

Foire aux questions sur le Web Reputation Score (WBRS) et le moteur de catégorisation Web (FAQ)

Table des matières

[Foire aux questions \(FAQ\) du Web Reputation Score \(WBRS\) et du Web Categorization Engine.](#)

[Que signifie le score de réputation Web ?](#)

[Que signifie la catégorisation Web ?](#)

[Comment trouver le score de réputation dans les journaux d'accès ?](#)

[Comment trouver le score de réputation dans mes rapports ?](#)

[Où vérifiez-vous les journaux de mise à jour du score de réputation Web \(WBRS\) ?](#)

[Comment vérifier si vous êtes connecté aux serveurs de mises à jour WBRS \(Web-Based Reputation Score\) ?](#)

[Comment déposer un litige pour la catégorisation Web ?](#)

[Comment introduire un litige pour le score de réputation Web ?](#)

[Un litige a été signalé, mais le score ou la catégorie n'est pas mis à jour sur Cisco Web Security Appliance \(WSA\) ou Cisco TALOS.](#)

[Cisco Web Security Appliance \(WSA\) affichant des résultats différents de Cisco TALOS, comment résoudre ce problème ?](#)

[Comment les scores de réputation Web sont-ils calculés ?](#)

[Quelle est la plage de scores pour chacune des catégories de réputation \(bonne, neutre, mauvaise\) ?](#)

[Plages de réputation Web et actions associées :](#)

[Politiques d'accès :](#)

[Politiques de décodage :](#)

[Politiques de sécurité des données Cisco :](#)

[Que signifie un site Web non classé ?](#)

[Comment bloquer les URL non classées ?](#)

[Fréquence de mise à jour de la base de données](#)

[Comment mettre une URL sur liste blanche/noire ?](#)

Foire aux questions (FAQ) du Web Reputation Score (WBRS) et du Web Categorization Engine.

Cet article décrit les questions les plus fréquemment posées sur la fonctionnalité de classement et de score de réputation Web (WBRS) avec l'appareil de sécurité Web Cisco (WSA).

Que signifie le score de réputation Web ?

Les filtres de réputation Web attribuent un score de réputation Web (WBRS) à une URL pour



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#

Comment trouver le score de réputation dans mes rapports ?

1. Accédez à **GUI -> Reporting -> Web Security Appliance (WSA) -> Web Tracking** de Cisco.
2. Recherchez le **domaine** que vous recherchez.
3. Dans la page **Résultats**, cliquez sur le lien nécessaire, et plus de détails apparaîtront comme ci-dessous.

Generated: 15 Jul 2019 23:46 (GMT +04:00) [Printable Overview](#)

Results

Displaying 1 - 1 of 1 items.

Time (GMT +04:00)	Website IP (count)	Hide All Details...	Disposition	Bandwidth	User / Client IP
15 Jul 2019 23:28:01	http://Webchatportal.brofax.com/success.txt <small>Content-Type: text/plain</small> Infrastructure and Content Delivery Networks		Allow	7958	10.152.21.199

Displaying 1 - 1 of 1 items.

[Columns...](#)

URL Category: Infrastructure and Content Delivery Networks

WBR Score: 1.5

Où vérifiez-vous les journaux de mise à jour du score de réputation Web (WBR) ?

Les journaux de mise à jour du score de réputation Web (WBR) sont disponibles sous `updater_logs`. Vous pouvez télécharger ces journaux via une connexion FTP à l'interface de gestion ou via l'interface de ligne de commande.

Pour afficher les journaux à l'aide du terminal :

1. Ouvrez Terminal.
2. Tapez la commande `tail`.
3. Choisissez le numéro des journaux (il varie en fonction de la version et du nombre de journaux configurés).
4. Les journaux s'affichent.

```
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 health 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
```

Comment vérifier si vous êtes connecté aux serveurs de mise à jour WBRs (Web-Based Reputation Score) ?

Afin de vous assurer que votre appareil de sécurité Web Cisco (WSA) est en mesure d'obtenir les nouvelles mises à jour. Veuillez vérifier que vous disposez de la connectivité aux serveurs de mise à jour Cisco sur les ports TCP (Transmission Control Protocol) 80 et 443 suivants :

```
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 '^['.
```

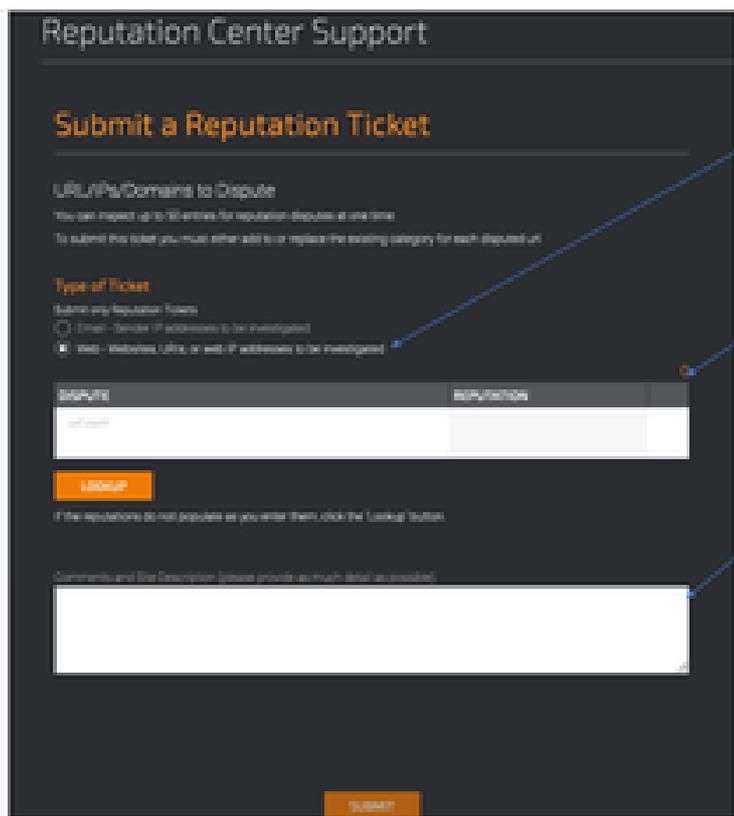
 Remarque : si vous avez un proxy en amont, effectuez les tests ci-dessus via votre proxy en amont.

Comment déposer un litige pour la catégorisation Web ?

Après avoir vérifié que Cisco Web Security Appliance (WSA) et Cisco TALOS ont le même score de réputation, mais que vous pensez toujours que ce résultat n'est pas valide, vous devez résoudre le problème en envoyant un litige à l'équipe Cisco TALOS.

Pour ce faire, cliquez sur le lien suivant : https://talosintelligence.com/reputation_center/support

Afin de soumettre le Litige, veuillez suivre les instructions ci-dessous.



The screenshot shows the 'Submit a Reputation Ticket' form on the Reputation Center Support page. The form includes a title, a section for 'URLs/IDs/Domains to Dispute', a 'Type of Ticket' section with radio buttons for 'Email' and 'Web', a table for 'URLs/IDs' and 'Reputation', a 'Lookup' button, a 'Comments and Site Description' text area, and a 'Submit' button. Annotations with arrows point to the 'Web' radio button, the 'Lookup' button, and the 'Comments and Site Description' text area.

Submit a Reputation Ticket

URLs/IDs/Domains to Dispute
You can input 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 any Reputation Types

Email - Domain IP addresses to be investigated

Web - Malicious URLs or web IP addresses to be investigated

URLs/IDs	Reputation
url.com	

Lookup

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

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

Submit

Choose 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.

Résultats après avoir cliqué sur Recherche et l'option permettant de modifier manuellement le score.

Type of Ticket

Submit only Reputation Tickets

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

DISPUTE	REPUTATION	
cisco.com	GOOD	X
	<input checked="" type="checkbox"/> Select a Reputation	
	<input type="checkbox"/> Neutral	
	<input type="checkbox"/> Poor	
	<input type="checkbox"/> Unknown	
url.com		

LOOKUP

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

 Remarque : les soumissions Cisco TALOS peuvent prendre un certain temps pour être reflétées dans la base de données. Si le problème est urgent, vous pouvez toujours créer une WHITELIST ou une BLOCKLIST, comme solution de contournement jusqu'à ce que le problème soit résolu à partir du serveur principal Cisco. pour ce faire, vous pouvez consulter cette section ([Comment faire une liste blanche ou une URL de liste noire](#)).

Comment introduire un litige pour le score de réputation Web ?

Après avoir vérifié que Cisco Web Security Appliance (WSA) et Cisco TALOS ont la même catégorisation, mais que vous pensez toujours que ce résultat n'est pas valide, vous devez résoudre ce problème en envoyant un litige à l'équipe Cisco TALOS.

Accédez à la page de soumission de la catégorisation sur le site Web de TALOS :
https://talosintelligence.com/reputation_center/support#categorization

Afin de soumettre le Litige, veuillez suivre les instructions ci-dessous.

Reputation Center Support

Web Categorization Support Ticket

URLs/Domain to Dispute
You can report 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	
<input type="text" value="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.

Pour mettre à jour la catégorie, choisissez dans le menu déroulant ce qui vous semble le mieux convenir au site Web, et assurez-vous de suivre les instructions relatives aux commentaires.

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	X
url.com		

Lookup

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).

Un litige a été signalé, mais le score ou la catégorie n'est pas mis à jour sur Cisco Web Security Appliance (WSA) ou Cisco TALOS.

Si vous avez déposé un dossier auprès de Cisco TALOS et que la réputation/le score n'a pas été mis à jour dans les 3 à 4 jours. vous pouvez vérifier vos paramètres de mise à jour et vous assurer que vous avez accès au serveur de mise à jour Cisco. Si toutes ces étapes sont correctes, vous pouvez ouvrir un ticket auprès du TAC Cisco et l'ingénieur Cisco vous aidera à assurer le suivi auprès de l'équipe Cisco TALOS.

 Remarque : vous pouvez appliquer la solution de contournement WHITELIST/BLOCKLIST pour appliquer l'action requise jusqu'à ce que la catégorie/réputation soit mise à jour par l'équipe Cisco TALOS.

5. Recherchez les messages "Critique/Avertissement", les journaux de mise à jour sont des erreurs très lisibles par l'homme, et vous guideront très probablement là où se trouve le problème.

6. En l'absence de réponse, vous pouvez ouvrir un ticket auprès de l'assistance Cisco et obtenir les résultats des étapes ci-dessus. L'assistance se fera un plaisir de vous aider.

Comment les scores de réputation Web sont-ils calculés ?

Certains des paramètres pris en compte lors de l'attribution d'un score à un site Web spécifique :

- Données de catégorisation URL
- Présence de code téléchargeable
- Présence de contrats de licence d'utilisateur final (CLUF) longs et obscurs
- Volume global et changements de volume
- Informations relatives au propriétaire du réseau
- Historique d'une URL
- Âge d'une URL
- Présence sur les listes de blocage
- Présence sur les listes d'autorisation
- Types d'URL des domaines populaires
- Informations du registraire de domaine
- Informations d'adresse IP

Quelle est la plage de scores pour chacune des catégories de réputation (bonne, neutre, mauvaise) ?

Plages de réputation Web et actions associées :

Politiques d'accès :

Score	Action	Description	Exemple
-10 à -6.0 (Faible)	Block	Mauvais site. La demande est bloquée, et aucune analyse supplémentaire des programmes malveillants se produit.	<ul style="list-style-type: none">• L'URL télécharge les informations sans autorisation utilisateur.• Pic soudain du volume d'URL.• L'URL est une faute de frappe sur un domaine populaire.
-5.9 à 5.9 (Neutre)	Analyser	Site indéterminé. La demande est transmise au moteur DVS pour analyse approfondie des programmes malveillants. Le moteur DVS analyse la requête	<ul style="list-style-type: none">• URL créée récemment et dotée d'une adresse IP dynamique et contient• contenu téléchargeable.• Adresse IP du propriétaire du réseau qui a

		et le contenu des réponses du serveur.	<p>un</p> <ul style="list-style-type: none"> • Score de réputation Web positif.
6.0 à 10.0 (Bon)	Allow	Bon site. La demande est autorisée. Aucune analyse des programmes malveillants requise.	<ul style="list-style-type: none"> • L'URL ne contient aucun contenu téléchargeable. • Domaine réputé, à volume élevé et à long historique. • Domaine présent sur plusieurs listes d'autorisation. • Aucun lien vers des URL de mauvaise réputation.

Politiques de décodage :

Score	Action	Description
-10 à -9.0 (Faible)	Goutte	Mauvais site. La demande est abandonnée sans notification envoyée à l'utilisateur final. Utilisation ce paramètre avec prudence.
-8.9 à 5.9 (Neutre)	Déchiffrer	Site indéterminé. La requête est autorisée, mais la connexion est déchiffrée et les politiques d'accès sont appliquées au trafic déchiffré.
6.0 à 10.0 (Bon)	Passthrough	Bon site. La demande est transmise sans inspection ni déchiffrement.

Politiques de sécurité des données Cisco :

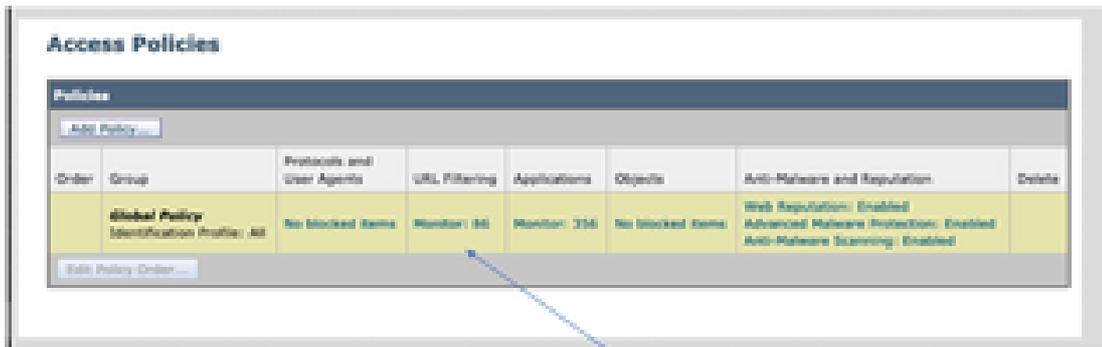
Score	Action	Description
-10 à -6.0 (Faible)	Block	Mauvais site. La transaction est bloquée et aucune analyse supplémentaire n'est effectuée.
-5.9 à 0.0 (Neutre)	Monitor	La transaction ne sera pas bloquée en fonction de la réputation Web et passera à la vérification du contenu (type et taille de fichier). Remarque Les sites sans score sont surveillés.

Que signifie un site Web non classé ?

Les URL non classées sont celles sur lesquelles la base de données Cisco ne dispose pas d'informations suffisantes pour confirmer leur catégorie. Il s'agit généralement de sites Web nouvellement créés.

Comment bloquer les URL non classées ?

1. Accédez à la stratégie d'accès souhaitée : Gestionnaire de sécurité Web -> Stratégies d'accès.



Click on the URL Filtering section in the required Policy

2. Faites défiler la page jusqu'à la section Uncategory URLs.



3. Choisissez l'une des actions souhaitées : Surveillance, Bloquer ou Avertir.

4. Soumettre et valider les modifications.

Fréquence de mise à jour de la base de données

La fréquence de vérification des mises à jour peut être mise à jour à l'aide de la commande suivante de 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

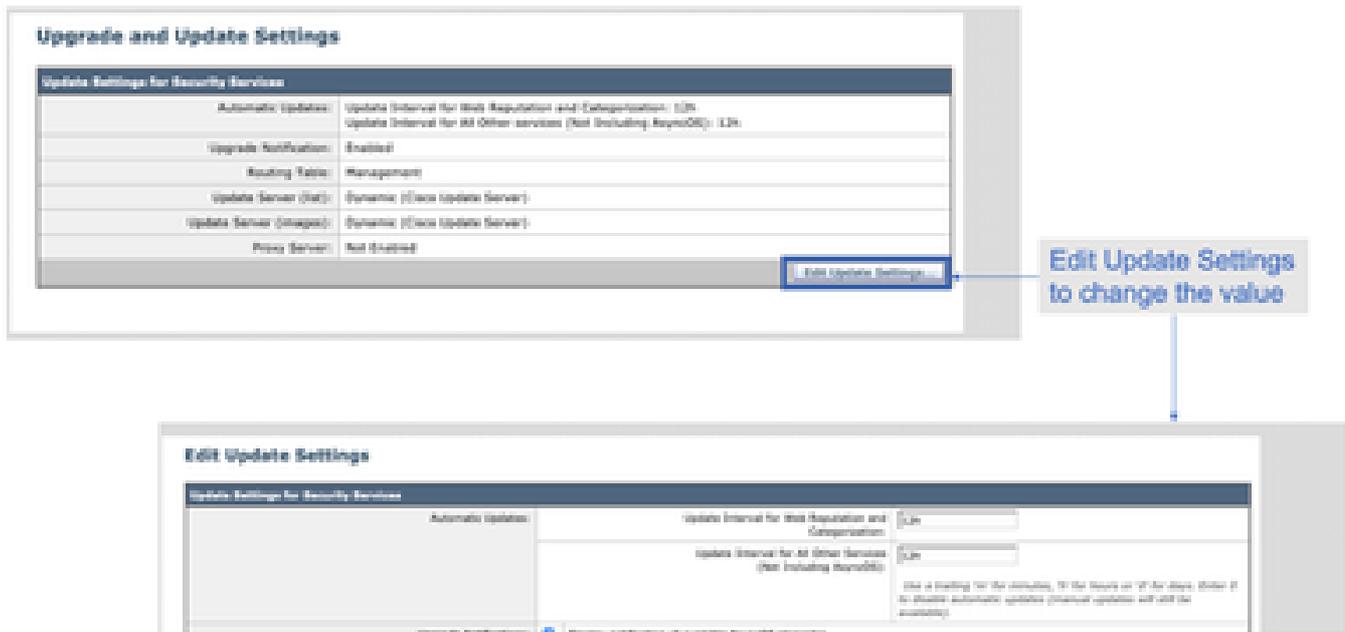
Choose the operation you want to perform:

- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates

[]>

 Remarque : la valeur ci-dessus indique la fréquence à laquelle nous vérifions les mises à jour, mais pas la fréquence à laquelle nous publions de nouvelles mises à jour pour les services de réputation et autres. les mises à jour peuvent être disponibles à tout moment.

OU à partir de l'interface GUI : Administration système -> Paramètres de mise à niveau et de mise à jour.



Comment mettre une URL sur liste blanche/noire ?

Parfois, les mises à jour des URL de Cisco TALOS prennent du temps, soit par manque d'informations, soit parce qu'il n'y a aucun moyen de modifier la réputation, car le site Web n'a toujours pas prouvé la modification du comportement malveillant. À ce stade, vous pouvez ajouter cette URL à une catégorie d'URL personnalisée qui autorise/bloque vos stratégies d'accès ou qui transmet/supprime votre stratégie de déchiffrement, et qui garantira que l'URL est transmise sans analyse ou vérification du filtrage des URL par l'appareil de sécurité Web (WSA) ou le blocage de Cisco.

pour mettre une URL sur liste blanche/noire, procédez comme suit :

1. Ajouter une URL dans la catégorie d'URL personnalisée.

Dans l'interface utilisateur graphique, accédez à Web Security Manager -> Custom and External URL Category.



2. Cliquez sur **Ajouter une catégorie** :



3. Ajoutez les sites Web similaires aux captures d'écran ci-dessous :

Custom and External URL Categories: Add Category

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. Accédez au filtrage URL dans la stratégie d'accès requise (**Gestionnaire de sécurité Web -> Stratégies d'accès -> Filtrage URL**).

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
	Global Policy Identification Profile: All	No blocked items	Monitor: All	Monitor: All	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. Sélectionnez la **WHITELIST** ou la **BLACKLIST** que nous venons de créer et incluez-la dans la politique.

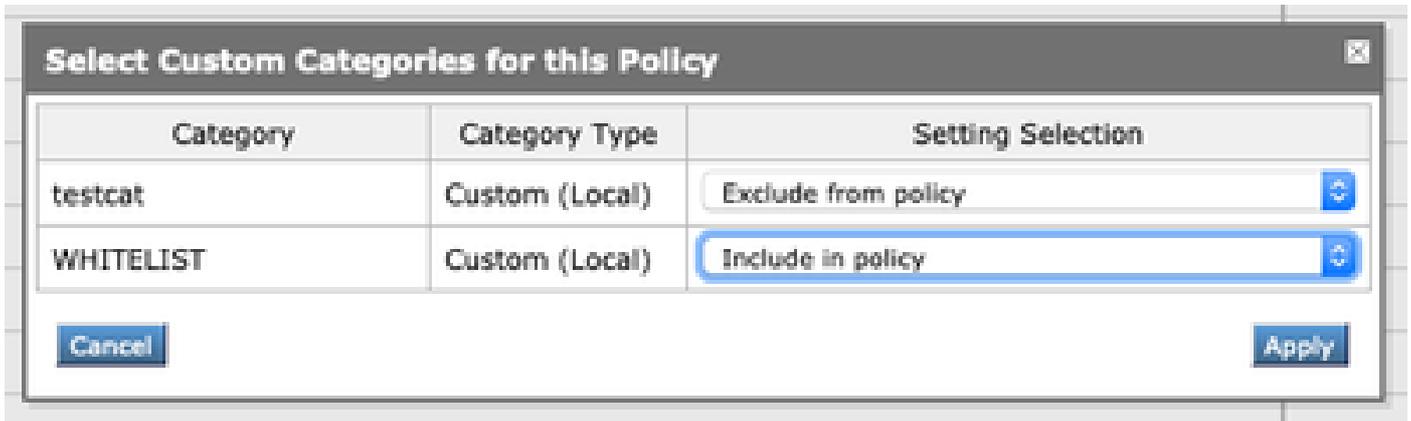
Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

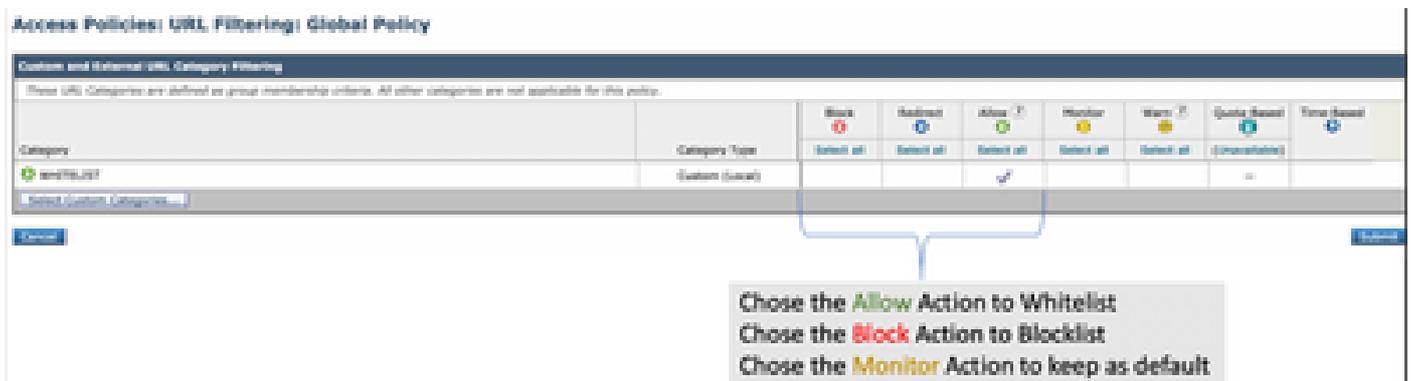
No Custom Categories are included for this Policy.

Select Custom Categories...

6. Incluez la catégorie de stratégie dans les paramètres de filtrage URL de stratégie comme ci-dessous.



7. Définissez l'action, Bloquer à la liste de blocage, Autoriser à la liste blanche. et si vous souhaitez que l'URL passe par les moteurs d'analyse, conservez l'action en tant que Surveillance.



8. Soumettre et valider les modifications.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.