Tripwire Enterprise Addon and App For Splunk Documentation

Release 3.1.0

Tripwire, Inc.

January 15, 2019

CONTENTS

CHAPTER

ONE

INTRODUCTION

The Tripwire Enterprise Add-on for Splunk enables a Tripwire Enterprise administrator to collect FIM, SCM, and audit events from Tripwire Enterprise, map them to the Splunk® Common Information Model (CIM), and input the data into Splunk. You can visualize the data with other Splunk apps, such as the Splunk App for Enterprise Security.

The following pages will guide the user through installation and setup of the Tripwire Enterprise Add-on for Splunk and the Tripwire Enterprise App for Splunk Enterprise.

CHAPTER

TWO

INSTALLATION AND SETUP

This section contains detailed instructions on the installation procedure.

Please read these sections carefully to ensure proper configuration of the Tripwire Enterprise Add-on for Splunk.

2.1 Prerequisites

The Tripwire Enterprise Add-on for Splunk requires a working installation of Tripwire Enterprise, version 8.2.x or higher.

In addition to the Tripwire Enterprise Add-on for Splunk, the optional Tripwire Enterprise App for Splunk Enterprise is available to visualize Tripwire data.

- The Tripwire Enterprise App for Splunk Enterprise.

2.2 Third-Party Prerequisites

In addition to a working installation of Tripwire Enterprise, the following third-party software is required to run the Tripwire Enterprise Add-on for Splunk. This software is not distributed by Tripwire, and users should consult the relevant documentation for more details on their use.

- Splunk 7.0.0
  - Splunk 7.0.0 or higher is required

2.3 Tripwire Enterprise Configuration

We recommend you create a new user in Tripwire Enterprise to be used by this Add-on.

A "least privileged" Tripwire Enterprise Splunk user includes:

- Node Management permissions: Create, Create ACL, Delete, Link, Load, Restart Agent Nodes, Update, Update Agent, Configurations, Upgrade, View
- Policy Test Management Permissions: Load

- Log Management Permissions: Load
- Report Management Permissions: Load
- Miscellaneous Permissions: Export Settings

> **Note:** These permissions are documented in Appendix I: Definitions of User Permissions in the Tripwire Enterprise User Guide. This Add-on will only read data out of the Tripwire Enterprise console. It will not make any changes.

2.4 Technology Add-on Installation

This section describes in detail the installation procedure of the Tripwire Enterprise Splunk Technology Add-on.

> **Note:** If you are upgrading from version 2.1 or lower of the Tripwire Enterprise Splunk Technology Add-on, you must delete the old "TA_tripwire_enterprise" add-on from the $SPLUNK_HOME/etc/apps directory prior to upgrading. You must also delete the old "SA_tripwire_enterprise_IDX" and "TA_tripwire_enterprise_FWD" add-ons if utilizing a distributed Splunk environment.

2.4.1 Single Splunk Enterprise System Installations

This section describes the process for installing the Tripwire Enterprise Add-on for Splunk on a single Splunk Enterprise system. If you're using a distributed Splunk environment with Heavy Forwarders, please see *Distributed Installations*.

1. **Create Splunk Data Input Locations** The locations that store data from Tripwire Enterprise must be created before installation. Ensure that this directory's permissions permit access by Splunk. Typically, this directory should be owned by the "splunk" system user. `/opt/teexports` -or- `C:\teexports`
2. **Install the Tripwire Splunk Add-on** Navigate to "Manage Apps" then "Install app from file". Select the ".spl" file containing the Tripwire Enterprise Add-on for Splunk and click upload.
3. **Restart Splunk Enterprise** Restart Splunk Enterprise as prompted to complete the installation.
4. **Configure the Add-on** Fill in the setup screen as prompted. Please see *Add-on Configuration Options* for more information on Setup configuration options.
5. **Restart Splunk Enterprise** Restart Splunk Enterprise to apply the configurations.
6. **Configure Tripwire Enterprise Syslog** Tripwire Enterprise Syslogs must be sent to Splunk Enterprise. To configure this, logon to the Tripwire Enterprise Console.

Navigate to "Settings –> Log Management" then forward Tripwire Enterprise log messages to the IP address of your Splunk Enterprise instance using the port specified in the *Add-on Configuration Options*.

2.4.2 Distributed Installations

Follow these instructions only if installing this Splunk Add-on in a distributed Splunk environment rather than on a single Splunk Enterprise system. This Add-on does not support Universal Forwarders, you must instead use Heavy Forwarders. You must be able to route from your Heavy Forwarder to the Tripwire Enterprise console so that data can be retrieved via the API. The Heavy Forwarder does not need to be installed on the same box as the Tripwire Enterprise console.

1. **Install the Add-on on one Search head.** We will configure the Add-on on this search head, which will generate a Technology Add-on for Forwarders and a Support Add-on for Indexers. From here we can distribute components of this Add-on to Indexers, Heavy Forwarders, and other Search Heads as necessary.
2. **Restart Splunk Enterprise** Restart Splunk Enterprise as prompted to complete the installation.
3. **Configure the Add-on** Fill in the Setup screen configuration parameters as if you were configuring the settings from your heavy forwarder using *Add-on Configuration Options* as a reference. Ensure that the "Monitor data on forwarders" checkbox is checked.
4. **Locate TA-tripwire_enterprise_FWD** You can find it in TA-tripwire_enterprise/appserver/addons/. This is generated automatically after completing the Setup screen for the Add-on.
5. **Locate SA-tripwire_enterprise_IDX** You can find it in TA-tripwire_enterprise/appserver/addons/. This is generated automatically after completing the Setup screen for the Add-on.
6. **Copy TA-tripwire_enterprise to all other Search Heads** Now that the Add-on is configured, copy TA-tripwire_enterprise to all other search heads while all inputs in default/inputs.conf are disabled. Make sure permissions on TA-tripwire_enterprise are set properly on your Search Heads.
7. **Enable the inputs for the forwarders** Open the TA-tripwire_enterprise_FWD/local/inputs.conf file on your Search Head and set 'disabled = 0' to each stanza. Doing this will enable these inputs before we copy TA-tripwire_enterprise_FWD to your Heavy Forwarders.
8. **Copy the Tripwire TA for Forwarders to Heavy Forwarders** Copy TA-tripwire_enterprise_FWD from your Search Head to $SPLUNK_HOME/etc/apps on your Forwarders. Make sure permissions on TA-tripwire_enterprise_FWD are set properly on your Heavy Forwarders.
9. **Create Splunk Data Input Locations** The locations that store data from Tripwire Enterprise must be created on each Heavy Forwarder. This directory should match the one specified by the Tripwire Data Directory setting as specified in the *Add-on Configuration Options*. Ensure that this directory's permissions permit access by Splunk. Typically, this directory should be owned by the "splunk" system user. By default the directory is `/opt/teexports` -or- `C:\teexports`.
10. **Copy the Support Add-on to your Indexers** Copy SA-tripwire_enterprise_IDX from your Search Head to $SPLUNK_HOME/etc/apps on your Indexers. Make sure permissions on SA-tripwire_enterprise_IDX are set properly on your Indexers.

11. **Restart Splunk Instances** Restart your indexers, forwarders, and search heads once everything is deployed to the appropriate places.

2.5 Add-on Configuration Options

This page describes in more detail the configuration options available in the add-on setup screen.

1. **Tripwire Data Directory** The directory that stored Tripwire Enterprise data will be stored in on disk to be consumed by Splunk. This is a required configuration option.
2. **Tripwire Listening Port** The port on which Splunk should listen for Tripwire Syslog messages. The default Syslog port is 514. This is a required configuration option if you wish to receive Syslog audit data from Tripwire Enterprise.
3. **Tripwire Enterprise Console** The IP address of the Tripwire Enterprise server.
4. **Verify SSL certificate of TE console** If your Splunk Enterprise system trusts Tripwire Enterprise's self-signed certificate, you can enable this option to enable SSL certification verification during communication to Tripwire Enterprise.
5. **Frequency of SCM Data Retrieval** The frequency at which to poll for new Tripwire SCM data. By default this is set to 1 day.
6. **Frequency of FIM Data Retrieval** The frequency at which to poll for new Tripwire FIM data. By default this is set to 1 hour.
7. **Timeout (in minutes) of FIM data retrieval.** How long the FIM SOAP report script should run before timing out. By default this is set to 59 minutes.
8. **Frequency of ECR Data Retrieval** The frequency at which to poll for Tripwire Element Content Report data. By default this is set to 1 day.
9. **Number of Historical Days to Populate** The number of days of data to collect from the Tripwire Enterprise console for the first time we pull data. By default is 14 days of data.
10. **showContentDiff Data** Enable the showContentDiff report option if using SOAP reports for FIM.
11. **Compare Previous Versions** FIM diffs will be based on previous versions rather than the baseline version for elements.
12. **Distributed Environment** Monitor data on forwarders. This option should be enabled on Search Heads. Please see *Distributed Installations* for more information.
13. **REST API - FIM** Use the Tripwire Enterprise REST API to pull FIM data rather than SOAP reports. The checkbox must be enabled to utilize this feature.
14. **Number of Worker Threads for FIM** Number of worker threads to spawn for FIM. This setting can be increased to increase the speed at which FIM data is gathered. We only recommend you increase this value if you are having trouble pulling in your FIM data in a timely manner.
15. **REST API - SCM** Use the Tripwire Enterprise REST API to pull SCM data rather than SOAP reports. The checkbox must be enabled to utilize this feature.

16. **Number of Worker Threads for SCM** Number of worker threads to spawn for SCM. This setting can be increased to increase the speed at which SCM data is gathered. We only recommend you increase this value if you are having trouble pulling in your SCM data in a timely manner.
17. **CSV list of policy names** A CSV list of the specific policy names that you would like to pull SCM data for. By default all SCM policies are pulled from Tripwire Enterprise.
18. **Pull and reindex all SCM results on the first run of each day.** In some cases you may wish to reindex all SCM policy result data each day so you can get a new snapshot of all test results each day. If this option is enabled, the first SCM data poll each day will reindex all SCM results instead of only pulling new SCM results.
19. **Exclude waivered test results from being gathered.** If using the REST API we will retrieve whether or not SCM results have a waiver applied to them. Enabling this option will exclude any waivered tests from being indexed into Splunk. This option only works if using the REST API for SCM data retrieval.
20. **CSV list of policy names to pull and reindex results for on the first run of each day.** Instead of reindexing all SCM results, you can specify a CSV list of the specific policy names that you would like to reindex data for each day. By default all policies specified in the CSV list of policy names are reindexed.
21. **ECR** The CSV list of Element Content Reports to run. You can preconfigure any Element Content Reports you would like in Tripwire Enterprise to retrieve element contents for any arbitrary elements you would like into Tripwire Enterprise. By default no Element Content Reports will be be run.
22. **Parse SQL Query Rules separately.** If there are SQL query rules in any of your element content reports, by default the results from those rules will be indexed into Splunk as a single text blob. If this option is enabled, the individual columns from the SQL results will be separated out into separate indexed fields in Splunk.
23. **Enable Debug Logging** Enabling this particular option will add more verbose logging to the $SPLUNK_HOME/var/log/splunk/tripwire.log log file. This should be disabled unless trying to diagnose an issue.
24. **Enable REST API logging.** Enabling this particular option will add more verbose logging around any REST API calls the Add-on is making to Tripwire Enterprise to the $SPLUNK_HOME/var/log/splunk/tripwire.log log file. This should be disabled unless trying to diagnose an issue.
25. **Username** The username to the Tripwire Enterprise console that we'll use for authentication to Tripwire Enterprise APIs. You should use a new account configured according to the permissions specified on the *Tripwire Enterprise Configuration* page.
26. **Password** The password for the username specified to the Tripwire Enterprise console.
27. **Confirm Password** Re-enter the password to confirm.

2.6 Multiple TE Consoles

By default, this Add-on supports a single Tripwire Enterprise console. Pulling data from multiple Tripwire Enterprise consoles involves making copies of the Add-on with slightly different configurations. There will be a unique copy of the Add-on for each Tripwire Enterprise console you wish to pull data from.

First, you must follow the steps to pull data for a single Tripwire Enterprise console. Either by following *Distributed Installations* or *Single Splunk Enterprise System Installations*.

1. Copy `TA-tripwire_enterprise_FWD` if using Heavy Forwarders or `TA-tripwire_enterprise` if using a single Splunk Enterprise instance. Rename it to `TA-tripwire_enterprise_FWD2` or `TA-tripwire_enterprise2`.
2. Go back to the Setup screen for the Add-on and modify the Tripwire Data Directory. The Tripwire Data Directory must be unique for each copy of the Add-on.
3. Set the IP for the next Tripwire Enterprise console you want to pull data from.
4. Set the username and password for the next Tripwire Enterprise console you want to pull data from.
5. Save the new configuration.
6. Go back to Step 1 and repeat until you have a unique copy of `TA-tripwire_enterprise_FWD` if using Heavy Forwarders or `TA-tripwire_enterprise` if using a single Splunk Enterprise instance for each Tripwire Enterprise console you wish to monitor.
7. In each copy of the Add-on, change each mention of TA-tripwire_enterprise or TA-tripwire_enterprise_FWD in local/inputs.conf to the new name of the Add-on directory.
8. If using Heavy Forwarders, distribute each of your unique `TA-tripwire_enterprise_FWD` Add-ons to your Heavy Forwarders in $SPLUNK_HOME/etc/apps.

2.7 App Installation

This section describes the process for installing the Tripwire Enterprise App for Splunk Enterprise. The Tripwire Enterprise App for Splunk Enterprise uses the data provided by the Tripwire Enterprise Technology Add-on (TA) for Splunk. The TA must be downloaded, installed and properly configured prior to using this App.

1. **Prepare the Tripwire Enterprise App for Installation** Unzip the tripwire-enterprise-app-for-splunk-enterprise.zip file. This file contains the .spl file you will install.
2. **Install the Tripwire Splunk App** Navigate to “Manage Apps” then “Install app from file”. Select the ”.spl” file containing the Tripwire Enterprise App for Splunk Enterprise and click upload. Restart Splunk Enterprise as prompted. Fill in the setup screen as prompted.

CHAPTER

THREE

TROUBLESHOOTING

The following are various troubleshooting notes and tips.

3.1 Logs

Log data can be found in $SPLUNK_HOME/var/log/splunk/tripwire.log

3.2 No Data

- Check logs to look for any errors.
- **Verify that Tripwire username and password provided in the setup step works properly. (log directly into TE c**
  NOTE: passwords cannot contain #$(*
- Make sure that your Tripwire Data Directories as specified in *Add-on Configuration Options* have been created and can be read by and written to by Splunk.

3.3 Warnings About asset_info Lookup Table

If there is a warning icon appearing after searches warning that asset_info does not exist, this means te_assets.csv lookup file does not exist in TA_tripwire_enterprise/lookups either on your Splunk Enterprise instance or your Search Heads if using a distributed Splunk Environment. This lookup table is automatically generated every hour based on the "TE Assets Lookup Table Builder" scheduled report.

This report generates data off of the te_assets_lookuptable_builder index. If it's not being created you can run a search for "index=te_assets_lookuptable_builder" in Splunk to validate that TE asset data is being indexed. If it isn't, the most likely cause is the script cannot access the TE API endpoint. You can test this by accessing TE in a browser using https://%server%/assetview/api/assets (replace %server% with your TE consoles name or IP)

3.4 Timezones

If you wish to override the timezone of a source, this can be done by modifying $SPLUNK_HOME/etc/system/local/props.conf and setting the TZ option. For Example:

[te_scm_csv]

TZ = UTC

[te_fim_csv]

TZ = UTC

CHAPTER

FOUR

RELEASE NOTES

4.1 Version 3.1.0

- Added a configurable timeout for FIM Retrieval
- Added an option to configure a CSV List of policies to re-index daily
- Added support for Splunk 6
- Addressed defect in element versions not having attributes

4.2 Version 3.0.0

- The add-on will now index TE asset data into a new "te_assets_lookuptable_builder" index, and there is a new scheduled report that will generate a lookup table from the new index. This will allow heavy forwarders to generate the data necessary for the "te_assets" lookup table, instead of requiring the search heads to gather this data themselves. This will also permit a deployment using multiple copies of the TA pointed at multiple TE consoles to function correctly.
- The TE asset data retriever will now retrieve node data if nodes have no IP addresses
- Continue gracefully in SCM REST data retrieval if parent groups for a node no longer exist
- New PDF documentation for how to install and configure the Add-on, including in distributed environments
- New documentation and support around pulling data from multiple TE consoles
- The following directories have been renamed for consistency and compatibility with the Splunk Enterprise Security App:

"TA_tripwire_enterprise" to "TA-tripwire_enterprise" "TA_tripwire_enterprise_FWD" to "TA-tripwire_enterprise_FWD" "SA_tripwire_enterprise_IDX" to "SA-tripwire_enterprise_IDX"

4.3 Version 2.1.0

- Added options to use the REST API for FIM/SCM

- Various bug fixes and improvements
- Added new tripwire.log in the Splunk log directory

4.4 Version 2.0.0

- Added a stand-alone TA for Tripwire Enterprise
- Addressed CIM Compliance for FIM data source
- FIM data sources have been normalized to the "Change Analysis" data model

4.5 Version 1.5.4

- Addressed defect for Splunk Enterprise 6.3 support

4.6 Version 1.5.3

- Added ability to load more detailed change data
- Addressed defect with special characters in passwords

4.7 Version 1.5.2

- Addressed defect in Windows SetUp screen

4.8 Version 1.5.1

- Availability of two add ons: TA_te and SA_te for distributed deployments
- Addresses minor issues deploying to Linux based Heavy Forwarders