Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Revise the enforcements used by the identity manager framework in Splunk Enterprise Security

Generated: 6/13/2022 8:38 am

Revise the enforcements used by the identity manager framework in Splunk Enterprise Security

Every five minutes when the identity manager runs, it automatically enforces configuration file settings used by the framework, including inputs.conf, props.conf, macros.conf, transforms.conf, and identityLookup.conf (deprecated).

With these enforcements enabled, if there are accidental changes made to your conf files, the settings are reverted back to the way they were. If you're doing manual testing or making changes on purpose to your conf files and you do not want the settings checked or reverted back, you can disable these enforcements.

Prerequisites

Perform the following prerequisite tasks before starting on these settings:

1. Collect and extract asset and identity data in Splunk Enterprise Security.
2. Format the asset or identity list as a lookup in Splunk Enterprise Security.
3. Configure a new asset or identity list in Splunk Enterprise Security.

Enable or disable enforcements

Use the global settings to enable or disable enforcements as follows. For the majority of users who configure settings through the Splunk Web UI, there is no need to disable these settings:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Global Settings** tab.
3. Scroll to the **Enforcements** panel.
4. Use the toggle to enable or disable.

Example

Using the example of **Enforce props**, you experience the following by default. If you add a custom field in **Identity Settings**, the field is automatically added to the props.conf file because the settings check occurs to sync and reload props to be consistent with the identity manager.

Using the example of **Enforce props**, you experience the following by disabling it. If you add a custom field in **Identity Settings**, then you have to add that custom field to the props.conf file manually because the settings check no longer occurs. With enforce props disabled, any manual identity settings changes made without using the Splunk Web UI are also ignored.

> After upgrading to Enterprise Security 6.2.0, you need to enable the Enforce props setting if you want the identity manager to automatically enforce configuration file settings. On a fresh installation, Enterprise Security 6.2.0 has Enforce props set to enabled by default and the setting is enforced continuously. However, prior versions only enforce once and then switch the setting to false right away. If you're already using a previous version of Enterprise Security with assets and identities, the /local/inputs.conf file already has enforce_props=false and it needs to be set back to true after you upgrade, if you want to ensure that settings are managed for you. The majority of users who configure settings through the Splunk Web UI will benefit from enabling the setting.