

Webレピュテーションスコア(WBRS)およびWeb分類エンジンに関するFAQ

内容

[Webレピュテーションスコア\(WBRS\)およびWeb分類エンジンに関するFAQ](#)

[Webレピュテーションスコアとは何ですか。](#)

[Web分類とは](#)

[アクセスログでレピュテーションスコアを見つける方法](#)

[レポートでレピュテーションスコアを見つける方法](#)

[Webベースのレピュテーションスコア\(WBRS\)の更新ログはどこで確認できますか。](#)

[Web-Based Reputation Score\(WBRS\)アップデートサーバに接続できるかどうかを確認するにはどうすればよいですか。](#)

[Webカテゴリのクレームを提出するにはどうすればよいですか。](#)

[Webレピュテーションスコアのクレームを提出するにはどうすればよいですか。](#)

[クレームが提出されましたが、Cisco Webセキュリティアプライアンス\(WSA\)またはCisco TALOSでスコアまたはカテゴリが更新されていません。](#)

[Cisco TALOSとは異なる結果が表示されるCisco Webセキュリティアプライアンス\(WSA\)、これを修正する方法](#)

[Webレピュテーションスコアはどのように計算されますか。](#)

[各レピュテーションカテゴリ\(良、中立、低\)のスコア範囲はどのくらいですか。](#)

[Webレピュテーション範囲とその関連アクション：](#)

[アクセスポリシー](#)

[復号化ポリシー](#)

[シスコデータセキュリティポリシー：](#)

[未分類のWebサイトの意味](#)

[未分類のURLをブロックする方法](#)

[データベースが更新される頻度](#)

[URLをホワイトリスト/ブラックリストに登録する方法](#)

Web(WBRS)WebFAQ

この記事では、Cisco Webセキュリティアプライアンス(WSA)を使用したWebレピュテーションスコア(WBRS)および分類機能に関するFAQについて説明します。

Webレピュテーションスコアとは何ですか。

Webレピュテーションフィルタは、Webベースのレピュテーションスコア(WBRS)をURLに割り当て、URLベースのマルウェアが含まれている可能性を判断します。Webセキュリティアプライアンスは、Webレピュテーションスコアを使用して、マルウェア攻撃が発生する前に検出して阻止します。Webレピュテーションフィルタは、アクセス、復号化、およびシスコデータセキュリティポリシーとともに使用できます。

Web分類とは

インターネットWebサイトは、これらのWebサイトの動作と目的に基づくカテゴリであり、プロキシの管理者が簡単にアクセスできるように、すべてのWebサイトURLを事前定義されたカテゴリに追加しました。定義済みのカテゴリの1つに属していないwebサイトは、未分類のWebサイトと呼ばれます。これは、新しいwebサイトの作成や、カテゴリを決定するための十分なデータ/トラフィックの不足が原因である可能性があります。そして時間ごとにこの変化が起こります

アクセスログでレピュテーションスコアを見つける方法

Cisco Webセキュリティアプライアンス(WSA)を通じて行うすべての要求には、Webベースのレピュテーションスコア(WBRS)スコアとURLカテゴリが添付されている必要があります。アクセスログを使用して表示する方法の1つは、次の例です。Webベースのレピュテーションスコア(WBRS)スコアは(-1.4)、URLカテゴリは次のとおりです。コンピュータとインターネット。

```
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

上のスクリーンショットのテキスト参照。

```
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","-","-,-,-,"-,-,-,-,-> -
```

注:

- アクセスログは、コマンドラインインターフェイス(CLI)から表示するか、管理インターフェイスIPでFile Transfer Protocol(FTP)方式を使用して接続してダウンロードできます (インターフェイスでFTPが有効になっていることを確認してください)。
- カテゴリの省略形の完全なリスト
: 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#on_1208638

レポートでレピュテーションスコアを見つける方法

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

| 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 |

Columns...

URL Category: Infrastructure and Content Delivery Networks

WBRs Score: 1.5

Webベースのレピュテーションスコア(WBRs)の更新ログはどこで確認できますか。

Web-Based Reputation Score(WBRs)更新ログはupdater_logsにあります。これらのログは、File Transfer Protocol(FTP)ログインを使用して管理インターフェイスにダウンロードできます。またはコマンドラインインターフェイス(CLI)を使用します。

ターミナルを使用してログを表示するには、次の手順に従います。

1. ターミナルを開きます。
2. コマンドtailを入力します。
3. ログ番号を選択します (バージョンと構成されているログの数によって異なります)。
4. ログが表示されます。

```
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
```

どのように確認するか次のように接続している場合 Webベースのレピュテーションスコア(WBRS) サーバの更新

Cisco Webセキュリティアプライアンス(WSA)が新しいアップデートを取得できることを確認します。次のTransmission Control Protocol(TCP)ポート80および443で、Cisco Updateのサーバに接続できることを確認してください。

```
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 '^']'.
```

注：アップストリームプロキシがある場合は、アップストリームプロキシを介して上記のテストを実行します。

Webカテゴリのクレームを提出するにはどうすればよいですか。

Cisco Webセキュリティアプライアンス(WSA)とCisco TALOSの両方に同じレピュテーションスコアが付いていることを確認した後でも、これは有効な結果ではないと考えた後、Cisco TALOSチームにクレームを提出して修正する必要があります。

これを行うには、次のリンクを使用します。

https://talosintelligence.com/reputation_center/support

クレームを送信するには、次の手順に従ってください。

The screenshot shows the 'Submit a Reputation Ticket' form in the Reputation Center Support interface. The form includes a 'Type of Ticket' section with radio buttons for 'Email - Sender IP addresses to be investigated' and 'Web - Websites, URIs, or web IP addresses to be investigated'. Below this is a table with columns 'DISPUTE' and 'REPUTATION'. The 'DISPUTE' column contains 'url.com'. A 'LOOKUP' button is present below the table. A 'Comments and Site Description' text area is at the bottom, followed by a 'SUBMIT' button. Three callout boxes provide instructions: 1. 'Chose Web related Dispute' points to the 'Web' radio button. 2. '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).' points to the 'url.com' entry in the table. 3. 'Please add the comments why you think this reputation should be changed. Examples. Malware Activity, scan results, business impact.' points to the 'Comments and Site Description' text area.

Lookupを押した後の結果と、スコアを手動で変更するオプション。

The screenshot shows the 'Type of Ticket' section with the 'Web' radio button selected. Below is a table with columns 'DISPUTE' and 'REPUTATION'. The 'DISPUTE' column contains 'cisco.com' and 'url.com'. The 'REPUTATION' column shows 'GOOD' for 'cisco.com' and a dropdown menu for 'url.com'. The dropdown menu has options: 'Select a Reputation', 'Neutral', 'Poor', and 'Unknown'. A red 'X' is visible in the rightmost column of the table. A 'LOOKUP' button is below the table. A note below the button says: 'If the reputations do not populate as you enter them, click the 'Lookup' button.'

注：Cisco TALOSの送信がデータベースに反映されるまでに時間がかかる場合があります。問題が緊急の場合は、シスコのバックエンドから問題が修正されるまでいつでも **WHITELIST**または**BLOCKLIST**を作成できます。これを行うには、このセクションを[チェックしてください \(ホワイトリストまたはブラックリストのURL\)](#)。

Webレピュテーションスコアのクレームを提出するにはどうすれ

ばよいですか。

Cisco Webセキュリティアプライアンス(WSA)とCisco TALOSの両方が同じ分類を持っていることを確認した後でも、これは有効な結果ではないと思われるため、Cisco TALOSチームとクレームを提出して修正する必要があります。

TALOSのWebサイトで分類申請ページに移動します。

https://talosintelligence.com/reputation_center/support#categorization

クレームを送信するには、次の手順に従ってください。

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 | |
|---------|--------------|---|
| url.com | | 0 |

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.

カテゴリを更新するには、ドロップダウンメニューからWebサイトに適していると感じるものを選択し、コメントのガイドラインに従ってください。

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">Computers and InternetUnknownNot ActionableAdultAdvertisementsAlcoholArtsAstrology | |

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).

クレームが提出されましたが、Cisco Webセキュリティアプライアンス(WSA)またはCisco TALOSでスコアまたはカテゴリが更新されていません。

Cisco TALOSにケースを提出し、レピュテーション/スコアが3 ~ 4日以内に更新されなかった場合。更新プログラムの設定を確認し、Cisco updateサーバに到達できることを確認できます。これらの手順がすべて正しければ、Cisco TACでチケットをオープンできます。シスコエンジニアがCisco TALOSチームのフォローアップを支援します。

注：カテゴリ/レピュテーションがCisco TALOSチームから更新されるまで、WHITELIST/BLOCKLISTの回避策を適用して、必要なアクションを適用できます。

Cisco Web Security Appliance (WSA) Cisco TALOSとは異なる結果を表示する、これを修正する方法

Cisco Webセキュリティアプライアンス(WSA)のデータベースが古くなっている可能性があります。主にアップデートサーバとの通信が原因で、次の手順に従って正しいアップデートサーバと接続を確認してください。

1.ポート80および443でCiscoアップデートのサーバに接続できることを確認します。

```
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.アップストリームプロキシがある場合は、アップストリームプロキシがアップストリームプロキシを介して上記のテストを行っていることを確認します。

3.接続に問題がなく、まだ違いが見られる場合は、手動で更新を強制します。updatenowをCLIから実行するか、またはGUI -> [Security services] -> [Malware protection] -> [updatenow]から実行します。

数分待ってから、問題が解決しない場合は、次の手順を確認してください。

4.この時点で、updater_logsを確認する必要があります。ターミナルを開く：CLI->tail-> (updater_logsログファイルの数を選択)。これにより、更新ログに新しい行のみが表示されます。

ログ行は、「Received remote command to signal a manual update」という行で始まる必要があります。

```
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. 「Critical/Warning」メッセージがないか確認します。更新ログは非常に人間が読み取り可能なエラーです。おそらく、問題の原因を特定できます。

6.回答がない場合は、上記の手順の結果を含むシスコサポートのチケットをオープンできます。お客様は喜んでサポートいたします。

Webレピュテーションスコアはどのように計算されますか。

特定のWebサイトにスコアを割り当てるときに考慮されるパラメータの一部を次に示します。

- URL分類データ
- ダウンロード可能なコードの存在
- 長い難読化されたエンドユーザライセンス契約(EULA)の存在
- グローバルなポリシーとポリシーの変更
- ネットワーク所有者情報
- URLの履歴
- URLの経過時間
- すべてのブロックリストにプレゼンス
- 許可リストのプレゼンス
- 一般的なドメインのURLタイプ
- ドメインレジストラ情報
- IPアドレス情報

各レピュテーションカテゴリ (良、中立、低) のスコア範囲はどのくらいですか。

Webレピュテーション範囲とその関連アクション :

アクセス ポリシー

| -10 -6.0 | Block | occurs. | <ul style="list-style-type: none">• URL•• URL• URL. |
|-----------------|-------|------------|---|
| -5.9 5.9 | | DVS DVS | <ul style="list-style-type: none">• URL• ダイナミックIPアドレスを含む• ダウンロード可能なコンテンツ• IP• 正のWebレピュテーションスコア。 |
| 6.0 10.0 () | | | <ul style="list-style-type: none">• URL••• URL |

復号化ポリシー

| | | |
|--|--|--|
| | | |
|--|--|--|

| | | |
|-----------------|--------|--|
| -10 -9.0 | [Drop] | |
| -8.9 5.9 | | |
| 6.0 10.0 () | | |

シスコデータセキュリティポリシー :

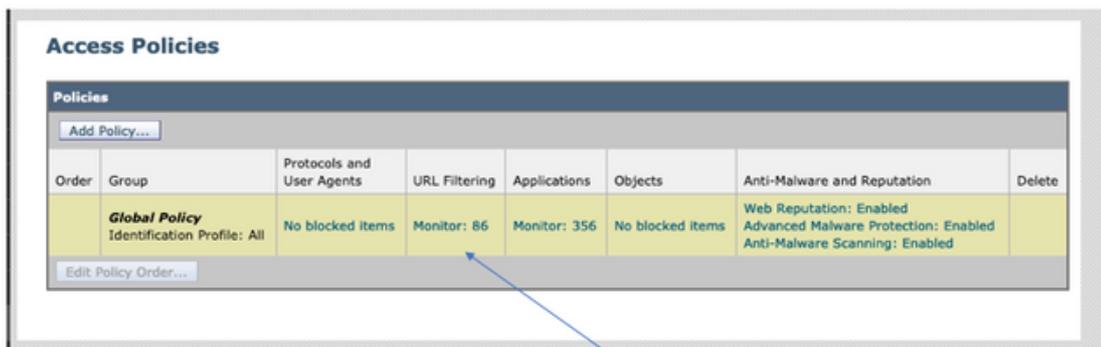
| | | |
|----------|-------|-----|
| | | |
| -10 -6.0 | Block | |
| -5.9 0.0 | | Web |

未分類のWebサイトの意味

未分類のURLは、シスコデータベースがカテゴリを確認するための十分な情報を持っていないURLです。通常、新しく作成されたwebサイト。

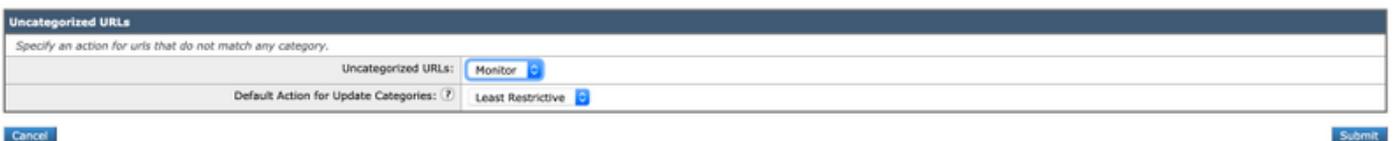
未分類のURLをブロックする方法

1.目的のアクセスポリシーに移動します。[Web Security Manager] -> [Access Policies] を選択します。



Click on the URL Filtering section in the required Policy

2. 「未分類URL」セクションまでスクロールします。



3.必要なアクション([モニタ(Monitor)], [ブロック(Block)], または[警告(Warn)]のいずれか)を選択します。

4.変更を送信し確定します。

データベースが更新される頻度

更新チェックの頻度は、CLIから次のコマンドを使用して更新できます。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:

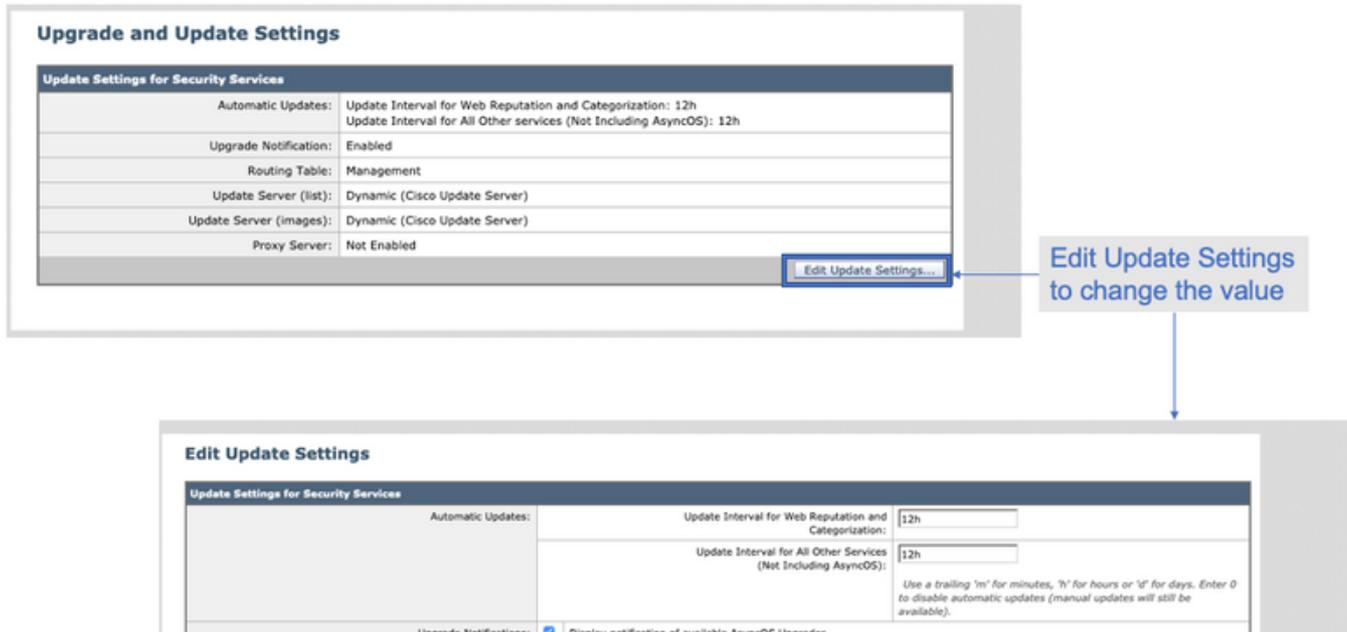
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates

[]>

注：上記の値は、アップデートをチェックする頻度を示していますが、レピュテーションや

その他のサービスに関する新しいアップデートをリリースする頻度を示すものではありません。アップデートはいつでも利用できます。

またはGUIから : [System Administration] -> [Upgrade and updates settings]。



URLをホワイトリスト/ブラックリストに登録する方法

十分な情報がないため、Cisco TALOSからのURLの更新に時間がかかることがあります。または、webサイトがまだ悪意のある動作の変更を証明していないため、レピュテーションを変更する方法はありません。この時点で、このURLをカスタムURLカテゴリに追加できます。このカテゴリは、アクセスポリシーで許可/ブロックするか、復号化ポリシーでパススルー/ドロップし、Cisco Webセキュリティアプライアンス(WSA)またはブロックによるスキャンまたはURLフィルタリングチェックなしでURLが配信されます。

URLをホワイトリスト/ブラックリストに登録するには、次の手順に従ってください。

1. カスタムURLカテゴリにURLを追加します。

GUIから、[Web Security Manager] -> [Custom and External URL Category]に移動します。



Reporting

Web Security Manager

Security Services

Upgrade and

Update Settings for

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

Custom and External URL Categories

Define Time Ranges and Quotas

Bypass Settings

L4 Traffic Monitor

Copyright © 2003-2018

al for Web Reputatic

al for All Other servi

co Update Server)

co Update Server)

ty Statement

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.Web

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
Sort URLs: Click the Sort URLs button to sort all site URLs in Alpha-numerical order.
Regular Expressions: (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)
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.([Web Security Manager] -> [Access Policies] -> [URL Filtering])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: 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.

Select Custom Categories...

6.ポリシーURLフィルタリング設定にポリシーカテゴリを含めます。

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

7.アクションを定義します。「ブロックリストにブロック」、「ホワイトリストに許可」です。URLがスキャンエンジンを通過するようにしたい場合は、Action as Monitorを保持します。

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 <input checked="" type="checkbox"/> | Select all | Select all | (Unavailable) | - |

Select Custom Categories.....

Cancel Submit

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

8.変更を送信し確定します。