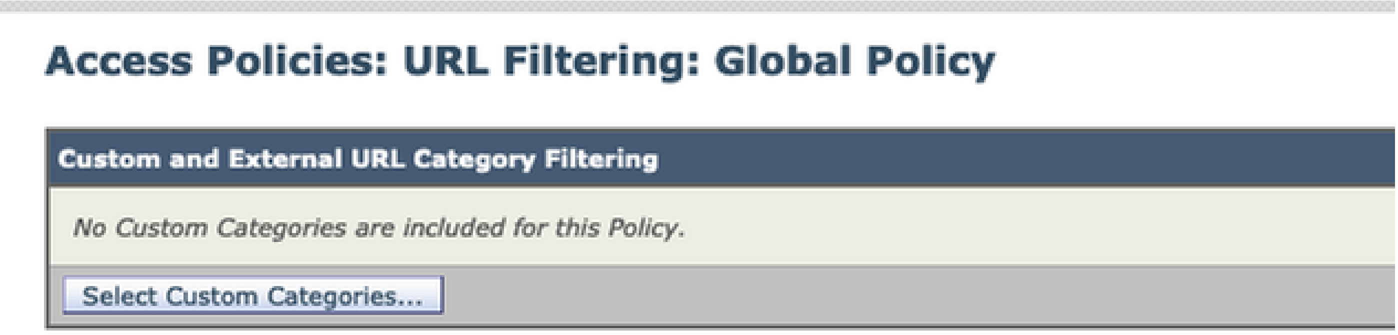
Access Policies

Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
	Global Policy Identification Profile: All	No blocked items	Monitor: 86	Monitor: 356	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	

Click on the URL Filtering section in the required Policy

5.

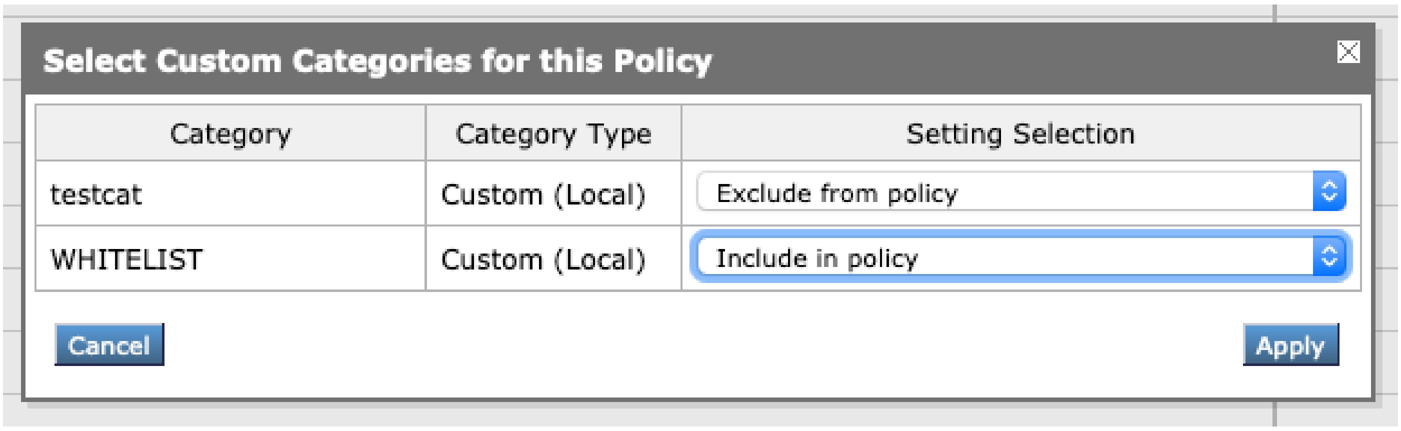


Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

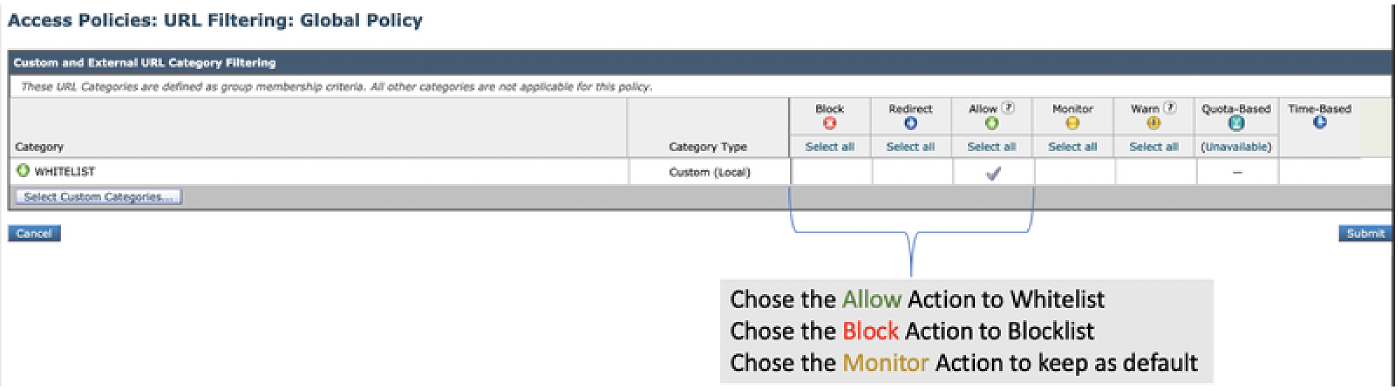
6.在策略URL過濾設定中包括策略類別，如下所示。



Select Custom Categories for this Policy

Category	Category Type	Setting Selection
testcat	Custom (Local)	Exclude from policy
WHITELIST	Custom (Local)	Include in policy

7.定義操作「阻止到阻止清單」、「允許到白名單」。如果您希望URL通過掃描引擎，請將「操作」保留為「監控」。



Access Policies: URL Filtering: Global Policy

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	Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	
WHITELIST	Custom (Local)			✓			–	

Chose the Allow Action to Whitelist
Chose the Block Action to Blocklist
Chose the Monitor Action to keep as default

8. Submit和Commit更改。