Advanced Malware Protection

The Cisco Advanced Malware Protection (AMP) integration equips routing and SD-WAN platforms to provide protection and visibility to cover all stages of the malware lifecycle:

- Before: Hardening the network border with firewall rules
- During: Blocking malware based on File Reputation and IPS Signatures
- After:
  - Using File Notifications to represent breaches that occurred;
  - Retrospectively detecting malware and providing automatic reporting;
  - During: Blocking malware based on File Reputation and IPS Signatures
  - Using advanced file analysis capabilities for detection and deeper insight into unknown files in a network

Table 1: Feature History

Release	Description
Cisco SD-WAN 19.1	Feature introduced. The Cisco Advanced Malware Protection (AMP) integration equips routing and SD-WAN platforms to provide protection and visibility to cover all stages of the malware lifecycle.

Overview of Advanced Malware Protection

The Cisco Advanced Malware Protection is composed of three processes:

- File Reputation: The process of using a 256-bit Secure Hash Algorithm (SHA256) signature to compare the file against the Advanced Malware Protection (AMP) cloud server and access its threat intelligence information. The response can be Clean, Unknown, or Malicious. If the response is Unknown, and if File Analysis is configured, the file is automatically submitted for further analysis.
- File Analysis: The process of submitting an Unknown file to the Threat Grid (TG) cloud for detonation in a sandbox environment. During detonation, the sandbox captures artifacts and observes behaviors of the file, then gives the file an overall score. Based on the observations and score, Threat Grid may change the threat response to Clean or Malicious. Threat Grid's findings are reported back to the AMP cloud, so that all AMP customers will be protected against newly discovered malware.

Note File analysis requires a separate Threat Grid account. For information about purchasing a Threat Grid account, contact your Cisco representative.

- Retrospective: By maintaining information about files even after they are downloaded, we can report on files that were determined to be malicious after they were downloaded. The disposition of the files could change based on the new threat intelligence gained by the AMP cloud. This re-classification will generate automatic retrospective notifications.

Configure and Apply an Advanced Malware Policy

To configure and apply an Advanced Malware Policy to a Cisco IOS XE SD-WAN device, do the following:

- Before you Begin, on page 2
- Configure and Apply an Advanced Malware Policy, on page 2
- Apply a Security Policy to a Device

Before you Begin

- Before you apply an IPS/IDS, URL filtering, or Advanced Malware Protection policy for the first time, you must upload the correct Cisco Security Virtual Image to vManage.
- To perform file analysis, you must configure the Threat Grid API Key as described in Configure Threat Grid API Key, on page 2

Configure Threat Grid API Key

To perform file analysis, you must configure your Threat Grid API key:

Step 1 Log into your Cisco AMP Threat Grid dashboard, and select your account details.

Step 2 Under your Account Details, an API key may already be visible if you've created one already. If you haven't, click Generate New API Key.

Your API key should then be visible under User Details > API Key.

Step 3 In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.

Step 4 In the Security screen, click the **Custom Options** drop-down and select **Threat Grid API Key**.

Step 5 In the Manage Threat Grid API key pop-up box, take these actions:

a) Choose a region from the **Region** drop-down.

b) Enter the API key in the **Key** field.

c) Click **Add**.

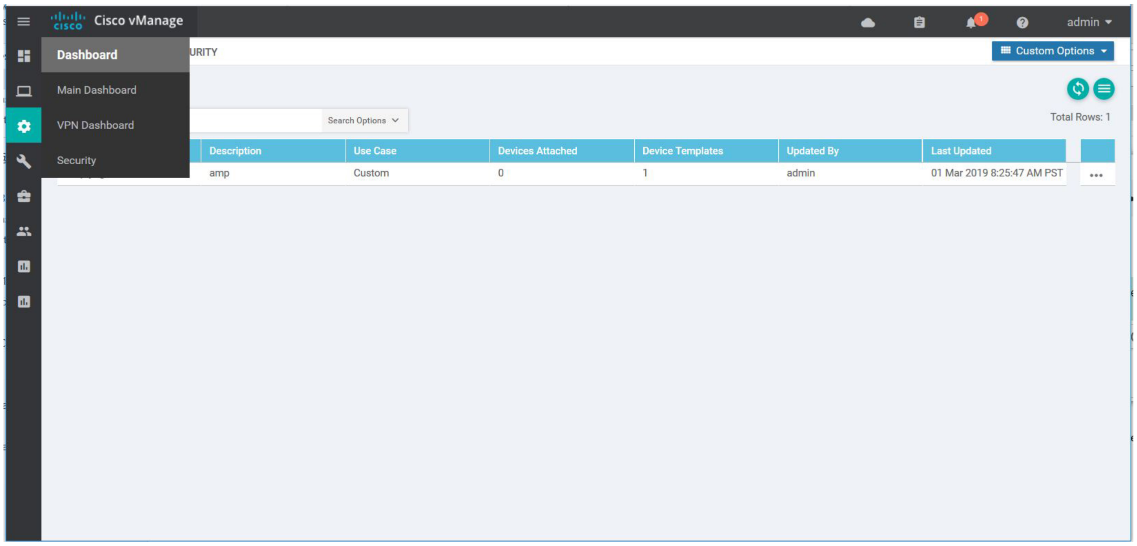
d) Click **Save Changes**.

Configuring an Advanced Malware Protection Policy

To configure an Advanced Malware Protection policy:

Step 1 In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.

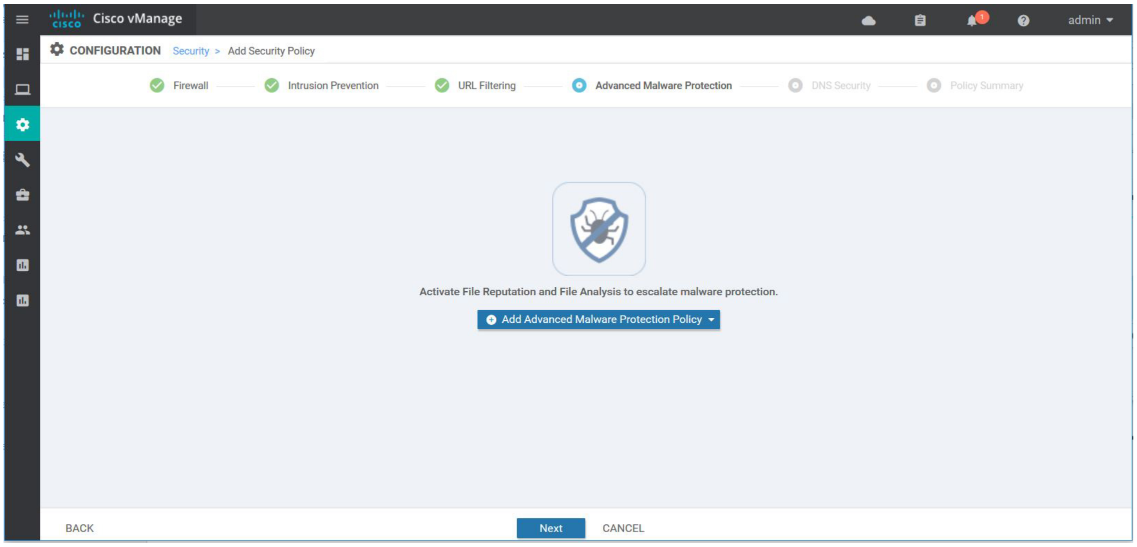
Step 2 Click **Add Security Policy**. The Add Security Policy wizard opens and various use-case scenarios display.



Description	Use Case	Devices Attached	Device Templates	Updated By	Last Updated
amp	Custom	0	1	admin	01 Mar 2019 8:25:47 AM PST

Step 3 In Add Security Policy, select **Direct Internet Access** and then click **Proceed**.

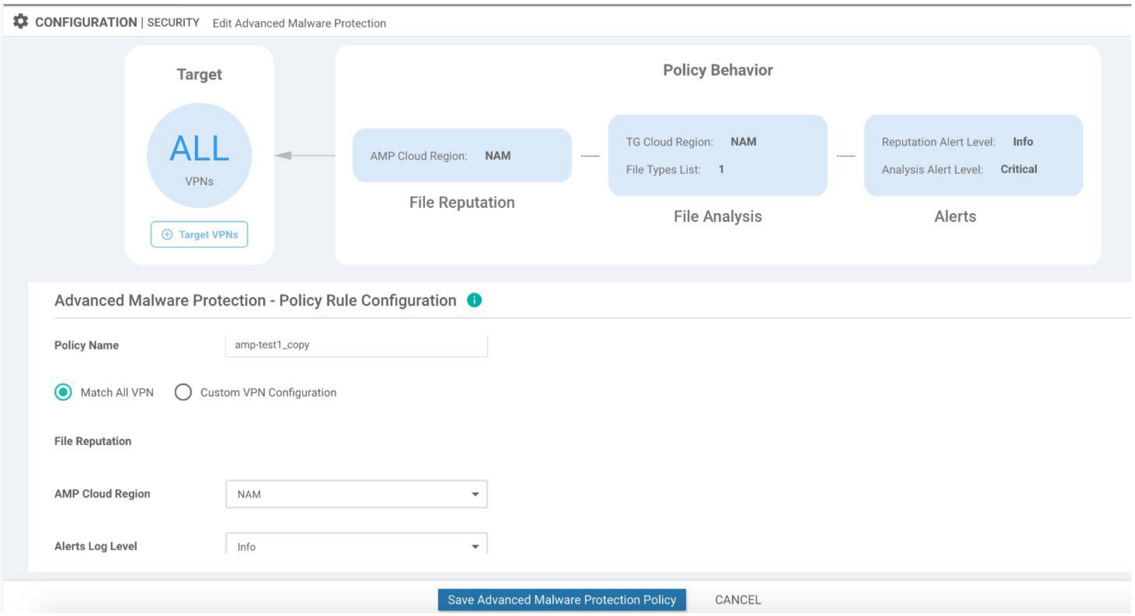
Step 4 In the Add Security Policy wizard, click **Next** as needed to select the **Advanced Malware Protection** tab.


Cisco vManage
admin
CONFIGURATION Security > Add Security Policy
Firewall
Intrusion Prevention
URL Filtering
Advanced Malware Protection
DNS Security
Policy Summary
Add Advanced Malware Protection Policy
BACK
Next
CANCEL
369307

Activate File Reputation and File Analysis to escalate malware protection.

Step 5 In the **Advanced Malware Protection** tab, click the **Add Advanced Malware Protection Policy** drop-down.

Step 6 Select **Create New**. The Add Advanced Malware Protection screen displays.


CONFIGURATION | SECURITY Edit Advanced Malware Protection
Target
ALL
VPNs
Target VPNs
Policy Behavior
File Reputation
File Analysis
Alerts
Advanced Malware Protection - Policy Rule Configuration
File Reputation
Save Advanced Malware Protection Policy
CANCEL
369308

AMP Cloud Region: NAM

TG Cloud Region: NAM
File Types List: 1

Reputation Alert Level: Info
Analysis Alert Level: Critical

Policy Name: amp-test1_copy

● Match All VPN ○ Custom VPN Configuration

AMP Cloud Region: NAM

Alerts Log Level: Info

Step 7 In the **Policy Name** field, enter a name for the malware policy. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8 Make sure that the **Match All VPN** button is selected. Select **Match All VPN** if you want to apply the policy to all the VPNs, or select **Custom VPN Configuration** to input the specific VPNs.

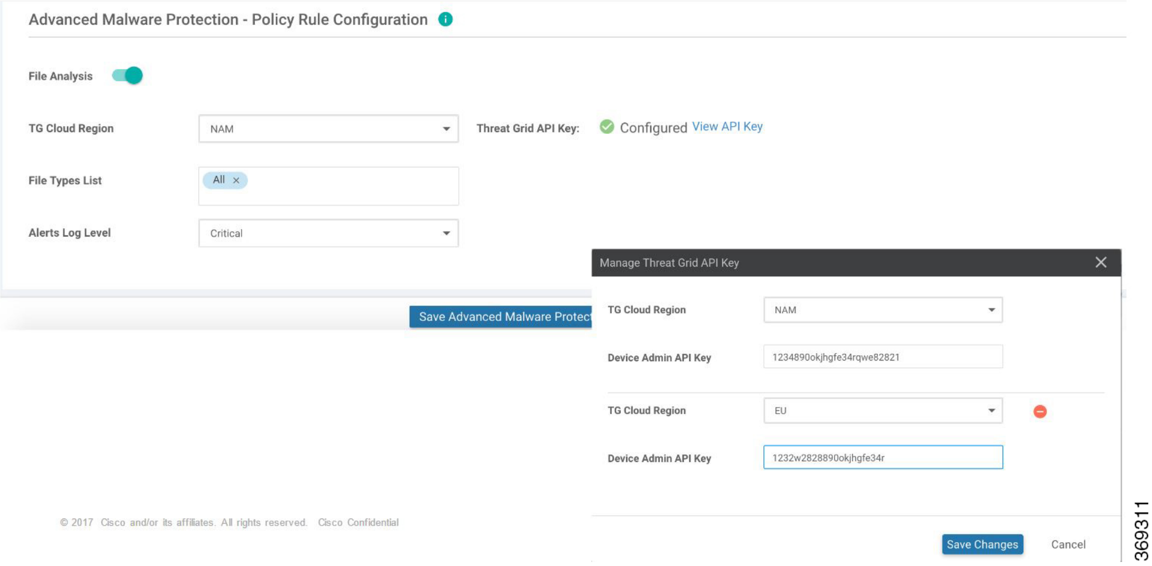
Step 9 From the **AMP Cloud Region** dropdown, select a global region.

Step 10 From the **Alerts Log Level** dropdown, select a severity level (Critical, Warning, or Info).

Note: Because the Info severity level generates multiple notifications and can affect system performance, this level should be configured only for testing or debugging and not for real-time traffic.

Step 11 Click **File Analysis** to enable Threat Grid (TG) file analysis.

Note Before you can perform this step, configure a threat grid API key as described in Configure Threat Grid API Key, on page 2.



Advanced Malware Protection - Policy Rule Configuration

File Analysis: on

TG Cloud Region: NAM

Threat Grid API Key: Configured

File Types List: All

Alerts Log Level: Critical

Manage Threat Grid API Key

TG Cloud Region: NAM

Device Admin API Key: 1234890okjhgfe34rqwe82821

TG Cloud Region: EU

Device Admin API Key: 1232w2828890okjhgfe34r

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Note File Analysis requires a separate Threat Grid license.

Step 12 From the **TG Cloud Region** dropdown, select a global region.

Note Configure the Threat Grid API Key by clicking on Manage API Key or as described in Configure Threat Grid API Key, on page 2

Step 13 From the **File Types List** dropdown, select the file types that you want to be analyzed.

Step 14 From the **Alerts Log Level** dropdown, select a severity level (Critical, Warning, or Info).

Step 15 Click **Target VPNs** to select the target VPNs or all VPNs, and then click **Add VPN**.

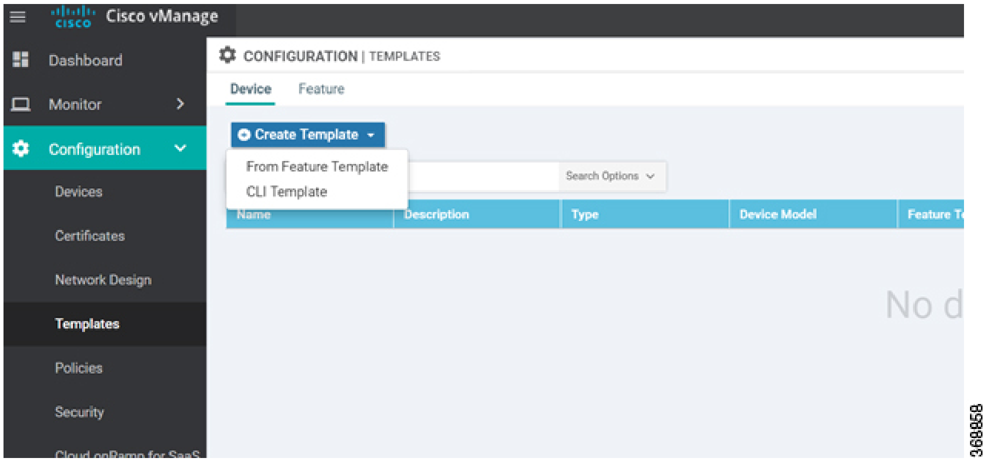
Step 16 Click **Save Changes**. The Policy Summary screen displays.

Step 17 Click **Next**.

Apply a Security Policy to a Device

To apply a security policy to a device:

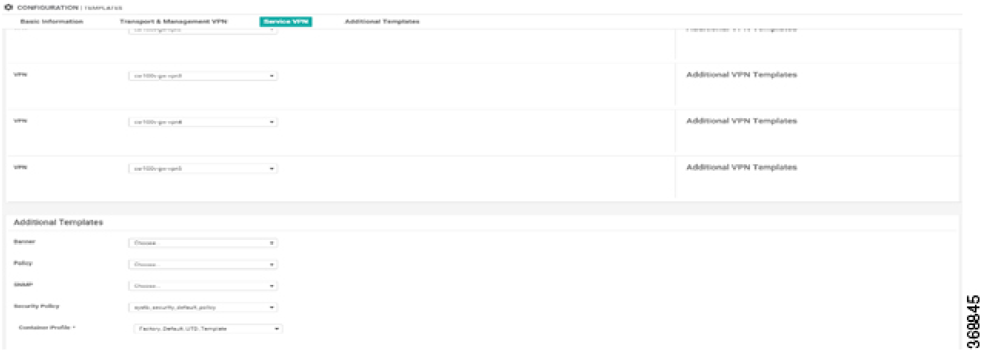
1. In vManage, select the **Configuration** > **Templates** screen.



2. In the Device tab, from the **Create Template** drop-down, select **From Feature Template**.

3. From the **Device Model** drop-down, select one of the IOS XE SD-WAN devices.

4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.



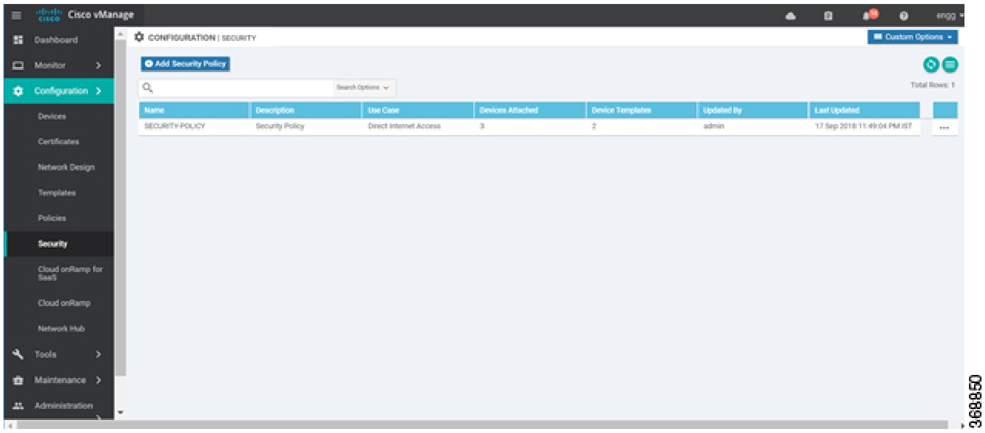
5. From the **Security Policy** drop-down, select the name of the policy you configured in the previous procedure.

6. Click **Create** to apply the security policy to a device.

Modify an Advanced Malware Protection Policy

To modify an Advanced Malware Protection policy, do the following:

1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.



Name	Description	Use Case	Devices Attached	Device Templates	Updated By	Last Updated	
SECURITY-POLICY	Security Policy	Direct Internet Access	3	2	admin	17 Sep 2018 11:49:04 PM IST	...

2. In the Security screen, click the **Custom Options** drop-down and select **Advanced Malware Protection**.

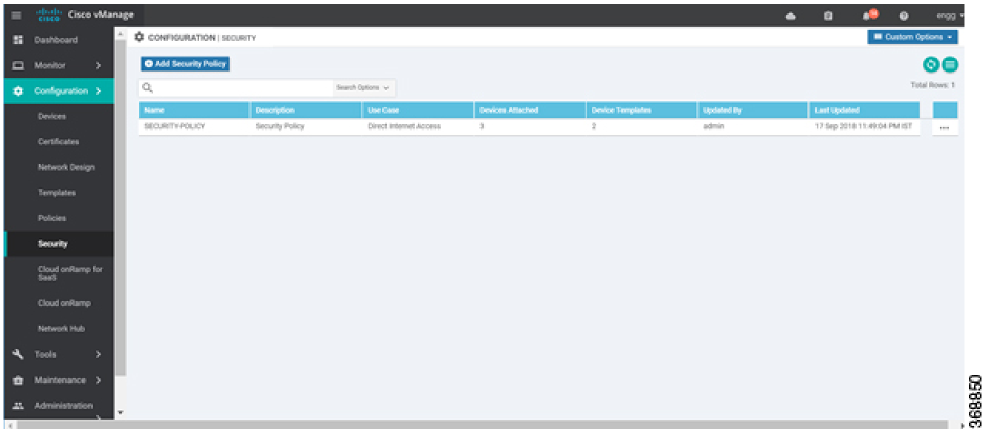
3. For the policy that you want to modify, click the **More Actions** icon to the far right of the policy and select **Edit**.

4. Modify the policy as required and click **Save Advanced Malware Protection Policy**.

Delete an Advanced Malware Protection Policy

To delete an Advanced Malware Protection policy, you must first detach the policy from the security policy:

1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.



Name	Description	Use Case	Devices Attached	Device Templates	Updated By	Last Updated	
SECURITY-POLICY	Security Policy	Direct Internet Access	3	2	admin	17 Sep 2018 11:49:04 PM IST	...

2. Detach the AMP policy from the security policy as follows:

   a. For the security policy that contains the AMP policy, click the **More Actions** icon to the far right of the policy and select **Edit**.

      The Policy Summary page is displayed.

   b. Click the **Advanced Malware Protection** tab.

   c. For the policy that you want to delete, click the **More Actions** icon to the far right of the policy and select **Detach**.

d. Click **Save Policy Changes**.

3. Delete the AMP policy as follows:

a. In the Security screen, click the **Custom Options** drop-down and select **Advanced Malware Protection**.

b. For the policy that you want to delete, click the **More Actions** icon to the far right of the policy and select **Delete**.

A dialog box is displayed.

c. Click **OK**.

Monitor Advanced Malware Protection

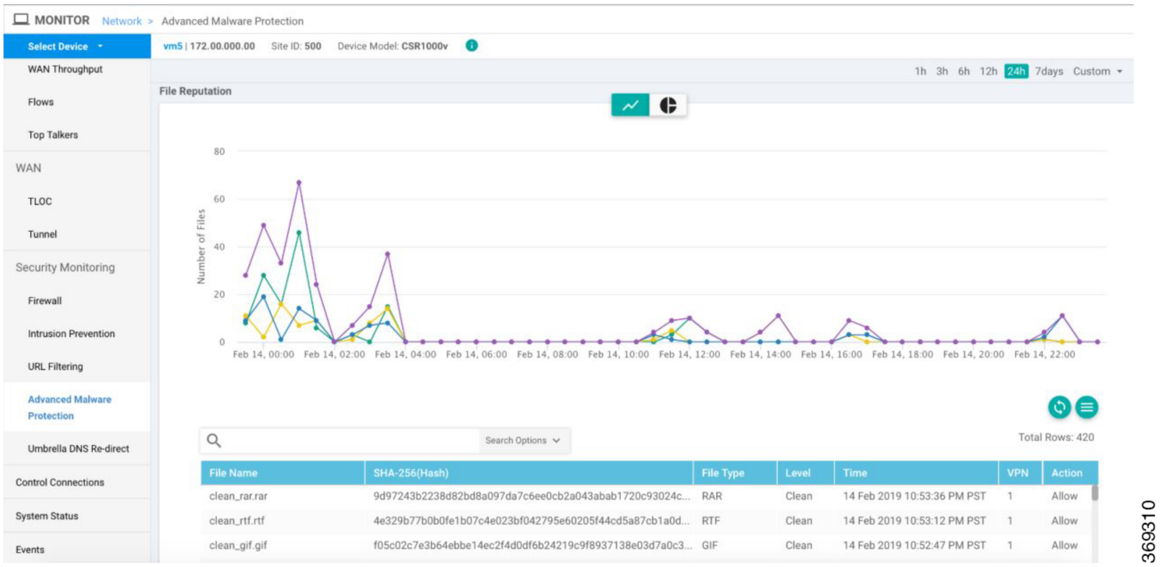
You can monitor Advanced Malware Protection from the Device Dashboard by using the following steps.

Step 1 From the **Monitor** > **Network** screen, select a device.

Step 2 In the left panel, under Security Monitoring, select the **Advanced Malware Protection** tab.

This tab shows the following:

- File Reputation – The graph or pie chart shows the total number of files transferred and how many are malicious, clean, or unknown. This tab area also includes a table with detailed information about each file that was inspected.
- File Retrospection – A table with detailed information about file retrospection events.
- File Analysis – A graph that shows the number of files that were uploaded to Threat Grid, and a table with detailed information about each file that was uploaded for analysis.



File Name	SHA-256(Hash)	File Type	Level	Time	VPN	Action
clean_rar.rar	9d97243b2238d82bd8a097da7c6ee0cb2a043abab1720c93024c...	RAR	Clean	14 Feb 2019 10:53:36 PM PST	1	Allow
clean_rtf.rtf	4e329b77b0b0fe1b07c4e023bf042795e60205f44cd5a87cb1a0d...	RTF	Clean	14 Feb 2019 10:53:12 PM PST	1	Allow
clean_gif.gif	f05c02c7e3b64ebbe14ec2f4d0df6b24219c9f8937138e03d7a0c3...	GIF	Clean	14 Feb 2019 10:52:47 PM PST	1	Allow

Troubleshoot Advanced Malware Protection

Malware in POP3 Account

If Cisco United Threat Defense (UTD) detects malware on a POP3 email server, UTD prevents email clients from downloading the email message with the malware, and then resets the connection between the email server and client. This prevents downloading any email after detection of the malware. Even later attempts to download email from the server fail if the problematic file remains on the server.

To resolve this, an administrator must remove the file(s) identified as malware from the server, to enable a new session between the server and client.

Rekey the Device Threat Grid API Key

To rekey the device Threat Grid API key from the Maintenance screen:

Step 1 In Cisco vManage, select the **Maintenance** > **Security** tab in the left side panel.

Step 2 Select the **Advanced Malware Protection** tab.

Step 3 Select the device or devices that you want to rekey.

Step 4 Select **Action** > **API Rekey**.