ThreatDV
Deployment and Best Practices

May 2017

Legal and notice information

ThreatDV Deployment and Best Practices

Contents

About this guide

Welcome to the ThreatDV Deployment and Best Practices.

This section covers the following topics:

Target audience

The intended audience includes technicians and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint security systems and associated devices. Users should be familiar with networking concepts and the following standards and protocols:

- TCP/IP
- UDP
- ICMP
- Remote Authentication Dial In User Service (RADIUS)
- Terminal Access Controller Access-Control System Plus (TACACS+)
- LDAP
- Ethernet
- Network Time Protocol (NTP)
- Secure Sockets Layer (SSL)
- Simple Network Time Protocol (SNTP)
- Simple Mail Transport Protocol (SMTP)
- Simple Network Management Protocol (SNMP)

Related documentation

A complete set of documentation for your product is available on the TippingPoint Threat Management Center (TMC) at: *https://tmc.tippingpoint.com*. The documentation generally includes installation and user guides, command-line interface (CLI) references, safety and compliance information, and release notes.

Conventions

This information uses the following conventions.

Typefaces

TippingPoint uses 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.

Product support

Get support for your product by using any of the following options:

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

International: See *https://tmc.tippingpoint.com*

Introduction

Threat Digital Vaccine (ThreatDV) is a premium subscription service that includes both the reputation feed and the malware filter package.

Reputation feed

The reputation feed enables you to monitor and block inbound and outbound communications with known malicious and undesirable hosts. It is a robust security intelligence feed powered by advanced analytics and a global reputation database of IPv4, IPv6, and Domain Name System (DNS) names. The reputation feed is updated multiple times a day to stay ahead of emerging threats and reduce your network security risks.

Malware filter package

The malware filter package is a set of filters that provide malware protection. These filters provide alerts on a wide range of malware families and are designed to detect post-infection traffic, including:

- Bot activity
- Phone-home
- Command-and-control (C&C)
- Data exfiltration
- Mobile threats
- Domain generation algorithms (DGA)

The malware filter package is updated weekly.

Reputation feed

The reputation feed continuously mines up-to-date security research from multiple internal and external sources. These sources enable the reputation feed to identify and isolate known and suspected compromised IP addresses and domain names. Subscribers define their security policies based on the categories and reputation scores of these IP addresses and domain names. Because updates are received every two hours, the network security of subscribers stays current.

Note: The former RepDV service has been renamed to *reputation feed*. The combination of the reputation feed and the malware filter package is referred to as *ThreatDV*.

The Security Management System (SMS) also supports user-defined reputation entries. These are separate entries that are not updated by the reputation feed from DVLabs.

Reputation scores

Each reputation entry has an associated reputation score that represents potential risk level. Reputation scores range from 1 to 100, with a score of 100 representing a definite threat. Reputation scores are categorized into the following five ranges:

- **80-100**: These IPs are blocked by default when using the recommended default profile.
- **60-79**: These IPs are known to be somewhat malicious, but may not have enough corroborating information.
- **40-59**: These IPs are likely to be malicious, but TippingPoint does not have enough information to assign them a score of 60.
- **23-39**: These IPs are mostly non-malicious in nature, but may have generated undesirable traffic.
- **0-19**: These IPs generally do not represent any threat, but may have generated slightly suspicious traffic.

You can use reputation scores to assess and reassign risk for reputation filters that are active on a device. If suspicious activity continues, you can assign a higher score to the reputation entry.

For more information, see the Rep Feed Dashboard on ThreatLinQ at *https://threatlinq.tippingpoint.com/*.

Best practices

To avoid inadvertently interrupting business-critical communications, be sure to whitelist critical hosts, such as your external partners.

Malware filter package

The malware filter package delivers a set of advanced filters that are specifically designed to detect and block malware.

Note: The former RepDV service has been renamed to *reputation feed*. The combination of the reputation feed and the malware filter package is referred to as *ThreatDV*.

Malware filter packages are delivered as Auxiliary DVs. Auxiliary DVs are filter packages that supplement the regular DV and can be activated and deployed independently of the regular DV. You can manage malware filter packages by using the Auxiliary DV feature from the SMS and the Local Security Manager (LSM). Malware filter packages are available on the TMC at *https://tmc.tippingpoint.com* to current subscribers of the ThreatDV service.

System requirements

The following platforms support the ThreatDV malware filters:

- Intrusion Prevention System (IPS) with TOS v3.7.0 or later installed
- Next Generation Firewall (NGFW) with TOS v1.1.1 or later installed
- Threat Protection System (TPS) with TOS v4.0.0 or later installed
- SMS with version 4.1 or later installed

Best practices

A majority of the filters in the malware filter package are disabled by default to prevent false positives or performance impacts. If you want to monitor traffic and enable filters with blocking or other disruptive action sets, first enable the filters in **Permit+Notify**.

Activate the malware filter package and review the filters contained in the package. You can determine which filters you need to apply immediately to address a specific threat. After you learn the behavior of the filters in your network environment, you can determine which actions (block, disable, or permit) to apply.

View malware filters

1. In the SMS, expand **Profiles > Inspection Profiles**.
2. Select **Global Search**.
3. Expand the Source Criteria section to reveal the Package Source options. Select **Auxiliary DV (Malware)**. You can also search a particular profile.

In the LSM, you can search filters while editing profiles. For more information, see the LSM documentation for your security device

DGA Defense filters

Various malware families use domain generation algorithms (DGA) to randomly generate a large number of domain names to avoid hard-coding IP addresses or domain names within the malware. The infected host then attempts to contact some of the generated domain names to communicate with its C&C servers.

DGA Defense filters use pattern recognition and linguistic analysis to detect algorithmically generated DNS requests from infected hosts. As part of the malware filter package, these filters protect your system against known malware families, in addition to suspicious domain names generated by unknown malware families.

Device deployment

To effectively use DGA Defense filters, your security device must be deployed so that it is in the flow of DNS requests from your network. If your security device is deployed between the DNS server and the Internet or other DNS servers, it could block normal DNS traffic.

Important: To avoid inadvertently blocking normal DNS traffic, add filter exceptions for your DNS servers. In some networks, a DNS server or aggregator may be behind the IPS, NGFW, or TPS. This may result in the DNS server or aggregator appearing to be infected with malware when it is actually just forwarding requests.

DGA filter set

The following are the different types of DGA filters:

- DNS response
- HTTP response

DNS response

There are two types of DNS Response DGA filters: NOERROR and NXDOMAIN.

The NOERROR filters detect a NOERROR DNS response. A NOERROR response to a DNS query means that the hostname that was queried exists and is well-formed.

The NXDOMAIN filters detect an NXDOMAIN DNS response. An NXDOMAIN response to a DNS query means that the hostname that was queried does not exist.

HTTP response

The HTTP response filters detect an HTTP response from a web server for a hostname that appears to be using a generic or unknown DGA.

This section only contains the DGA filter set with generic DNS and HTTP response filters. For more information about DGA filters for a particular malware family, such as BankPatch or Dyre, use the filter details in the SMS. See *View DGA filters* on page 11.

19665: DNS: Suspicious DNS Lookup NOERROR Response (DGA)

This filter detects a NOERROR response to a DNS query for a hostname that appears to be using a generic or unknown Domain Generation Algorithm. The NOERROR response means that the queried domain is valid and exists. This could indicate an active attempt by a malware campaign to exfiltrate data or otherwise control a breached host. However, due to the nature of this detection method, this filter is prone to false positives in certain situations as outlined below.

What It Does

This filter is effective at detecting breached hosts that are compromised by an unknown family of malware and are involved in active communication with a Command and Control server. It can be used to find and remediate malware infections.

What It Doesn't Do

This filter will not prevent a host from becoming breached in the first place. This detection method is post-infection only. It should also be noted that this filter only detects the DNS portion of communication with a Command and Control server. Other parts of the exploitation chain such as HTTP, FTP, or other protocols are out of the scope of this filter.

Deployment Recommendations

There is some risk of false positives (see Examples below) as well as performance impacts in DNS-heavy environments. Because of this, the filter is not enabled by default, and it is recommended that you fully vet this filter in your particular environment before enabling it. This filter is most effective when deployed with trace enabled so that you can examine the hostname that was being queried and decide on further actions from there.

Examples

True positives:

- tvjky3xzsmbxvpqgd.com
- zbjvpmtovtusimgw.com
- mzqdx.com

False positives:

- Acronymized domains (especially Chinese acronyms) such as sxbznqp.com

For additional information on filters, see the documentation on the *Threat Management Center (TMC)*.

20602: DNS: Suspicious DNS Lookup NXDOMAIN Response (DGA)

This filter detects an NXDOMAIN response to a DNS query for a hostname that appears to be using a generic or unknown Domain Generation Algorithm. The NXDOMAIN response means that the queried domain does not currently exist. This is an extremely strong indicator that the host sending out the DNS queries has been breached and is attempting to contact a Command and Control server in order to receive further instructions.

What It Does

This filter is effective at detecting breached hosts that are compromised by an unknown family of malware. It can be used to find and remediate malware infections before the host is able to find and communicate with a Command and Control server.

What It Doesn't Do

This filter will not prevent a host from becoming breached in the first place; it is post-infection only. This detection method is not effective for catching malware that is actively in communication with a Command and Control server. It should also be noted that this filter only detects the DNS portion of communication with a Command and Control server. Other parts of the exploitation chain such as HTTP, FTP, or other protocols are out of the scope of this filter.

Deployment Recommendations

This filter does not suffer from any known false positives or performance impacts and can be safely enabled by default. If you are wanting an even more conservative approach, it can be enabled with thresholding, but you should be aware that different families of malware send their DNS queries at different frequencies, so some fine-tuning may be required. This filter is most effective when deployed with trace enabled so that you can examine the hostname that was being queried and decide on further actions from there.

Examples

True positives:

- tvjky3xzsmbxvpqgd.com
- zbjvpmtovtusimgw.com
- mzqdx.com

False positives:

- none

For additional information on filters, see the documentation on the *Threat Management Center (TMC)*.

24119: HTTP: Suspicious HTTP Host Header HTTP Response (DGA)

This filter detects an HTTP request to a web server for a hostname that appears to be using a generic or unknown DGA.

What It Does

This filter is effective at detecting breached hosts that may be compromised by malware and are involved in active communication with a Command and Control server. It can be used to find and remediate malware infections.

What It Doesn't Do

This filter will not prevent a host from becoming breached in the first place. This detection method is post-infection only. It should also be noted that this filter only detects the HTTP portion of communication with a Command and Control server. Other parts of the exploitation chain such as DNS, FTP, or other protocols are out of the scope of this filter.

Deployment Recommendations

There is some risk of false positives as well as performance impacts in HTTP-heavy environments. Because of this, the filter is not enabled by default, and it is recommended that you fully vet this filter in your particular environment before enabling it. This filter is most effective when deployed with trace enabled so that you can examine the hostname that was being queried and decide on further actions from there.

Examples

True positive: Host: aadcd15734d97346bb85f545dc8ca03e7e.com

Best practices

The NOERROR filters inspect nearly every DNS response. Evaluate these filters individually to ensure that there are no performance impacts. You can safely enable these filters in **Permit+Notify+Trace** to examine each event and make an informed decision.

The NXDOMAIN filters are much less likely to have performance impacts or false positive concerns. Enable trace so that you can identify the domain name that is being requested to determine if it is a DGA or a valid host. You can safely enable these filters in **Block+Notify+Trace**.

View DGA filters

1. In the SMS, expand **Profiles > Inspection Profiles** and select **Global Search**.
2. In the Search Criteria screen, expand the Filter Criteria section to reveal the filter-specific options.
3. In **Filter Name**, enter `DGA` and click **Search**.
4. Browse the list of DGA filters.

For more information, see *View malware filters* on page 6.

Collecting event data

After you have imported, activated, and distributed the DGA filter set, you can collect event data on the filters. This section describes how to collect event data and covers the following topics:

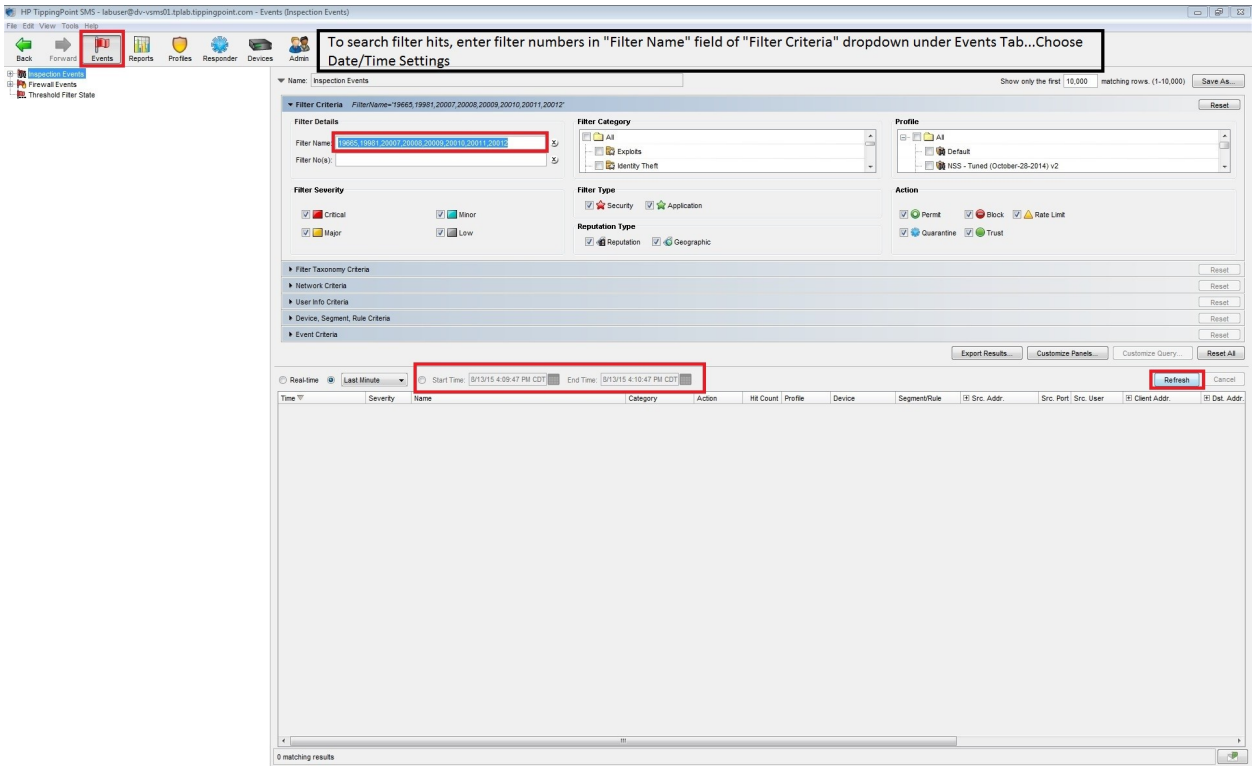
- *Inspect filter events* on page 12
- *Save packet traces* on page 13
- *Save event logs* on page 13

For more information about events, see the SMS documentation.

Inspect filter events

To confirm if the DGA filters have been triggered:

1. In the SMS, select **Events**.
2. Expand the **Name** list and select **Inspection Events**.

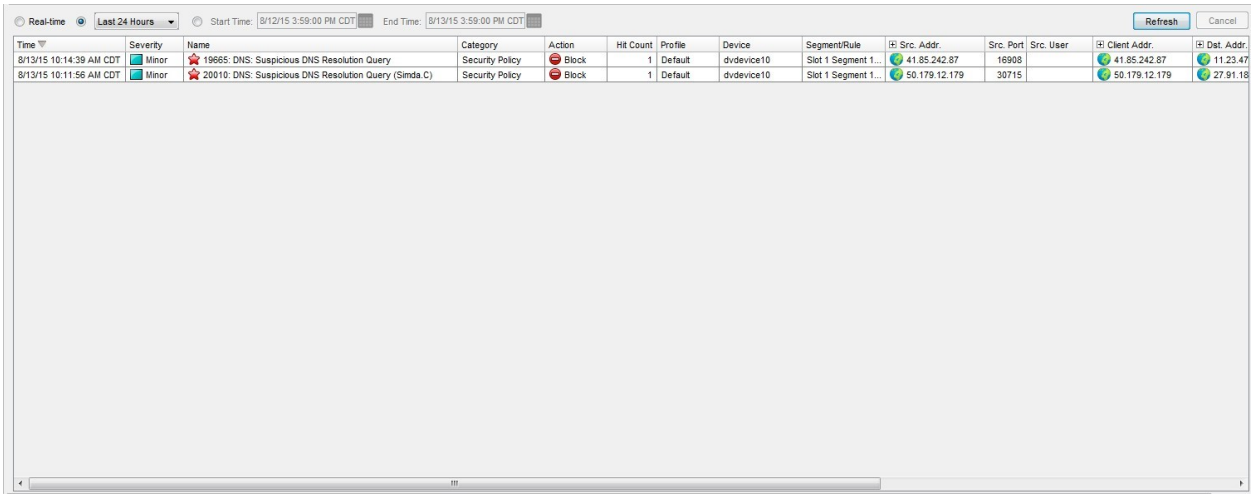


3. Expand **Filter Criteria** and enter the DGA filter numbers in the **Filter Name** box.
4. Click **Refresh**.

Save packet traces

After inspecting filter events, you can save packet traces.

1. Right-click an event (or multiple events) and select **Packet Trace**.



2. Click **Save**.
3. In the **Save File** dialog, save your data in a file with a name that uses the format `DDMMYYYY_FilterNumber.pcap`.
4. Click **Save**.

Save event logs

1. In the SMS, select **Profiles** > **Inspection Profiles** > **Default** (or your selected Profile of choice).
2. Expand **Filter Criteria** and enter the DGA filter numbers in the **Filter Name** box.
3. Click **Search**.

   Confirm all filter numbers searched are displayed in the **Search Results** pane.
4. Highlight all the results in the table.
5. Right-click and select **Export to file**.

   Confirm that the file type is set to **CSV (comma delimited)**.
6. Click **Save**.

Deploy the malware filter package

Subscribers to the ThreatDV service can download the latest malware filter package from the TMC at *https://tmc.tippingpoint.com/TMC/*. Malware filter package updates are delivered on a weekly basis, but follow a schedule independent from the regular DVs.

Note: A majority of the filters in the malware filter package are disabled by default to prevent false positives or performance impacts. For more information, see *Malware filter package best practices* on page 6.

In general, when you deploy the malware filters:

- Use your initial deployment as a trial run to detect potential problem areas.
- To establish an initial baseline, enable a subset of the malware filters with the recommended **Permit +Notify** action set. If you suspect an imminent threat, enable the filter that addresses the threat with a **Block** or **Block+Notify** action.
- Monitor events and evaluate the filters that are triggering to determine if they constitute a true threat or a false-positive.
- Adjust the filter settings accordingly to ensure the appropriate response. For example, change the action from **Permit** to **Block** or **Block+Notify** where needed.
- Continue monitoring, evaluating, and adjusting to mitigate any threats. Any gaps in your protection should be addressed through this process.

Manually download and import a malware filter package to the SMS

1. In a web browser, open *https://tmc.tippingpoint.com/TMC/*. If you have not already done so, create a TMC account.
2. On the TMC menu, select **Releases** > **ThreatDV** > **Auxiliary DV (Malware)**.

   The Auxiliary DV (Malware) Packages page opens with the most recent version at the top of the list.
3. Click **Download** next to the package in the list.
4. Review the End User License Agreement (EULA), and then click **Accept** to continue (or **Decline** to cancel).
5. On the File Download screen, click **Save**.

   Note: To avoid unexpected behavior on the SMS, do not change the file name.
6. In the SMS, select **Profiles** > **Auxiliary DV** to display the Auto Auxiliary DV Activation screen.
7. In the Auxiliary DV Inventory section, click **Import**.

8. Select the malware filter package, and then click **OK**. The file imports and displays in the DV Inventory section.

To verify the malware filter package is installed, navigate to the Profiles section in your SMS and click **Auxiliary DVs**. The package information is displayed in the Auxiliary DV Inventory section. Make sure the Auxiliary DV malware filter package is listed.

Set up automatic updates on the SMS

Use the following steps to configure the SMS to automatically update Auxiliary DV packages.

1. In the SMS, select **Profiles** > **Auxiliary DV** to display the Auto Auxiliary DV Activation screen.
2. In the Auto Auxiliary DV Activation screen, click **Edit**.
3. In the Auto DV Settings, select the automatic options to apply, and then click **OK**.
   - Automatic Download – Automatically get latest Auxiliary DV updates on the SMS when available.
   - Automatic Activation – Activate the Auxiliary DV after it is downloaded to the SMS.
   - Automatic Distribution – Distribute the Auxiliary DV package updates after it is downloaded to the SMS and activated.

   Note: When all three options are selected, the installed malware filter package on devices managed by the SMS will be updated with each refresh provided on the TMC.

Activate a malware filter package on the SMS

Use the following steps to activate packages that have been deactivated or are not automatically activated.

1. In the SMS, select **Profiles** > **Auxiliary DV** to display the Auto Auxiliary DV Activation screen.
2. On the Auto Auxiliary DV Activation screen inventory listing, select the Auxiliary package to activate, and then click **Activate**. If you choose to deactivate an Auxiliary DV package, select the package and then click **Deactivate**.

   Note: You cannot delete a package that is active on a device until it has been deactivated.

Distribute an inspection profile on the SMS

Use the following steps to distribute inspection profile overrides.

1. In the SMS, select **Profiles** > **Inspection Profiles** > **Default** (or your selected Profile of choice).
2. Click **Distribute**.
3. In the **Inspection Profile Distribution** window, select the appropriate device or devices.

Deployment tasks without an SMS

You can manually download the malware filter package from the TMC at *https://tmc.tippingpoint.com/TMC/* if:

- You are not using the SMS to manage your IPS, NGFW, or TPS device
- Your device is registered for the ThreatDV service

Note: Before you can use the malware filter package, you must enable the filters in a profile on the LSM.

Verify reputation feed is enabled

Use the LSM to verify that a ThreatDV license is enabled. For a standalone device:

- On the LSM System Summary page, select **License** and verify that the Reputation Permit status is Allow.
- To view the currently installed version of the license package, navigate to **System** > **Update** > **Update Summary** and view the Currently Installed Versions listed. If no version number or "N/A" is listed, then the ReputationDV service is not enabled for the device.

Install the malware filter package

Use the LSM to download and install the malware filter package to the local device. For a standalone device:

1. In the LSM, expand **System** > **Update**, and then click **Install Package**.
2. Follow the steps provided to access the TMC, select the package from the **Releases** menu, and then download the package to the local device. Note the download location.
3. After verifying available disk space – if you need to free disk space to meet the requirements, delete older versions of DV packages that are no longer used - select the options you want to apply:
   - Enable High Priority Preferences – Give the DV update process highest priority.

     Note: The system does not prioritize updates over attacks.
   - Enable Layer-2 Fallback – Place the device in Layer-2 Fallback mode during the DV update process.
4. Select the package you downloaded to the device and click **Install**.

View currently installed versions

Use the LSM to verify that the malware filter package installed successfully. For a standalone device:

1. In the LSM, expand **System** > **Update**.
2. Click **Update Summary** and scroll to the Auxiliary DV Packages section.

The currently installed Auxiliary DVs by type, version description, and function are displayed. Verify that the malware filter package is on the list.

Get malware filter package updates

To update the malware filter package, see *Manually download and import a malware filter package to the SMS* on page 14. Devices that are not managed by the SMS do not support automatic updates for the malware filter package.

Note: Auto update can be enabled using the Auto Auxiliary DV Activation feature on the SMS.

For a standalone device:

1. In the LSM, expand **System** > **Update**.
2. Select the Auxiliary Malware Filter Package and click **Update Now**.

   The latest update is downloaded from the TMC and installed on the device.

Troubleshooting tips

Use the following tips to address errors you might encounter during deployment of the malware filter package. For more information about known issues with the malware filter package feature, review the product release notes on the TMC at *https://tmc.tippingpoint.com/TMC/*.

Importing malware filter packages on the SMS

If a `Package not found` error is displayed when you use **Import** to import a malware filter package on the SMS, this typically indicates that the SMS client is out of sync with the server data.

To resynchronize the data:

1. Log out of the session, and then log back in.
2. Try to import the package again.

If you are unsuccessful, contact a support representative. See *Product support* on page 3.

Backing up the malware filter package

The SMS might fail to display the malware filter package information properly when using the system backup features. For example, only the activated packages might appear on the System Backup page for the malware filter package after a restore procedure, even though a complete restore was successful.

Adaptive Filter Control

If you enable Adaptive Filter Configuration (AFC), the behavior of a ThreatDV malware filter might be altered according to the AFC mode enabled for the device.