

# Perguntas frequentes sobre Web Reputation score (WBRs) e Web Categorization Engine (FAQ)

## Contents

- [Perguntas frequentes sobre Web Reputation score \(WBRs\) e Web Categorization Engine \(FAQ\).](#)
- [Qual é o significado da pontuação do Web Reputation?](#)
- [O que significa categorização da Web?](#)
- [Como encontrar pontuação de reputação nos registros de acesso?](#)
- [Como encontrar pontuação de reputação em meus relatórios?](#)
- [Onde você verifica os logs de atualização da Pontuação de reputação baseada na Web \(WBRs\)?](#)
- [Como você verifica se tem conectividade com servidores Web Reputation Score \(WBRs\)?](#)
- [Como você arquiva uma disputa pela categorização da Web?](#)
- [Como você arquiva disputa por pontuação do Web Reputation?](#)
- [Uma disputa foi arquivada, mas a pontuação ou categoria não está sendo atualizada no Cisco Web Security Appliance \(WSA\) ou no Cisco TALOS.](#)
- [Cisco Web Security Appliance \(WSA\) mostrando resultados diferentes do Cisco TALOS, como corrigir isso?](#)
- [Como as pontuações do Web Reputation estão sendo calculadas?](#)
- [Qual é a faixa de pontuação para cada uma das categorias de reputação \(boa, neutra, ruim\)?](#)
- [Intervalos do Web Reputation e suas ações associadas:](#)
- [Políticas de acesso:](#)
- [Políticas decriptografia:](#)
- [Políticas de segurança de dados da Cisco:](#)
- [O que significa site sem categoria?](#)
- [Como você bloqueia URLs sem categoria?](#)
- [Com que frequência o banco de dados é atualizado?](#)
- [Como listar uma URL na lista branca/negra?](#)

## Perguntas frequentes sobre Web Reputation score (WBRs) e Web Categorization Engine (FAQ).

Este artigo descreve as perguntas mais frequentes sobre a pontuação do Web Reputation (WBRs) e o recurso de categorização com o Cisco Web Security Appliance (WSA).

### Qual é o significado da pontuação do Web Reputation?

Os filtros do Web Reputation atribuem uma pontuação de reputação baseada na Web (WBRs) a um URL para determinar a probabilidade de que ele contenha malware baseado em URL. O Web Security appliance usa pontuações de reputação da Web para identificar e interromper ataques de malware antes que eles ocorram. Você pode usar filtros do Web Reputation com políticas de acesso, descriptografia e segurança de dados da Cisco.



3. Na página **Resultados**, clique no link necessário e mais detalhes aparecerão como abaixo.

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

Time (GMT +04:00)	Website (count)	Hide All Details...	Disposition	Bandwidth	User / Client IP
15 Jul 2019 22:28:31	<a href="http://detectportal.firefox.com/success.txt">http://detectportal.firefox.com/success.txt</a> 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. Columns...

URL Category: Infrastructure and Content Delivery Networks

WBRs Score: 1.5

## Onde você verifica os logs de atualização da Pontuação de reputação baseada na Web (WBRs)?

Os registros de atualizações da Pontuação de Reputação Baseada na Web (WBRs) podem ser encontrados em `updater_logs`, você pode fazer o download desses registros através do login do Protocolo de Transferência de Arquivos (FTP - File Transfer Protocol) na interface de gerenciamento. ou via CLI (Command Line Interface, interface de linha de comando).

Para exibir registros usando terminal:

1. Abrir **terminal**.
2. Digite a **cauda** do comando.
3. Escolha o **número dos registros** (varia dependendo da versão e do número de registros configurados).
4. Os registros serão exibidos.

```
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 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
```

## Como verificar se você tem conectividade com Pontuação de reputação baseada na Web (WBRs) atualiza servidores?

Para garantir que o Cisco Web Security Appliance (WSA) possa obter as novas atualizações, verifique se você tem a conectividade com os servidores da atualização da Cisco nas seguintes portas TCP (Transmission Control Protocol) 80 e 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:** Se você tiver algum proxy de upstream, faça os testes acima por meio do proxy de upstream.

## Como você arquiva uma disputa pela categorização da Web?

Depois de verificar se o Cisco Web Security Appliance (WSA) e o Cisco TALOS têm a mesma pontuação de reputação, mas ainda assim você acha que esse não é um resultado válido, isso

precisa ser corrigido enviando uma disputa com a equipe do Cisco TALOS.

Isso pode ser feito usando o seguinte link: [https://talosintelligence.com/reputation\\_center/support](https://talosintelligence.com/reputation_center/support)

Para **enviar o litígio**, siga as instruções abaixo.

The screenshot shows the 'Submit a Reputation Ticket' form. It includes a table with columns 'DISPUTE' and 'REPUTATION'. A 'LOOKUP' button is present. A callout box points to the 'Web' radio button under 'Type of Ticket'. Another callout box points to the 'LOOKUP' button. A third callout box points to the 'Comments and Site Description' text area.

**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.**

Resulta após a pesquisa e a opção de alterar manualmente a pontuação.

The screenshot shows the 'Type of Ticket' section with two radio buttons. Below it is a table with columns 'DISPUTE' and 'REPUTATION'. A dropdown menu is open over the 'REPUTATION' column for 'cisco.com', showing options: 'GOOD', 'Select a Reputation', 'Neutral', 'Poor', and 'Unknown'. A 'LOOKUP' button is visible below the table.

DISPUTE	REPUTATION
cisco.com	GOOD ✓ Select a Reputation Neutral Poor Unknown
uri.com	

**Note:** Os envios do Cisco TALOS podem levar algum tempo para serem refletidos no banco de dados, se o problema for urgente, você sempre poderá criar um **WHITELIST** ou **BLOCKLIST**, como uma solução alternativa até que o problema seja corrigido do back-end da Cisco. para fazer isso, você pode marcar esta seção ([Como fazer lista branca ou URL da](#)

[lista negra](#)).

## Como você arquiva disputa por pontuação do Web Reputation?

Depois de verificar se o Cisco Web Security Appliance (WSA) e o Cisco TALOS têm a mesma Categorização, mas ainda assim você acha que esse não é um resultado válido, isso precisa ser corrigido enviando uma disputa com a equipe do Cisco TALOS.

Acesse a página de envio de categorização no site do TALOS:  
[https://talosintelligence.com/reputation\\_center/support#categoryization](https://talosintelligence.com/reputation_center/support#categoryization)

Para **enviar o litígio**, siga as instruções abaixo.

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		

**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)

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.

Para atualizar a Categoria, escolha no menu **suspenso** o que você acha que ele se encaixa melhor no site e certifique-se de seguir as diretrizes de comentários.

# 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	<ul style="list-style-type: none"><li>Computers and Internet</li><li>Unknown</li><li>Not Actionable</li><li>Adult</li><li>Advertisements</li><li>Alcohol</li><li>Arts</li><li>Astrology</li></ul>	

**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).

**Uma disputa foi arquivada, mas a pontuação ou categoria não está sendo atualizada no Cisco Web Security Appliance (WSA) ou no Cisco TALOS.**

Caso tenha registrado um caso no Cisco TALOS e a reputação/pontuação não tenha sido atualizada em 3 a 4 dias. você pode verificar as configurações das atualizações e verificar se tem acesso ao servidor de atualização da Cisco. se todas essas etapas estiverem ok, você pode abrir um tíquete com o Cisco TAC, e o engenheiro da Cisco ajudará você a acompanhar a equipe do Cisco TALOS.

**Note:** você pode aplicar a solução WHITELIST/BLOCKLIST para aplicar a ação necessária até que a categoria/reputação seja atualizada pela equipe do Cisco TALOS.

**Cisco Web Security Appliance (WSA) mostrando resultados**

## diferentes do Cisco TALOS, como corrigir isso?

O banco de dados pode estar desatualizado no Cisco Web Security Appliance (WSA) devido a vários motivos, principalmente comunicação com nossos servidores de atualização. Siga estas etapas para verificar se você tem os servidores de atualização e a conectividade corretos.

1. Verifique se você tem a conectividade para os servidores da atualização da Cisco nas portas 80 e 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. Se você tiver algum proxy de upstream, certifique-se de que o proxy de upstream certifique-se de fazer os testes acima através do proxy de upstream.

3. Se a conectividade estiver boa e você ainda vir a diferença, force as atualizações manualmente: **atualize agora** a partir da CLI, ou a partir da **GUI->Serviços de segurança -> Proteção contra malware -> atualizar agora**.

Aguarde alguns minutos e, se isso não funcionar, verifique a próxima etapa.

4. Neste ponto, você precisará verificar os updater\_logs: **terminal aberto: CLI->tail-> (escolha o número do arquivo de log updater\_logs.)** isso fará com que os logs de atualização exibam apenas as novas linhas.

As linhas de registro devem começar com esta linha "**Comando remoto recebido para sinalizar uma atualização manual**":

```
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. Verifique se há alguma mensagem de "**Crítico/Aviso**", os registros de atualização são erros muito legíveis por humanos e, muito provavelmente, o guiará por onde está o problema.



6. Se não houver resposta, você poderá abrir um tíquete com o suporte da Cisco com os resultados das etapas acima e eles terão o prazer de ajudar.

## Como as pontuações do Web Reputation estão sendo calculadas?

Alguns dos parâmetros que estão sendo considerados ao atribuir uma pontuação a um site específico:

- Dados de categorização de URL
- Presença de código para download
- Presença de contratos de licença de usuário final (EULAs) longos e obscuros
- Volume global e alterações no volume
- Informações do proprietário da rede
- Histórico de um URL
- Idade de um URL
- Presença em qualquer lista de bloqueio
- Presença em qualquer lista de permissão
- Tipos de URL de domínios populares
- Informações do agente de registro
- informação de endereço IP

## Qual é a faixa de pontuação para cada uma das categorias de reputação (boa, neutra, ruim)?

Intervalos do Web Reputation e suas ações associadas:

Políticas de acesso:

Pontuação	Ação	Descrição	Exemplo
-10 a -6.0 (Pobre)	Bloqueio	Site ruim. A solicitação está bloqueada, e nenhuma outra verificação de malware ocorre.	<ul style="list-style-type: none"><li>• O URL faz o download de informações sem permissão de usuário.</li><li>• Aumento repentino no volume de URL.</li><li>• URL é um erro de digitação de um domínio popular.</li></ul>
-5.9 a 5.9 (Neutro)	Analisar	Site indeterminado. A solicitação é passado ao mecanismo DVS para mais verificação de malware. O mecanismo DVS verifica a solicitação e conteúdo de resposta do servidor.	<ul style="list-style-type: none"><li>• URL recém-criada que tem um endereço IP dinâmico e contém conteúdo para download.</li><li>• Endereço IP do proprietário da rede que tem pontuação positiva do Web Reputation</li></ul>
6.0 a 10.0 (Bom)	Permissão	Bom local. A solicitação é permitida. Não é necessária verificação de malware.	<ul style="list-style-type: none"><li>• O URL não contém conteúdo para download.</li><li>• Domínio republicável de alto volume com histórico longo.</li></ul>

			<ul style="list-style-type: none"> <li>• Domínio presente em várias listas de permissões</li> <li>• Nenhum link para URLs com reputação ruim</li> </ul>
--	--	--	---

## Políticas de descryptografia:

Pontuação	Ação	Descrição
-10 a -9.0 (Pobre)	Largar	Site ruim. A solicitação é liberada sem aviso enviado ao usuário final. Use essa configuração com cuidado.
-8.9 a 5.9 (Neutro)	Descryptografar	Site indeterminado. A solicitação é permitida, mas a conexão é descryptografada e as Políticas de acesso são aplicadas ao tráfego descryptografado.
6.0 a 10.0 (Bom)	Passar	Bom local. A solicitação é passada sem nenhuma inspeção ou descryptografia.

## Políticas de segurança de dados da Cisco:

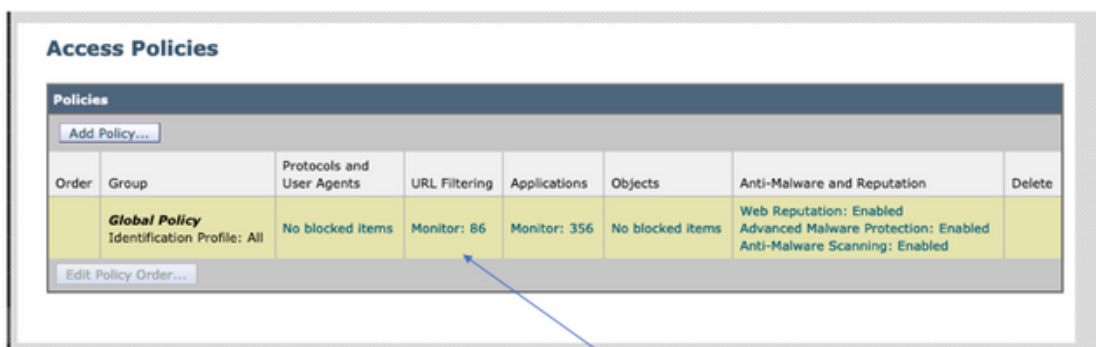
Pontuação	Ação	Descrição
-10 a -6.0 (Pobre)	Bloqueio	Site ruim. A transação está bloqueada e não ocorre mais verificação.
-5.9 a 0.0 (Neutro)	Monitor	A transação não será bloqueada com base no Web Reputation e prosseguirá para verificações de conteúdo (tipo e tamanho do arquivo). Observação Sites sem pontuação são monitorados.

## O que significa site sem categoria?

URLS sem categoria são aqueles que o banco de dados da Cisco não tem informações suficientes para confirmar sua categoria. geralmente sites recém-criados.

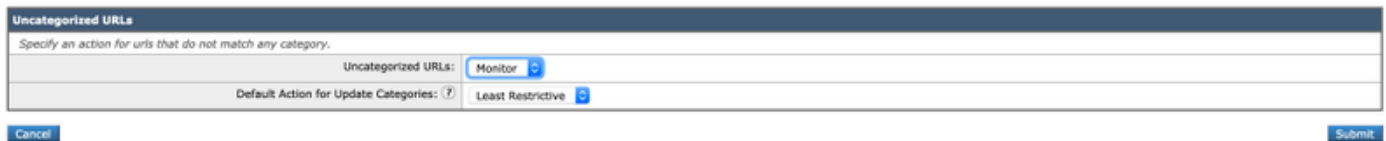
## Como você bloqueia URLS sem categoria?

1. Vá para a política de acesso desejada: **Web Security Manager -> Políticas de Acesso.**



Click on the URL Filtering section in the required Policy

2. Role para baixo até a seção URLs sem categoria.



3. Escolha uma das ações desejadas, Monitorar, Bloquear ou Avisar.

4. Enviar e confirmar alterações.

## Com que frequência o banco de dados é atualizado?

A frequência de verificação de atualizações pode ser atualizada usando o seguinte comando da CLI: **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

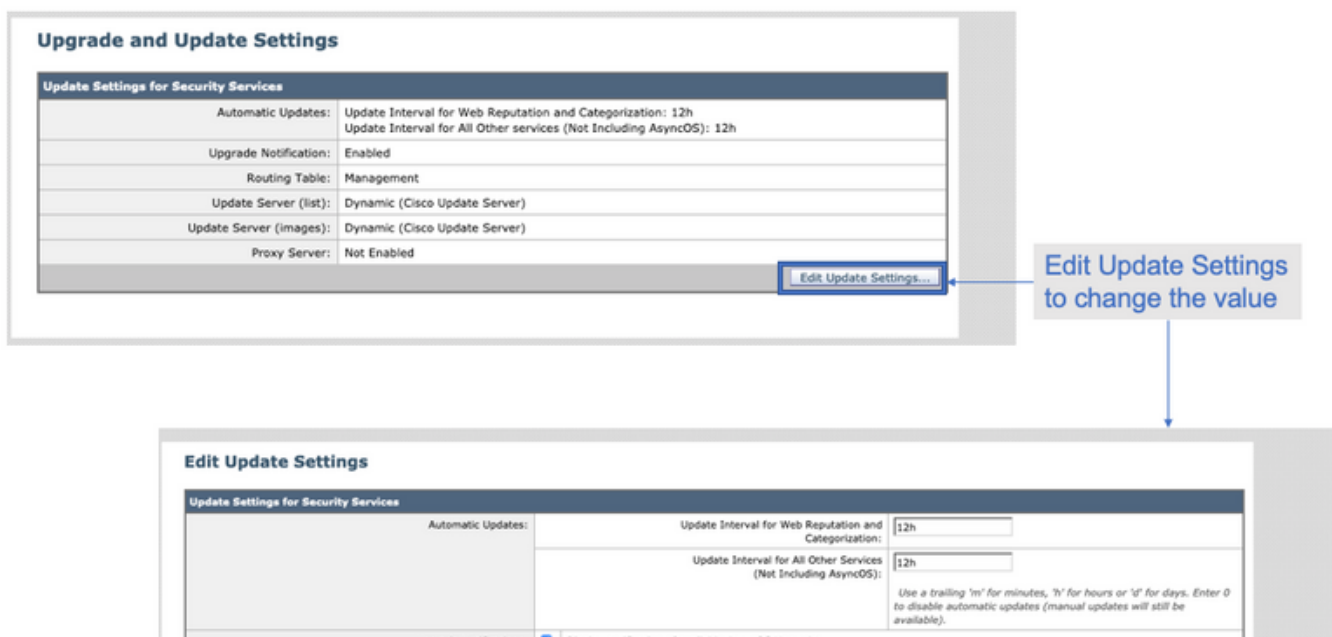
Upgrade notification: enabled

Choose the operation you want to perform:

- SETUP - Edit update configuration.
  - VALIDATE\_CERTIFICATES - Validate update server certificates
  - TRUSTED\_CERTIFICATES - Manage trusted certificates for updates
- [ ]>

**Note:** o valor acima mostra a frequência com que verificamos atualizações, mas não a frequência com que lançamos novas atualizações para a reputação e outros serviços. as atualizações podem estar disponíveis a qualquer momento.

OU da GUI: **System Administration -> Upgrade e atualiza as configurações.**



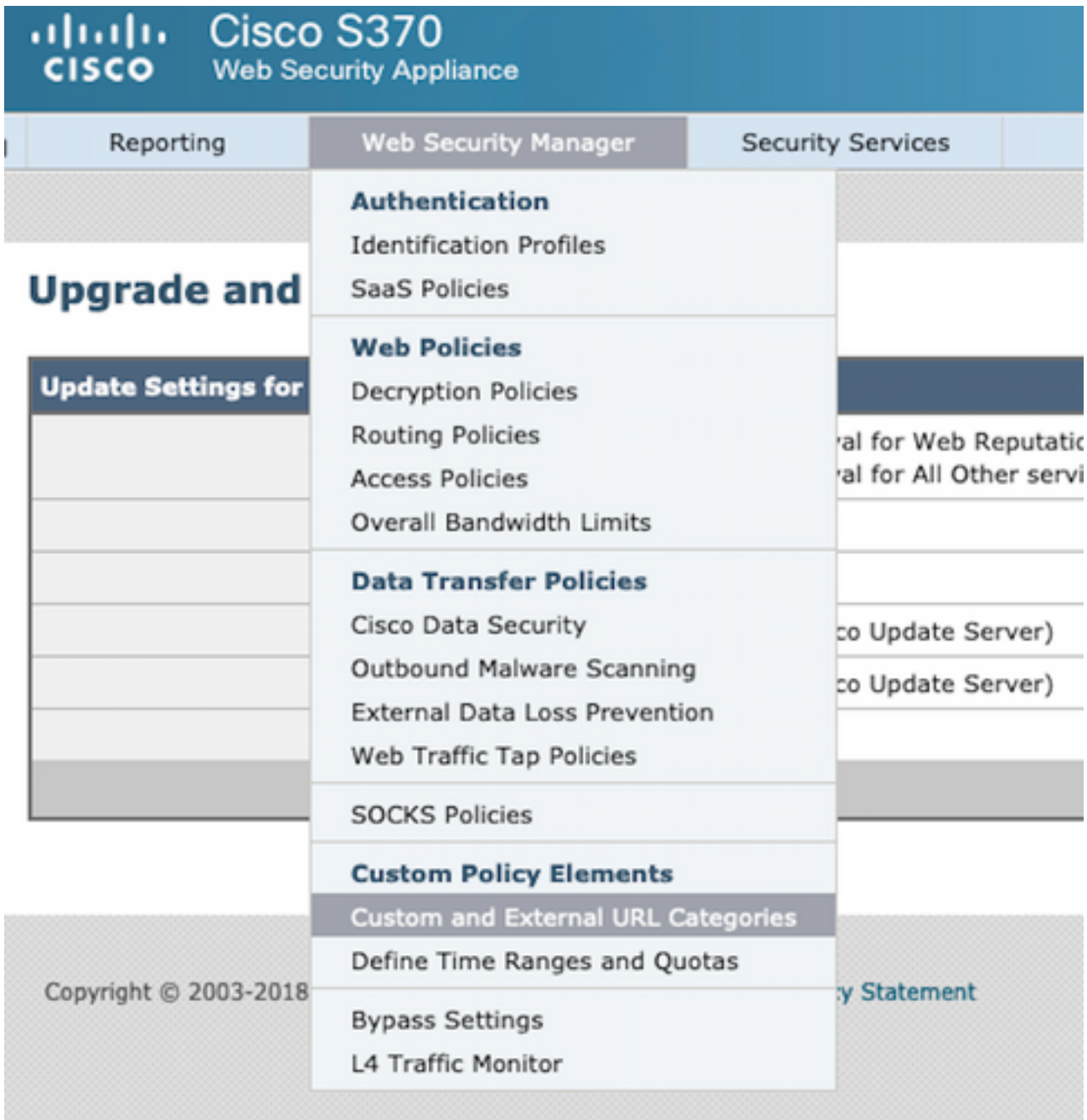
## Como listar uma URL na lista branca/negra?

Às vezes, as atualizações de URLs do Cisco TALOS levam tempo, devido à falta de informações suficientes. ou não há como mudar a reputação porque o site ainda não provou a mudança no comportamento mal-intencionado. neste ponto, você pode adicionar este URL a uma categoria de URL personalizada que permita/bloqueie suas políticas de acesso ou passe-por/soltar em sua Política de descryptografia, e que garantirá que o URL seja entregue sem verificação ou verificação de filtragem de URL pelo Cisco Web Security Appliance (WSA) ou bloco.

para enviar uma URL para uma lista branca/lista negra, siga estas etapas:

1. Adicionar URL na categoria de URL personalizada.

Na GUI, vá para **Web Security Manager -> Custom and External URL Category.**



2. Clique em **Adicionar categoria:**

**Custom and External URL Categories**

Categories List					
<a href="#">Add Category...</a>					
Order	Category	Category Type	Last Updated	Feed Content	Delete
1	<a href="#">googledrive</a>	Custom (Local)	N/A	-	
2	<a href="#">Trusted URLs</a>	Custom (Local)	N/A	-	

3. Adicione os sites semelhantes às capturas de tela abaixo:

## Custom and External URL Categories: Add 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 Regular Expressions: ?  
Enter one regular expression per line.

Cancel Submit

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. Vá para a filtragem de URL na política de Acesso necessária (**Web Security Manager -> Access Policies -> URL Filtering**).

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
	<b>Global Policy</b> 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. Selecione o **WHITELIST** ou **BLACKLIST** que acabamos de criar e inclua-o na política.

## Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

Select Custom Categories...

6. Inclua a Categoria da política nas configurações de filtragem de URL da política, conforme abaixo.

### Select Custom Categories for this Policy

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

7. Defina a ação, Bloquear na Lista de Bloqueios, Permitir à Lista de Whitelist. e se desejar que a URL passe pelos mecanismos de verificação, mantenha a ação como monitor.

#### 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
WHITELIST	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	

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

8. Enviar e confirmar alterações.