Configure AMP Enabler

About Cisco Secure Endpoint

Cisco Secure Endpoint for macOS is used as a medium for deploying Advanced Malware Protection (AMP) for endpoints. It pushes the AMP software to a subset of endpoints from a server hosted locally within the enterprise and installs AMP services to its existing user base. This approach provides the Cisco Secure Client for macOS administrator with an additional security agent that detects potential malware threats happening in the network, removes those threats, and protects the enterprise from compromise. It saves bandwidth and time taken to download, requires no changes on the portal side, and can be done without authentication credentials being sent to the endpoint.

For Windows, AMP Enabler is no longer a part of Cisco Secure Client, as Cisco Secure Client for Windows offers full integration with Cisco Secure Endpoint, formerly AMP for Endpoints.

AMP Enabler Deployment

Note The link above directs you to documentation for Cisco Secure Endpoint, formerly AMP. When Cisco Secure Endpoint integration becomes available on macOS with a later 5.x version of Cisco Secure Client, AMP Enabler will no longer be a feature.

With macOS, you can install AMP Enabler without needing system administrator privileges. You will create and configure a policy, create a group, assign the policy to it, and then choose that group when you download the installer. To get the AMP Enabler software distributed appropriately, refer to https://console.amp.cisco.com/help/en/wwhelp/wwhimpl/js/html/wwhelp.htm.

After you have created policies and assigned them to groups, you can begin deploying the connectors to devices in your organization. AMP Enabler is a macOS-only feature, which is a plugin that lets the connector talk to the cloud when Cisco Secure Client is running.

AMP Enabler Profile Editor

An administrator can choose to use the standalone editor to create the AMP profile and then upload it to Secure Firewall ASA. Otherwise, the embedded profile editor is configured in the ISE UI under Policy Elements or in ASDM. For the trusted local web server to work with the AMP Profile Editor, you must use the key tool command to import the root CA certificate into the JAVA certificate store:

For macOS—sudo keytool-import-keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

- Name
- Description
- Install AMP—Choose if you want to configure this profile to install AMP.
- Uninstall AMP—Choose if you want to configure this profile to uninstall AMP. No input is expected in other fields if uninstall is chosen.
- Mac Installer—Enter the local hosting server address or URL where the .pkg file is located.
- Check—Click to run a check on the URL to ensure it is valid. A valid URL is one that is reachable and contains a certificate that is trusted. If the server is reachable and a connection is established at this URL, you can save the profile.
- Add to Start Menu —Creates Start menu shortcuts.
- Add to Desktop — Creates a desktop icon.
- Add to Context Menu —If you choose this option, you can right click from any file or folder and choose **Scan Now** to activate the scan.

Status of AMP Enabler

Any messages related to the actual download of AMP and the installation appear as a partial tile of the Cisco Secure Client UI. Users see messages when antimalware protection is installing or uninstalling and are given any indications of failure or necessary reboots. After installation, all AMP-related messages are in the AMP UI and not the Cisco Secure Client UI.

Note AMP Enabler is available for Cisco Secure Client on macOS only, as Cisco Secure Client 5.0 for Windows includes a full Cisco Secure Endpoint module, formerly AMP for Endpoints, with a full Secure Client Cloud Management integration. Cisco Secure Client Cloud Management integrates security portofolios and delivers unified visibility (with shared context and metrics), built-in integrations, accelerated threat investigations, and remediation across your security ecosystem. Refer to Secure Client Cloud Management to link your Secure Endpoint account.