TippingPoint Deployment Note: Threat Digital Vaccine (ThreatDV)

Reputation Digital Vaccine (RepDV) is now the Threat Digital Vaccine (ThreatDV), a premium subscription service that includes both the reputation database from Reputation Digital Vaccine (RepDV) plus the new Malware Filter Package.

Important: If you already subscribe to RepDV, your subscription will automatically switch to a ThreatDV subscription. See Deploy the Malware Filter Package on page 3 for information on downloading and deploying the Malware Filter Package.

Reputation Feed

Previously known as Reputation DV, Reputation Feed enables organizations 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. Reputation feed is updated multiple times a day to stay ahead of emerging threats and reduce customer security risks.

Malware Filter Package

The Malware Filter Package is new set of filters that uses a different technology than the Reputation Feed to provide targeted malware protection. These filters alert on a wide range of currently active malware families. These filters are designed to detect post-infection traffic such as:

- Bot activity
- Phone-home
- Command-and-control
- Data exfiltration

The Malware Filter Package is updated at least weekly to provide malware protection for your network.

Malware Filter Package

ThreatDV: Malware Filter Package delivers an additional layer of malware protection through advanced threat protection filters. The use of the malware filters with the Reputation Feed provides the most comprehensive security coverage for enterprise environments. The Malware Filter Package is available now on the Threat Management Center (TMC) to current subscribers of the ThreatDV service, formerly known as Reputation Digital Vaccine (RepDV).

Note: To align with the new ThreatDV bundling of these security offerings, the RepDV service has been renamed to Reputation Feed. The combination of Reputation Feed and Malware Filter Package is referred to as ThreatDV.

System requirements

The ThreatDV Malware filters are supported on the following platforms:

- IPS running TOS 3.7 or later
- Security Management System (SMS) running version 4.1 or later
- ThreatDV license enabled for your HP TippingPoint system

Note: The Malware Filter Package is not supported on the Next Generation Firewall (NGFW) appliances.

Malware Filter Package best practices

The Malware Filter Package is disabled by default when activated. HP DVLabs does not recommend turning on all filters in the Malware Filter Package installed on your device, except to establish a baseline. For best results, activate the Malware Filter Package and review the filters contained in the package to 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 based on your analysis.

When you create a profile, it will inherit the default profile settings regarding how to treat specific categories of filters. Malware filters are included in the Virus category. The recommended default action set for Virus category filters is not a Block action. Update the malware profile to override and change the action for the malware filters. For more information about the filter categories, refer to your product documentation.

View filters

The Malware Filter Package is delivered within the Auxiliary DV framework on a weekly basis. Use the SMS search function or the Local Security Manager (LSM) to search the filters:

- On the SMS, expand **Profiles** > **Inspection Profiles** and select **Global Search**. In the Search Criteria screen, expand the Source Criteria section to reveal the Package Source options. Select **Auxiliary DV (Malware)**. You can also search a profile for filters that are included in the profile.
- On the LSM, use the filter search facility and enter keyword "malware filter package" to display the malware filters

Note: For more information about searching for filters, see the SMS or LSM documentation. For more information about Auxiliary DV packages, see What is an Auxiliary DV on page 3.

What is Auxiliary DV?

Auxiliary DV is the architectural framework that allows you to manage filter package updates apart from Digital Vaccine packages on the SMS and IPS security devices. The Malware filter Package is delivered through the Auxiliary DV framework.

Auxiliary filter packages work in conjunction with the regular Digital Vaccine by augmenting the protection provided by the regular DV. Auxiliary filter packages do not duplicate any filters in the regular or any other filter package. The Auxiliary framework supports multiple types of concurrently active filter packages on a device, which means you can install or distribute an active Malware Filter Package without a conflict with the installed Digital Vaccine package.

You can manage the Malware Filter Packages using the Auxiliary DV features on the SMS and IPS devices during the initial launch period of the ThreatDV.

Deploy the Malware Filter Package

Customers who have the Reputation Feed (RepDV) service enabled can download the Malware Filter Package from the TMC to begin receiving regular updates. The Malware Filter Package updates are delivered on a weekly basis, but on a schedule independent from the regular Digital Vaccines.

⚠ HP DVLabs recommends proceeding with caution when implementing the Malware filters, which are disabled by default. Because of the breadth of these filters, there is a potential impact on performance and a higher rate of false positives.

In general, when you deploy the Malware Filters:

- Consider your initial deployment a trial run to detect potential problem areas.
- To establish an initial baseline, enable all malware filters by using 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 notifications 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.

SMS Filter Package Deployment

The following topics are specific to deployment tasks. For additional information, such as searching filters in installed filter packages and monitoring events and notifications, see Related documentation on page 8.

Manually download and install the Malware Filter Package

Use the following steps to download the Malware Filter Package from the Threat Management Center (TMC) and import it 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. See the *Read Me First* document that accompanied your product for the instructions.
2. On the TMC menu, select **Releases** > **ThreatDV** > **Auxiliary DV (Malware)**.

   The Auxiliary DV (Malware) Packages page will open with the most recent version at the top of the list.
3. Click the **Download** button next to the appropriate package in the list.
4. Review the End User License Agreement (EULA), then click **Accept** to continue (to cancel, click **Decline**).
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 that the Malware Filter Package is installed, navigate to the Profiles section on your SMS and click **Auxiliary DVs**. The package information is displayed in the Auxiliary DV Inventory section. Make sure that 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 on download to the SMS.
   - Automatic Distribution — Distribute the Auxiliary DV package updates when downloaded to SMS.

   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 procedure 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.

Deployment tasks without an SMS

You can manually download the Malware Filter Package from the TMC if:

- You are not using the SMS to manage your IPS device(s)
- Your device(s) are registered for the ThreatDV service

Note: Before you can use the Malware Filter Package, you must enable the filters in a profile.

Verify Reputation Feed is enabled

Use the following method to verify that a ReputationDV license is enabled on an IPS 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 on an IPS Device

Use the following steps to download and install the Malware Filter Package to the local device.

1. In the LSM navigation menu, expand **System** > **Update**, and then click **Install Package**.
2. On the Install Package screen, 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 give priority to 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 these steps to verify the Malware Filter Package installed successfully.

1. In the LSM navigation pane, 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 displays. Verify the Malware Filter Package is on the list.

Get Malware Filter Package updates on the device

Standalone IPS devices do not support automatic updates for the Malware Filter Package. To update the Malware Filter Package, use Manually download and install the Malware Filter Package on page 4.

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

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.

   Note: Enable Auto Update using the Auto Auxiliary DV Activation feature on the SMS.

Troubleshooting tips

The following tips will help you address errors you may encounter during deployment of the Malware Filter Package. For additional information about known issues with the Malware Filter Package feature in the SMS or the IPS, review the release notes for the respective product on the TMC.

Importing Malware Filter Packages on 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 re-synchronize 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 Support Information on page 8.

Setting up Auto Update notification

SMS 4.1 does not fully support DV Notification popups for the Malware Filter Package updates when DV Notification Popups is enabled in the Auto Auxiliary DV Activation screen. As a workaround, auto updates can be enabled.

HP recommends that you set up automatic updates of the Malware Filter Package by enabling the following options in the Auto Auxiliary DV Activation screen:

- Auto Download
- Auto Activation
- Auto Distribution

Backing up the Malware Filter Package

The SMS may fail to display the Malware Filter Package information properly when using the system backup features on the SMS. 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), there is the potential that the behavior of a ThreatDV Malware Filter may be altered according to the AFC mode enabled for the device.

Related documentation

For information about how to work with the malware filters in the SMS or in the device LSM or CLI, see the product documentation available on the Threat Management Center (TMC) at https://tmc.tippingpoint.com/TMC.

Support Information

HP TippingPoint is committed to providing quality customer support for all of our 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), https://tmc.tippingpoint.com/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.

Legal and notice information

Printed in the United States.