HP TippingPoint

Security Management System
Advanced Threat API Guide

Version 4.3.0

Edition: July 2015

Legal and notice information

HP TippingPoint Security Management System Advanced Threat API Guide

Contents

About this guide

This guide provides information required to integrate an advanced threat device with the HP TippingPoint Security Management System (SMS) alongside one or more inline HP TippingPoint Intrusion Prevention System (IPS) devices and other HP TippingPoint network appliances.

This section includes the following topics:

Target audience

This guide is intended for advanced threat device vendors who are responsible for implementing the advanced threat application side of the integration with HP TippingPoint security systems and associated devices. Users should be familiar with networking concepts and the following standards and protocols:

- TCP/IP
- UDP
- ICMP
- Ethernet
- Simple Network Time Protocol (SNTP)
- Simple Mail Transport Protocol (SMTP)
- Simple Network Management Protocol (SNMP)

Related documentation

A complete set of product documentation for the Security Management System is available online. The product document set generally includes conceptual and deployment information, installation and user guides, CLI command references, safety and compliance information, and release notes.

For information about how to access the online product documentation, refer to the *Read Me First* document in your product shipment.

Conventions

This information uses the following conventions.

Typefaces

HP TippingPoint publications use the following typographic conventions for structuring information:

Convention	Element
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes. Example: Click **OK** to accept.
Italics font	Text emphasis, important terms, variables, and publication titles
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
Monospace, italic font	• Code variables • Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

Messages

Messages are special text that is emphasized by font, format, and icons.

⚠ **Warning!** Alerts you to potential danger of bodily harm or other potential harmful consequences.

⚠ **Caution:** Provides information to help minimize risk, for example, when a failure to follow directions could result in damage to equipment or loss of data.

Note: Provides additional information to explain a concept or complete a task.

Important: Provides significant information or specific instructions.

Tip: Provides helpful hints and shortcuts, such as suggestions about how to perform a task more easily or more efficiently.

Customer support

HP TippingPoint is committed to providing quality customer support for all of its products. If you need customer support, contact the HP support center for your product. You can find the customer support contact information for your product in the Read Me First document that is in your product shipment. The Read Me First document is also available on the HP TippingPoint Threat Management Center (TMC).

If this is your first purchase of an HP TippingPoint product, contact customer support to register your product and access online support.

Self-service portal

HP provides an online self-service portal for HP TippingPoint customers. The Self-Service Portal provides a tool for customers to manage their support cases. After registering for an account, you can submit new technical support cases and manage existing ones. For more information about accessing the online Self-Service Portal, refer to the *Read Me First* document.

Contacting support

To expedite your support request, please take a moment to gather some basic information from your records and from your system before contacting customer support. For example, your support representative may need your device serial number and the versions of your product software to assist you. For additional details about contacting support and gathering needed information before contacting support, refer to the *Read Me First* document.

HP website

For the name of the nearest HP authorized reseller, see the Contact HP Worldwide website:

http://www.hp.com/country/us/en/wwcontact.html

Advanced Threat Device Integration & Reputation Overview

The SMS Reputation Management API enables customers to utilize intelligence sourced from their advanced threat solutions to provide in-line blocking at wire speed with HP TippingPoint Next Generation IPS and HP TippingPoint Next Generation Firewall (NGFW) appliances. This provides an advanced layer of protection to prevent advanced malware from communicating to command/control systems, non-patient zero infections, and prevent malware from spreading.

SMS Integration

An advanced threat application integrated in an SMS environment can help your customers disrupt malware communications, isolate infected resources, and protect critical resources. The integrated environment enables flexible action and enforcement options based on advanced threat-provided metadata and reputation data from Digital Vaccines (DVs) and the Reputation Database.

An integrated environment enables customers to take enforcement actions, such as:

- Block against command and control network traffic generated by malware source.
- Send notifications when an infected host attempts to initiate communications.
- Quarantine an infected host.
- Block network traffic against malware source.

The Advanced Threat device uses the SMS Reputation Management API to connect with the SMS, enabling the device to trigger reputation events.

Reputation Database

The HP TippingPoint *Reputation Database* is a collection of IP addresses and DNS names on an SMS that represents potential risks to network security. The Reputation Database contains entries that are either user-generated or contained in Reputation Digital Vaccines, or both. The entries in the Reputation Database are used to create reputation filters that target specific network security needs. See Reputation Filters on page 6.

Reputation entries can be tagged or untagged. A *tagged* entry consists of an IP or DNS address plus a reputation tag category and associated values. An *untagged* entry contains only an IP or DNS address and can function either as a black list or white list.

As a vendor, you can define reputation tag categories through the SMS client, and leverage the data output from your advanced threat device to import data as reputation entries to the SMS. Once the data is imported to the SMS Reputation Database as tagged reputation entries, these can be distributed to other SMS-managed devices on the network.

Reputation Tag Categories

Reputation *tag categories* define the types of tags that can be used to categorize Reputation Database entries. A reputation tag category is either created by the Reputation Digital Vaccine (Rep DV) service or defined manually. Customers create new reputation tag categories in the SMS so that the data included in the CSV file can be successfully imported into the SMS Reputation Database.

Note: Reputation entries imported from a CSV file must adhere to specific Reputation import rules. See Reputation Import Record Format on page 9.

Tag categories that begin with *Reputation DV* are reserved. Specifically, the Rep DV service uses tag categories of *Reputation DV Country*, *Reputation DV Exploit Type*, and *Reputation DV Source*.

All reputation tag categories have the following attributes:

- **Name**: Name to identify the reputation tag category. All specified names must be unique.
- **Type**: Type of data tags that this category contains (text, list, date, boolean value, or numeric range).
- **Description**: (Optional) Descriptive text that indicates how tags of this category are to be used.

Depending on the tag category *type*, there may be additional attributes to define, as described in the table below.

Type	Description
Text	Text string. Specify the **Maximum Length**, up to 255 characters.
List	List of possible values for tags of this category.
Date	Flexible date format definition. **Specify Input Format**. For specific information, refer to the Date/Time Format Characters table in the Tag Categories embedded help panel in the SMS client.
Yes/No	Boolean value, Yes or No.
Numeric Range	Flexible range that can be defined within the limits of a 32-bit signed integer. Specify **Minimum Value** and **Maximum Value**.

Reputation Filters

A *reputation filter* associates an action set (defined on the SMS) with one or more entries in the Reputation Database. An *action set* determines how the system responds when a packet triggers a filter. Default actions include *Block*, *Permit*, *Notify*, and *Trace*. The SMS client also enables you to create custom action sets that include *Quarantine* and *Rate Limit*.

When the reputation filter is distributed to a device, the specified actions are applied to traffic that matches the tagged entries in the Reputation Database. When you create a reputation filter using a tag category from the Reputation Database, any address associated with the tag category is included in the filter.

Note that reputation filters are created on the SMS and distributed to SMS-managed devices.

Profiles

A *profile* is a collection of filters or rules that enable you to set up security configuration options for HP TippingPoint solutions. Profiles enable you to distribute filters to multiple devices, specific devices, physical segments controlled by a specific device, or even virtual segments.

Profiles are created and modified through the SMS client, which is also used to distribute profiles to managed devices. Each profile can be distributed separately, to specific devices. When a profile is distributed, it includes shared settings (such as action sets, notification contacts, and services) as well as associated filters and filter setting modifications.

SMS Reputation Management API

The following information describes the initial network topology, method for importing reputation entries into the Reputation Database, the reputation import record format, and performance guidelines.

It should be noted that Reputation Management is one portion of the SMS Web API. For more information about the full external SMS API, refer to *HP TippingPoint Security Management System External Interfaces* documentation included in the latest SMS release.

Integrated Environment

In the proposed integrated environment, an out-of-line advanced threat device is connected to the customer's LAN environment with a switch. The switch is configured to replicate traffic from one port to another port so that you can allow pass-through traffic and redirect duplicate traffic to the advanced threat device.

The SMS Reputation Management API enables an advanced threat device to connect with the SMS through a secure Web interface, enabling the advanced threat device to update the Reputation Database. This, in turn, allows administrators to leverage advanced threat intelligence to create reputation filters and better protect their systems.

Important: Before the advanced threat device can send reputation entries to the SMS, tag categories must be defined in the SMS client to map data output from the advanced threat device to the Reputation Database. For more information about defining tag categories, see Mapping Advanced Threat Data to Reputation Tag Categories on page 17.

Note: When interfacing with the SMS programmatically, the client must be able to trust the certificate on the SMS, whether it is self signed or signed by an outside source.

CSV File Import

The SMS Reputation Management API allows you to import reputation entries from your advanced threat device into the Reputation Database. File Import parameters can be passed to the SMS as an HTTP POST request via a command line tool for HTTP scripting or programmatically by using an HTTP client to communicate to the SMS through Web APIs.

The SMS imports reputation entries through a CSV file upload. To avoid performance issues, adhere to the issues documented in Reputation Import Record Format on page 9.

The following example shows how to import a CSV file to the SMS the cURL command.

Note: By default, the SMS requires SMS Administrator credentials with SuperUser access.

```
curl -v -k -F "file=@outputFile.txt""https://10.99.1.123/repEntries/
import?smsuser=<user_name>&smspass=<password>&type=ipv4"
```

`-v` Enables "verbose" mode for debugging.

`-k` Allows cURL to perform insecure transfers over SSL connections.

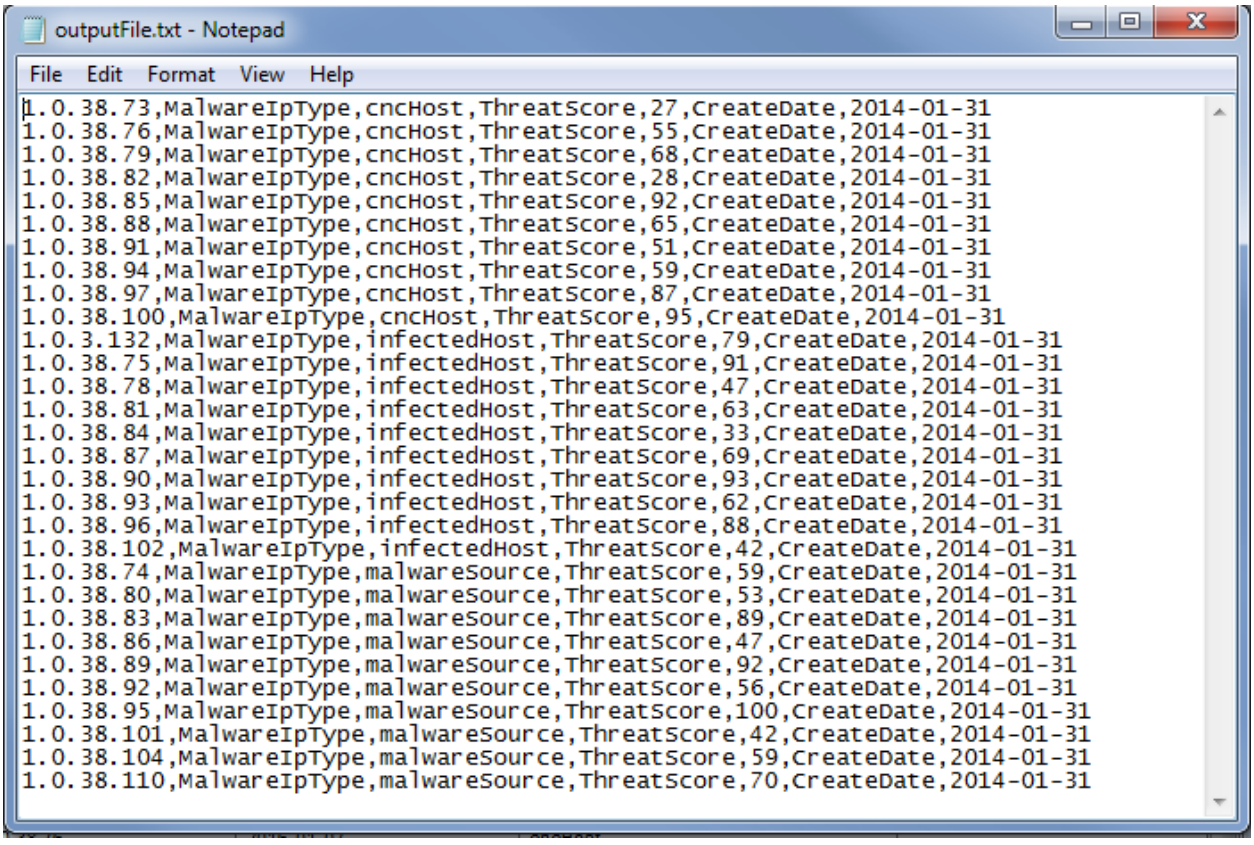
`-F` Enables cURL to emulate a user pressing a submit button, using the Content-Type multipart/form-data according to RFC 2388.

In the example above:

- `"file=@outputFile.csv"` specifies the CSV file to be imported into the SMS Reputation Database.
- `10.99.1.123` is the IP address of the SMS server.
- `<user_name>` is the user name for an account with appropriate capabilities for Reputation Management tasks.
- `<password>` is the password for the SMS user account.
- `ipv4` designates the type of entries contained in the file: IPv4, IPv6, or DNS. The SMS supports these three types, but all entries within a single file must be the same type.

If the reputation entries you import do *not* have tags (that is, the entries are untagged), the imported data merges with existing address values. If there are different tag values for the same tag category, the value for the imported entry is used and the old value is discarded.

The following example shows data from a CSV file to be imported as reputation entries.



Reputation Import Record Format

The SMS expects imported reputation files to be in CSV format and to follow the rules described in the table below. For reference, the rules are divided into files, fields, addresses and tags.

Files	
CSV Format	The import file must be in comma separated value (CSV) format.
Each line is made up of one or more fields separated by commas.	
Each line represents one entry, and entries must not span lines.	
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.	
Blank Lines	The import file may not contain any blank lines within the body.
Blank lines after the last line are ignored.	
Fields	
Double Quotes	A field may be enclosed in double-quotes. For a value that contains a comma that is not a field separator, enclose the field in a double quote. To represent a double-quote character within a quoted value, use two double-quotes.
Addresses	

Address Types	Only one type of address (IPv4, IPv6 or DNS domain name) can be contained in the file. Mixing of types within a file is not allowed. The first field on each line must be the IPv4 address, IPv6 address or DNS name for that entry. The remaining fields on a line are optional. If present, remaining fields are processed as tag category/tag value pairs.
DNS Entries	A DNS entry matches any lookups that contain the specified string. For example, foo.com matches foo.com, www.foo.com, and images.foo.com. To specify an exact DNS entry match, enclose the DNS name in square brackets. For example, [foo.com] matches only foo.com, and does NOT match www.foo.com or images.foo.com.
CIDR Values	CIDR values are be normalized. Any bits outside the portion of the address specified by the prefix length are changed to zero.
Tags	
SMS Parity	Any tag categories that appear in the file must exist on the SMS prior to import.
Character Case	In tag category names and tag values, character case is significant.
Yes/No tag categories	For yes/no tag categories, character case is insignificant.
For yes/no tag categories, the text “yes,” regardless of case, denotes a yes value. All other values are considered no.	
Tag Pairs	Empty tag pairs (tag category/tag value) in 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.

Tag pairs (tag category/tag value) do not have to appear in the same order on each line.	
Tag Categories	It is not necessary that every entry specify every tag category, or even the same tag categories as other entries in the file.

Add or Delete Reputation Entries

The SMS Reputation Management API allows you to add reputation entries to or delete reputation entries from the Reputation Database using HTTP calls.

When you add reputation entries, use a comma (,) as a delimiter between a tag category name and the tag category value.

Entries that are associated with a LIST tag category can include multiple values only when the **Allow Multiple Values?** check box is selected (on the Edit Tag Category dialog box in the SMS). The list values must be separated by ~~~. For example: `MalwareIpType,malwareSource~~~cncHost`

If the LIST Tag Value Category is restricted to just one value, then the tag category name would be followed by the one value. For example: `MalwareIpType,infectedHost`

Adding a reputation entry requires a parameter called `TagData`. *Deleting* a reputation entry requires a parameter for `ip` or `dns` and the parameter `criteria` with the value `entry`.

Adding a Reputation Entry

The parameter values for TagData must be UTF-8 encoded.

The following example adds a reputation entry for tag category MalwareIpType and CreatedDate:

```
https://10.99.1.123/repEntries/add?smsuser=<user_name>&smspass=<password>
&ip=1.1.1.1&TagData=MalwareIpType,infectedHost,CreatedDate,"Jan
  22, 2014"
```

In the example above:

- `10.99.1.123` is the IP address of the SMS server.
- `1.1.1.1` is the IP address of the infected host (list value for MalwareIpType tag category).
- `"Jan 22, 2014"` is the list value for the CreatedDate tag category in the format MMM d, yyyy.

Deleting a Reputation Entry

The Delete API can delete one or more IP addresses and DNS entries in a single call. Add one or more IP or DNS parameters to the request. For example:

```
https://10.99.1.123/repEntries/delete?smsuser=<user_name>
&smspass=<password>&ip=1.1.1.1&ip=1.1.1.2&dns=malware.source1.com
&dns=malware.source2.com&criteria=entry
```

In above example:

- `10.99.1.123` is the IP address of the SMS server.
- `1.1.1.1` and `1.1.1.2` are the entries that will be deleted from the Reputation Database.
- `malware.source1.com` and `malware.source2.com` are the DNS entries that will be deleted from the Reputation Database.

Query Reputation Entries

SMS Reputation Management API allows a client to query reputation user-provided entries for an IP address or a DNS address. The table below describes the parameters to be specified in a query.

Parameter	Description
smsuser	Required. User name for an SMS administrator.
smspass	Required. Password for the user specified in the smsuser parameter.
ip	IP address of either IPv4 or IPv6 format. More than one IP address can be added to the query. At least one ip or dns parameter must be specified.
dns	DNS name. More than one DNS name can be added to the query. At least one ip or dns parameter must be specified.

The following example shows the host URL the client uses for the query:

```
https://10.99.1.123/repEntries/query
```

- `10.99.1.123` is the IP address of the SMS server

Successful HTTP response codes are `200` and `204`. A response code of `200` indicates the query was a success and data is being returned. A response code of `204` indicates the query did not find the IP or DNS entries in the Reputation Database, and no data is being returned.

Note that at least one IP address or DNS name must be specified in a query request, but the request can contain only one type: *either* ip or dns. Below are some examples.

Example (IP parameters):

```
https://10.99.1.123/repEntries/query?smsuser=<smsusername>
&smspass=<smspassword>&ip=1.1.1.1&ip=1.1.1.2&ip=1.1.1.3
```

Example (DNS parameters):

```
https://10.99.1.123/
    repEntries/query?smsuser=<smsusername>&smspass=<smspassword>
&dns=www.test1.com&dns=www.test2.com&dns=www.test3.com
```

The SMS responds to a query request with a mime-type of *text/plain* with default character encoding of UTF-8. For each IP address and DNS name specified in the query, the SMS will return all matching entries. For example, if the query request includes eight IP addresses, there will be eight values returned. Each value is terminated by a <new-line> character, so each returned value appears on its own line.

If you have a query IP address of `1.0.0.1` and the database has user entries of `1.0.0.1`, `1.0.0.0/24`, and `1.0.0.0/16` the returned result for this one IP will be 3 rows:

```
1.0.0.0/16,AtaHost,myata.device.com,MalwareIpType,infectedHost
```

```
1.0.0.0/24, AtaHost,myata.device.com,MalwareIpType,infectedHost
```

```
1.0.0.1, AtaHost,myata.device.com,MalwareIpType,infectedHost
```

As noted in the above example, the signature of the return value has also changed, and the matching *IP address/DNS* is appended to the beginning of the reputation entries so you can see "HOW" the entry was stored in the database.

The format of the returned values is equivalent to the format used during the “Add” service:

```
"Tag Class","Value",…
```

where `Value` is either a single value or a list of values. If a Tag class supports multiple values, it is represented by a list of values separated with three tildes, for example: "value” and "value1~~~value2~~~value3".

The following examples show a sample request and a sample response.

Request:

```
https://10.99.1.123/ repEntries/query?
smsuser=<smsusername>&smspass=<smspassword>&ip=1.1.1.1&ip=1.1.1.2
```

Response:

```
AtaHost,myata.device.com,MalwareIpType,infectedHost
```

```
AtaHost,myata.device.com,ThreatScore,28,MalwareIpType,
cncHost~~~infectedHost,Fri Jan 31 00:00:00CST2014
```

Performance Guidelines

Performance levels can vary greatly according to the number of files to be imported into the Reputation Database, the number of entries in each CSV file, the number and type of devices the SMS manages on the customer’s network, and the customer’s environment in general.

The SMS is limited to a maximum of 20 tag categories for the Reputation Database, and the maximum number of reputation entries is 6,000,000; however, we suggest limiting the number of entries in a file to 10,000. The maximum number of IP or DNS values that can be specified in a single query is 10,000.

The SMS can upload one CSV file at a time, and each file can contain multiple entries. Returned addresses are ordered from lowest to highest address, regardless of the order in which they are specified in a query.

Caution: Flooding the SMS with multiple files (with single or few entries) can cause performance issues. We recommend monitoring the growth of the Device Distribution queue size to ensure that the devices can sustain the number of changes to the entries.

Important: In releases prior to SMS 4.1, the SMS prevented concurrent processing of uploaded files by refusing file uploads until the previous upload was complete. As such, we cannot guarantee that frequent updates will be processed, and data loss may still occur even when a successful HTTP response code of 200 is returned. While integration is possible in versions prior to 3.6, we recommend SMS 4.1 for production deployments as SMS version 4.1 supports concurrent file import.

The file upload interval on the advanced threat device should be configurable, as it will allow the network administrator to control the number of distributions that occur. Customers that have a large number of devices may want to increase the interval so that their SMS is not overloaded with frequent distributions.

As a best practice, customers must tune their deployment so that the rate of Advanced Threat Entry submissions to the SMS does not result in increasing the depth of the device distribution queue. The rate of submission depends on the following:

- The API used for the submission: CSV file import or ADD API.
- The number of entries on the SMS. As such, a small Reputation Database has a higher number of distributions than a large Reputation Database.
- The time it takes to synch reputation entries to the devices in the customer's deployment.

Initial Rate Guidelines

The initial out-of-the-box guidelines for the CSV file import and Add/Delete API include the following:

- **CSV File Import:** Limit the rate of submission to approximately no more than one CSV file every two minutes.
- **Add/Delete API:** bursts up to 1,000 in intervals of five minutes.

CSV Add

Worst case: one entry per request

Submitting a file with only one entry (every few seconds or more) is the least efficient way to submit an entry to the SMS, as each request results in a distribution and a sync time, and the SMS can quickly get overwhelmed with distributions.

Note: The File Upload API uses the ADD API when a file contains 10 or less records, and this can help performance by reducing the number of distributions. This threshold can be configured with the assistance of the TippingPoint support team.

Best case: more than 1,000 entries per request

Batching a large number entries in one file is the most efficient way to add entries to the SMS, as there is no limit on the number of entries in a file, and each file will cause a distribution to the device.

Add API

One entry per request by design

A best practice when using this API is to send requests in bursts up to 1,000 entries, and bursts should be done in intervals to allow distributions to complete.

This depends on the number of entries in the Reputation Database and the time required to sync reputation entries to the devices in the customer's deployment. Sending one entry every few seconds is the worst case, as this results in a distribution, and the sync time between the SMS and the device can overwhelm the SMS with distributions.

Delete API

One entry per request by design

A best practice when using this API is to send requests in bursts up to 1,000 entries, and bursts should be done in intervals to allow distributions to complete.

This depends on the number of entries in the Reputation Database and the time required to sync reputation entries to the devices in the customer's deployment. Sending one entry every few seconds is the worst case, as this result in a distribution, and the sync time between the SMS and the device can overwhelm the SMS with distributions.

API Minimum Supported SMS Versions

Upcoming SMS releases will add support for API features as indicated in the table below.

Release	API Feature	Description
SMS 3.5 and later	Create Reputation Entries	Provides the ability to create reputation entries by importing them into the Reputation Database via CSV file.
SMS 4.1	Add Reputation Entries	Provides the ability to add reputation entries to the Reputation Database using HTTP.
SMS 4.1	Delete Reputation Entries	Provides the ability to delete reputation entries from the Reputation Database using HTTP.
SMS 4.1	Query Reputation Entries	Provides the ability to query reputation entries using HTTP.

Network Enforcement & Policy Management Using Advanced Threat Device Data

The information in this section describes tasks required to import reputation entries into the SMS Reputation Database from an advanced threat device, use these entries to build reputation filters, and distribute the filters to managed devices.

This information will enable customers to leverage advanced threat data in an integrated environment and to set up the following responses to reputation event triggers:

- *Block* action against the command and control network traffic and the malware source.
- *Permit + Notify* action for attempted communications from an infected host.
- *Block* or *Quarantine* an infected host.

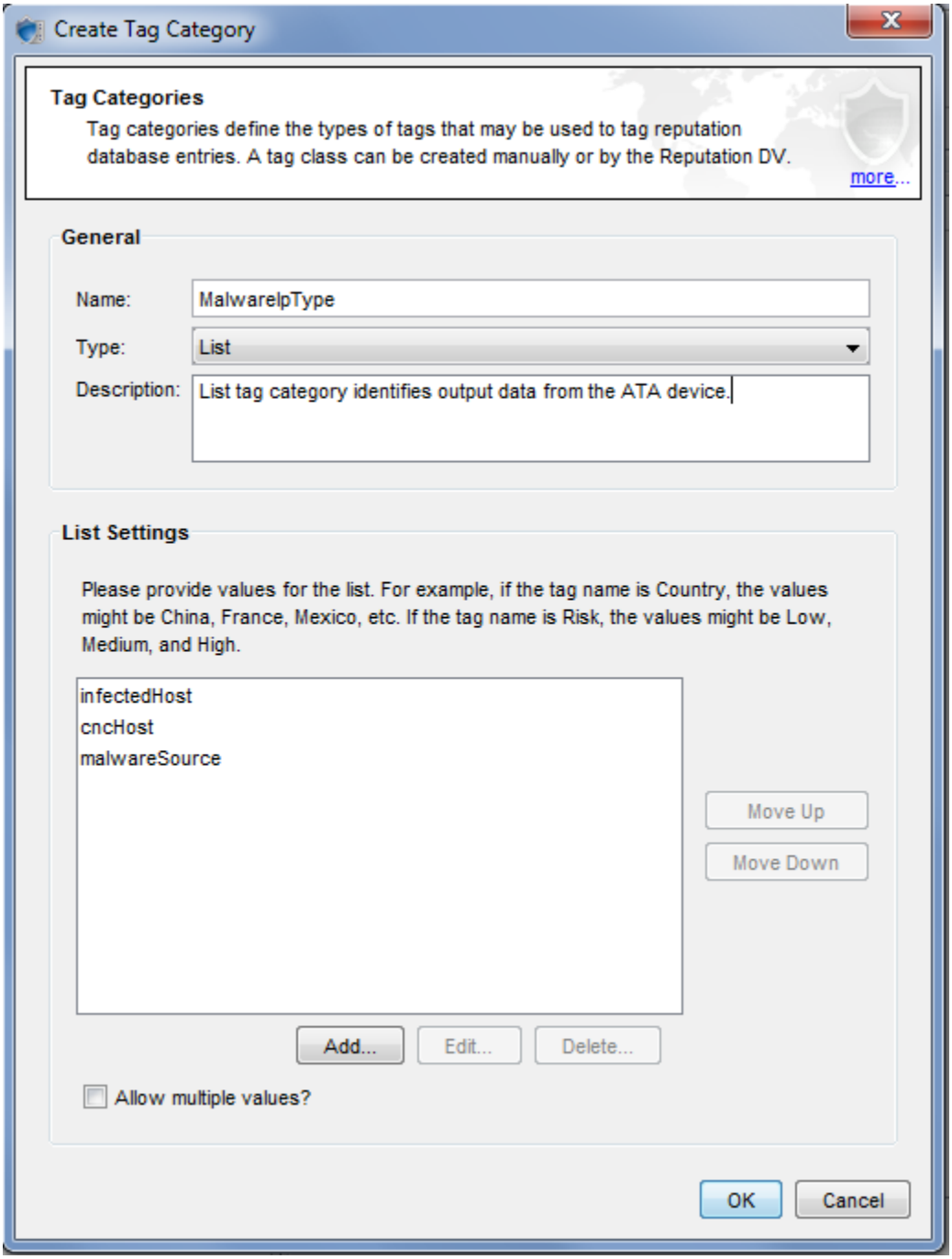
Mapping Advanced Threat Data to Reputation Tag Categories

Note: Before the SMS can use data imported from an advanced threat device, reputation tag categories must be manually created to map the data that will be used to create reputation entries. Reputation tag categories used for this purpose are created in the SMS client. For more information about tag categories, see Reputation Tag Categories on page 5.

Before creating tag categories, the SMS administrator must know which data from the advanced threat device-generated data to map. For example, the advanced threat device output includes address information for the infected host, the malware source, and a CnC host. In this case, the SMS administrator might create a *list* tag category in which list values correspond to the advanced threat device data.

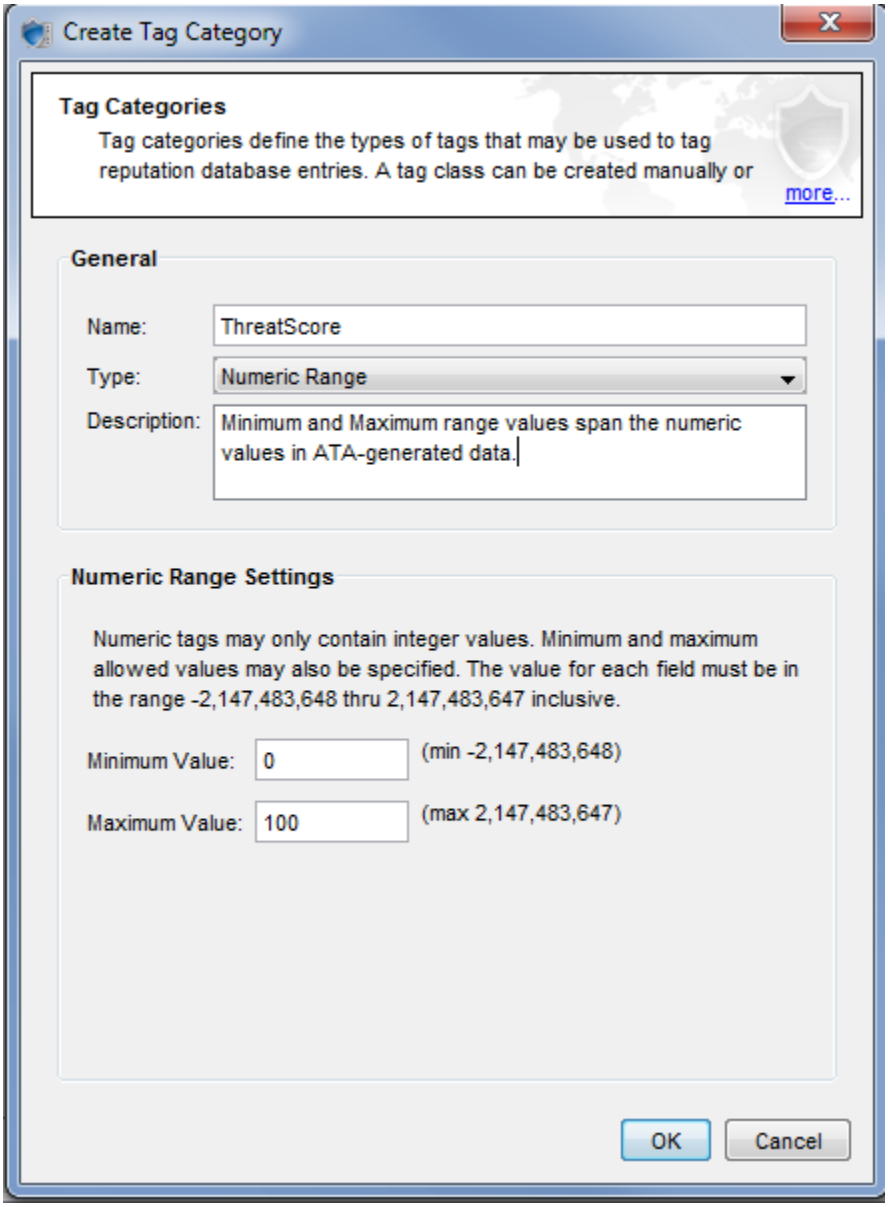
Note: The SMS is limited to a maximum of 20 tag categories for the Reputation Database, regardless of type.

Below is an example of a list tag category called *MalwareIpType*. List values would vary depending by advanced threat device, but would map data to be imported into the Reputation Database. In this example, the list values include *infectedHost*, *cncHost*, and *malwareSource*.



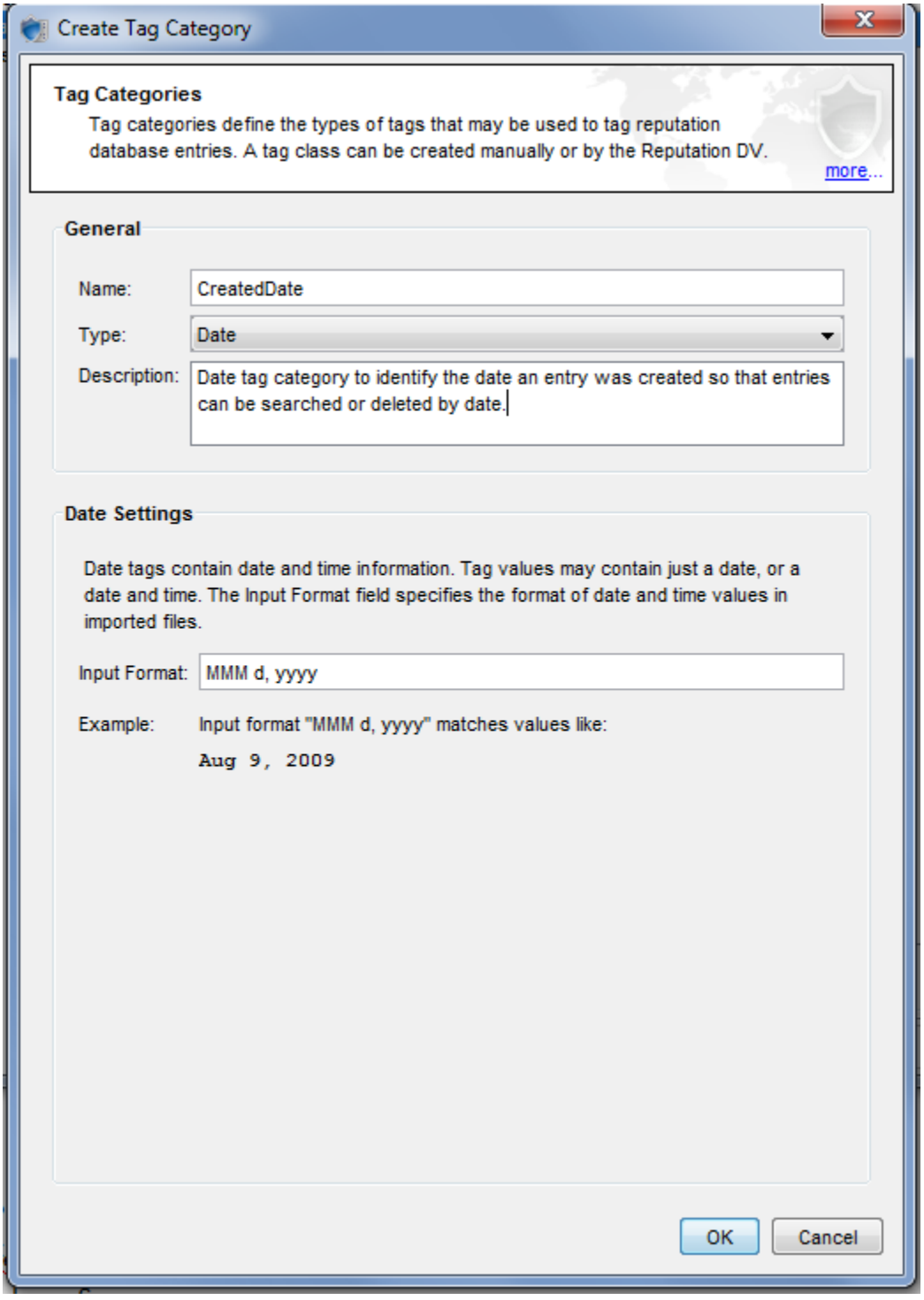
Some advanced threat devices provide a numeric range to indicate how likely it is that a host is infected or how much risk a particular type of malware presents. in this case, the SMS administrator might create a numeric range tag category so that a high-risk assessment could be used by the SMS to trigger a specific response.

The following example shows a numeric range tag category that might be used to map incoming values from an advanced threat device to the SMS. In this example, the tag category name, *ThreatScore*, matches the incoming data from the advanced threat device, and the numeric range *0-100* includes values from the advanced threat device data that indicate high risk.



The best practice is to include a date for imported entries, so that the SMS administrator can search for reputation entries by date and can delete obsolete data in batches.

The following example shows a date tag category that identifies the date that specific data was imported into the Reputation Database from an advanced threat device.

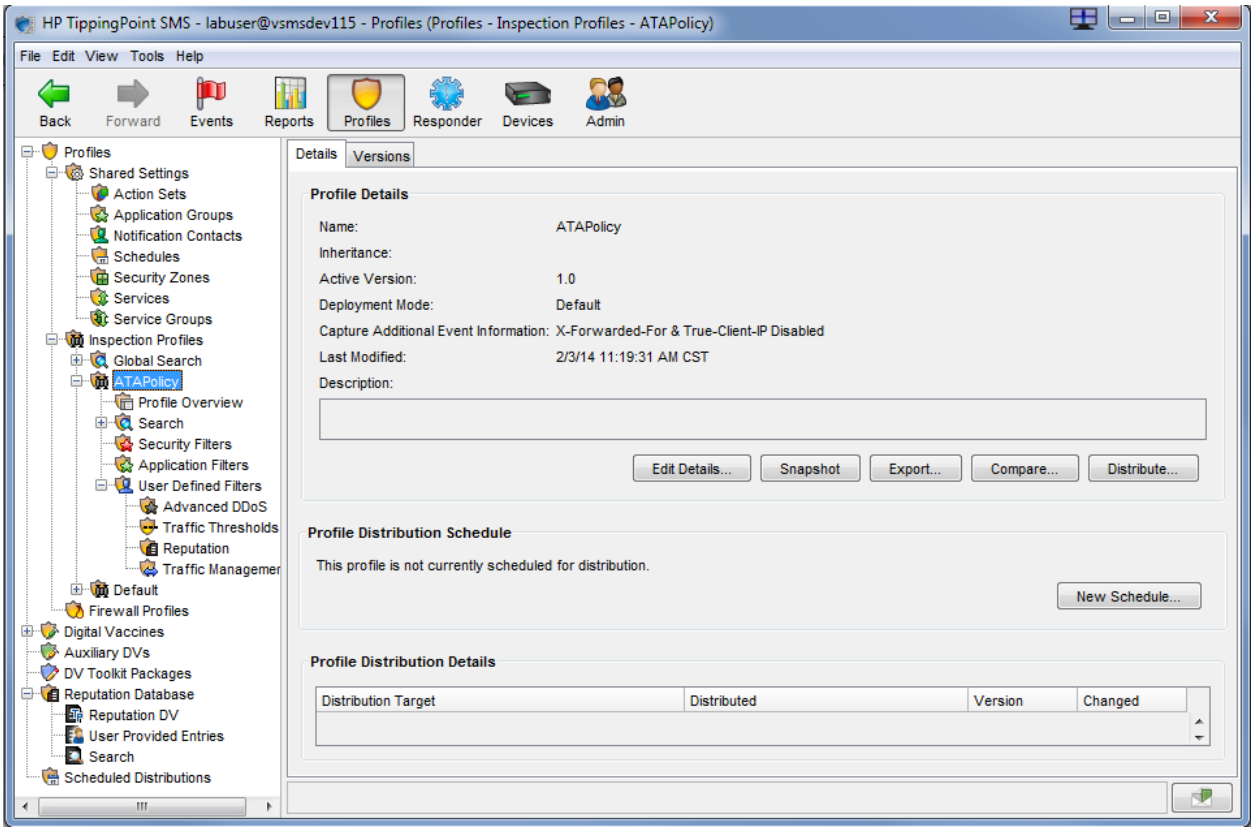

Create Tag Category
Tag Categories
Tag categories define the types of tags that may be used to tag reputation database entries. A tag class can be created manually or by the Reputation DV.
more...
General
Name:
CreatedDate
Type:
Date
Description:
Date tag category to identify the date an entry was created so that entries can be searched or deleted by date.
Date Settings
Date tags contain date and time information. Tag values may contain just a date, or a date and time. The Input Format field specifies the format of date and time values in imported files.
Input Format:
MMM d, yyyy
Example:
Input format "MMM d, yyyy" matches values like:
Aug 9, 2009
OK
Cancel

Transforming Imported Reputation Entries into Distributed Policy

Once reputation entries are imported from an advanced threat device, these entries can be used to create reputation filters associated with specific action sets. For more information on *reputation filters* and *action sets*, see Reputation Filters on page 6.

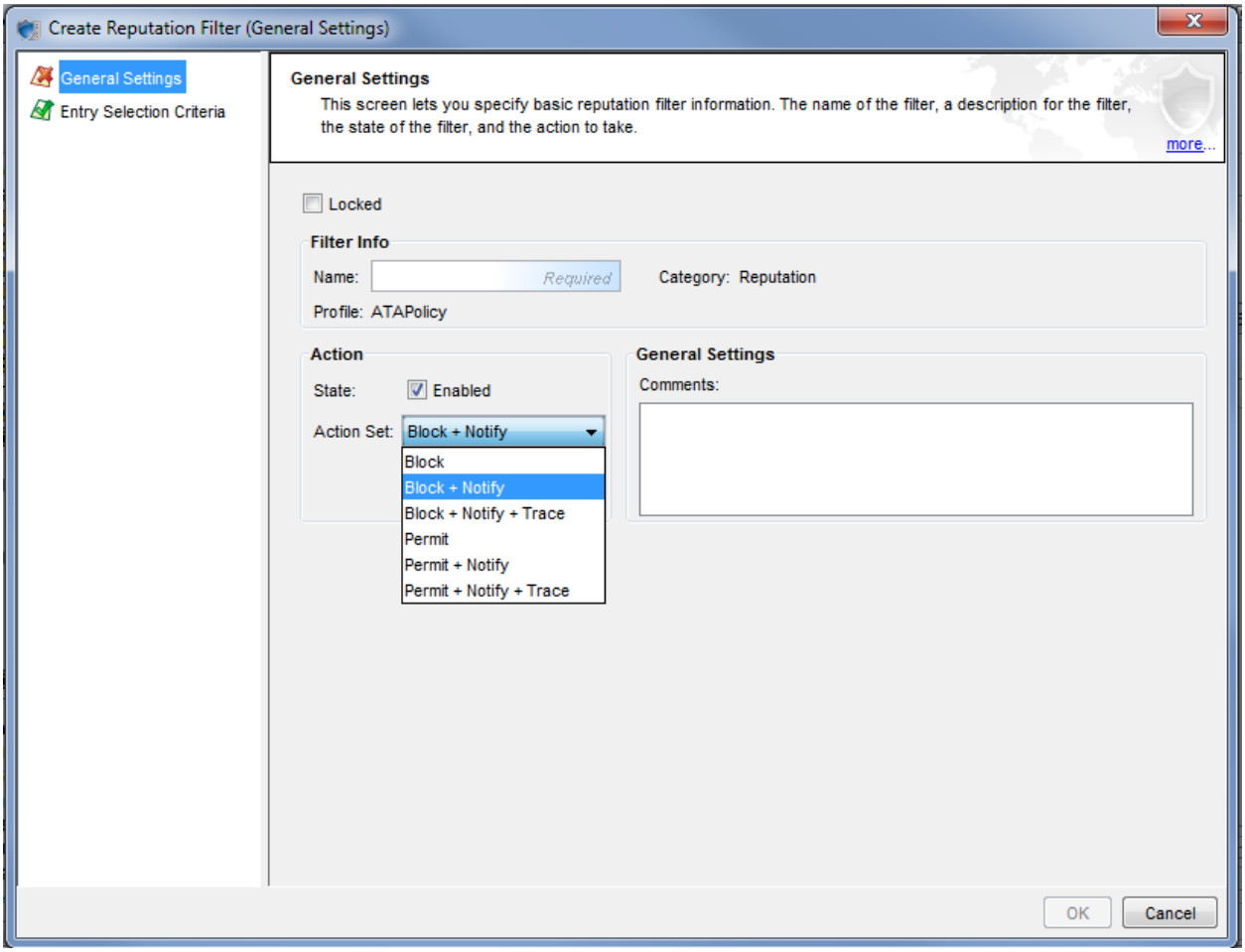
The SMS uses profiles to distribute filters, filter setting modifications, and associated actions to managed devices. For more information about profiles, see Profiles on page 6. Before creating reputation filters, an SMS administrator typically creates an inspection profile, which becomes the vehicle for distributing the security policy.

In the following example, an SMS administrator has created an inspection profile called *ATAPolicy* in which reputation filters will be created and distributed.

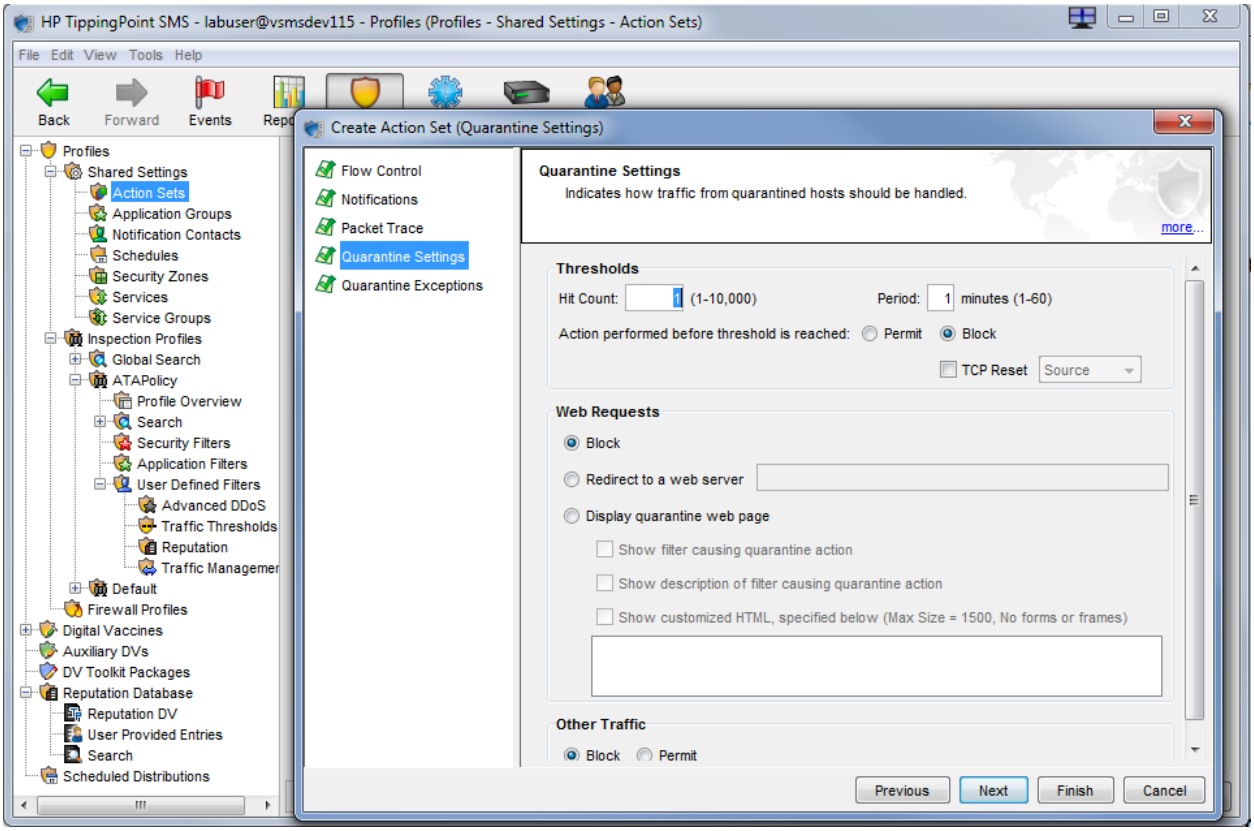


The inspection profile enables you to manage your distribution (e.g., all devices, some devices, specific segments, etc.), and it allows you to track where the filters you create will be distributed.

The SMS administrator uses the Create Reputation Filter wizard to create reputation filters. The General Settings screen prompts for basic filter information: Name, State, Action Set, and Comments.



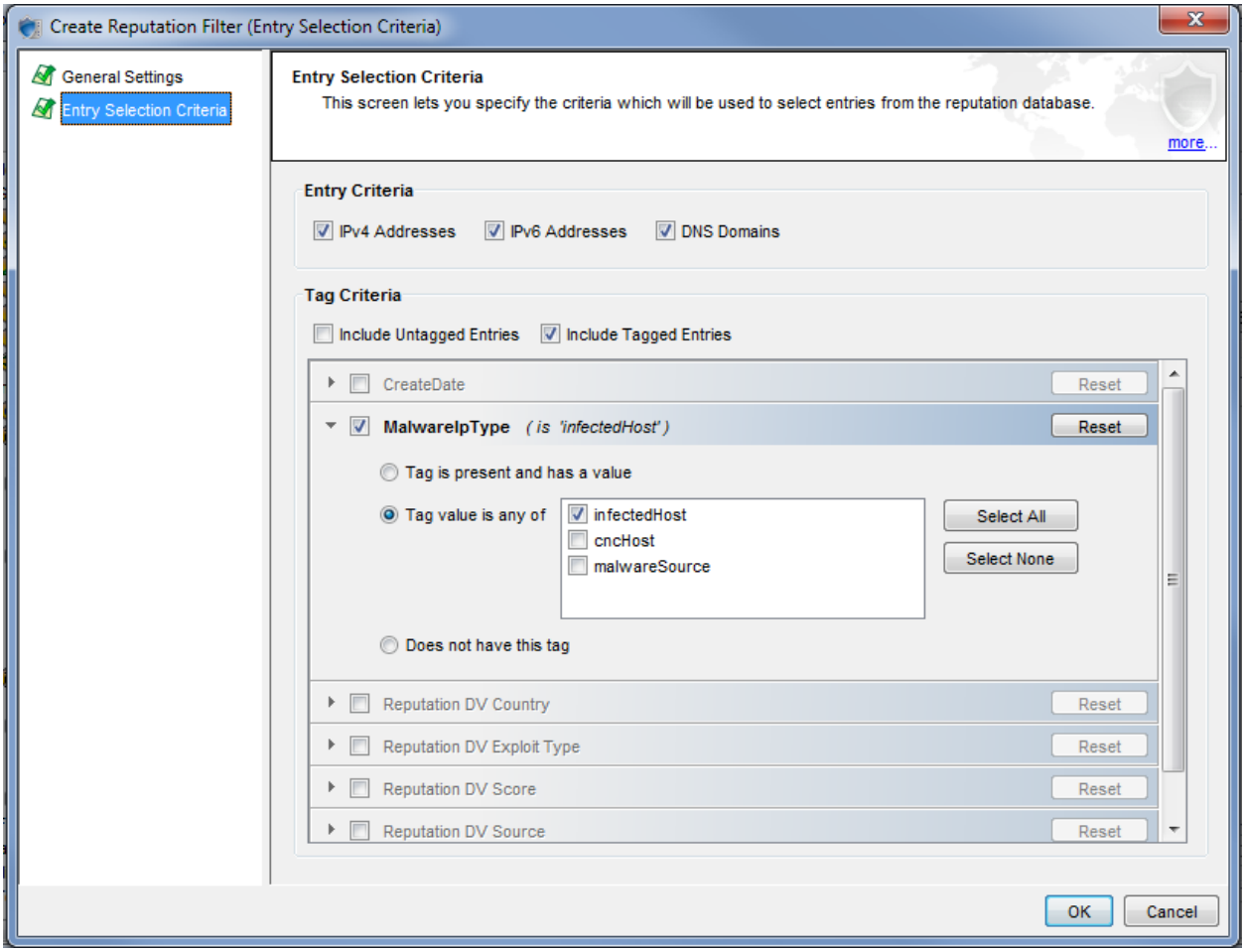
Block, *Permit*, and *Notify* actions are available by default. For a *Quarantine* response, the SMS administrator can create a custom action set under Shared Settings in the SMS client (see the image below). Creating a custom action set for Quarantine response allows you to set packet trace options, specify options to handle traffic from quarantined hosts, and to configure exceptions.

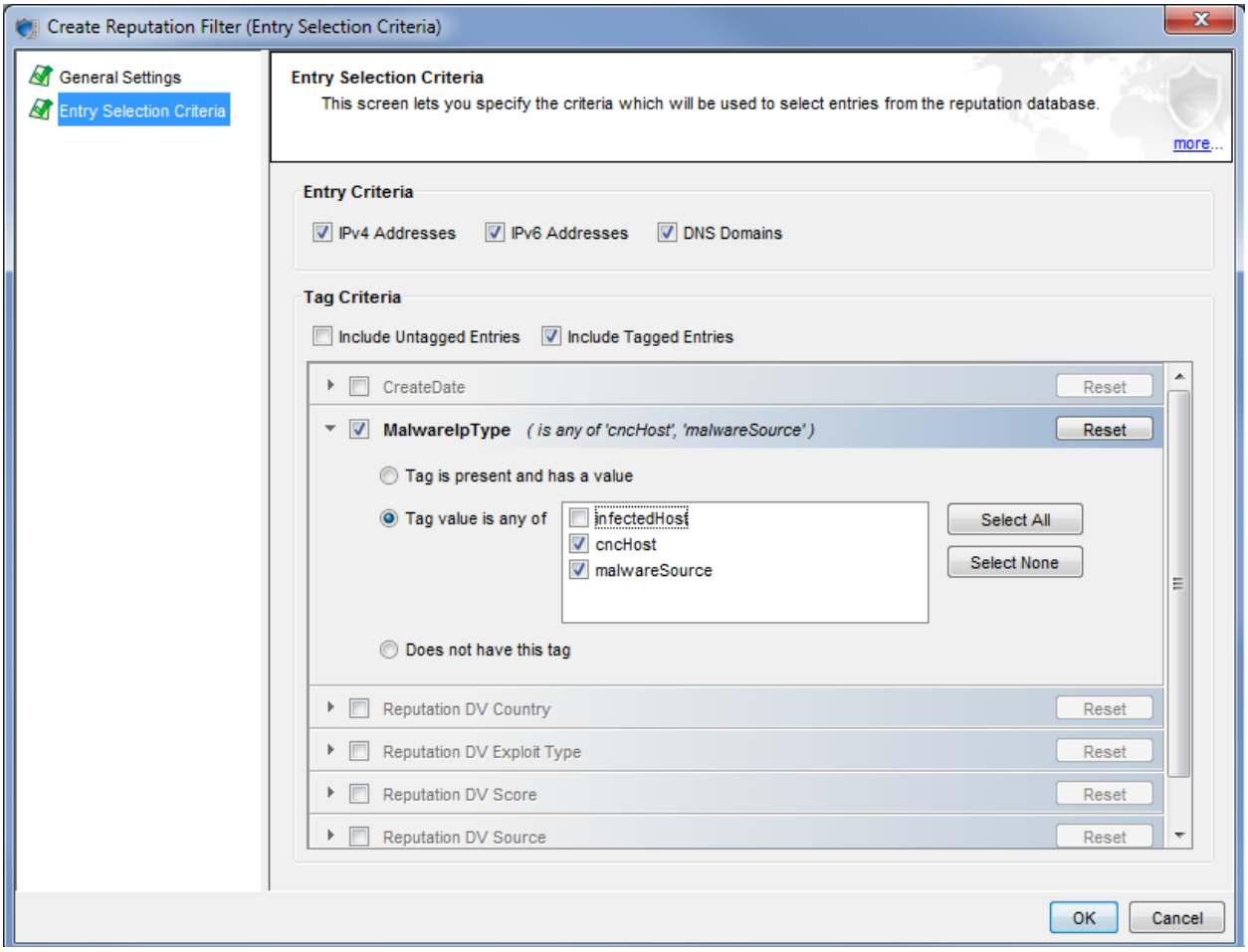


In the SMS Create Reputation Filter wizard, the Entry Selection Criteria screen enables the administrator to specify criteria to use for selecting entries from the Reputation Database. The administrator uses this screen to specify the reputation tag categories for the filter. For more details, see Mapping Advanced Threat Data to Reputation Tag Categories on page 17.

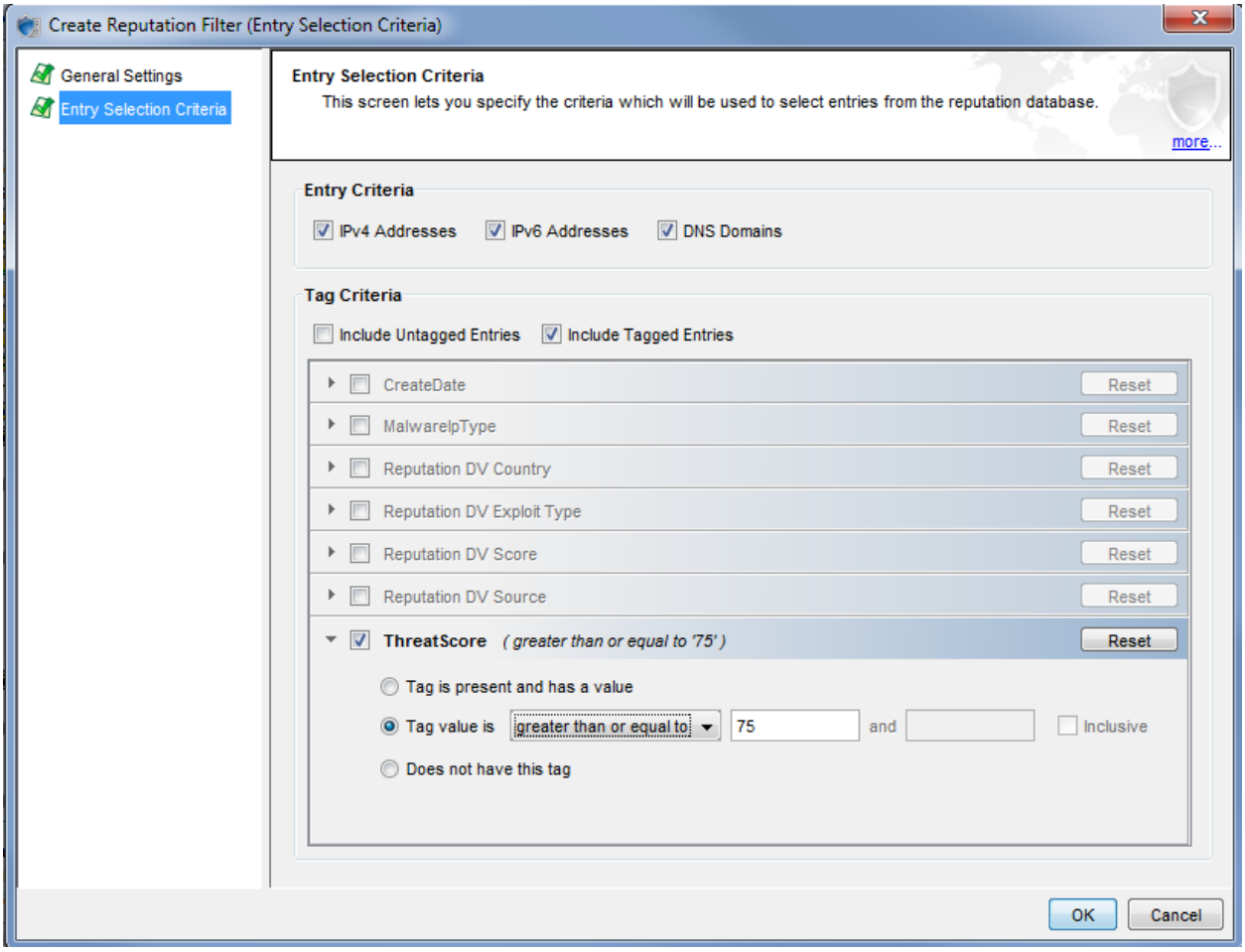
The following examples show Entry Selection Criteria for reputation filters using the tag category examples in Mapping Advanced Threat Data to Reputation Tag Categories on page 17.

The images below show entry selection criteria for reputation filters that match list values from the MalwareIpType reputation category tag shown at the beginning of this chapter.

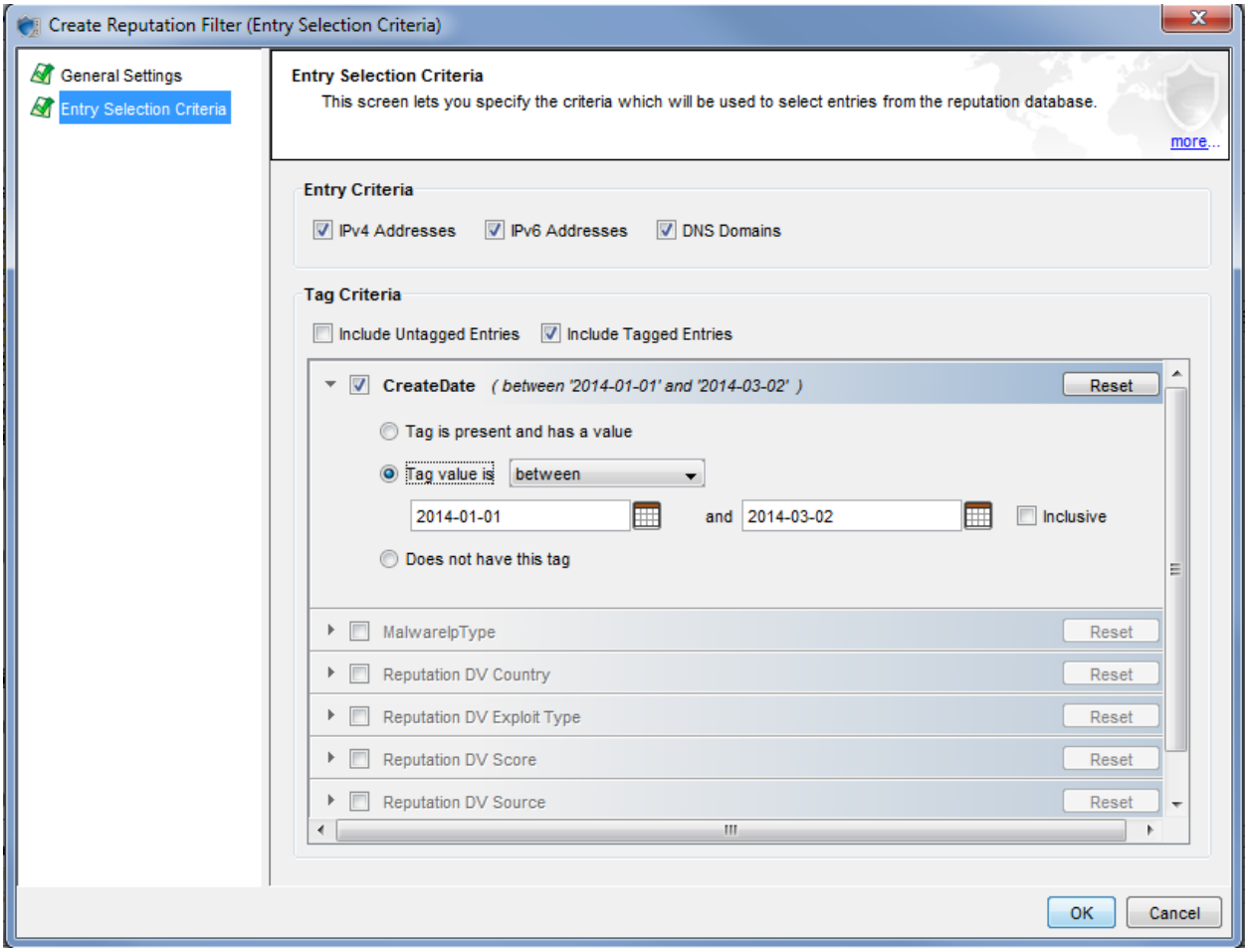

Create Reputation Filter (Entry Selection Criteria)
General Settings
Entry Selection Criteria
Entry Selection Criteria
This screen lets you specify the criteria which will be used to select entries from the reputation database.
more...
Entry Criteria
IPv4 Addresses
IPv6 Addresses
DNS Domains
Tag Criteria
Include Untagged Entries
Include Tagged Entries
CreateDate
Reset
MalwareIpType (is 'infectedHost')
Reset
Tag is present and has a value
Tag value is any of
infectedHost
cncHost
malwareSource
Select All
Select None
Does not have this tag
Reputation DV Country
Reputation DV Exploit Type
Reputation DV Score
Reputation DV Source
OK
Cancel



The following image shows a reputation filter created to identify entries that have a Threat Score of 75 or greater.



The following image is an example of a reputation filter to identify entries created between January 1, 2014 and March 3, 2014, in yyyy-MM-dd format.



After adding reputation filters to the profile, the administrator distributes the profile to the appropriate devices or segments. Once the profile is distributed, any updates to the Reputation Database entries from the advanced threat device will automatically update the profile and cause it to be redistributed.

Searching Reputation Entries

The SMS client enables you to search reputation entries using Filter Criteria (e.g., “Reputation” filter category), Source Criteria, Additional Criteria (e.g., associated action), or Filter Taxonomy Criteria. For more information about searching reputation entries, see the *HP TippingPoint Security Management System User Guide*.

Deleting Reputation Entries

The SMS client enables users to delete reputation entries from the Reputation Database. For more information about deleting reputation entries using the SMS client, see the *HP TippingPoint Security Management System User Guide*.

You can also delete a reputation entry by HTTP request. For information about deleting a reputation entry using this method, see Deleting a Reputation Entry on page 11.