Cisco AMP

Malware Analysis Software

Introduction

Cisco AMP for Endpoints (Cisco AMP) is an intelligent, enterprise-class advanced malware analysis and protection solution used to detect, track, analyze, control, and block advanced malware. It provides protection before, during, and after an attack. Cisco AMP is not a replacement for antivirus, it performs more in-depth analysis than the average antivirus.

The Cisco AMP agent is installed on designated faculty/staff computers and can be seen running in the system tray. Cisco AMP will monitor files on your computer as well as files that are being downloaded to the computer. If a threat is detected, the Cisco AMP icon in the system tray will pop up and show that a file has been detected and blocked. Think of it like a more intelligent antivirus.

Finding Cisco AMP on your PC

1. If Cisco AMP is installed, an icon under the hidden icons area of your computer will be visible (bottom right).

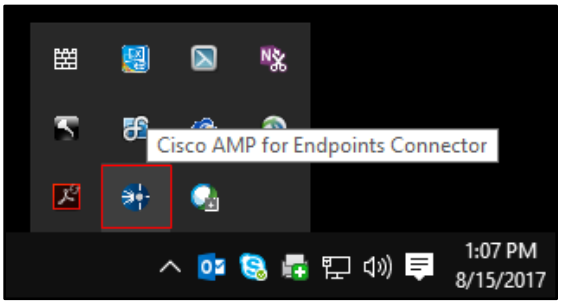

Figure 1

2. Right click the **Cisco AMP for Endpoints Connector icon** and select **Open Cisco AMP for Endpoints**. The **Cisco AMP for Endpoints** window will appear with three menu options:

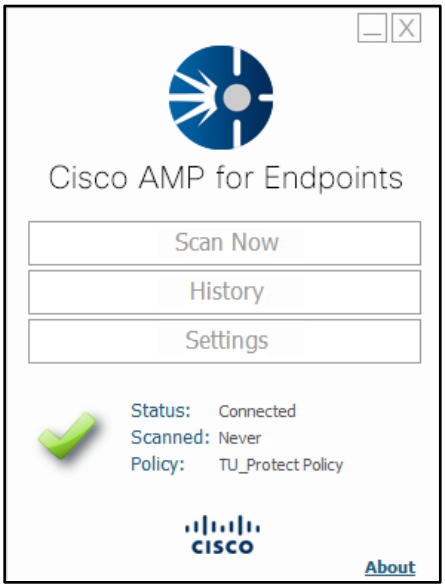

Figure 2

a. **Scan Now-** Choose from the three options to perform a scan on the computer:

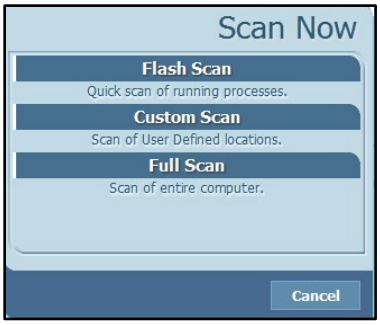

Figure 3

- **Flash Scan**- Quick scan of everything that is currently running.
- **Custom Scan**- Perform a scan on selected files.
- **Full Scan**- Scan all files on your computer.

b. **History-** Browse through the files recently scanned by Cisco AMP. If you wish to filter the files further, use the drop-down list arrows beside the various fields in the **View By** area at the top of the window.

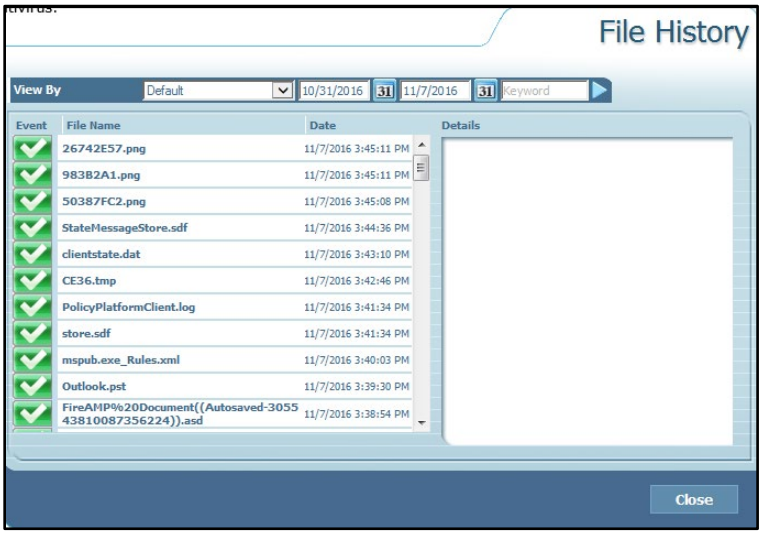

Figure 4

- **File Type** – The first drop down menu allows you to choose from a variety of file types including: **Default**, **Clean File History**, **Quarantined File History**, **Scan History** and **All File Events**.

Figure 5

- **Date Range**: Click the **date icons** beside the 2nd and 3rd fields to select a beginning and ending date for your search.

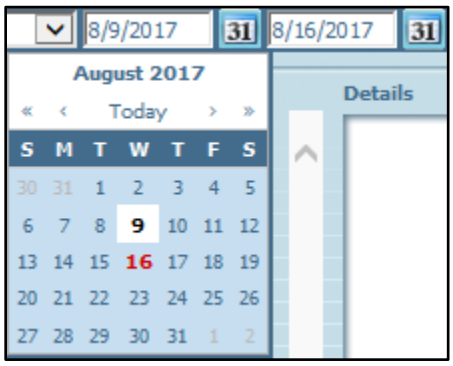

Figure 6

- **Keywords** – enter any specific keywords that you will help you find a file. You must click the **X** to delete the word **Keyword** before entering your criteria.

Figure 7

- Select the **right-pointed arrow** to perform your search. Results will show up in the box below the search fields.

c. **Settings-** Adjust the settings of Cisco AMP (disabled by the host).

3. If Cisco AMP detects a threat, a dialog box will appear.

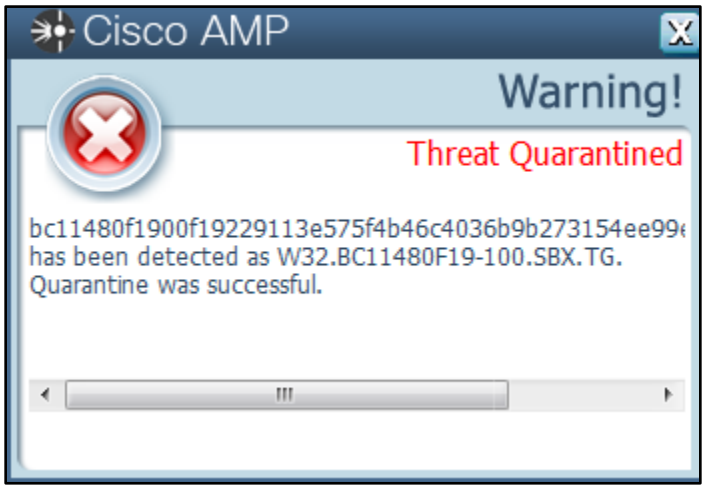

Figure 8

Frequently Asked Questions (FAQ)

What do I do if a Cisco AMP alert shows up on my computer?

Whether it is a legit block or a false positive, please contact OTS as soon as possible. You may enter a support request on your own through TechHelp at https://techhelp.towson.edu. You can also call the Faculty/Staff Help Center or Student Computing Services Desk at 410-704-7937 and follow the prompts.

Who will be protected by this service?

Designated faculty/staff computers have Cisco AMP. If you have a Cisco AMP icon in the system tray, you are protected. You can open that icon and status should say connected.

Am I protected off campus?

If you have a laptop and the agent is installed, you are protected off campus.

Do I have to update anything?

No, the agent will update automatically and it communicates with an up to date database of advanced threats.

I received an alert but did not attempt to download anything.

Cisco AMP continues to monitor and analyze files on the computer even after they are downloaded and installed. Just because the file was benign when installed, it still may be used as an attack vector in the future.

Should I regularly schedule scans?

No, you do not need to, but if you come across an abnormality you should conduct a full scan of the computer and report anything malicious to OTS.