Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Manage assets and identities in Splunk Enterprise Security

Generated: 4/21/2022 9:19 am

Manage assets and identities in Splunk Enterprise Security

Use the Asset and Identity Management page to enrich and manage asset and identity data using lookups. The Asset and Identity Management interface replaces the previously separate menus for Identity Management, Identity Correlation, and Identity Lookup Configuration. You need to have the edit_modinput_identity_manager capability to use it. See Configure users and roles in the *Installation and Upgrade Manual*.

When the identity manager runs, it processes all of the asset and identity input configurations that have changed. If the source has been updated, the identity manager dispatches the SPL created by a custom-built search.

The SPL search uses a custom search command that handles the merging and updating of new data to existing data. The custom search command merges data based on key fields and policies that you define here.

Assets and identities that need to be deleted are updated in the KV store with a `_delete` flag set to `True` so that the delete operation can persist and be completed at a later time.

The custom search command returns the merged data, which is updated or inserted to the KV store using `outputlookup append=T`. The identity manager checks and processes rows that are marked for deletion.

> If you have customized the menu bar in Splunk Enterprise Security, the Asset and Identity Management navigation and page do not display. See Restore the default navigation to restore them.

Prerequisites

Perform the following prerequisite tasks before starting any of the tasks listed in the table:

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.

Asset and identity management tasks

Complete the following tasks to manage configuration settings for assets and identities. These tasks do not need to be performed in any particular order.

Task	Description	Documentation
Configure asset lookup configuration	The asset lookup configuration settings create the policy that updates the inputs.conf file to point to a lookup and update your assets. You can change settings such as the following: • Add an asset input stanza for the lookup source • Rank the order for merging assets • Disable or enable asset lookups • Modify asset lookups • Manually add static asset data • Disable the demo asset lookups	Manage asset lookup configuration policies in Splunk Enterprise Security
Configure asset field settings	Configure asset field settings for lookup matching. You can change settings such as the following: • Add or edit an asset field • Enable case-sensitive matching for asset fields	Manage asset field settings in Splunk Enterprise Security

Task	Description	Documentation
	• Revise multivalue field limits for assets	
Create identity lookup configuration	Create an identity lookup configuration policy to update and enrich your identities. You can change settings such as the following: • Add an identity input stanza for the lookup source • Rank the order for merging identities • Modify identity lookups	Manage identity lookup configuration policies in Splunk Enterprise Security
Configure identity field settings	Configure identity settings for lookup matching. You can change settings such as the following: • Add or edit an identity field • Enable case-sensitive matching for identity fields • Revise multivalue field limits for identities	Manage identity field settings in Splunk Enterprise Security
Configure Correlation setup	When asset and identity correlation is enabled, Splunk Enterprise Security compares indexed events with asset and identity data in the asset and identity lists to provide data enrichment and context. You can change settings such as the following: • Disable correlation for all sourcetypes • Enable correlation selectively by sourcetype • Enable correlation for all sourcetypes • Correlation and entity zones	Manage correlation setup in Splunk Enterprise Security
Search preview	You can test the asset and identity merge process if you want to confirm that the data produced by the merge process is expected and accurate. You can test the following: • asset_lookup_by_str • asset_lookup_by_cidr • identity_lookup_expanded	Use the search preview to test the merge of asset and identity data in Splunk Enterprise Security
Configure global settings	Configure the global settings of the identity manager modular input to revise the way the identity manager works by default.	• Disable merge for assets and identities in Splunk Enterprise Security • Enable entity zones for assets and identities in Splunk Enterprise Security • Ignore values for assets and identities in Splunk Enterprise Security • Revise the enforcements used by the identity manager framework in Splunk Enterprise Security • Revise the miscellaneous settings used by the identity manager framework in Splunk Enterprise Security • Revise asset and identity lookup memory usage behavior in Splunk Enterprise Security • Reset asset and identity collections immediately in Splunk Enterprise Security