

Advanced Malware Protection

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

- Overview of Advanced Malware Protection, on page 1
- Configure and Apply an Advanced Malware Policy, on page 2
- Modify an Advanced Malware Protection Policy, on page 5
- Delete an Advanced Malware Protection Policy, on page 5
- Monitor Advanced Malware Protection, on page 6
- Troubleshoot Advanced Malware Protection, on page 6
- Rekey the Device Threat Grid API Key, on page 6
- Configure Advanced Malware Protection for Unified Security Policy, on page 7

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.



Note The maximum file size that will be inspected by AMP is 10 MB.



Note File Reputation supports the following file types: ACCDB, ALZ, AMF, AMR, ARJ, ASF, AUTORUN, BINARY_DATA, BINHEX, BMP, BZ, CPIO_CRC, CPIO_NEWC, CPIO_ODC, DICM, DMG, DMP, EGG, EICAR, ELF, EPS, FFMPEG, FLAC, FLIC, FLV, GIF, GZ, HLP, HWP, ICO, IMG_PCT, ISHIELD_MSI, ISO, IVR, JAR, JARPACK, JPEG, LHA, M3U, MACHO, MAIL, MAYA, MDB, MDI, MIDI, MKV, MNY, MOV, MP3, MP4, MPEG, MSCAB, MSCHM, MSOLE2, MSWORD_MAC5, MSZDD, MWL, NEW_OFFICE, NTHIVE, OGG, OLD_TAR, ONE, PCAP, PDF, PGD, PLS, PNG, POSIX_TAR, PSD, PST, RA, RAR, REC, REG, RIFF, RIFX, RIM, RMF, RPM, RTF, S3M, SAMI, SCRENC, SIS, SIT, SMIL, SWF, SYLKc, SYMANTEC, TIFF, TNEF, TORRENT, UUENCODED, VMDK, WAV, WEBM, WMF, WP, WRI, XLW, XPS, ZIP, ZIP_ENC, 7Z, 9XHIVE.

- 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. File Analysis supports a maximum file size of 10MB.



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 Catalyst SD-WAN device, do the following:

- Before you Begin, on page 3
- Configure an Advanced Malware Policy

- 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

Note A NAT direct internet access route is necessary to apply Advanced Malware Protection Policy.

Configure Threat Grid API Key

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

Procedure

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

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

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

Step 3 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.

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

Step 5 In the Manage Threat Grid API key dialog box, perform these steos:

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

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.

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

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

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

Step 5 From **Advanced Malware Protection**, click **Add Advanced Malware Protection Policy** in the drop-down menu.

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

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 Ensure **Match All VPN** is chosen. Choose **Match All VPN** if you want to apply the policy to all the VPNs, or choose **Custom VPN Configuration** to input the specific VPNs.

Step 9 From the **AMP Cloud Region** drop down menu, choose a global region.

Step 10 From the **Alerts Log Level** drop down menu, choose 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.

Note
File Analysis requires a separate Threat Grid license.

Step 12 From the **TG Cloud Region** drop down menu, choose 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

Step 13 From the **File Types List** drop down menu, choose the file types that you want to be analyzed.

Step 14 From the **Alerts Log Level** drop down menu, choose a severity level (Critical, Warning, or Info).

Step 15 Click **Target VPNs** to choose the target service 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. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.



Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose one of the devices.

5. Click **Additional Templates**.

   The **Additional Templates** section is displayed.

6. From the **Security Policy** drop-down list, choose the name of the policy you configured previously.
7. Click **Create** to apply the security policy to a device.
8. Click **…** next to the device template that you created.
9. Click **Attach Devices**.
10. Choose the devices to which you want to attach the device template.
11. Click **Attach**.

Note If you are migrating from older releases to Cisco IOS XE Release 17.2 or later with Application lists and the zone-based firewall that is configured in Cisco SD-WAN Manager, you must first remove the security template from the base template and push the base template. Thereafter, reattach the security template and then push the template to the device.

Note When a Zone based firewall template in attached to a Cisco IOS XE Catalyst SD-WAN device running on Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, there may be an increase in time for completion of tasks. This is due to the updates in the software version of Cisco vManage Release 20.6.1.

Modify an Advanced Malware Protection Policy

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. In the Security screen, click the **Custom Options** drop-down menu , choose **Policies/Profiles**, and then choose **Advanced Malware Protection**.
3. For the desired policy you want to modify, click **...** and choose **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. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Detach the AMP policy from the security policy as follows:
   a. For the security policy that contains the AMP policy, click **...** and choose **Edit**.

The Policy Summary page is displayed.

b. Click **Advanced Malware Protection**.

c. For the policy that you want to delete, click **...** and choose **Detach**.

d. Click **Save Policy Changes**.

3. To delete the AMP policy, perform these steps:

a. In the Security screen, click the **Custom Options** drop-down menu , choose **Policies/Profiles**, and then choose **Advanced Malware Protection**

b. For the policy that you want to delete, click **...** and choose **Delete**.

c. Click **OK**.

Monitor Advanced Malware Protection

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

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**, and choose a device.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**, and choose a device.

Step 2 Under Security Monitoring, click **Advanced Malware Protection** in the left pane.

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:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Security**.

Step 2 Click **Advanced Malware Protection**.

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

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

Configure Advanced Malware Protection for Unified Security Policy

You can create an advanced malware protection policy specifically for use in a unified security policy. When created, the advanced malware protection policy is included in the advanced inspection profile and applied to the unified security policy for implementation in Cisco IOS XE Catalyst SD-WAN devices.

To configure advanced malware protection for a unified security policy, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Custom Options**.
3. Click **Policies/Profiles**.
4. Click **Advanced Malware Protection** in the left pane.
5. Click **Add Advanced Malware Protection Policy**, and choose **Create New**.
6. Click **Policy Mode** to enable the unified mode. This implies that you are creating an advanced malware protection policy for use in the unified security policy.



Note

- Target VPNs are not applicable for the advanced malware protection used in a unified security policy.
- You can enable Policy Mode only when creating advanced malware protection policies. You cannot configure the unified mode once the policy is saved.

7. Enter a policy name in the **Policy Name** field.
8. From the **AMP Cloud Region** drop-down list, choose a global region.
9. From the **Alerts Log Level** drop-down list, choose 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.

10. Click **File Analysis** to enable Threat Grid file analysis.

Note Before you can perform Step 10, configure a threat grid API key as described in Configure Threat Grid API Key.

File Analysis requires a separate Threat Grid license.

11. From the **TG Cloud Region** drop-down list, choose a global region.

Note Configure the Threat Grid API Key by clicking **Manage API Key** or as described in Configure Threat Grid API Key.

From the **File Types List** drop-down list, choose the file types that you want to be analyzed.

12. From the **Alerts Log Level** drop-down list, choose a severity level (Critical, Warning, or Info).
13. Click **Save Advanced Malware Protection Policy**.