Globally Trust-listing Automox Through EPP Application Control

In some cases, a customer might run into an issue where their chosen endpoint protection platform (EPP) is preventing Automox from being installed or working.

Depending on how EPP solutions are tuned, they can occasionally block other operational tools, such as those introducing patching and configuration changes, due to a false-positive conviction from their behavioral logic. The good news is that EPPs have workarounds to override these false convictions and allow legitimate operational tools to be trusted. If you experience this scenario with your EPP and Automox, your EPP will typically provide an easy way to globally "trust-list" Automox specifically in your environment.

Each EPP manages global trust-listing for operational tools such as Automox differently. The most effective and long-term solution to globally allowing Automox from your EPP console is through the directory or path-based trust policy. In cases where a hash-based trust policy is the only option, please note that after each agent update, the hash will need to be updated as well.

Below is more information on the various application controls to provide to customers to walk them through the process of their specific EPP.

Direct links current as of August 20, 2020.

- Direct link for S1 users to access directly in S1 Management Console (external direct link)
- Scope Hierarchy with Exclusions and Blacklists in the SentinelOne Management Console (Video)
- Exclusions in the SentinelOne Management Console (video)

- Direct link for CS customers to access directly from Falcon console

- Carbon Black (guide)
- Carbon Black Product Tour (Video)

- Blackberry Cylance Protect (Starts on page 161)
- Blackberry Cylance Optics (Starts on page 62)