TippingPoint™
5.0.0
URL Reputation Filtering Deployment and Best Practices Guide
## Contents

**Introduction to URL Reputation Filtering** ........................................................................................................... 1

Getting started ......................................................................................................................................................... 1

General requirements and restrictions .................................................................................................................. 3

Sources for URL reputation .................................................................................................................................. 3

  - ThreatDV URL Reputation Feed .................................................................................................................. 3
  - User-Defined URL Entries .......................................................................................................................... 5
  - Deep Discovery integration .......................................................................................................................... 6

**Deployment** .................................................................................................................................................... 7

Prerequisites .............................................................................................................................................................. 7

1. Manage your system .......................................................................................................................................... 7

   - Add a device .................................................................................................................................................. 7
   - Download and distribute DV packages ........................................................................................................ 7

2. Add a URL to the database ............................................................................................................................ 8

   - Specify URL criteria .................................................................................................................................. 8
   - Wildcards .................................................................................................................................................... 12

3. Configure your Inspection profile ................................................................................................................ 13

   - Create a URL Reputation filter ................................................................................................................. 13
   - Configure HTTP Context for the inspection profile ................................................................................. 14
   - Specify URL exceptions ............................................................................................................................ 15

4. Distribute an Inspection profile to segments ............................................................................................... 16

   - URL Reputation Filtering packages ........................................................................................................ 17
   - Policy package ........................................................................................................................................... 17
   - User-Defined URL Entries package ......................................................................................................... 17

**Best practices and use cases** .......................................................................................................................... 18
Configure for best performance........................................................................................................... 18
Monitor the reputations of URLs.......................................................................................................... 19
Avoid overblocking............................................................................................................................... 19
Add URL entries...................................................................................................................................19
Delete URL entries............................................................................................................................... 21
Import URL entries from a file............................................................................................................. 22
Manage URL entries............................................................................................................................ 24
Edit tag categories in URL entries.......................................................................................................25
Search for entries in the User-Defined URL Entries database............................................................26
View untruncated URLs........................................................................................................................27
HTTP mode.......................................................................................................................................... 27
SSL decryption..................................................................................................................................... 27
Manage the external drive................................................................................................................... 28
Preserve URL entries across a cluster................................................................................................ 28
Deep Discovery integration.................................................................................................................. 29
Filters with URL, DNS, and IP entries................................................................................................. 31
Web service calls................................................................................................................................. 31
CLI shortcuts.........................................................................................................................................32
Glossary................................................................................................................................................. 34
category................................................................................................................................................ 34
category settings...................................................................................................................................34
domain wildcard....................................................................................................................................34
maximum depth.................................................................................................................................... 34
Introduction to URL Reputation Filtering

URL filters are a type of reputation filter that provide a control to block access to websites. With URL filters, organizations have more granular reputation controls than reputation filters based merely on domains or IP addresses. For example, instead of blocking everything at www.mywebsite.com, URL Reputation Filtering can be configured to block only specific websites like www.mywebsite.com/malicious/stuff but still allow access to www.mywebsite.com/useful/information.

The targeted websites can come from a user-defined list of sites (User-Defined URL Entries database) or from a reputation feed (ThreatDV URL Reputation Feed), or both. Sites on the list are compiled based on their reputation rating from various sources (see Sources for URL reputation on page 3).

In addition, URL Reputation Filtering facilitates a deeper integration with Trend Micro Deep Discovery devices that are managed by the TippingPoint Security Management System (SMS).

With this enhanced management of Internet traffic, you can see the following improvements:

- Prevention of network infections, including malicious code and spyware
- Increased network user productivity
- Prevention of users from accessing inappropriate or high-security-risk sites
- More efficient use of network bandwidth and resources

Getting started

A URL Reputation Filtering policy begins much like a policy for DNS or IP reputation.

1. Create a reputation filter based on URL entries in the ThreatDV URL Reputation Feed or the User-Defined URL Entries database, or both.

2. After you add the URL filter to an inspection profile, distribute the profile to specified segments on the device.

3. When an HTTP request to or from any website within the ThreatDV URL Reputation Feed or the User-Defined URL Entries database matches the filter, the device either blocks or permits access to the site based on the filter's configured action set.

4. If traffic is permitted, digital vaccine (DV) inspection still occurs even though reputation inspection stops.

Figure 1 on page 2 graphically shows the steps that a device configured with URL Reputation Filtering takes when a user attempts to access a website.
Filters based on IP or DNS rules control access to everything (good and bad) at the site. Because of the increased granularity of URL Reputation Filtering, users who want to override entries in the ThreatDV URL Reputation Feed can create URL exceptions to blocked websites (users can create IP and DNS exceptions as well). However, IP and DNS rules supersede URL rules. So, for example, if a DNS rule is already set up to block www.mywebsite.com, a URL exception rule for www.mywebsite.com/exception would not be enforced because the DNS request occurs before the HTTP request. Even if the URL rule belongs to a higher-prioritized filter than the DNS rule, you would have to disable the DNS rule first for this URL exception to succeed.
General requirements and restrictions

Before you configure URL Reputation Filtering in a reputation profile, note the following prerequisites:

• Only the following Threat Protection System (TPS) devices running TOS v5.0.0 or later support URL Reputation Filtering:
  ◦ T Series TPS (440T and 2200T)
  ◦ TX Series TPS (8200TX and 8400TX)
  ◦ Virtual TPS (vTPS)

• Configuration can be accomplished only on TPS or vTPS devices that are managed by an SMS running version 5.0.0 or later.

• Both your SMS (version 5.0.0) and your TPS (TOS v5.0.0) require Digital Vaccine (DV) version 8990 or later.

• The HTTP Context (Hostname, URI, method) option must be enabled for your inspection profile. For more information, see Configure HTTP Context for the inspection profile on page 14.

  Note: If this option is disabled, any attempts to create a reputation filter that uses URL Reputation Filtering will generate an error. If a reputation filter with URL Reputation Filtering has already been configured and you attempt to disable this option, a confirmation dialog alerts you that URL Reputation Filtering will also be disabled.

• Access to a reputation database. See Sources for URL reputation on page 3.

Sources for URL reputation

Organizations compile their list of sites to block based on the security reputations of the URLs. The reputation of a URL can be defined by using one or a conglomeration of the following sources:

• ThreatDV URL Reputation Feed on page 3

• User-Defined URL Entries on page 5

• Deep Discovery integration on page 6

ThreatDV URL Reputation Feed

Because the threat status of a website can change continuously, you can rely on a feed from the Threat Digital Vaccine (ThreatDV) to keep your lists current. The ThreatDV feed contains a database of URLs considered to be malicious.
The ThreatDV URL Reputation Feed can be accessed on the TippingPoint Threat Management Center (TMC) at https://tmc.tippingpoint.com/ with a ThreatDV subscription and entitlement bundle. This feed is updated multiple times a day.

Every entry in the ThreatDV URL Reputation Feed has a score of 100 (malicious). Any score value you assign for your filter should be relative to that and include the value 100 in any of the following ways:

- \( =100 \) (equals 100)
- \( <=100 \) (less than or equal to 100)
- \( <100 \) – 100 (specifies a range between any number less than 100 and 100; an **Inclusive** checkbox enables you to include both the minimum value and the maximum value in the range.)

Ensure that your filter also satisfies the following requirements:

- The filter must be active.
- The URLs check box must be selected as Entry Criteria.
- Reputation DV Score is the only tag category selected.
When you configure your inspection profile, you can specify exceptions to this database. Exceptions prioritize the enforcement of one action set over another for a set of URLs; for example, a Permit action set over a Block or Quarantine action. For more information, see Specify URL exceptions on page 15.

User-Defined URL Entries

Specify your own criteria for blocking or permitting access to websites. The SMS loads this User-Defined URL Entries database to the external drive of the device for storage.

Use the following guidelines when adding URLs to the User-Defined URL Entries database.

- A maximum of 100,000 user-defined URL entries are supported for each managed device.

  **Note:** Because the SMS distributes entries across different devices, you can configure more than 100,000 user-defined URL entries on the SMS.

- A maximum of 10 URL Reputation filters is supported for each managed device.
• The domain name portion of the URL must consist of ASCII characters. Multibyte characters are supported after the domain name (that is, the path). The path portion of the URL is case-sensitive.

• You cannot add URLs that require users to specify credentials.

• The only schemes supported are http and https. Other schemes, such as ftp, are not supported.

• No user-defined URL entry can exceed 4k in length.

For more information, see 2. Add a URL to the database on page 8.

For more information on creating and configuring an inspection profile, see the SMS User Guide.

Deep Discovery integration

You can enable Trend Micro Deep Discovery Analyzer devices to update the User-Defined URL Entries database with high-risk URLs. When the Deep Discovery Analyzer device identifies a malicious URL, it sends the URL to the SMS where it gets added to the User-Defined URL Entries database.

For more information on integrating URL Reputation Filtering with Deep Discovery Analyzer devices, see Deep Discovery integration on page 29.
Deployment

Configuration for a URL filter is similar to configuration for an IP filter or DNS filter. Follow these basic steps:

1. Manage your TPS system on page 7
2. Add URL entries to the Reputation database on page 8
3. Configure your inspection profile on page 13
4. Distribute an Inspection profile to segments on page 16

Prerequisites

Ensure your environment meets the requirements specified in General requirements and restrictions on page 3.

1. Manage your system

To use Reputation profiles and filters, first manage your TPS or vTPS device on the SMS.

Note: When you add a device to the SMS, the SMS does not pull in any pre-existing URL Reputation Filtering configuration as part of device discovery. This configuration can only be passed from the SMS to the device, not from the device to the SMS. If you move a device with URL Reputation Filtering configured from one SMS to another, reset the URL Reputation Filtering on the device.

Add a device

Add a device (Devices > New Device) to the SMS so that you can track, control, and report on the traffic that passes through it; update the software and filters installed on it; and manage its network configuration.

Important: When you add a TPS or vTPS device, always distribute an inspection profile to all segments to begin protecting network traffic. By default, when you add a vTPS or TPS device, all filter categories are disabled in the Default security profile.

For more information on adding a device to the SMS, refer to the SMS User Guide.

Download and distribute DV packages

URL Reputation Filtering requires Digital Vaccine (DV) version 8990 or later. Both your SMS (version 5.0.0) and your TPS (TOS v5.0.0) must have this DV version. After a Digital Vaccine (DV) that supports URL Reputation Filtering has been activated, you cannot activate an older DV.

For information on how to download and distribute DV packages, refer to the SMS User Guide.
2. Add a URL to the database

You can choose to rely solely on a Threat Digital Vaccine (ThreatDV) feed to keep your lists current. For more targeted entries and deeper control, you can also define the criteria for your own URL entries. These entries are then added to the SMS Reputation Database using the same navigation that the administrators use for IP address entries or DNS entries.

Specify URL criteria

You can specify a URL as a tagged entry or as an untagged entry. Tagged entries provide more granular criteria, such as the ThreatDV score and your own score. Entries with tags provide more options for tracking and blocking suspicious traffic. Untagged entries contain only an address and function as a list of sites to track.

1. Select Profiles > Reputation Database > User Entries.
2. In the User Entries panel, click Add.
3. In the Create Reputation Entry dialog, click URL and specify the URL you want to add.
4. (Optional) Configure tag categories to narrow your entry.
   - To configure predefined categories, choose from the list of available tag categories.
     
     Note: When you use predefined categories, consider that the categories can be changed or removed altogether by subsequent ThreatDV updates.
   - To configure your own tag categories, click Add Tag Category. In the Create Tag Category dialog:
     a. Provide a name and type for your tag category.
     b. (Optional) Provide a description for your tag category.
     c. Configure the settings for the tag category type you selected. A tag category type can take one of the following forms:
        - **Text** – The most flexible type of tag category because it supports arbitrary text strings (maximum 255 characters). A text tag category can use the following operatives:
          
          ```
          = case sensitive
          = ignore case
          contains case sensitive
          contains ignore case
          ```
        - **List** – Narrows tags to a value that matches one of the items from the list of possible values defined in the tag category.
        - **Numeric range** – Confines a tag to any integer between a specified range; the minimum value is -2,147,483,648 and the maximum value is 2,147,483,647. A numeric tag category can use the following operatives:
          
          ```
          =
          ```
- **Boolean** – Narrows tags to a value that matches one of two possible values. For example, Yes or No, True or False. A Boolean tag category can only use the = operative.

- **Date** – Specifies a date or both a date and time. A date category can use the same operatives as a numeric tag category. The following table shows formatting options for August 9, 2009 3:04:08 PM CDT.

### Table 1. Format of date and time tag category

<table>
<thead>
<tr>
<th>Letter</th>
<th>Date/Time Component</th>
<th>Presentation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>Era designator</td>
<td>Text</td>
<td>AD</td>
</tr>
<tr>
<td>y</td>
<td>Year</td>
<td>Numeral (2 digits)</td>
<td>09</td>
</tr>
<tr>
<td>yy</td>
<td>Year</td>
<td>Numeral (2 digits)</td>
<td>09</td>
</tr>
<tr>
<td>yyy</td>
<td>Year</td>
<td>Numeral (2 digits)</td>
<td>09</td>
</tr>
<tr>
<td>yyyy</td>
<td>Year</td>
<td>Numeral (4 digits)</td>
<td>2009</td>
</tr>
<tr>
<td>M</td>
<td>Month</td>
<td>Numeral (no leading zero)</td>
<td>8</td>
</tr>
<tr>
<td>MM</td>
<td>Month</td>
<td>Numeral (leading zero)</td>
<td>08</td>
</tr>
<tr>
<td>MMM</td>
<td>Month</td>
<td>Text (abbreviated)</td>
<td>Aug</td>
</tr>
<tr>
<td>MMMM</td>
<td>Month</td>
<td>Text (full)</td>
<td>August</td>
</tr>
<tr>
<td>w</td>
<td>Week in year</td>
<td>Numeral</td>
<td>33</td>
</tr>
<tr>
<td>Letter</td>
<td>Date/Time Component</td>
<td>Presentation</td>
<td>Example</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------</td>
<td>--------------</td>
<td>---------</td>
</tr>
<tr>
<td>W</td>
<td>Week in month</td>
<td>Numeral</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>Day in year</td>
<td>Numeral</td>
<td>221</td>
</tr>
<tr>
<td>d</td>
<td>Day in month</td>
<td>Numeral (no leading zero)</td>
<td>9</td>
</tr>
<tr>
<td>dd</td>
<td>Day in month</td>
<td>Numeral (leading zero)</td>
<td>09</td>
</tr>
<tr>
<td>F</td>
<td>Day of week in month (e.g., 2nd Sunday)</td>
<td>Numeral</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>Day of week</td>
<td>Text (abbreviated)</td>
<td>Sun</td>
</tr>
<tr>
<td>EE</td>
<td>Day of week</td>
<td>Text (abbreviated)</td>
<td>Sun</td>
</tr>
<tr>
<td>EEE</td>
<td>Day of week</td>
<td>Text (abbreviated)</td>
<td>Sun</td>
</tr>
<tr>
<td>EEEE</td>
<td>Day of week</td>
<td>Text (full)</td>
<td>Sunday</td>
</tr>
<tr>
<td>a</td>
<td>AM/PM indicator</td>
<td>Text</td>
<td>PM</td>
</tr>
<tr>
<td>H</td>
<td>Hour of day (0–23); midnight displayed as 0</td>
<td>Numeral</td>
<td>15</td>
</tr>
<tr>
<td>k</td>
<td>Hour of day (1–24); midnight displayed as 24</td>
<td>Numeral</td>
<td>15</td>
</tr>
<tr>
<td>K</td>
<td>Hour in AM/PM (0–11); midnight and noon displayed as 0</td>
<td>Numeral</td>
<td>3</td>
</tr>
<tr>
<td>Letter</td>
<td>Date/Time Component</td>
<td>Presentation</td>
<td>Example</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------</td>
<td>--------------</td>
<td>---------</td>
</tr>
<tr>
<td>h</td>
<td>Hour in AM/PM (1–12); midnight and noon displayed as 12</td>
<td>Numeral</td>
<td>3</td>
</tr>
<tr>
<td>m</td>
<td>Minute of hour</td>
<td>Numeral (no leading zero)</td>
<td>4</td>
</tr>
<tr>
<td>mm</td>
<td>Minute of hour</td>
<td>Numeral (leading zero)</td>
<td>04</td>
</tr>
<tr>
<td>s</td>
<td>Second of minute</td>
<td>Numeral (no leading zero)</td>
<td>8</td>
</tr>
<tr>
<td>ss</td>
<td>Second of minute</td>
<td>Numeral (leading zero)</td>
<td>08</td>
</tr>
<tr>
<td>S</td>
<td>Millisecond of minute</td>
<td>Numeral (no leading zero)</td>
<td>7</td>
</tr>
<tr>
<td>SS</td>
<td>Millisecond of minute</td>
<td>Numeral (leading zero)</td>
<td>07</td>
</tr>
<tr>
<td>z</td>
<td>General time zone</td>
<td>Text (abbreviated)</td>
<td>CDT</td>
</tr>
<tr>
<td>zz</td>
<td>General time zone</td>
<td>Text (abbreviated)</td>
<td>CDT</td>
</tr>
<tr>
<td>zzz</td>
<td>General time zone</td>
<td>Text (abbreviated)</td>
<td>CDT</td>
</tr>
<tr>
<td>zzzz</td>
<td>General time zone</td>
<td>Text (full)</td>
<td>Central Daylight Time</td>
</tr>
<tr>
<td>Z</td>
<td>Time zone</td>
<td>RFC 822 time zone</td>
<td>-0500</td>
</tr>
</tbody>
</table>

All of the different tag categories share the following search options:

- Tag is present and has a value.
- Does not have this tag.
The following examples show user-defined tag categories that you can apply to your URL entries:

- Malicious = Y/N
- Color-coded entries = Red/Yellow/Green
- EnteredBy = IP address of user or free-form text up to 255 characters
- MyScore = Numeric value ranging from 1 to 100

Wildcards

Wildcards can be used for both user-defined URLs entries and exceptions that you want to add. Use the following guidelines when configuring wildcards:

- You can use a single wildcard string: `\*`
  
  **Note:** Because the `*` character is a valid URL character, when used as a wildcard it must be escaped with a backslash (`\`), which is an invalid URL character.

- The wildcard can occur only at the beginning (domain wildcard on page 34) or end (path wildcard on page 35) of the URL, or both.

- A domain wildcard must be followed by a slash (`/`), after which the path starts. Domain wildcards cover both `http://` and `https://`.

  **Note:** A domain wildcard can apply only to the domain portion of the URL and not to the path. For example, `\*/start/\*` would match `http://www.mywebsite.com/start/path/to/resource` but will not match `http://www.mywebsite.com/now/start/path/to/resource`.

- A path wildcard must always be preceded by a slash (`/`), which separates path elements.

- By default, the SMS enforces a maximum of 12 slashes (`/`) that can precede a wildcard in a URL path. This limitation is called the maximum depth on page 34. The number of characters between slashes does not matter. For example,

  - `http://mywebsite.com/eighteen/nineteen/\*` has the same depth as
  - `http://mywebsite.com/x/y/\*`
  
  because each URL has three slashes that precede the wildcard in the path.

**Example**

Each of the following wildcard examples successfully matches URL `http://mywebsite.com/path/to/resource`:

- **Domain wildcard usage:** `\*/path/to/resource`
- **Path wildcard usage:** `http://mywebsite.com/\*`
• Path wildcard usage: http://mywebsite.com/path/*
• Path wildcard usage: http://mywebsite.com/path/to/*
• Both domain and path wildcard usage: */path/*
• Both domain and path wildcard usage: */path/to/*

3. Configure your Inspection profile

After your entries have been added to the User-Defined URL Entries database, configure an inspection profile to monitor the websites.

Use the following topics to configure an Inspection profile:

• Create a URL Reputation filter on page 13
• Configure HTTP Context for the inspection profile on page 14
• Specify URL exceptions on page 15

For more information on creating and configuring an inspection profile, refer to the SMS User Guide.

Create a URL Reputation filter

2. Click New Reputation to create a new reputation filter.
3. Enter a filter title in the Name field, and then select the Locked check box if you want to prevent the ability to edit the filter.
4. Select the appropriate action from the Action Set drop-down list, and select the Enabled check box to enable the filter. If you clear this check box, the reputation filter will not be distributed to the device.
5. (Optional) Provide a brief description or comment about the reputation filter in the Comments field.
6. Click Entry Selection Criteria and specify the following items:
   a. Entry Criteria — Select URLs to include URL address entries from both the ThreatDV URL Reputation Feed and the User-Defined URL entries in the filter.
   b. Tag Criteria — Select the type of entries (tagged or untagged) to include in the filter and then select the check box next to any tag category you want to include. For more information on tags, see Specify URL criteria on page 8.

   Note: If the tag criteria contains Does not have this tag, when you distribute the profile, the SMS sends all entries that do not have this tag category to the device including ThreatDV, geographic, and user-provided entries.
7. Click OK.
Configure HTTP Context for the inspection profile

Configure your Reputation profile to generate events with URL data using the following steps.

**Note:** URL Reputation Filtering requires that the HTTP Context option is selected. If this option is disabled, any attempts to create a reputation filter that uses URL Reputation Filtering will generate an error. If you attempt to disable this option on a profile that already has this configured, a confirmation dialog alerts you that URL Reputation Filtering will also be disabled.

1. From the Profiles navigation pane, expand **Inspection Profiles** and select [profile_name].
2. In the Details tab, click **Edit Details**.
3. Select **HTTP Context (Hostname, URI, Method)**.

   ![Figure 3. Enable HTTP Context](image)

4. Click **OK** to configure the profile to extract HTTP metadata from the filter alerts.
Specify URL exceptions

If a URL filter blocks a website that you do not want blocked, you can create a URL exception. Any URL you add as an exception will not get matched to the URL filters in the profile. When you create an exception, your action sets for that entry take precedence over action sets that the ThreatDV URL Reputation Feed has configured for the entry.

Note: Exceptions apply to all filters in the profile.

When you create URL exceptions, remember that IP addresses and DNS host names take precedence. For example, if your DNS rule blocks www.mywebsite.com, you cannot create a URL exception rule for www.mywebsite.com/exception, because DNS filtering preempts the URL lookup. This is true even if the URL rule belongs to a higher-prioritized filter than the DNS rule.

1. From the Profiles navigation pane, expand Profiles > Inspection Profiles > [profile_name] > Reputation/Geo.

Caution: Scan your network hosts before disabling or creating exceptions to specific attack protection filters. Some operating systems install default services that might be vulnerable to attack. If you disable or add an exception to a filter that protects a service that you do not know about, you might increase your network vulnerability.

2. Click the Reputation URL Exceptions tab.

3. Do one of the following:
   • To edit an existing URL exception, select a URL and click Edit.
   • To create a new URL exception, click Add.

4. (Optional) Select Locked if you want to lock the settings.

5. Type the URL exception in the URL field.
Exceptions can contain the single \* wildcard string only at the beginning or end of the URL, or both. For more information on wildcards, see *Wildcards* on page 12.

6. Click **OK**.

To view a list of all Reputation exceptions available for distribution, select **Profiles > Inspection Profiles > [profile_name] > Profile Overview** and select the Reputation Exceptions tab.

### 4. Distribute an Inspection profile to segments

**Note:** When you enter a significant number of changes to filters within a profile, the period of time required for distributing the profile increases. If you unsuccessfully distribute profiles due to time-out, contact a TippingPoint technical support representative to assist in extending the time-out setting for your profile distribution needs.

1. Select **Profiles > Inspection Profiles**.
2. Select a profile, and click **Distribute**.
3. To distribute the profile to inspection segments:
a. In the Targets section, select the **Inspection Segments** tab.
b. To Allow Segment Selection, choose one of the following items from the **Organize By** drop-down box:
   - **Segment Group**
   - **Device**
c. Select the appropriate group(s).

4. For a high priority distribution, select the **High Priority** check box.

**URL Reputation Filtering packages**

During a package distribution, the SMS uploads two packages to the device:

- **Policy package** on page 17
- **User-Defined URL Entries package** on page 17

**Policy package**

The first package the SMS uploads to the device is the Policy package. This package contains profile information, including URL filters, in addition to any existing IP and DNS filters. New and updated Reputation filters are integrated into your existing reputation policy.

**User-Defined URL Entries package**

After the Policy package is uploaded, the SMS automatically determines if it must also upload and install the User-Defined URL Entries package.

This package contains the User-Defined URL Entries database (an xml file) and administrative files. All entries in this database contain criteria, such as reputation score, source, and custom categories. URL filters use this criteria to determine which actions to take on specific URLs.

For example, you can set all URLs tagged as `Malicious=Yes` to a **Block** action set. Or you can tag specific URLs in the database with exception criteria and then create a rule that permits matching traffic with a **Permit + Notify** action set.

The SMS installs the package and associates entries in the database to matching filters the same way it does for IP and DNS reputation.

**Note:** User-Defined URL Entries are part of the same Reputation Database on the SMS as IP and DNS entries but are sent separately. IP and DNS have their own separate distribution tasks. Updates to the User-Defined URL Entries package get distributed along with the profile. The synchronization tasks for updated URL entries are displayed under the Activity tab on the Reputation Database screen.
Best practices and use cases

Use the following topics for tips and recommended configuration guidelines so that you get the best use of URL Reputation Filtering.

- **Configure for best performance** on page 18
- **Monitor the reputations of URLs** on page 19
- **Avoid overblocking** on page 19
- **URL database management**
  - *Add URL entries* on page 19
  - *Delete URL entries* on page 21
  - *Import URL entries from a file* on page 22
  - *Manage URL entries* on page 24
  - *Edit tag categories in URL entries* on page 25
- **Search for entries in the User-Defined URL Entries database** on page 26
- **View untruncated URLs** on page 27
- **HTTP mode** on page 27
- **SSL decryption** on page 27
- **Manage the external drive** on page 28
- **Preserve URL entries across a cluster** on page 28
- **Deep Discovery integration** on page 6
- **Filters with URL, DNS, and IP entries** on page 31
- **Web service calls** on page 31
- **CLI shortcuts** on page 32

**Configure for best performance**

When configuring URL Reputation Filtering, be aware of the following factors that can affect performance.

*Packet loss and blocked streams*
URL Reputation Filtering can sometimes lead to packet loss and dropped streams. TCP attempts at retransmission can lead to network congestion and reduced throughput. However, blocking high-risk sites generally improves both the security and performance of your network.

**Wildcards**

A URL path can have a maximum depth of 12 slashes (/) preceding a wildcard. Even with this limitation, any user-defined URL that has a multi-element path with a wildcard will impact performance. This is because a query must be performed for each path element to determine whether it has the wildcard. The closer to the maximum depth that the wildcard occurs, the bigger the impact on performance.

For more information on wildcards, see *Wildcards* on page 12.

**User-Defined URL Entries**

The number of entries in the User-Defined URL Entries database will have a negligible but increasing effect on performance.

A maximum of 100,000 user-defined URL entries and 10 URL Reputation filters are supported for each managed device.

**Monitor the reputations of URLs**

The reputation of websites can change frequently. To avoid the task of monitoring the status of thousands of websites, you can entrust TippingPoint Digital Vaccine threat intelligence to stay current with ever-evolving internet environments and emerging threats. URL Reputation Filtering is licensed as part of Threat Digital Vaccine (ThreatDV). Users who buy a subscription to ThreatDV will now get both the IP and DNS Reputation feeds and the ThreatDV URL Reputation Feed. The ThreatDV package includes:

- Protection against the latest advanced malware threats
- Reputation feeds that are updated multiple times a day
- Continuous analysis and re-evaluation of reputations based on activity, source, category, and threat.

**Avoid overblocking**

Because the determination of whether URL traffic matches a particular filter involves hashing, false positives occasionally occur. When false positives occur, "safe" URLs get inadvertently blocked. When this interferes with critical applications, inconvenienced users can overwhelm IT with support tickets.

False positives happen rarely and can be resolved by specifying exceptions. For more information, see *Specify URL exceptions* on page 15.

**Add URL entries**

A URL is a string comprised of characters, both reserved and unreserved, defined by RFC standards.
Many different strings can represent the same URL. Normalization on page 34, a background process that transforms a URL into its canonical format, enables a filter's action set to apply to all strings that represent the same URL. For example, a user can enter either:

http://mywebsite.com/

or

http://mywebsite.com/%25

Both will get normalized as http://mywebsite.com/%25.

This functionality is stored in the device software and gets shared with the SMS. Before saving URLs to the database, the SMS attempts to decode and normalize them.

**General guidelines**

- The only schemes supported are http and https. Other schemes, such as ftp, are not supported.
- You cannot add URLs that include credentials, such as username and password.
- No user-defined URL entry can exceed 4k in length.
- Some entries can be the result of a third-party product that abbreviates a much longer, cumbersome URL so that it can be more easily shared. Because these URLs are merely masks that redirect to the original URL, any action set applied to the smaller URL will also apply to its longer version—provided that the longer, original URL is less than the maximum 4k limit.

**Syntax guidelines**

- Because the asterisk (*) character is a valid URL character, escape it with a backslash (\) whenever you use it as a wildcard. For more information on wildcards, see *Wildcards* on page 12.
- The domain name portion of the URL is not case-sensitive. The path portion of the URL is case-sensitive.
- Avoid URLs with multiple forward slashes in a row.
- Both absolute and relative URLs are supported and will be normalized. A slash (/) at the end of a URL path is normalized to be the same as a path that does not end in a slash.
- For entries that contain query strings, URL Reputation Filtering only works with an exact match. For example, a database entry of http://mywebsite.com/path/to/resource?a=4 yields the following results:
  - **Filter match** – http://mywebsite.com/path/to/resource?a=4
  - **No filter match** – http://mywebsite.com/path/to/resource
  - **No filter match** – http://mywebsite.com/path/to/resource?a=5
Similarly, traffic URLs with query strings must explicitly match an entry in the database in order for filtering to take affect. For example, a database entry of http://mywebsite.com/path/to/resource yields the following results:

- **Filter match** – http://mywebsite.com/path/to/resource
- **No filter match** – http://mywebsite.com/path/to/resource?a=4
- **No filter match** – http://mywebsite.com/path/to/resource?a=5

A wildcard string (\*) cannot be used as a query string. For example, the following use of the wildcard string is not permitted:

| http://mywebsite.com/path/to/resource?\* |

As a workaround, you can use the wildcard string earlier in the path:

| http://mywebsite.com/path/to/\* |

### Import guidelines

- The file can contain only URL entries.
- For URL entries, the import file must be delimited by a pipe (|) instead of commas, and entries can be URLs only or URLs with one or more associated tags.
- If the import results in errors, the SMS displays which specific entries were in error. The SMS also provides a correct count of the valid entries that were successfully imported. As a best practice, do not import a file with more than 10,000 entries.

  **Note:** The SMS ignores any invalid entries imported from a file.

- For detailed information on importing entries from a file, see [Import URL entries from a file](#) on page 22.

For more information, see [Specify URL criteria](#) on page 8.

### Delete URL entries

Entries in the ThreatDV URL Reputation Feed are read-only and cannot be modified. Only User-Provided URL Entries can be modified. If you find that a URL entry in the feed is being reported as malicious and you know that this information is incorrect, you can submit a correction by contacting the Trend Micro Technical Assistance Center (TAC).

To bypass URL entries in the feed, create a list of exceptions in your profile. For more information, see [Specify URL exceptions](#) on page 15.

You can delete entries in the User-Provided URL Entries database one-at-a-time or all at one time.

**To delete single entries in the User-Provided URL Entries database:**

1. Select **Profiles > Reputation Database > Search Entries** in the navigation pane.
2. Enter the criteria of the URL entry you want removed, and click **Search**.
3. Select the entry from the results panel and click Delete.

Alternatively, you can remove single entries using the web API. For more information, see Web service calls on page 31.

**To delete all of the URLs in the User-Provided URL Entries database at one time:**

1. Select Profiles > Reputation Database > User Entries in the navigation pane.
2. Click Delete All to remove all URLs in the database.

**Import URL entries from a file**

You can create a file that contains the information you want to add to the Reputation Database. The import file must be delimited by a pipe (|) instead of commas, with each line made up of one or more fields separated by pipes.

**Use the following guidelines when you import data to the Reputation Database.**

**Format rules:**

- **File contents** – The file can contain only URLs. Mixing in IPv4/IPv6 addresses and DNS domain names is not permitted.
- **Maximum number of entries** – Limit the total number of entries in one file to 10,000 or less.
- **Syntax** – The import file must have each line consisting of one or more fields separated by pipes (#). The RFC defines these unreserved characters: `- . _ ~`
  - The RFC defines these reserved characters: `/ ? : # [ ] @ ! $ & ' ( ) * + , ; =`
  - All other characters are invalid.
  - Any URL entry with a space in it will get the space converted to a + by the normalization process.
  - Any URL entry with a pipe (|) in it must have the pipe character escaped with a backslash (\). For example, to import the following URL with pipes in its syntax:
    - http://mywebsite.com/index.htm?today=Thurday\|weather=sun\|degree=25
    - you must enter it in the file for importing as:
    - http://mywebsite.com/index.htm?today=Thurday\|weather=sun\|degree=25
    - When a pipe is used as a delimiter in a URL's embedded text, it does not need to be escaped with a backslash:
    - http://fileImporttagsWithPipe.com/index.htm?today=Thursday\|weather=sun\|degree=25|BlackList|True|Description|Embedded pipe char \| is contained in the description
  - Each line represents one entry, and entries must not span lines.
  - The first field on each line must be the URL name for that entry. The remaining fields on a line are optional. If present, remaining fields are processed as tag category/tag value pairs.
Any line that has a first non-white space character of “#” is considered a comment. Comment lines are discarded during import. There is no support for inline comments.

The import file cannot contain any blank lines within the body; blank lines after the last line are ignored.

To represent a double-quote character within a quoted value, use two double-quotes.

- **Valid URL entry example** – The following example shows a valid URL entry:
  
  ```
  http://www.mywebsite.jp|BlackList|true|EnteredBy|Arnold
  ```

**Tag category rules:**

- **Prerequisites** – Any tag categories that appear in the import file must exist on the SMS prior to the import.

- **Case-sensitive** – Except for yes/no tag categories, character case is significant in all tag category names and tag values.

- **yes/no categories** – For yes/no tag categories, the text *yes*, regardless of case, denotes a *yes* value. All other values are considered *no*.

- **Empty fields** – Empty pairs of fields are ignored. If a tag category field is empty, an error occurs and the entry is not imported. If a tag value field is empty, the corresponding tag category is discarded and the next field of the entry is processed; it is equivalent to the tag category not appearing on that line at all.

- **Consistency** – Tag category/value pairs need not appear in the same order on each line. It is not necessary that every entry specify every tag category, or even the same tag categories as other entries in the file.

- **Invalid entries** – If a category does not exist or if the value does not match the category type (for example, 123 for a Boolean tag category), the upload process fails.

- **Valid tag entry examples** – The following examples show valid tag entries in a URL entry:
  
  ```
  http://www.mywebsite.com|Colors|Green|MyScore|80|EnteredBy|Doctor Who
  http://fileImporttagsWithPipe.com/index.htm?today=Thursday\ |weather=sun\ |degree=25| BlackList|True|Description|Embedded pipe char \| is contained in the description
  ```

**To import URL entries from a file:**

1. Select **Profiles > Reputation Database > User Entries**.
2. Click **Import**.
3. Specify the path of the file you would like to import, or click **Browse** and select the file.
4. Click **Next** to upload the file.
5. From the Import Reputation Entries dialog, select **URL** as the type of entries in the import file and then click **Next**.
6. Specify the tags to use with the imported entries.

- Import tags from file — Indicates that tags in the import file should be applied to imported entries.
- Specify tags to apply to all imported entries — Select this option to display a screen from which you can choose the tags, and their values, to apply to imported entries.
- Import tags from file and specify tags to apply to all imported entries — Select this option to apply both tags from the import file and tags you select from the next screen to imported entries. Conflicts are handled according the setting of the User-specified tags override tags from import file option.
- User-specified tags override tags from import file — This option is available only when the Import tags from file and specify tags to apply to all imported entries option is selected. This item specifies how to handle tags in the file and tags you specify on the next screen that have the same name. If this option is selected, tags you select on the next screen will take precedence over tags from the import file. If this option is not selected, tags from the file will take precedence over tags you specify on the next screen.

Manage URL entries

The SMS supports an unlimited number of user-provided entries to the Reputation Database.

The time it takes before users begin to see their imported entries appear on the SMS depends on the following factors:

- The number of user entries being added.
- The number of user entries that already exist.
- The congestion of the reputation processing queue.
- The interval that you set for how often the SMS polls the User-Defined URL Entries database for updates and distributes them. Specify this interval from the Database Synchronization Editor dialog (Profiles > Reputation Database > User-Provided Entries > User-Provided Settings > Edit):
Changes to anything in the Reputation Database on page 35 are automatically synchronized to devices which have reputation filters active. URL entries in the User-Provided URL Entries database can also be updated by manually performing a full sync. A full sync is only needed for recovery purposes and is usually done with assistance from the Technical Assistance Center (TAC). When a full sync is performed, all reputation entries, including IP, DNS, and URL, are synced at one time.

A manual sync accomplishes everything that an automatic sync from the TMC does. For more information on performing a full sync, refer to "Perform a full synchronization of the Reputation Database" in the SMS User Guide.

For more information on setting the synchronization interval, refer to "Set the synchronization interval of the User-Defined URL Entries" in the SMS User Guide.

**Edit tag categories in URL entries**

You can repeatedly add an entry in the User-Defined URL Entries database with different tag values. Each time you click Add, all the different tag values for the URL entry merge.
If you specify new tag values for the URL entry and then click **Update**, your latest tag values replace the tag values that were previously configured.

**Note:** Tag categories created by the ThreatDV URL Reputation Feed are read-only and cannot be modified.

1. Select **Profiles > Reputation Database > Search Entries**.
2. From the list of entries, select a user-defined entry whose tag categories you want to change and click **Edit** to enter new tag values.
3. Do one of the following:
   - Click **Update** to replace your tag category settings.
   - Click **Add** to merge your tag category settings with your previously configured settings.

### Search for entries in the User-Defined URL Entries database

Use the following guidelines to perform searches within the User-Defined URL Entries database.

**Note:** This topic describes searching for user-defined URLs. A search of the ThreatDV URL Reputation Feed (**Profiles > Reputation Database > ThreatDV URL Lookup**) is limited only to checking whether a URL is present or not. If the URL is present, the Reputation DV score is provided.

Searches of the User-Defined URL Entries database can be one of the following categories:

- **Simple search** — Searches for entries with only one tag category. For example: `FoundOn = <date>`.
- **Compound search** — Searches for entries with many tag categories. For example: `Malicious = true and MyScore is present and has a value`.

**To search the User-Defined URL Entries database:**

**Note:** Searches are not case-sensitive.

1. Select **Profiles > Reputation Database > Search Entries**.
2. In the Entry Criteria panel, click the **URL** check box. To search for an exact sequence of characters or path elements, enter the text in the URL field and select the **Exact Match** check box.
3. For Tag Criteria to include in the search, use the check box next to the name of the tag category to include it in the search criteria. Use the expanded view to add specific tag search criteria. For more information on tag categories, see *Specify URL criteria* on page 8.
4. Select one or more tag categories to include in the search. When you select a tag, the default criteria is **Tag is present and has a value**.
5. To select other criteria, expand the entry and select the applicable criteria.
6. Click **Search**.

**Note:** The SMS can display only a maximum of 10,000 matches per search. If you also specify IP Address and DNS Domain as entry criteria, the SMS displays those matches before it displays URL matches. To ensure that your search displays any URL matches within the 10,000-match limit, be as specific as possible in your search criteria.

### View untruncated URLs

Because a 255-character limit of entries in the Reputation logs also exists, the logs truncate long entries by appending an ellipses (…) after the 255-character limit is reached. This is necessary for readability and retrievability. To see the full URL in such cases, do one of the following:

- From the SMS, double-click the log entry and view the complete metadata.
- From the LSM, download the log to view the complete metadata.
- From the CLI, enter the `tab` option to view the complete metadata. For example:

```
show log-file reputationAlert tab
```

### HTTP mode

HTTP mode enables all TCP ports to be treated as HTTP ports for inspection purposes. Typically, this feature is enabled only on devices that primarily handle HTTP traffic. If a flow does not have HTTP traffic, HTTP processing stops so that optimum performance is maintained.

URL entries that are added to the User-Defined URL Entries cannot specify port numbers. Because of this constraint, URL Reputation Filtering monitors the system ports in specific ways. For example, if an administrator wants to add `http://www.mywebsite.com/a/b/c` as a user-defined URL in the database, the way port monitoring is handled depends on the following scenarios:

- If HTTP mode is enabled, URL Reputation Filtering attempts to match that URL on HTTP traffic coming from any port.
- If HTTP mode is **disabled**, URL Reputation Filtering attempts to match that URL on HTTP traffic coming from ports 80, 3128, 8000, 8080, and from any ports that the administrator has defined for the HTTP service.

### SSL decryption

URL Reputation filtering works within the decrypted flow of inbound SSL traffic for the HTTPS protocol.
Manage the external drive

T Series TPS devices use an external CFast card for storage. TX Series TPS devices use an external solid state disk (SSD) for storage. Because the URL databases are stored on these external drives, URL Reputation Filtering stops whenever you unmount, format, and remove the drives.

When the external drive is reformatted or the encryption status changes, all URL data on the drive will be lost. Users must redistribute the ThreatDV URL Reputation Feed and the User-Defined URL Entries to the device before URL Reputation filtering can be enabled again.

When you unmount the external drive, a system log warning informs you that all access to URL databases, including both the ThreatDV URL Reputation Feed and the User-Defined URL Entries, will be lost. If you must remove and replace the external drive, follow these guidelines:

- To avoid disk corruption and to preserve the data stored on these drives, use the command line interface (CLI) to first unmount the drive before you remove it. For more information on the removal and installation of external drives, consult your product hardware installation or CLI documentation at: https://tmc.tippingpoint.com/TMC

- Always reformat an external drive from one device before you mount it into another device.

- The T Series CFast card supports 8 GB of storage. The TX Series SSD supports 32 GB of storage. By default, 3.5 GB is reserved on the external storage drives to support the Reputation databases. If this storage space ever needs to be reconfigured, use the following command:

```
log-storage externalReserve RESERVESIZE [MB]
```

**Note:** The reserved space used to store the Reputation database is sufficient for most operating environments. Change the size of this reserved space only when rare circumstances require it. Reducing the reserved space can interfere with URL Reputation Filtering. Conversely, you cannot increase the reserved space to more than one half of the entire drive space.

Preserve URL entries across a cluster

In an SMS high availability cluster, any URL entries that are added, updated, or deleted from the Reputation database can be shared between the primary server and the passive server.

To preserve any updates to the Reputation database across an SMS cluster, make sure that the Include historical event data check box is selected in the SMS High Availability Wizard (Admin > High Availability > Configure).
Deep Discovery integration

With Deep Discovery Analyzer devices, threat intelligence and insights can be shared with other TippingPoint devices. The ability of a Deep Discovery Analyzer device to detect and analyze high-risk URLs in real time and feed them into the User-Defined URL Entries database provides an extra area of protection for your network.

1. Ensure your Deep Discovery Analyzer device is in communication with the SMS.
   
   For more information, see "Configure URL Threat Analysis" in the SMS User Guide.

2. Configure URL Threat Analyzer:
   
   a. Select Events > URL Threat Analysis.
   
   b. From the URL Threat Analyzer Configuration pane, click Edit.
   
   c. In the URL Threat Analyzer Configuration dialog, select the Add High Risk Analysis Results to URL Reputation Database check box and click OK.
3. Configure an Inspection profile with a URL filter that has criteria of Trend Micro Severity is High.

The following figure shows a profile, URL-Filtering, with URL as a source and with criteria as Trend Micro Severity is High.

**Figure 7. URL Reputation Filtering inspection profile**

The SMS syncs any entries matching this expression to managed devices.

Any traffic that matches an entry triggers an event, and the event information gets sent to the Deep Discovery Analyzer device for analysis.

If the analyzed entry is assigned a High severity, it gets automatically added to the User-Defined URL Entries database.

**Figure 8. Entry added to database**

**Important:** The point at which you set the high-risk analysis feature on the Deep Discovery Analyzer device affects which URLs get automatically added to the User-Defined URL Entries database by the SMS. Only new URLs that the Analyzer device had not inspected prior to the feature being enabled get automatically added to the database. Any URLs that the Analyzer device inspected before the high-risk analysis feature was enabled have to be manually added to the database.

When a URL entry matches criteria in the Reputation filter, that entry gets synced to the managed devices. The configured action set will be applied.
Filters with URL, DNS, and IP entries

URL Reputation filtering is configured and enforced much the same way Reputation filters are prioritized. IP rules take precedence if the IP address is your DNS server, or if an IP Reputation entry blocks access to a hostname that is otherwise permitted by a DNS request.

Unless cached, DNS requests also happen before HTTP requests. For DNS Reputation rules to be enforced, the managed device must be positioned somewhere in the network where it can see DNS traffic.

You still have the option to match domain names even if DNS entries are cached or if the managed device cannot see DNS traffic because of its position in the network. URL Reputation Filtering enables you to set a profile attribute to enforce DNS Reputation in HTTP requests. This way, a DNS Reputation Filter can identify a specific DNS in normal HTTP traffic without having to perform a DNS Server request.

2. Click Edit Settings.
3. In the Edit Reputation Settings dialog, select the checkbox under Reputation Enforcement Options.

Note: When this option is selected, you can verify whether URL Reputation Filtering matched something because of the DNS filter or the URL filter by checking the logs.

Web service calls

You can programmatically interface with the SMS using the web API. You must have HTTPS or HTTP service available in order to send API requests to the SMS. By default, HTTPS service to the SMS is enabled.

The Reputation rep servlet, which enables you to use the web API to manage the SMS reputation database, now supports URL values as input from the web service.
Use the following rep servlets to interface with the SMS Reputation database:

**Import reputation entries**

```
repEntries/import
```

Uploads a file (one file at a time) with one or more reputation entries. For example, to import a file with URL entries to the SMS:

```
curl -v -k -F "file=@/path/to/file.csv" "http[s]://<sms_server>/repEntries/import
  ?smsuser=<user_name>&smspass=<password>&type=url"
```

**Add reputation entries**

```
repEntries/add
```

Creates one or more reputation entries. For example, to add a URL reputation entry with tag categories MalwareUrlType:

```
curl -v -k "http[s]://<sms_server>/repEntries/add
  ?smsuser=<user_name>&smspass=<password>&url=http://abc.com/tomorrow
  &TagData=CreatedDate,"Jan 22, 2014"
```

To add URL entries using a file import:

```
curl -v -k -F "file=@/home/isaac/Downloads/TestData/testadd.csv"
  "https://vsmsdev90/repEntries/import?smsuser=labuser&smspass=test99**&type=url"
```

**Delete reputation entries**

Deletes one or more reputation entries using a file import. For example, to delete URL entries using a file import:

```
curl -v -k -F "file=@/home/isaac/Downloads/TestData/testdelete.csv"
  "https://vsmsdev90/repEntries/delete?smsuser=labuser&smspass=test99**&type=url"
```

**Query reputation entries**

```
repEntries/query
```

Searches the reputation database for one or more reputation entries. You can specify up to 10,000 entries in a single request. For example, to query multiple URL entries:

```
curl -v -k "http[s]://<sms_server>/repEntries/query
  ?smsuser=<smsusername>&smspass=<smspassword>&url=http://abc.com/tomorrow
  &url=http://abc.com/today"
```

For more information on the Reputation web API—including best practices, syntax parameters and rules, and examples—refer to the *Security Management System Web API Guide*.

**CLI shortcuts**

Use the following TPS CLI debug commands to get information on URL Reputation entries:

- To collect information about the User-Defined URL Entries:
To query the User-Defined URL Entries for filters that match a specified URL:

```
device{}debug reputation user-url-db list-filters <url>
```

**Note:** If a URL has a space in it (for example, `http://domainname.com/image 1.jpg`), you must put double quotes around the URL when using the debug reputation command to query it:

```
device{}debug reputation user-url-db list-filters "http://mywebsite.com/image 1.jpg"
```

To display URL Reputation activity on the device:

```
device{}debug np stats show npUrlReputationStats
```

To get an indication of how many URL entries are present and how many entries match each URL Filter:

```
device{}debug reputation user-url-db stats
```

To normalize URLs:

```
device{}debug reputation normalize-url "<url>"
```
Glossary

category
An organizational classification system for DV filters. A category groups the filters into three main categories based on the type of filter: Application Protection, Infrastructure Protection, and Performance Protection. These categories are used to organize and locate filters in the device Local Security Manager (LSM) web application.

category settings
Settings used to assign global configurations to filters.

For example, a reputation filter responds to traffic that matches the addresses of tagged entries in the Reputation Database that have been screened using specified tag categories. Category settings consist of the following global parameters:

- **State** – determines whether filters within the subcategory are enabled or disabled. If a category is disabled, all filters in the category are disabled.

- **Action set** – determines the action set that filters within a category will execute when a filter match occurs. If the Recommended action set is configured, filters within the category are configured with the settings recommended by the DV team. Users can override the category setting on individual filters by editing the filter to define custom settings.

domain wildcard
URL wildcard that occurs only at the beginning of a URL. For example, */path/to/resource. A domain wildcard is always followed by a slash (/), after which the path starts. Domain wildcards support both http:// and https:// protocols.

maximum depth
A limitation for URL reputation entries that prohibits the introduction of a wildcard string (*) after a specific number of slashes in the path URI. The SMS rejects any URL entries with wildcards entered beyond the 12th path segment (for example, http://mywebsite.com/one/two/three/four/five/six/seven/eight/nine/ten/eleven/twelve/*). The maximum depth for entries in the User URL Reputation Entries database is 5. For example, http://mywebsite.com/w/x/y/z/* is a valid entry and http://mywebsite.com/v/w/x/y/z/* returns an error. The maximum depth for URL exceptions is 4. For example, http://mywebsite.com/x/y/z/* is a valid entry and http://mywebsite.com/w/x/y/z/* returns an error.

normalization
Background process that transforms a URL into its canonical format so that a filter's action set can apply to all strings that represent the same URL. RFC3986 describes this format. This functionality is stored in the device software and gets shared with the SMS. Before saving URLs to the database, the SMS attempts to decode and normalize them before the Bloom Filter analyzes them. For example, the percent-encoded URL http://mywebsite.com/p%61th gets normalized to its canonical format http://mywebsite.com/path.
**path wildcard**

URL wildcard that occurs only at the end of a URL. For example, http://a.com:80/path/\*. A path wildcard is always preceded by a slash (/), which separates path elements. No more than 12 slashes can precede a path wildcard in a URL.

**Reputation Database**

The Reputation Database is the collection of IP addresses, DNS names, and URLs on a device that represent potential risks to network security. The reputation entries can be user-provided, ThreatDV-service provided, or both.

**Reputation profile**

A profile with a collection of reputation filters that associate an action set with one or more suspect IP addresses, domains, or URLs. You can create multiple Reputation profiles so that each profile has customized filters and updates, which can then be distributed to specific devices and segment groups.

**ThreatDV Reputation Feed**

A type of DV that filters IP addresses and DNS names based on reputation score and other factors determined by the security research organization within Trend Micro. Periodic updates occur automatically through the Reputation service and are available for automatic or manual download to devices.

**ThreatDV URL Reputation Feed**

A type of DV that filters URLs based on reputation score and other factors determined by the security research organization within Trend Micro. Periodic updates occur automatically through the Reputation service and are available for automatic or manual download to devices.