WBRS (Web Reputation Score) e Domande frequenti (FAQ) sul Web Categorization Engine

Sommario

WBRS (Web Reputation Score) e FAQ (Web Categorization Engine).

Qual è il significato di Punteggio reputazione Web?

Che cosa significa categorizzazione Web?

Come trovare il punteggio di reputazione nei log degli accessi?

Come trovare il punteggio di reputazione nei report?

Dove è possibile controllare i registri degli aggiornamenti WBRS (Web-Based Reputation Score)?

Verifica della presenza di connettività ai server WBRS (Web-Based Reputation Score)

In che modo è possibile archiviare una controversia per la categorizzazione Web?

In che modo è possibile creare una controversia per il punteggio Web Reputation?

È stata aperta una controversia ma il punteggio o la categoria non vengono aggiornati in Cisco Web Security Appliance (WSA) o Cisco TALOS.

Come risolvere il problema relativo a Cisco Web Security Appliance (WSA) che mostra risultati diversi rispetto a Cisco TALOS?

Come vengono calcolati i punteggi della reputazione Web?

Qual è la gamma di punteggi per ciascuna categoria di reputazione (buono, neutro, scarso)?

- Intervalli reputazione Web e azioni associate:
- Criteri di accesso:
- Criteri di decrittografia:
- Criteri di sicurezza dei dati Cisco:

Che cosa significa sito Web non classificato?

Come si bloccano gli URL non classificati?

Con quale frequenza il database viene aggiornato?

Come mettere in lista bianca/nera un URL?

WBRS (Web Reputation Score) e FAQ (Web Categorization Engine).

In questo articolo vengono descritte le domande più frequenti sul punteggio Web Reputation Score (WBRS) e sulla funzionalità di categorizzazione di Cisco Web Security Appliance (WSA).

Qual è il significato di Punteggio reputazione Web?

I filtri Web Reputation assegnano un punteggio Web-Based Reputation Score (WBRS) a un URL per determinare la probabilità che contenga malware basato su URL. Web Security Appliance utilizza i punteggi della reputazione Web per identificare e arrestare gli attacchi di malware prima che si verifichino. È possibile utilizzare i filtri reputazione Web con i criteri di accesso,

decrittografia e sicurezza dei dati Cisco.

Che cosa significa categorizzazione Web?

I siti Internet sono categorie basate sul comportamento e lo scopo di questi siti Web, al fine di rendere più facile per gli amministratori dei proxy, abbiamo aggiunto ogni URL del sito Web a una categoria predefinita, dove può essere identificato per scopi di sicurezza e di report. i siti Web che non appartengono a una delle categorie predefinite, sono chiamati siti Web senza categoria, che può essere dovuto alla creazione di nuovi siti Web e la mancanza di dati/traffico sufficiente, per determinare la sua categoria. e questo cambia nel tempo.

Come trovare il punteggio di reputazione nei log degli accessi?

A ogni richiesta effettuata tramite Cisco Web Security Appliance (WSA) deve essere associato un punteggio Web-Based Reputation Score (WBRS) e una categoria URL. Uno dei modi per visualizzarlo è tramite i log degli accessi. Di seguito è riportato un esempio: il punteggio Web-Based Reputation Score (WBRS) è (-1,4) e la categoria URL è Computer e Internet.

Riferimento di testo per lo screenshot precedente.

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

---

Note:

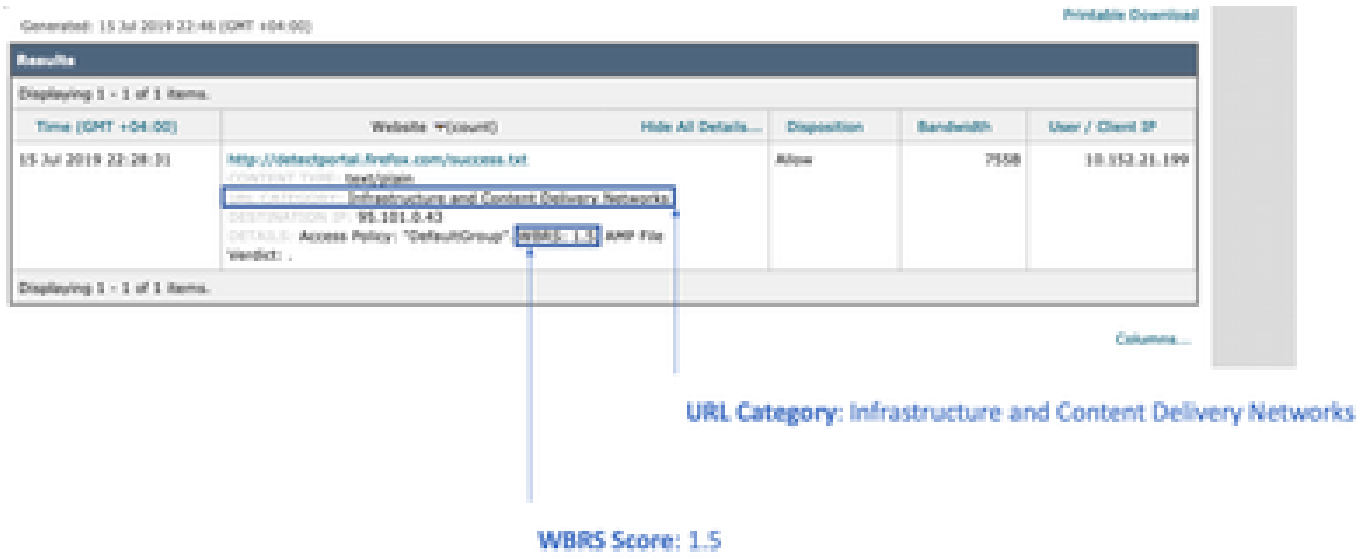
- I log degli accessi possono essere visualizzati dall'interfaccia della riga di comando (CLI) o scaricati utilizzando il metodo FTP (File Transfer Protocol) sull'indirizzo IP dell'interfaccia di gestione (verificare che FTP sia abilitato sull'interfaccia).
- Abbreviazione elenco completo categorie: 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#c

---

Come trovare il punteggio di reputazione nei report?

1. Accedere alla **GUI di** Cisco Web Security Appliance (WSA) -> **Reporting** -> **Web Tracking**.

2. Cercare il **dominio** desiderato.
3. Nella pagina **Risultati**, fare clic sul collegamento necessario per visualizzare ulteriori dettagli come indicato di seguito.



Dove è possibile controllare i registri degli aggiornamenti WBRS (Web-Based Reputation Score)?

I registri degli aggiornamenti Web-Based Reputation Score (WBRS) sono disponibili in updater_logs, è possibile scaricarli tramite l'accesso FTP (File Transfer Protocol) all'interfaccia di gestione o tramite l'interfaccia della riga di comando (CLI).

Per visualizzare i registri mediante il terminale:

1. Aprire Terminal.
2. Digitare il comando tail.
3. Scegliere il numero di log (varia a seconda della versione e del numero di log configurati).
4. Verranno visualizzati i registri.

```
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
```

Come è possibile verificare la presenza di connettività ai server di aggiornamento WBRS (Web-Based Reputation Score)?

Per verificare che Cisco Web Security Appliance (WSA) sia in grado di ottenere i nuovi aggiornamenti. Verificare di disporre della connettività ai server di Cisco Update sulle seguenti porte 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 '^]'.
```

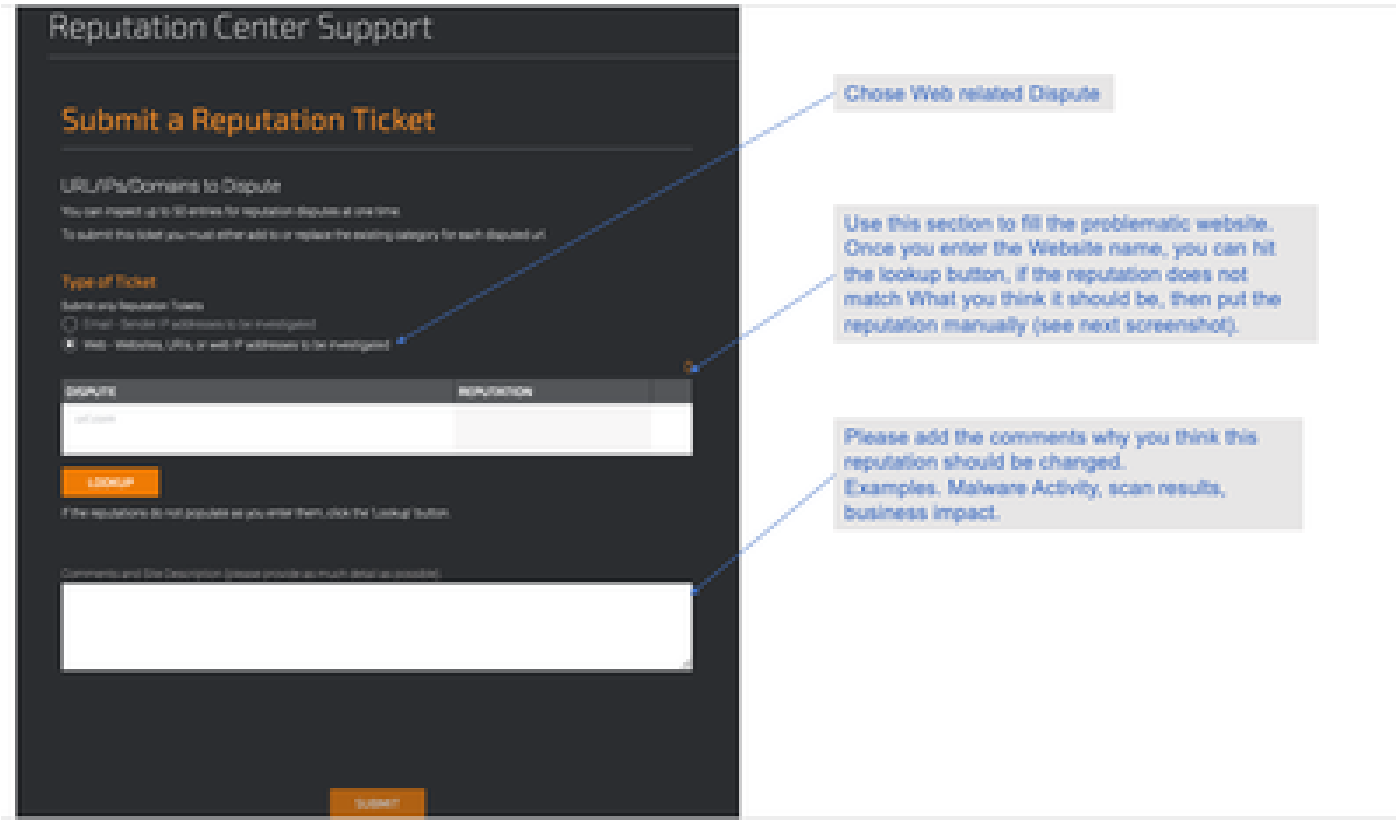
Nota: se si dispone di un proxy upstream, eseguire i test descritti in precedenza tramite il proxy upstream.

In che modo è possibile archiviare una controversia per la categorizzazione Web?

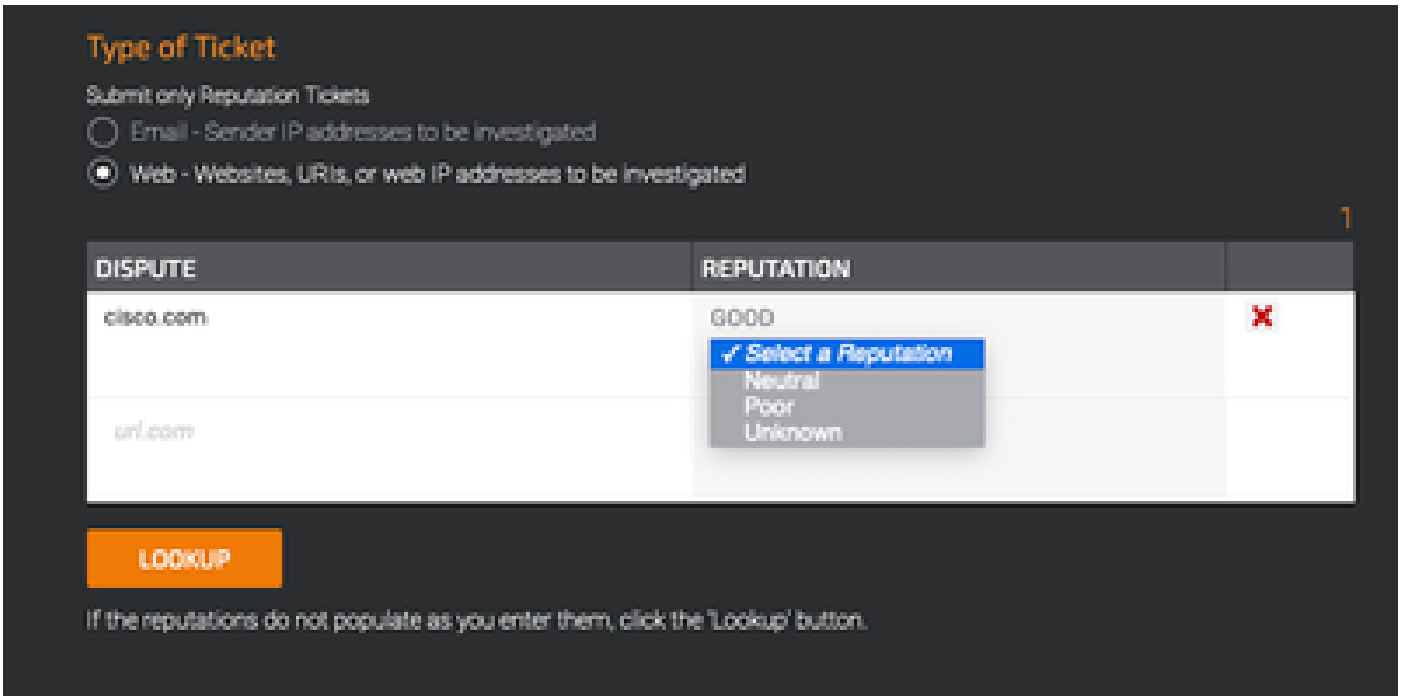
Dopo aver verificato che Cisco Web Security Appliance (WSA) e Cisco TALOS abbiano lo stesso punteggio di reputazione, ma comunque ritieni che non sia un risultato valido, devi risolvere il problema inoltrando una controversia con il team Cisco TALOS.

A tale scopo, è possibile utilizzare il collegamento seguente: https://talosintelligence.com/reputation_center/support

Per inviare la controversia, segui le istruzioni riportate di seguito.



Risultati dopo aver selezionato Ricerca e l'opzione per modificare manualmente il punteggio.



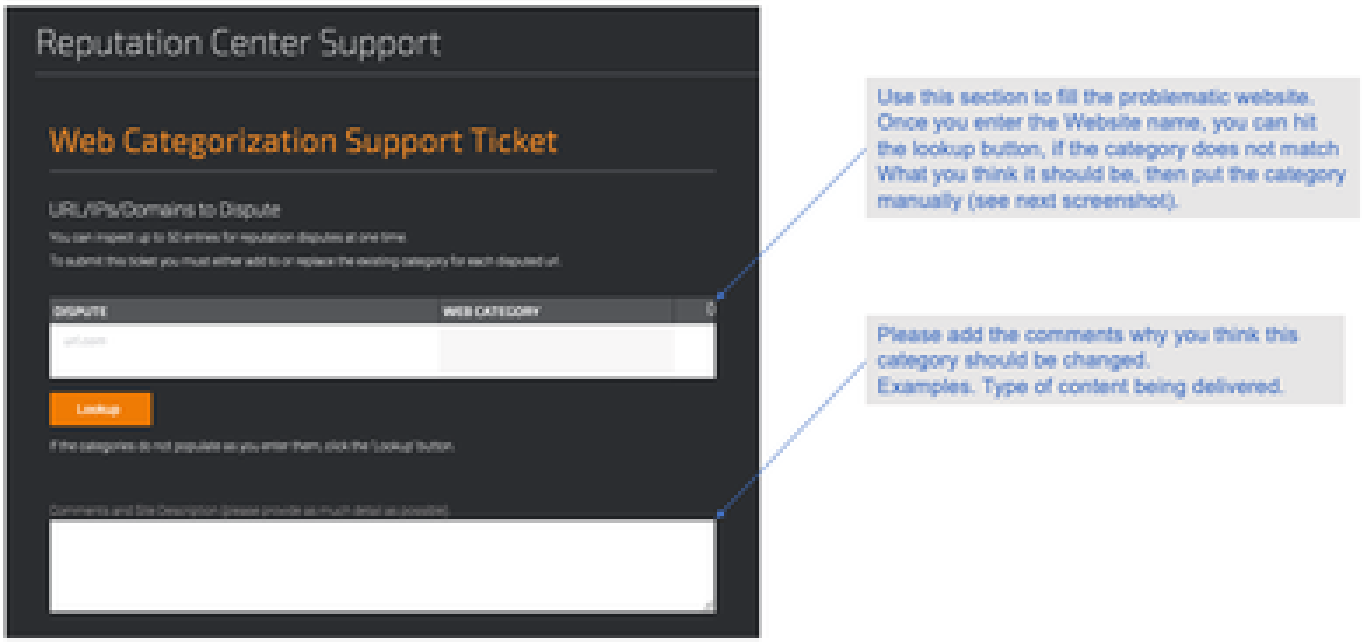
Nota: se il problema è urgente, è possibile creare sempre un WHITELIST o un BLOCKLIST, come soluzione alternativa finché il problema non viene risolto dal back-end Cisco. A tale scopo, è possibile controllare questa sezione (How To Whitelist or BlackList URL).

In che modo è possibile creare una controversia per il punteggio Web Reputation?

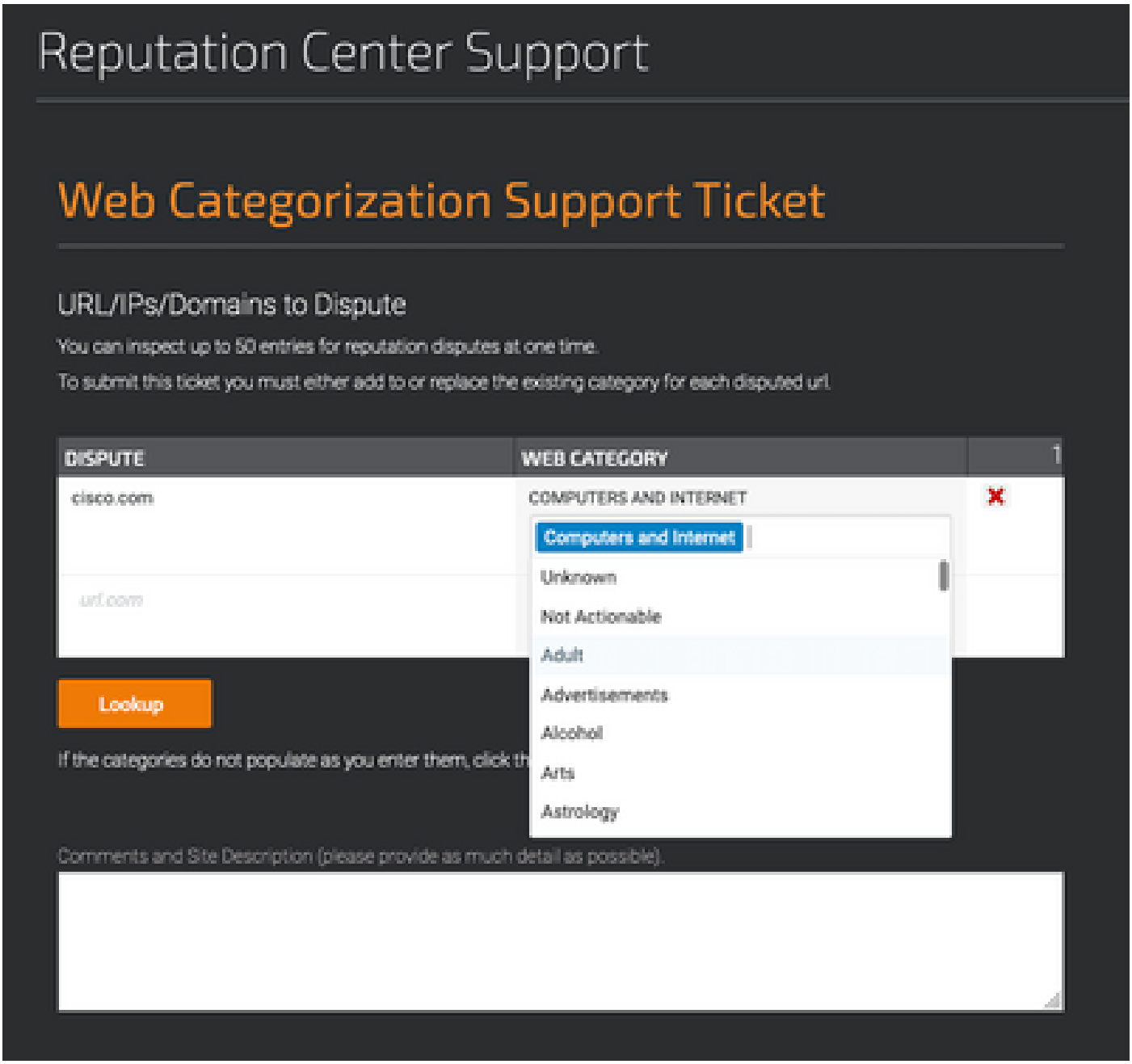
Dopo aver verificato che Cisco Web Security Appliance (WSA) e Cisco TALOS abbiano la stessa categorizzazione, ma sia comunque considerato un risultato non valido, è necessario risolvere il problema inoltrando una controversia con il team Cisco TALOS.

Visitare la pagina di inoltro della categorizzazione nel sito Web TALOS: https://talosintelligence.com/reputation_center/support#categorization

Per inviare la controversia, segui le istruzioni riportate di seguito.



Per aggiornare la categoria, scegliere dal menu a discesa quello che si ritiene più adatto al sito Web e assicurarsi di seguire le linee guida per i commenti.



È stata aperta una controversia ma il punteggio o la categoria non vengono aggiornati in Cisco Web Security Appliance (WSA) o Cisco TALOS.

Nel caso in cui sia stata presentata una richiesta di assistenza in Cisco TAC e la reputazione/il punteggio non sia stato aggiornato entro 3-4 giorni. è possibile controllare le impostazioni degli aggiornamenti e verificare di essere raggiungibili sul server di Cisco update. Se tutte queste procedure sono state completate, è possibile procedere e aprire una richiesta di assistenza in Cisco TAC, mentre il tecnico Cisco fornirà assistenza per contattare il team Cisco TALOS.

Nota: è possibile applicare la soluzione WHITELIST/BLOCKLIST per applicare l'azione necessaria finché la categoria/reputazione non viene aggiornata dal team Cisco TALOS.

Come risolvere il problema con Cisco Web Security Appliance (WSA) che mostra risultati diversi rispetto a Cisco TALOS?

Il database può non essere aggiornato su Cisco Web Security Appliance (WSA) per diversi motivi, principalmente per la comunicazione con i server di aggiornamento. Per verificare la presenza di server di aggiornamento e connettività corretti, eseguire la procedura seguente.

1. Verificare di disporre della connettività per i server degli aggiornamenti Cisco sulle porte 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 si dispone di un proxy upstream, assicurarsi che il proxy upstream esegua i test sopra indicati tramite il proxy upstream.

3. Se la connettività è corretta e la differenza persiste, forzare gli aggiornamenti manualmente: updatenow dalla CLI o dalla GUI->Security services -> Malware protection -> updatenow.

Attendere alcuni minuti. Se il problema persiste, controllare il passaggio successivo.

4. A questo punto è necessario controllare il file di log updater_logs: open terminal: CLI->tail-> (scegliere il numero di file di log updater_logs). In questo modo i log di aggiornamento visualizzeranno solo le nuove righe.

Le righe del registro devono iniziare con la riga "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. Verificare la presenza di messaggi "Critico/Avvertenza". I log di aggiornamento sono errori molto leggibili dall'utente e molto probabilmente consentono di individuare la posizione del problema.

6. Se non c'è stata risposta, allora puoi aprire una richiesta di assistenza con il supporto Cisco seguendo i risultati delle operazioni precedenti, e i clienti saranno lieti di ricevere assistenza.

Come vengono calcolati i punteggi della reputazione Web?

Alcuni dei parametri presi in considerazione quando si assegna un punteggio a un sito Web specifico:

- Dati di categorizzazione URL
- Presenza di codice scaricabile
- Presenza di contratti di licenza con l'utente finale lunghi e offuscati
- Volume globale e variazioni di volume
- Informazioni sul proprietario della rete
- Cronologia di un URL
- Età di un URL
- Presenza in tutti gli elenchi di blocco
- Presenza in qualsiasi elenco Consenti
- Tipi di URL dei domini più diffusi
- Informazioni sul registrar
- Informazioni sull'indirizzo IP

Qual è la gamma di punteggi per ciascuna categoria di reputazione (buono, neutro, scarso)?

Intervalli reputazione Web e azioni associate:

Criteri di accesso:

Punteggio	**Azione**	**Descrizione**	**Esempio**
da -10 a -6,0 (Insufficiente)	Block (Blocca)	Sito non valido. La richiesta è bloccata, e nessun'altra scansione del malware si verifica.	• L'URL scarica le informazioni senza. • autorizzazione utente. • Picco improvviso nel volume URL. • URL è un tipo di dominio popolare.
da -5,9 a 5,9 (Neutro)	Scansione	Sito indeterminato. La richiesta è passato al motore DVS per ulteriori analisi malware. OSPF (Open Shortest Path First) Il motore DVS analizza la	• URL creato di recente con un • indirizzo IP dinamico e contiene • contenuto scaricabile.

		richiesta e il contenuto della risposta del server.	• Indirizzo IP del proprietario della rete con • Punteggio Web Reputation positivo.
da 6.0 a 10.0 (Buono)	Allow (Autorizza)	Buon sito. Richiesta consentita. Nessuna analisi malware richiesta.	• L'URL non contiene contenuto scaricabile. • Dominio di volumi elevati e affidabili con cronologia prolungata. • Dominio presente in più elenchi Consenti. • Nessun collegamento a URL con reputazione scarsa.

Criteri di decrittografia:

Punteggio	**Azione**	**Descrizione**
da -10 a -9,0 (Insufficiente)	Drop	Sito non valido. Richiesta eliminata senza alcun avviso inviato all'utente finale. Utilizzo con cautela.
da -8,9 a 5,9 (Neutro)	Decrittografa	Sito indeterminato. Richiesta consentita, ma la connessione è decrittografata e i criteri di accesso vengono applicati al traffico decrittografato.
da 6.0 a 10.0 (Buono)	Pass-through	Buon sito. La richiesta viene inoltrata senza ispezione o decrittografia.

Criteri di sicurezza dei dati Cisco:

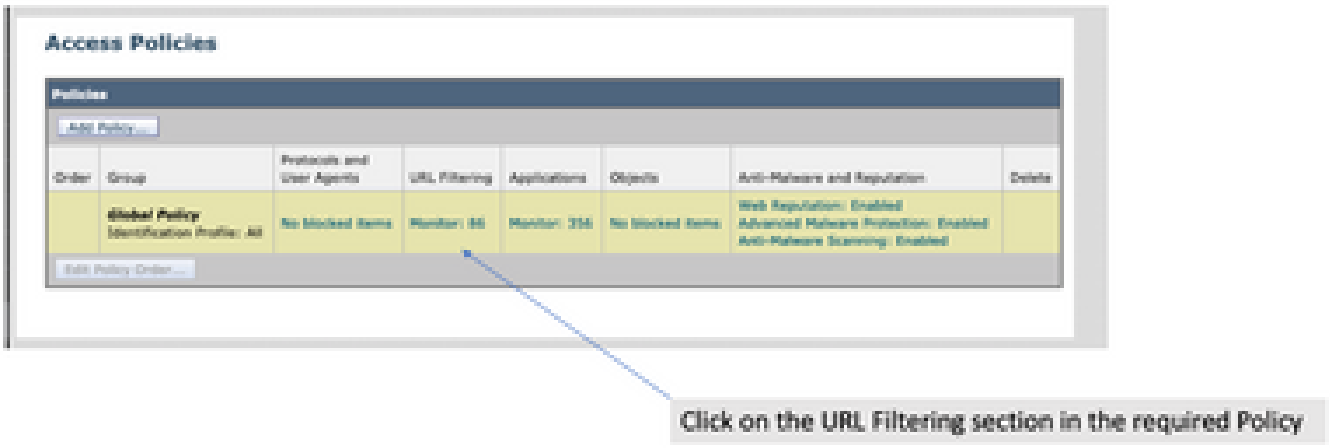
Punteggio	**Azione**	**Descrizione**
da -10 a -6,0 (Insufficiente)	Block (Blocca)	Sito non valido. La transazione è bloccata e non viene eseguita alcuna ulteriore analisi.
da -5,9 a 0,0 (Neutro)	Monitor (Monitora)	La transazione non verrà bloccata in base alla reputazione Web e procederà ai controlli del contenuto (tipo e dimensioni del file). Nota I siti senza punteggio vengono monitorati.

Che cosa significa sito Web non classificato?

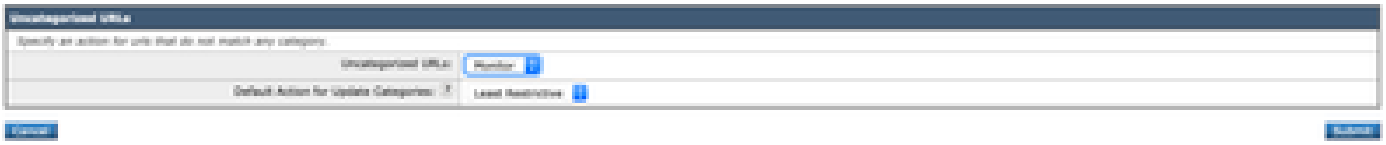
Gli URL non classificati sono quelli per cui il database Cisco non dispone di informazioni sufficienti per confermare la categoria. In genere, sono siti Web appena creati.

Come si bloccano gli URL non classificati?

1. Andare al criterio di accesso desiderato: Web Security Manager -> Criteri di accesso.



2. Scorrere verso il basso fino alla sezione URL non classificati.



3. Scegliere una delle azioni desiderate, Monitoraggio, Blocco o Avvisa.

4. Sottomettere e confermare le modifiche.

Con quale frequenza il database viene aggiornato?

La frequenza di controllo degli aggiornamenti può essere aggiornata usando il seguente comando dalla CLI: **updateconfig**

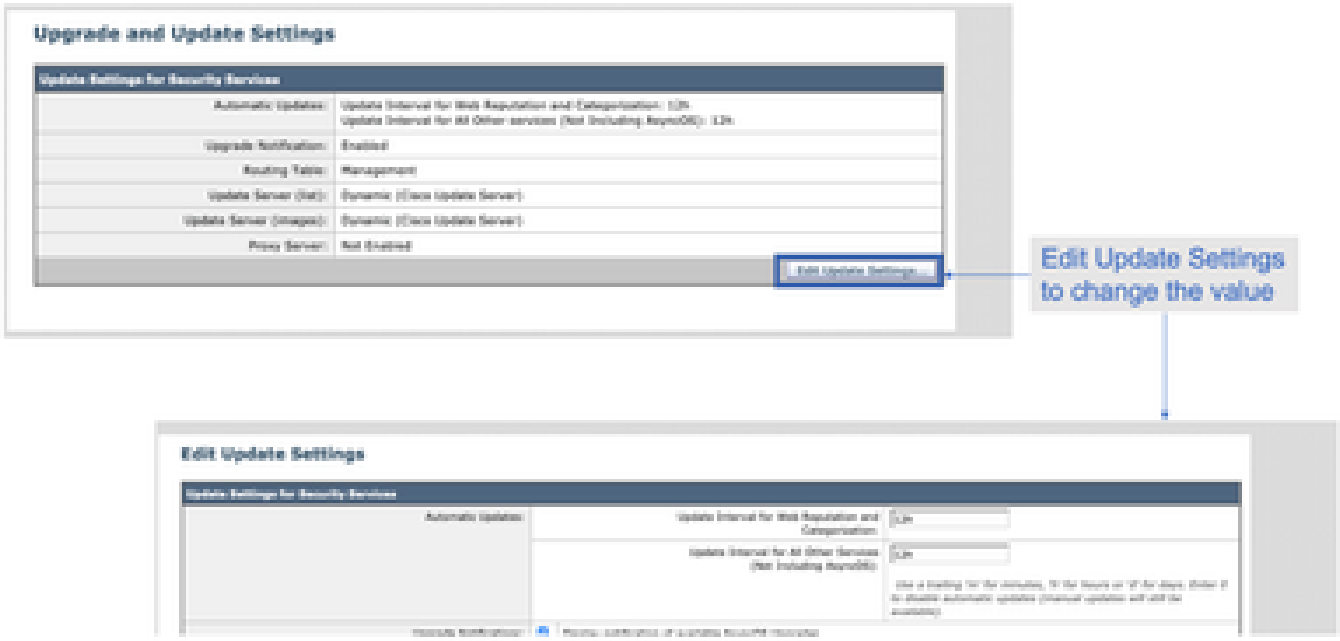
<#root>

```
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
[]>
```

 Nota: il valore precedente indica la frequenza con cui vengono controllati gli aggiornamenti, ma non la frequenza con cui vengono rilasciati nuovi aggiornamenti per la reputazione e altri servizi. Gli aggiornamenti possono essere disponibili in qualsiasi momento.

O dalla GUI: Amministrazione del sistema -> Aggiorna le impostazioni.



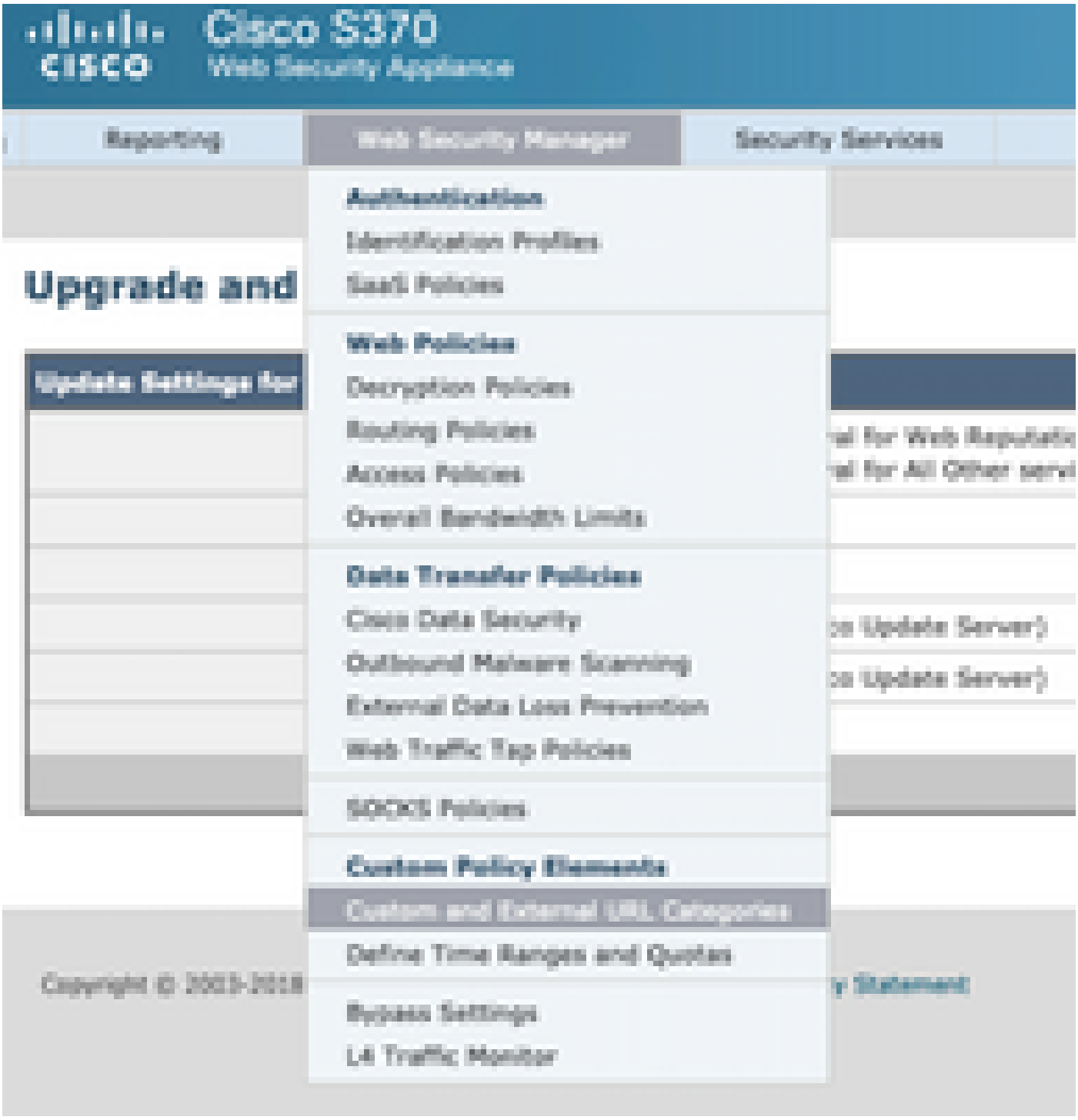
Come mettere in lista bianca/nera un URL?

A volte gli aggiornamenti per gli URL da Cisco Talos impiegano tempo, sia per la mancanza di informazioni sufficienti sia per non modificare la reputazione. In alternativa, non è possibile modificare la reputazione perché il sito Web non ha ancora dimostrato il cambiamento nel comportamento dannoso. a questo punto è possibile aggiungere l'URL a una categoria URL personalizzata che consenta/blocchi i criteri di accesso o passi-attraverso/rilascia i criteri di decrittografia e che garantisca la consegna dell'URL senza scansione o filtro URL da parte di Cisco Web Security Appliance (WSA) o blocco.

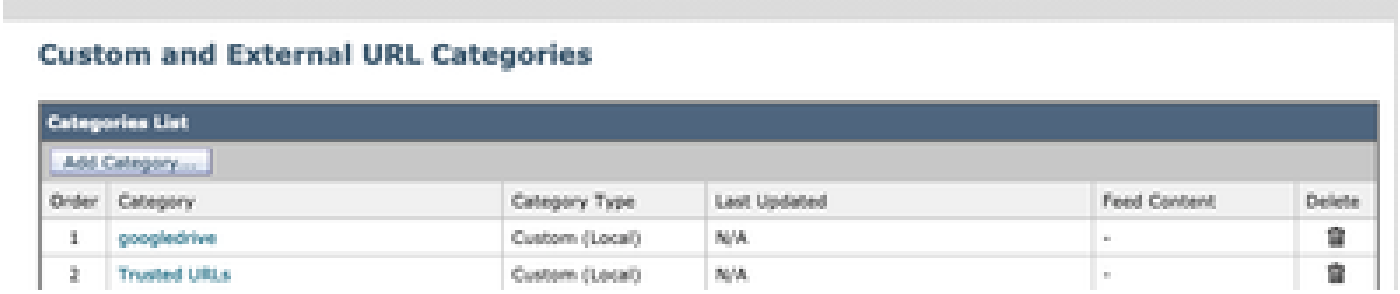
per inserire un URL nella lista bianca/nera, procedere come segue:

1. Aggiungere un URL nella categoria dell'URL personalizzato.

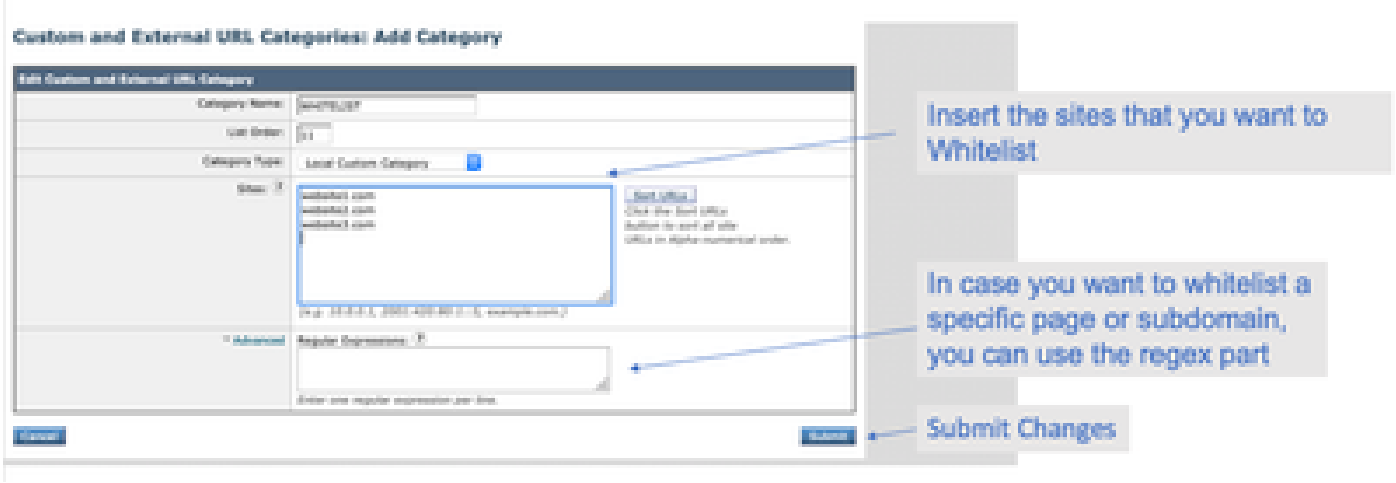
Dalla GUI, andare a Web Security Manager -> Categoria URL esterno e personalizzato.



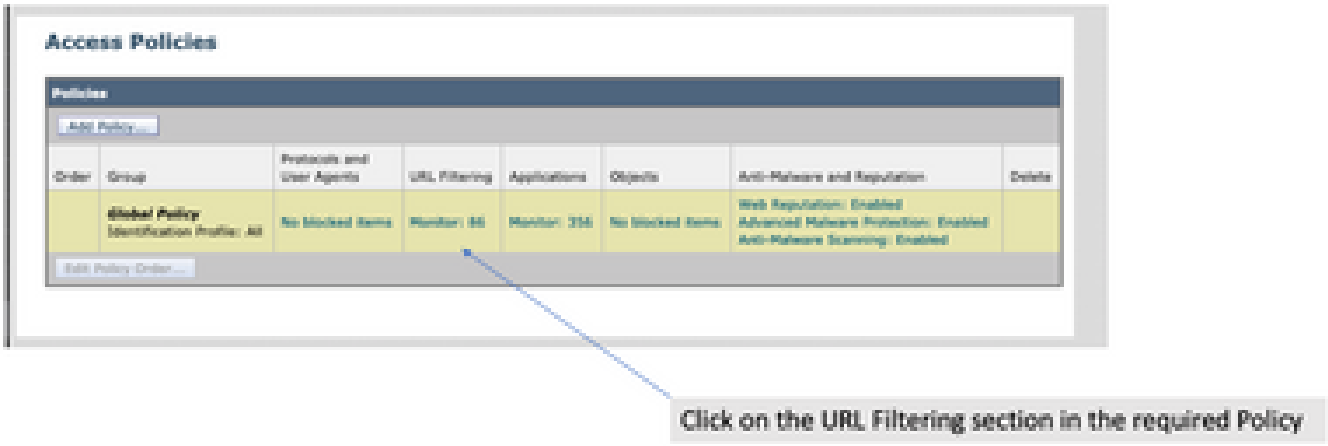
2. Fare clic su **Add Category** (Aggiungi categoria):



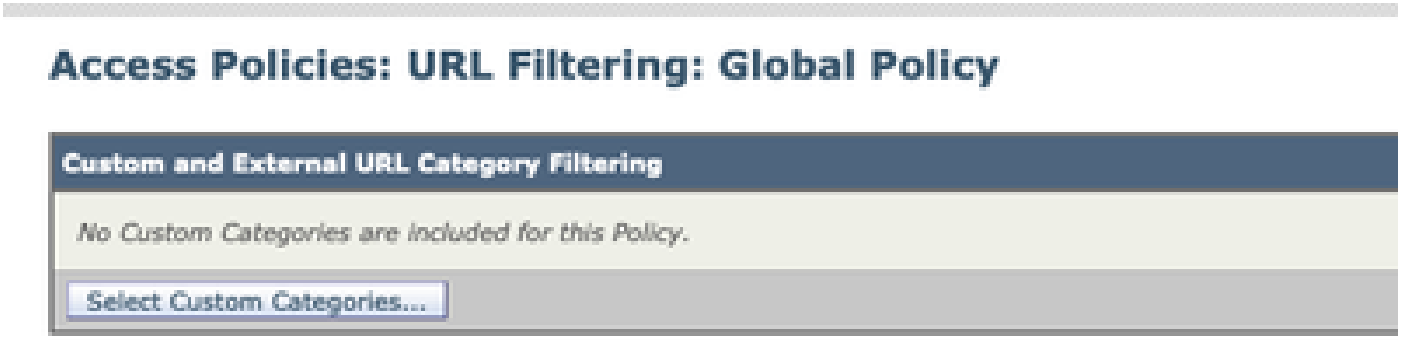
3. Aggiungi i siti web simili agli screenshot seguenti:



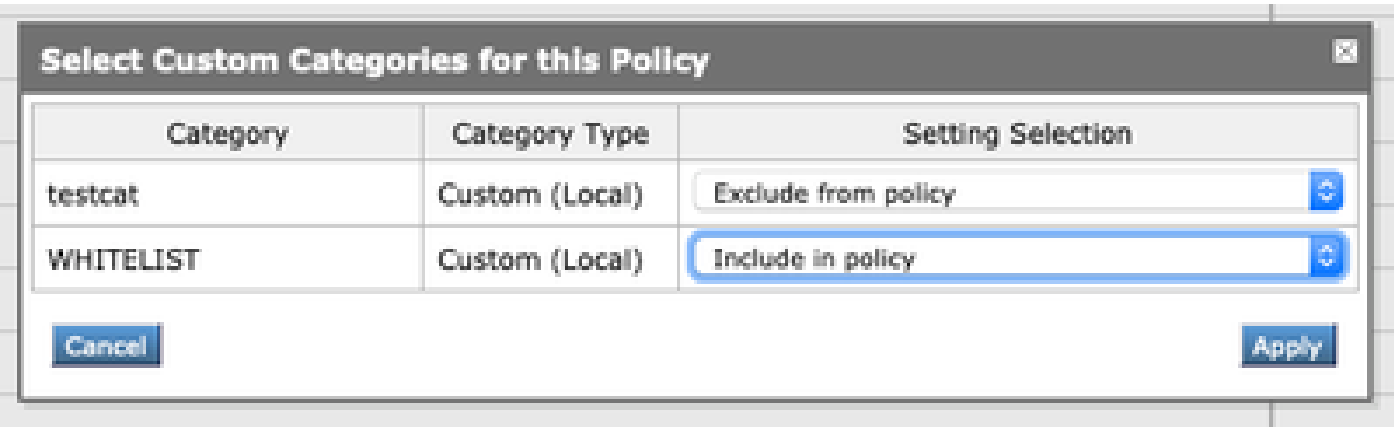
4. Accedere al filtro URL nei criteri di accesso richiesti (**Web Security Manager -> Criteri di accesso -> Filtro URL**).



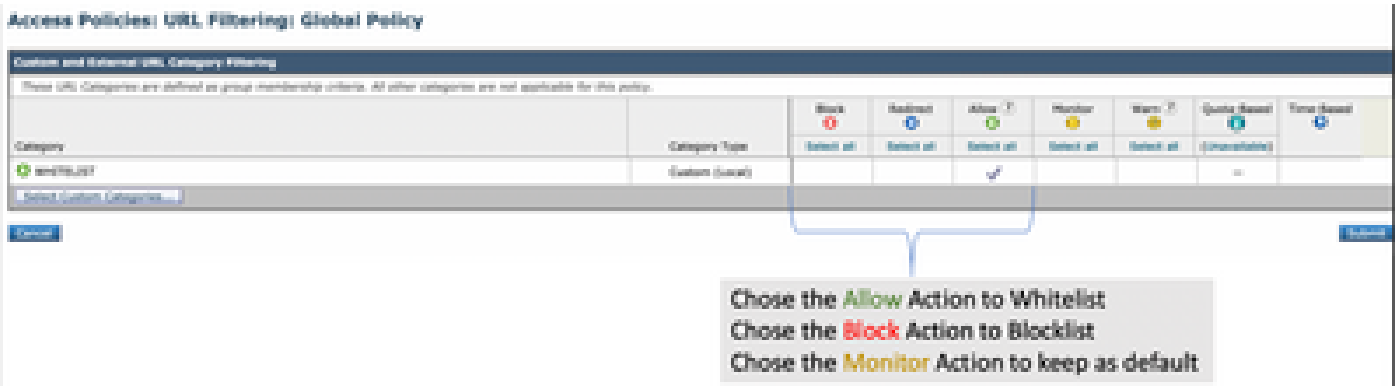
5. Selezionare la **LISTA BIANCA o LA LISTA NERA** appena creata e includerla nel criterio.



6. Includere la categoria dei criteri nelle impostazioni del filtro URL dei criteri come indicato di seguito.



7. Definire l'azione, da Blocca a Elenco blocchi, da Consenti a Elenco bianco. Se si desidera che l'URL passi attraverso i motori di scansione, mantenere l'azione come Controllo.



8. Sottomettere e confermare le modifiche.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).