Trend Micro™ TippingPoint™

URL Reputation Filtering Deployment and Best Practices Guide

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that the Security Management System collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Legal Notice

Publication: February 2023

Introduction to URL Reputation Filtering

URL reputation filters provide more granular control for blocking access to websites than reputation filters based merely on domains or IP addresses. For example, instead of blocking everything at `www.mywebsite.com`, you can configure URL Reputation Filtering 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 the Threat Digital Vaccine (Threat DV) URL Reputation Feed, or both. The Trend Micro™ TippingPoint™ DVLabs threat intelligence team compile sites on the Threat DV URL Reputation Feed based on reputation ratings from various sources. *Learn more on page 5* about these sources for URL reputation.

In addition, URL Reputation Filtering facilitates a deeper integration with any Trend Micro™ Deep Discovery™ devices that you manage using 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

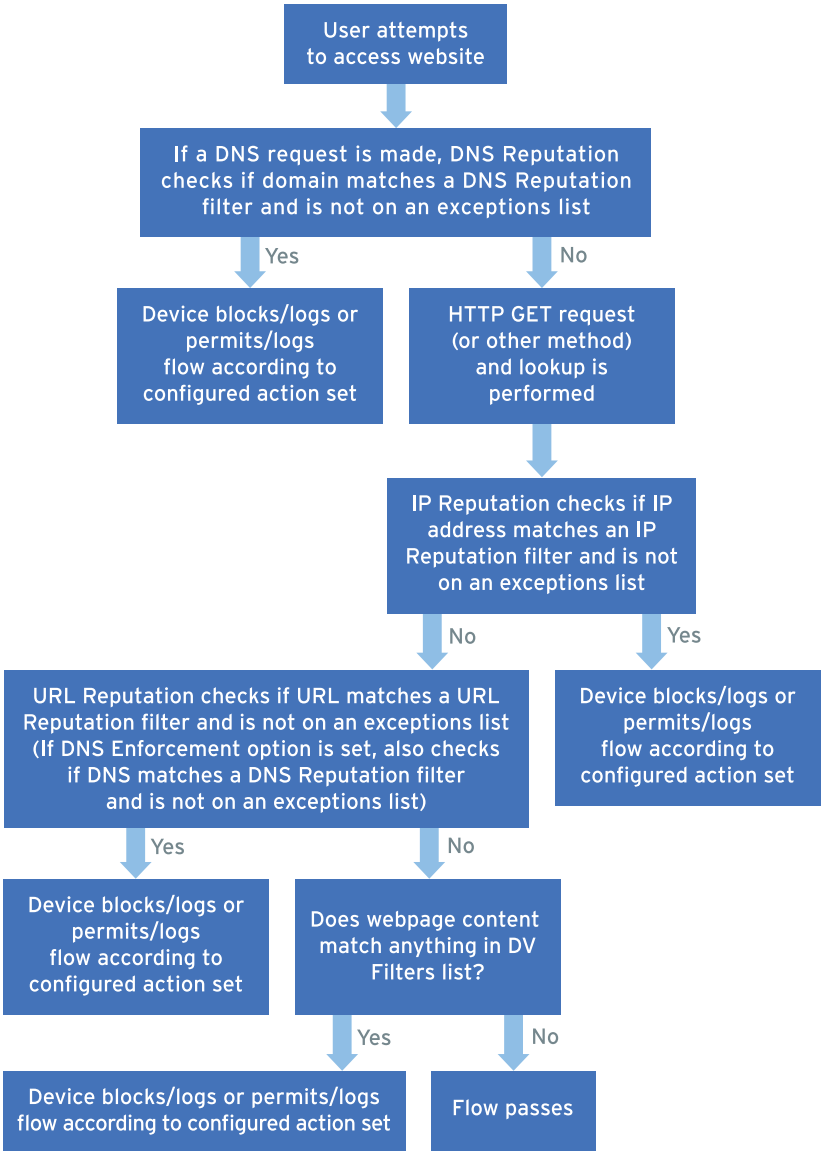
Getting started

Create a URL Reputation Filtering policy much like you would create a policy for DNS or IP reputation.

1. Create a reputation filter based on URL entries in the Threat DV URL Reputation Feed or the User-Defined URL Entries database, or both. *Learn more on page 5* about these sources for URL reputation.

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 Threat DV 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 action set you configure for the filter.
4. If the action set permits traffic, Digital Vaccine inspection still occurs even though reputation inspection stops.

The following figure on page 3 graphically shows the steps that a device configured with URL Reputation Filtering takes when a user attempts to access a website.


User attempts to access website
If a DNS request is made, DNS Reputation checks if domain matches a DNS Reputation filter and is not on an exceptions list
Yes
No
Device blocks/logs or permits/logs flow according to configured action set
HTTP GET request (or other method) and lookup is performed
IP Reputation checks if IP address matches an IP Reputation filter and is not on an exceptions list
No
Yes
URL Reputation checks if URL matches a URL Reputation filter and is not on an exceptions list (If DNS Enforcement option is set, also checks if DNS matches a DNS Reputation filter and is not on an exceptions list)
Device blocks/logs or permits/logs flow according to configured action set
Yes
No
Device blocks/logs or permits/logs flow according to configured action set
Does webpage content match anything in DV Filters list?
Yes
No
Device blocks/logs or permits/logs flow according to configured action set
Flow passes

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 Threat DV 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 you already set up a DNS rule 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 TippingPoint 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 Threat Protection System (vTPS)
- Each TPS or vTPS device that has URL Reputation Filtering configured must be managed by an SMS appliance running version 5.0.0 or later.
- Both your SMS appliance and your TPS or vTPS devices require DV version 8990 or later.
- You must enable the **HTTP Context (Hostname, URI, method)** option for your inspection profile. *Learn more on page 17* about how to configure HTTP Context for an inspection profile.

Note

If this option is disabled, you will see an error for any attempt to create a reputation filter that uses URL Reputation Filtering. 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. *Learn more on page 5* about access to this database.

Sources for URL reputation

Organizations compile their list of sites to block based on the security reputations of the URLs. One or a conglomeration of the following sources define the reputation of a URL:

- *Threat DV URL Reputation Feed on page 5*
- *User-Defined URL Entries on page 7*
- *Deep Discovery integration on page 7*

Threat DV URL Reputation Feed

Because the threat status of a website can change continuously, you can rely on a feed from the Threat Digital Vaccine (Threat DV) to keep your lists current. The Threat DV feed contains a database of URLs considered to be malicious.

You can access the Threat DV URL Reputation Feed can at the Threat Management Center (TMC) at https://tmc.tippingpoint.com/. You must have a Threat DV subscription and entitlement bundle. The URL Reputation Feed is updated multiple times a day.

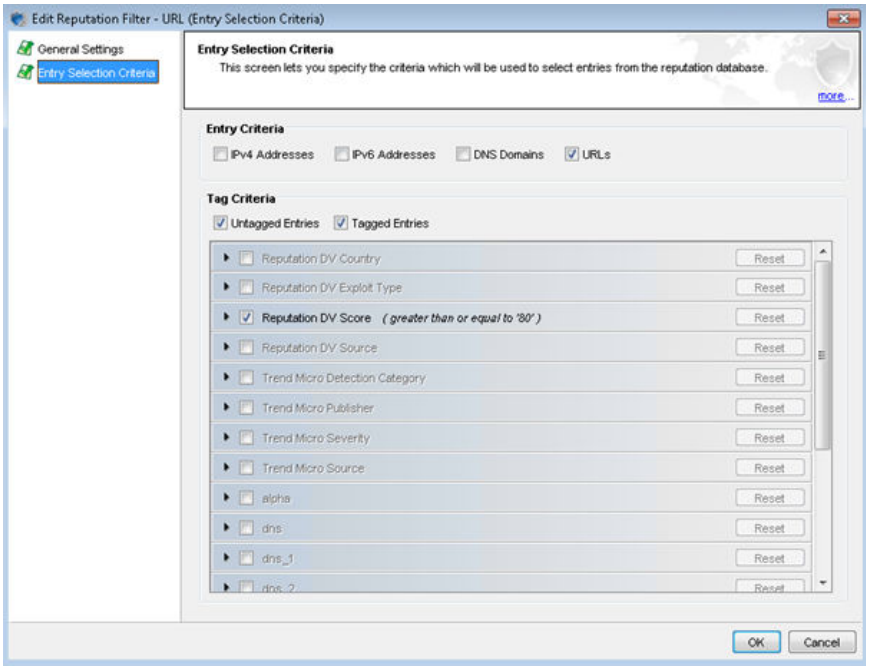
Every entry in the Threat DV URL Reputation Feed has a score of 100 (malicious). Assign a score for your filter relative to that score, and include the value `100` in any of the following ways:

- =100 (equals 100)

- <=100 (less than or equal to 100)
- <100 – 100 (specifies a range between any number less than 100 and 100; when you select the **Inclusive** checkbox, you 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 checkbox must be selected as Entry Criteria.
- Reputation DV Score must be 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, you can prioritize a **Permit** action set

over a **Block** or **Quarantine** action. *Learn more on page 19* about specifying URL exceptions.

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.

- Each managed device supports a maximum of 100,000 user-defined URL entries.

Note

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

- Each managed device supports a maximum of 10 URL Reputation filters.
- 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 database supports only the `http` and `https` schemes. Other schemes, such as `ftp`, are not supported.
- No user-defined URL entry can exceed 4 k in length.

Learn more on page 9 about adding user-defined URLs to this database.

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

Deep Discovery integration

You can enable 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.

Learn more on page 38 about integrating URL Reputation Filtering with Deep Discovery Analyzer devices.

Deployment

You configure a URL filter much the same way as you configure an IP filter or DNS filter. Follow these basic steps:

1. *Manage your TPS system on page 8*
2. *Add URL entries to the Reputation database on page 9*
3. *Configure your inspection profile on page 16*
4. *Distribute an Inspection profile to segments on page 21*

Prerequisites

Ensure your environment meets the requirements specified in *General requirements and restrictions on page 4*.

Manage your system

To use Reputation profiles and filters, first manage your TPS or vTPS device with 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 manage a TPS or vTPS device with an SMS, always distribute an inspection profile to all segments to begin protecting network traffic. By default, when you add a vTPS or TPS device to an SMS, 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

The SMS and any of its managed devices that will have URL Reputation Filtering enabled must have DV version 8990 or later.

As a best practice, activate the latest DV *after* upgrading your SMS version. If the latest DV is already activated *before* you upgrade your SMS version:

1. Activate the DV version prior to the latest version.
2. Upgrade the SMS.
3. Activate the latest DV version.

After a DV that supports URL Reputation Filtering has been activated, you cannot activate a DV that does not support it.

For information on how to download and distribute DV packages, refer to the *SMS User Guide*.

Add a URL to the database

You can choose to rely solely on a Threat DV feed to keep your lists current. For more targeted entries and deeper control, you can also define the criteria for your own URL entries. Use the same navigation to add these entries to the

SMS Reputation Database that you would 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 Threat DV 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.

Procedure

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 Threat DV 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:

```
=
<=
<
>=
>
between inclusive
between not inclusive
```

- **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`.

Letter	Date/Time Component	Presentation	Example
G	Era designator	Text	AD

Letter	Date/Time Component	Presentation	Example
y	Year	Numeral (2 digits)	09
yy	Year	Numeral (2 digits)	09
yyy	Year	Numeral (2 digits)	09
yyyy	Year	Numeral (4 digits)	2009
M	Month	Numeral (no leading zero)	8
MM	Month	Numeral (leading zero)	08
MMM	Month	Text (abbreviated)	Aug
MMMM	Month	Text (full)	August
w	Week in year	Numeral	33
W	Week in month	Numeral	3
D	Day in year	Numeral	221
d	Day in month	Numeral (no leading zero)	9
dd	Day in month	Numeral (leading zero)	09
F	Day of week in month (e.g., 2nd Sunday)	Numeral	2
E	Day of week	Text (abbreviated)	Sun

Letter	Date/Time Component	Presentation	Example
EE	Day of week	Text (abbreviated)	Sun
EEE	Day of week	Text (abbreviated)	Sun
EEEE	Day of week	Text (full)	Sunday
a	AM/PM indicator	Text	PM
H	Hour of day (0–23); midnight displayed as 0	Numeral	15
k	Hour of day (1–24); midnight displayed as 24	Numeral	15
K	Hour in AM/PM (0–11); midnight and noon displayed as 0	Numeral	3
h	Hour in AM/PM (1–12); midnight and noon displayed as 12	Numeral	3
m	Minute of hour	Numeral (no leading zero)	4
mm	Minute of hour	Numeral (leading zero)	04
s	Second of minute	Numeral (no leading zero)	8
ss	Second of minute	Numeral (leading zero)	08

Letter	Date/Time Component	Presentation	Example
S	Millisecond of minute	Numeral (no leading zero)	`7`
SS	Millisecond of minute	Numeral (leading zero)	`07`
z	General time zone	Text (abbreviated)	`CDT`
zz	General time zone	Text (abbreviated)	`CDT`
zzz	General time zone	Text (abbreviated)	`CDT`
zzzz	General time zone	Text (full)	`Central Daylight Time`
Z	Time zone	RFC 822 time zone	`-0500`

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

Use wildcards for both user-defined URLs entries and exceptions that you want to add. Configure wildcards using the following guidelines:

- Enable decryption for HTTPS traffic (**Profiles** > **Shared Settings** > **SSL** > **Server Proxies** > **SSL Server Proxy Config** > **Decrypted Service**) so that the wildcard filter can be applied to the SSL-encrypted HTTPS traffic.
- 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**) or end (**path wildcard**) 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**. 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/\*`

Configure your Inspection profile

After you add your entries 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 16*
- *Configure HTTP Context for the inspection profile on page 17*
- *Specify URL exceptions on page 19*

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

Create a URL Reputation filter

Procedure

1. Select **Profiles > Inspection Profiles > [*profile_name*] > Reputation/Geo** .

2. Click **New Reputation** to create a new reputation filter.
3. Enter a filter title in the **Name** field, and then select the **Locked** checkbox 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** checkbox to enable the filter. If you clear this checkbox, 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 Threat DV 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 checkbox next to any tag category you want to include. *Learn more on page 10* about specifying URL criteria.

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 Threat DV, geographic, and user-provided entries.

7. Click **OK**.

What to do next

Learn more on page 41 about configuring reputation filters.

Configure HTTP Context for the inspection profile

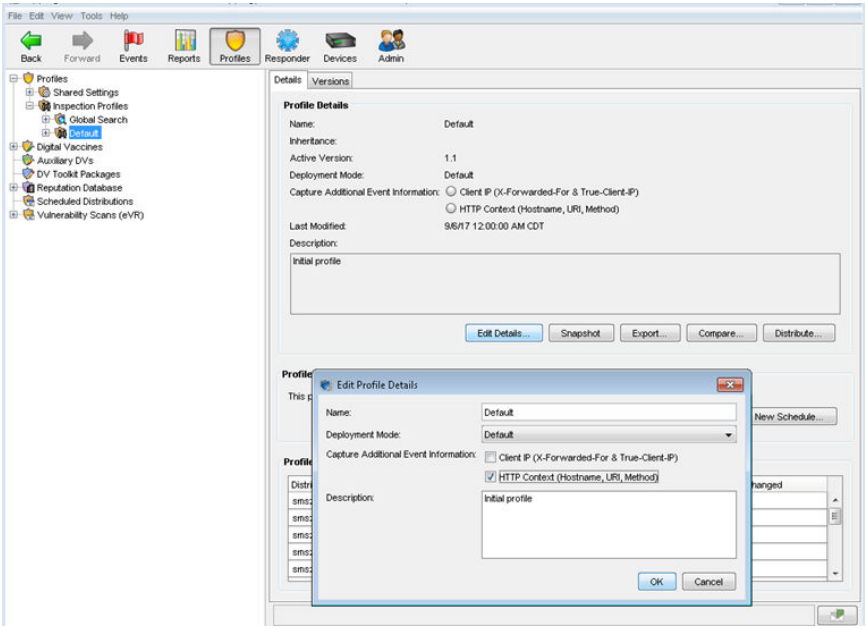
Configure your Reputation profile to generate events with URL data using the following steps.

Note

URL Reputation Filtering requires that the **HTTP Context** option is selected. If you disable this option, 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.

Procedure

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)**.



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.

Procedure

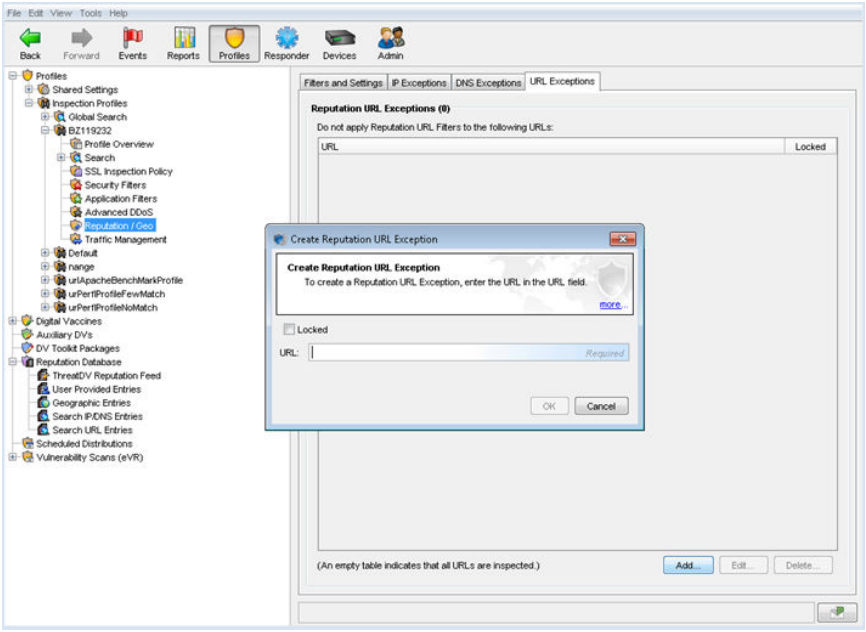
1. From the Profiles navigation pane, expand **Profiles > Inspection Profiles > [*profile_name*] > Reputation/Geo**.

CAUTION!

Scan your network hosts before creating exceptions to or disabling 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. *Learn more on page 15* about wildcards.

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.

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.

Procedure

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** checkbox.

URL Reputation Filtering packages

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

- *Policy package on page 22*

- *User-Defined URL Entries package on page 22*

Policy package

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

User-Defined URL Entries package

After the SMS uploads the Policy package, 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 belong to the same Reputation Database on the SMS as IP and DNS entries, but they 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. To see synchronization tasks for updated URL entries, check 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

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.

Learn more on page 15 about wildcards.

User-Defined URL Entries

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

Each managed device supports a maximum of 100,000 user-defined URL entries and 10 URL Reputation filters.

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 DV threat intelligence to stay current with ever-evolving internet environments and emerging threats. URL Reputation Filtering is licensed as part of Threat Digital Vaccine (Threat DV). When you buy a subscription to Threat DV, you get both the IP/DNS Reputation feeds and the Threat DV URL Reputation Feed. The Threat DV 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. To help avoid them, specify exceptions. *Learn more on page 19* about specifying URL exceptions.

Add URL entries

A URL comprises characters, both reserved and unreserved, defined by RFC standards.

Many different strings can represent the same URL. **Normalization**, 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`.

The device software stores this functionality and shares it with the SMS. Before saving URLs to the database, the SMS attempts to decode and normalize them.

General guidelines

- The database supports only the `http` and `https` schemes. 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 4 k 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 4 k limit.

Syntax guidelines

- Because the asterisk (`*`) character is a valid URL character, escape it with a backslash (`\`) whenever you use it as a wildcard. *Learn more on page 15* about using wildcards.
- 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.
- The database supports and normalizes both absolute and relative URLs. 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, you *cannot* use the following use of the wildcard string:

```
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.
- You must delimit the URL entries in the import file by a pipe (|) instead of commas. URL entries can be either URLs only or URLs with one or more associated tags.
- If the import results in errors, the SMS displays which specific entries caused the errors. 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.

- *Learn more on page 28* about importing entries from a file.

Learn more on page 10 about specifying URL criteria.

Delete URL entries

Entries in the Threat DV URL Reputation Feed are read-only and cannot be modified. You can only modify and delete User-Provided URL Entries. If you know that a URL entry in the feed is incorrectly being reported as malicious, you can submit a correction by contacting Support.

To bypass URL entries in the feed, create a list of exceptions in your profile. *Learn more on page 19* about specifying URL exceptions.

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. *Learn more on page 42* about using web service calls to remove URL entries.

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. Delimit the entries in the import file with a pipe (|) instead of commas so that each line comprises one or more fields separated by pipes.

Before you begin

Use the following guidelines when you import data to the Reputation Database using a file.

Format rules:

- **File contents –** The file can contain only URLs. You cannot mix in IPv4/IPv6 addresses and DNS domain names.
- **Maximum number of entries –** Limit the total number of entries in one file to 10,000 or less.
- **Syntax –** Separate one or more fields of each line in the file with 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 you use a pipe as a delimiter in a URL's embedded text, you do not have to escape it 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.
- Specify the URL name for that entry in the first field on each line. The remaining fields on a line are optional. If you populate the remaining fields, the import processes them as tag category/tag value pairs.
- Any line that has a first non-white space character of # is considered a comment. The import discards comment lines. Inline comments are not supported.
- 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 in the import file must exist on the SMS prior to the import.

- **Case-sensitive –** All tag category names and tag values are case-sensitive except for yes/no tag categories.
- **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 –** The import ignores empty pairs of fields. An empty tag category field generates an error and import of the entry fails. An empty tag value field causes the import to discard the corresponding tag category and the import continues to process the next field of the entry, as if the line did not have the tag category at all.
- **Consistency –** You do not have to list tag category/value pairs 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:

Procedure

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. The import handles conflicts according to how you set the **User-specified tags override tags from import file** option.
   - **User-specified tags override tags from import file** — This option is available only when you select the **Import tags from file and specify tags to apply to all imported entries** option. This item specifies how to handle tags in the file and tags you specify on the next screen that have the same name. If you select this option, tags you select on the next screen take precedence over tags from the import file. If you do not select this option, tags from the file take precedence over tags you specify on the next screen.

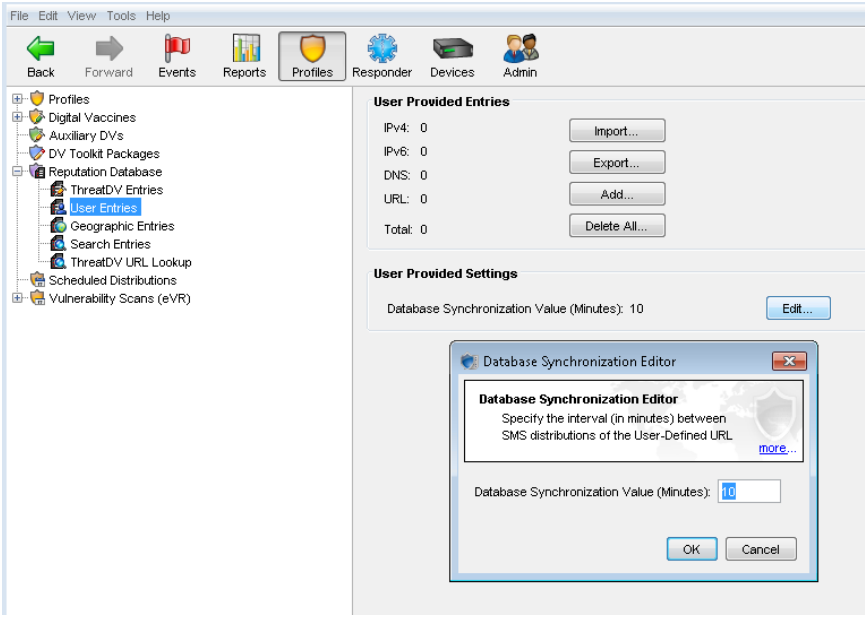
Manage URL entries

You can add an unlimited number of user-provided entries to the Reputation Database.

The time it takes before you begin to see your imported entries listed in the database depends on the following factors:

- The number of user entries you add.
- 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):



The SMS automatically synchronizes any changes to the **Reputation Database** to devices that have reputation filters active. You can also manually update URL entries in the User-Provided URL Entries database by performing a full sync. A full sync is only needed for recovery purposes and usually requires assistance from Support. When you perform a full sync, 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 and setting the synchronization interval, refer to 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 you previously configured.

Note

Tag categories created by the Threat DV URL Reputation Feed are read-only and cannot be modified.

Procedure

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

Searching for user-defined URLs differs from a search of the Threat DV URL Reputation Feed (**Profiles > Reputation Database > ThreatDV URL Lookup**), which can only determine whether a URL is present or not. If the URL is present, the Reputation DV score is provided.

You can perform one of the following searches of the User-Defined URL Entries database:

- **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, select the **URL** checkbox. To search for an exact sequence of characters or path elements, enter the text in the URL field and select the **Exact Match** checkbox.
3. For Tag Criteria to include in the search, select the checkbox 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. *Learn more on page 10* about tag categories.
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

The Reputation logs limit entries to 255 characters. The logs truncate a long entry by appending an ellipses (. . .) after the entry reaches the 255-character limit. This facilitates 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 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 you enable HTTP mode, URL Reputation Filtering attempts to match that URL on HTTP traffic coming from any port.

- If you *disable* HTTP mode, 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. Because of decryption limitations, TippingPoint devices currently do not inspect outbound (web browsing) HTTPS traffic against URL reputation filters.

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 you reformat the external drive or when the encryption status changes, all URL data on the drive will be lost. Users must redistribute the Threat DV URL Reputation Feed and the User-Defined URL Entries to the device before you can enable URL Reputation filtering again.

When you unmount the external drive, a system log warning informs you that all access to URL databases, including both the Threat DV 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 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 on the 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, the external storage drives reserve 3.5 GB to support the Reputation databases. If you ever need to reconfigure this storage space, use the following command:

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

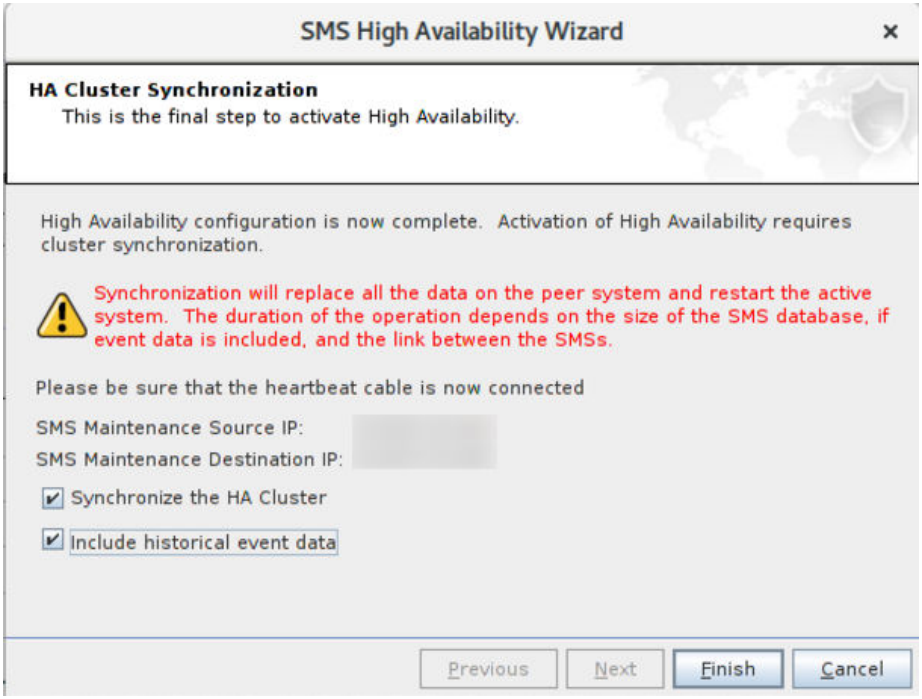
Note

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, the primary server and the passive server can share any URL entries that you add, update, or delete from the Reputation database.

To preserve any updates to the Reputation database across an SMS cluster, make sure that you select the **Include historical event data** checkbox in the SMS High Availability Wizard (**Admin > High Availability > Configure**).



Deep Discovery Analyzer integration

Deep Discovery Analyzer devices enable you to share threat intelligence and insights 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.

Procedure

1. Ensure your Deep Discovery Analyzer device is in communication with the SMS.

Learn more about configuring URL Threat Analysis in the *SMS User Guide*.

2. Configure URL Threat Analyzer:

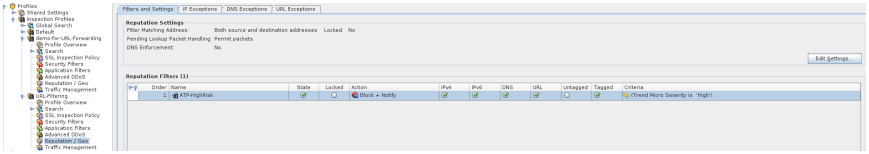
   a. Select **Events > URL Threat Analysis**.

   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** checkbox and click **OK**.

3. Configure an Inspection profile with a URL filter that has criteria of `Trend Micro Severity is High`.

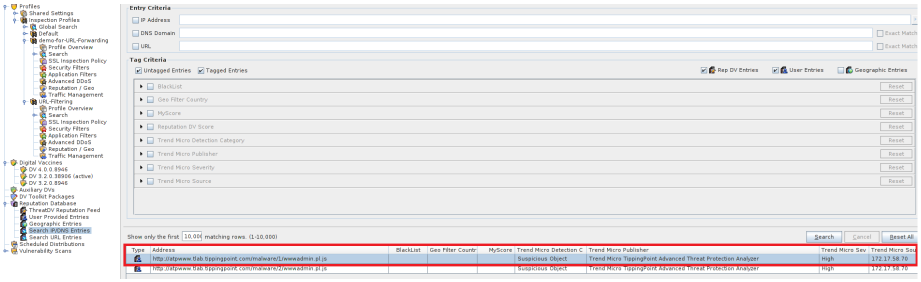
   The following figure shows a profile, `URL-Filtering`, with URL as a source and with criteria as `Trend Micro Severity is High`.



   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.

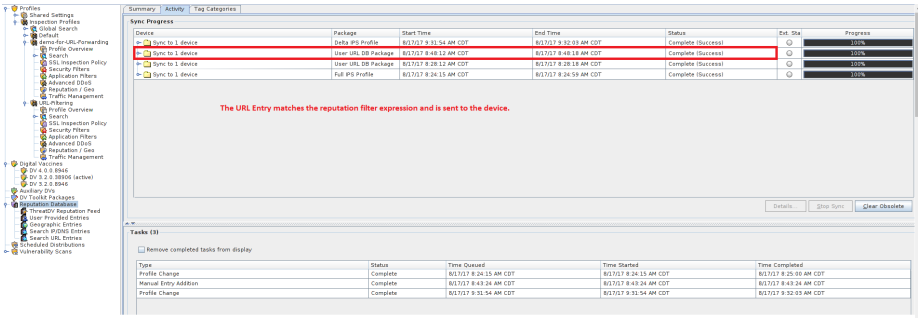
Any analyzed entry with a High severity gets automatically added to the User-Defined URL Entries database.



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 Deep Discovery Analyzer device had not inspected prior to your enabling the feature get automatically added to the database. Any URLs that the Deep Discovery 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 applies.



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 matches 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 occur before HTTP requests. For DNS Reputation rules to be enforced, you must position the managed device 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.

To set a profile attribute to enforce DNS Reputation in HTTP requests:

Procedure

1. Select **Profiles > Profiles > Inspection Profiles > [Profile Name] > Reputation/Geo**.
2. Click **Edit Settings**.
3. In the Edit Reputation Settings dialog, select the checkbox under **Reputation Enforcement Options**.

Note

When you select this option, check the logs to verify whether URL Reputation Filtering matched something because of the DNS filter or the URL filter.

Web service calls

Use the web API to programmatically interface with the SMS. 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"
```

Learn more about the Reputation web API—including best practices, syntax parameters and rules, and examples—from 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:

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

- 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`), enclose the URL with double quotes when using the debug reputation command to query it:

```
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.

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. You 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. The device software stores this functionality and shares it 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,Threat DV-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 you can then distribute to specific devices and segment groups.

Threat DV 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. Periodic updates occur automatically through the Reputation service. You can download these updates automatically or manually to devices.

Threat DV 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. Periodic updates occur automatically through the Reputation service. You can download these updates automatically or manually to devices.