Configure AMP Enabler

About AMP Enabler

AnyConnect AMP Enabler is used as a medium for deploying Advanced Malware Protection (AMP) for endpoints. It pushes the AMP for Endpoints 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 AnyConnect user base administrators 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.

AMP Enabler Deployment

You can install the AMP agent without needing system administrator privileges. To get the AMP for Endpoints software distributed appropriately, you must go through the following workflow.

1. Log into the AMP for Endpoints portal.
2. Configure the appropriate policies on the AMP for Endpoints portal. Depending on the policies you set, the appropriate AMP for Endpoint software package is built. The software package is an .exe file for Windows or a .pkg file for macOS. For Windows, you have the option to choose a redistributable .exe.

Note AMP connector downloads only from port 443 are supported.

3. Download the generated kit (either Windows or macOS) onto the local server.
4. Log into the ASA or ISE headend to create the AMP Enabler profile and save it.

Note We recommend that you configure the profile only for one headend, either ASA or ISE, especially when using ISE posture.

5. On the ASA or ISE headend, choose the AMP Enable module in the optional modules list and also specify the AMP Enabler profile.

   The profile you create is used for the AnyConnect AMP Enabler. The AMP Enabler along with this profile is pushed to the endpoints from the ASA or ISE headend.

AMP Enabler Profile Editor

An administrator can choose to use the standalone editor to create the AMP Enabler profile and then upload it to ASA. Otherwise, the embedded AMP Enabler 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 Windows—keytool -import -keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

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 for Endpoints—Choose if you want to configure this profile to install AMP for Endpoints.
- Uninstall AMP for Endpoints—Choose if you want to configure this profile to uninstall AMP for Endpoints. No input is expected in other fields if uninstall is chosen.
- Windows Installer—Enter the local hosting server address or URL where the .exe file is located.
- 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 on the AMP Enabler tile of the AnyConnect UI. After installation, all AMP related messages are in the AMP for Endpoint UI. For example, users see messages when antimalware protection is installing or uninstalling and are given any indications of failure or necessary reboots.