Splunk® Supported Add-ons
Splunk Add-on for Cisco ISE released

Generated: 11/05/2022 11:57 am

Table of Contents

Overview

Splunk Add-on for Cisco ISE

Version	4.2.0
Vendor products	Cisco ISE v2.0, v2.4, v2.7, v3.0, v3.1

The Splunk Add-on for Cisco ISE lets a Splunk software administrator work with Cisco Identity Service Engine (ISE) syslog data. You can use the Splunk platform to analyze these logs directly or use them as a contextual data source to correlate with other communication and authentication data in the Splunk platform.

This add-on provides the inputs and CIM-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security, the Splunk App for PCI Compliance, and Splunk IT Service Intelligence.

You can download the Splunk Add-on for Cisco ISE at https://splunkbase.splunk.com/app/1915.

Hardware and software requirements for the Splunk Add-on for Cisco ISE

To install and configure the Splunk Add-on for Cisco ISE, you must be member of the `admin` or `sc_admin` role.

Cisco ISE setup requirements

Before you install the Splunk Add-on for Cisco ISE, confirm that you have the following:

- The IP Address of the Splunk platform that will receive the data.
- The port that will be used on the Splunk Enterprise system as a network input.
- Access to the ISE Administration interface.
- Network connectivity between Splunk Enterprise and Cisco ISE.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run this add-on.

- For Splunk Enterprise system requirements: see System Requirements in the Splunk Enterprise *Installation Manual*.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise *Installation Manual*, which includes information about forwarders.

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

Installation overview for the Splunk Add-on for Cisco ISE

Complete the following steps to install and configure this add-on on your supported platform:

1. Install the add-on for Cisco ISE.
2. Configure data collection using Splunk Connect for Syslog to receive the log data from Cisco ISE.
3. Configure Cisco ISE to send the log files that you need in a way that can be accessed by Splunk Enterprise.
4. Verify your configurations using an test index first, to ensure your data is flowing to Splunk Enterprise and is source typed as you expect. Troubleshoot, if necessary, before switching to your production index.

Installation and Configuration

Install the Splunk Add-on for Cisco ISE

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise.

If you are not using a distributed deployment, or you need further instructions on how to install an add-on in your specific deployment environment, see the installation walkthroughs section at the bottom of this page for links to installation instructions specific to a single-instance deployment, distributed deployment, or Splunk Cloud.

Where to install this add-on

Unless otherwise noted, all supported add-ons can be safely installed to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in *Splunk Add-ons* for more information.

This table provides a reference for installing this specific add-on to a distributed deployment of Splunk Enterprise.

Splunk instance type	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where Cisco ISE knowledge management is required.
Indexers	Yes	Conditional	This add-on includes index-time operations and must be installed on either indexers or heavy forwarders.
Heavy Forwarders	Yes	Conditional	This add-on includes index-time operations and must be installed on either indexers or heavy forwarders.
Universal Forwarders	Yes	No	This add-on supports forwarders of any type for data collection.

Distributed deployment feature compatibility

This table describes the compatibility of this add-on with Splunk distributed deployment features.

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality.
Indexer Clusters	Yes	You can install this add-on on an indexer cluster for all index-time functionality.
Deployment Server	Yes	Supported for deploying the configured add-on.

Installation walkthroughs

The *Splunk Add-Ons* manual includes an Installing add-ons guide that helps you successfully install any Splunk-supported add-on to your Splunk platform.

For a detailed walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud

Configure inputs for the Splunk Add-on for Cisco ISE

You must configure Cisco ISE to send logs to Splunk Enterprise via syslog. To configure your appliance to send data to syslog, see Configure Cisco ISE to send logs to Splunk Enterprise.

For information on how to configure a Splunk forwarder or single-instance to receive a syslog input, see Get data from TCP and UDP ports in the *Getting Data In* manual.

Configure Cisco ISE to send logs to Splunk Enterprise for the Splunk Add-on for Cisco ISE

To enable to Splunk Enterprise to receive data from your Cisco ISE remote system logging, complete these steps:

1. Create a remote logging target.
2. Add the target to the appropriate logging categories.

The following sections provide detailed configuration instructions.

For more information, see the Logging section of the *Cisco ISE Administrator Guide* provided by Cisco.

Create remote logging target

1. In Cisco ISE, choose **Administration > System > Logging > Remote Logging Targets**.
2. Click **Add**.
3. Configure the following fields:

Field	Value	Description
Name	Splunk	Target name, also used below in the category
IP Address	1.1.1.2 (for example)	IP address of the Splunk Enterprise system
Port	515 (for example)	Port that you are using on the Splunk Enterprise system or port configured for TCP or UDP input on Splunk Connect for Syslog (SC4S) or syslog aggregator (for example, rsyslog, syslog-ng) as a network input.
Target Type	UDP	Best practice. NOT the default.
Maximum Length	8192	Events will be broken if you use a smaller value.

4. Tune all other fields at your discretion.
5. Add the new port(s) in order to enable receiving logs into Splunk
    - If the "Target Type" is TCP use **Settings** > **Data Inputs** > **TCP** > **New Local TCP**
    - If the "Target Type" is UDP use **Settings** > **Data Inputs** > **UDP** > **New Local UCP**
6. Click **Save**.
7. Go to the **Remote Logging Targets** page and verify the creation of the new target.

Add the new target to your desired logging categories

1. Choose **Administration > System > Logging > Logging Categories**.
2. Click the radio button next to the category that you want to edit, then click **Edit**.
3. Add the Splunk target that you created to the following categories. These are default log collection settings and can be tuned at your discretion:
    - AAA Audit
    - Failed Attempts
    - Passed Authentications
    - AAA Diagnostics
    - Accounting
    - RADIUS Accounting
    - Administrative and Operational Audit
    - Posture and Client Provisioning Audit
    - Posture and Client Provisioning Diagnostics
    - MDM
    - Profiler
    - System Diagnostics
    - System Statistics
4. Click **Save**.
5. Go to the **Logging Categories** page and verify the configuration changes that were made to the specific categories.

Confirm your installation and setup

To confirm that events are showing up correctly, run the following search over the last 15 minutes:

```
sourcetype=cisco:ise:syslog
```

If the search returns events from your ISE server, then you have successfully configured the add-on.

Upgrade the Splunk Add-on for Cisco ISE

Upgrade from v4.1.0 to v4.2.0

Upgrade from Splunk Add-on for Cisco ISE v4.1.0 to v4.2.0 requires no additional steps to be performed.

Upgrade from v4.0.0 to v4.1.0

Upgrade from Splunk Add-on for Cisco ISE v4.0.0 to v4.1.0 requires no additional steps to be performed.

Upgrade an indexer cluster from Splunk Add-on for Cisco ISE version 3.0.0

1. On the cluster master of your indexer cluster Splunk platform deployment, navigate to `$SPLUNK_HOME/etc/master-apps/Splunk_TA_cisco-ise/local/` .
2. Open `props.conf` and edit the `cisco:ise` stanza to remove the following line:
   `DATETIME_CONFIG = /etc/slave-apps/Splunk_TA_cisco-ise/default/datetime_udp.xml`
3. Edit the `cisco:ise:syslog` stanza to remove the following line:

```
DATETIME_CONFIG = /etc/slave-apps/Splunk_TA_cisco-ise/default/datetime_udp.xml
```

4. Save your changes.
5. Push the configurations to your peer nodes.

Configure data collection using Splunk Connect for Syslog

To use Splunk Connect for Syslog to collect Syslog data, see the documentation at: https://github.com/splunk/splunk-connect-for-syslog/blob/main/docs/sources/vendor/Cisco/cisco_ise.md

Reference

Lookups for the Splunk Add-on for Cisco ISE

The Splunk Add-on for Cisco ISE has the following **lookups**. The lookup file maps fields from Cisco ISE systems to CIM-compliant values in the Splunk platform. The lookup files are located at `$SPLUNK_HOME/etc/apps/Splunk_TA_cisco-ise/lookups`.

Filename	Description
`cisco_ise_message_catalog_420.csv`	Maps `MESSAGE_CODE` to `MESSAGE_CLASS`, `MESSAGE_TEXT`
`cisco_ise_service.csv`	Maps `MESSAGE_CODE` to `SERVICE`
`cisco_ise_change_message_code_420.csv`	Maps `MESSAGE_CODE` to `change_type`, `command`, `object`, `object_attrs`, `object_category`, `result`

Sourcetypes for the Splunk Add-on for Cisco ISE

The Cisco ISE logs record information useful for auditing, fault management, and troubleshooting. The Splunk Add-on for Cisco ISE provides the index-time and search-time knowledge for Cisco log events in the following format:

Sourcetype	Description	CIM data models
`cisco:ise:syslog`	cisco-ise-system-statistics	n/a
	cisco-ise-authentication	Authentication
	cisco-ise-passed-authentication	Authentication
	cisco-ise-failed-authentication	Authentication
	cisco-ise-guest-authentication	Authentication
	cisco-ise-guest-authentication-failed	n/a
	cisco-ise-profiler	n/a
	cisco-ise-provision-succeeded	n/a
	cisco-ise-provision-failed	n/a
	cisco-ise-alarm	n/a
	cisco-ise-alert	Alerts
	cisco-ise-change	n/a
	cisco-ise-endpoint-service	Endpoint Service
	cisco-ise-traffic	Network Traffic
	cisco-ise-change-all	Change:All_Changes
	cisco-ise-change-account	Change:Account_Management
	cisco-ise-inventory	Inventory
	cisco-ise-guest-authentication-failed-attempts	Authentication

If all the following conditions are true, the Splunk Add-on for Cisco ISE automatically sets the source type for Cisco ISE records as `cisco:ise:syslog`:

- Your Splunk platform consumes syslog data either directly or through a syslog aggregator.
- You configured your Cisco ISE devices to send logs either directly to your Splunk platform instance or syslog to your aggregator.
- The Cisco ISE records include `sourcetype=syslog`.

If you have configured the Splunk platform to acquire your Cisco ISE log data in a different way, you should manually set the sourcetype to `cisco:ise:syslog` at the input phase. For more information about configuring sourcetypes, see the Configure sourcetypes chapter in the *Getting Data In* manual, part of the Splunk Enterprise documentation.

Troubleshoot

Troubleshoot the Splunk Add-on for Cisco ISE

For helpful troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons. You can also access these support and resource links.

"Invalid key in stanza" message in the console output

This issue occurs in version 4.0.0 because pxgrid and EPS workflow actions have been removed. If the user has configured the workflow actions in an earlier version after upgrade below messages can be seen in the console.

```
Invalid key in stanza [EPS_Quarantine_By_Framed_IP_Address] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 10: ise.host (value: Please
update ISE host information before enabling).
Invalid key in stanza [EPS_Quarantine_By_Framed_IP_Address] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 11: ise.version (value: 1.2).
Invalid key in stanza [EPS_QuarantineByIPAddress] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 22: ise.host (value: Please
update ISE host information before enabling).
Invalid key in stanza [EPS_QuarantineByIPAddress] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 23: ise.version (value: 1.2).
Invalid key in stanza [EPS_QuarantineByMAC] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 34: ise.host (value: Please
update ISE host information before enabling).
Invalid key in stanza [EPS_QuarantineByMAC] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 35: ise.version (value: 1.2).
Invalid key in stanza [EPS_UnquarantineByIPAddress] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 46: ise.host (value: Please
update ISE host information before enabling).
Invalid key in stanza [EPS_UnquarantineByIPAddress] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 47: ise.version (value: 1.2).
Invalid key in stanza [EPS_UnquarantineByMAC] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 58: ise.host (value: Please
update ISE host information before enabling).
Invalid key in stanza [EPS_UnquarantineByMAC] in
/opt/splunk/etc/apps/Splunk_TA_cisco-ise/local/workflow_actions.conf, line 59: ise.version (value: 1.2).
```

To eliminate these messages from the console, remove the `workflow_actions.conf` file from `$SPLUNK_HOME/etc/apps/Splunk_TA_cisco-ise/local/` location.

"AggregatorMiningProcessor Error" message in the `splunkd` log file

These messages occur because the hard-coded path of `datetime_config` has been removed. If you have set the custom path for`datetime_config` in `$SPLUNK_HOME/etc/master-apps/Splunk_TA_cisco-ise/local/props.conf` file, then the below error displays in `splunkd.log` file and events are not ingested in the Splunk.

```
07-03-2020 05:28:39.830 +0000 ERROR AggregatorMiningProcessor - Uncaught exception in Aggregator, skipping
an event: Can't open DateParser XML configuration file
"/opt/splunk/etc/apps/Splunk_TA_cisco-ise/default/datetime_udp.xml": No such file or directory -
data_source="test", data_host="idx3", data_sourcetype="cisco:ise:syslog"
```

To mitigate this issue, see the Upgrade an indexer cluster from Splunk Add-on for Cisco ISE version 3.0.0.

Troubleshoot upgrading

If you are having issues upgrading to version 2.2.2, see the following sections:

Upgrade from 2.2.0 or 2.1.1 to 2.2.2

There are no known issues when upgrading from versions 2.2.0 or 2.1.1 to 2.2.2.

Upgrade from 2.1.0 to 2.2.2

Version 2.1.1 of this add-on changed the timestamp extraction behavior. That release corrected the way that the Splunk platform selects the timestamp from the three timestamps available in Cisco ISE data. This change may cause a time jump in your data at the upgrade point.

Upgrade from versions older than 2.1.0 to 2.2.2

If you have any version of the Splunk Add-on for Cisco ISE currently installed that is older than version 2.1.0, version 2.2.2 will not update or replace your current installation. Because the pre-2.1.0 community-supported versions of this add-on had a different folder structure, this add-on behaves as a new installation, not as an upgrade.

To upgrade from any version prior to 2.1.0 to version 2.2.2, complete these steps:

1. Download and install version 2.2.2 of the add-on from Splunkbase.
2. Disable your previous version in the Splunk platform.
3. Enable version 2.2.2 of the add-on.
4. Create and adjust your local .conf files as needed to match your old configurations.
5. Verify your configurations work as expected.
6. Delete the older version of the add-on.

Release notes

Release notes for the Splunk Add-on for Cisco ISE

Version 4.2.0 of the Splunk Add-on for Cisco ISE was released on July 14, 2022.

About this release

Version 4.2.0 of the Splunk Add-on for Cisco ISE is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1, 8.2, 9.0
CIM	5.0.1
Platforms	Platform independent
Vendor Products	Cisco ISE version 2.0, 2.4, 2.7, 3.0 and 3.1

New features

Version 4.2.0 of the Splunk Add-on for Cisco ISE has the following new features.

- Added support for Cisco ISE v3.1
- Added support for CIM v5.0.1
- Added support for new eventtypes and the datamodels, which are mentioned in the following table:

eventtype	Data model mapped
`cisco-ise-inventory`	Inventory:Network
`cisco-ise-change-all`	Change:All_Changes
`cisco-ise-guest-authentication-failed-attempts`	Authentication

- Below mentioned table indicates the data model support added for respective MESSAGE_CODE

MESSAGE_CODE	Data Model support added in this release
11036, 25012, 25016, 25018, 25020, 25045, 25046, 35000, 35001, 35046, 35048, 35050, 35051, 35055, 5417, 60164, 60191, 61075, 61236, 91002, 91006, 91007	Alerts
11213, 11507, 11521, 11522, 11806, 11808, 12300, 12301, 12302, 12310, 12313, 12500, 12552, 12561, 12800, 12801, 12802, 12804, 12805, 12806, 12807, 12810, 12811, 12812, 12813, 12816, 51001, 51002, 51021, 5205, 5231, 5236, 5405, 5413, 5418, 5436, 5440, 5441, 60080, 60204	Authentication
51003, 51101, 52000	Change.Account_Management
52001, 58003, 58004, 58016, 60094, 60106, 60153, 60208, 60216, 60237, 90051, 90200, 91003	Change.All_Changes
88010	Inventory.Network

- Extractions for `signature` and `signature_id` have been fixed as previously signature was used in both fields. `signature` will be extracted from `MESSAGE_TEXT` `signature_id` will be extracted from `MESSAGE_CODE`
- New CIM field extraction added for `user_name`
- Previously, a comma (,) occurred sometimes in the value of the field. Corrected the implementation such that the comma (,) is excluded from the value of the field

Fixed issues

Version 4.2.0 of the Splunk Add-on for Cisco ISE contains the following fixed issues.

If no issues appear below, no issues have yet been reported:

Known issues

Version 4.2.0 of the Splunk Add-on for Cisco ISE contains the following known issues.

If no issues appear below, no issues have yet been reported:

Third-party software attributions

Version 4.2.0 of the Splunk Add-on for Cisco ISE does not incorporate any third-party software or libraries.

Release history for the Splunk Add-on for Cisco ISE

The latest version of the Splunk Add-on for Cisco ISE is version 4.2.0. Please see Release notes for the Splunk Add-on for Cisco ISE for the release notes of the latest version.

Version 4.2.0 of the Splunk Add-on for Cisco ISE was released on April 13, 2021.

Version 4.1.0

Version 4.1.0 of the Splunk Add-on for Cisco ISE is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.3, 8.0, 8.1
CIM	4.19.0
Platforms	Platform independent
Vendor Products	Cisco ISE version 2.0, 2.4, 2.7 and 3.0

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

Version 4.1.0 of the Splunk Add-on for Cisco ISE has the following new features.

- Added Support for new event types `cisco-ise-endpoint-service`, `cisco-ise-change` and `cisco-ise-traffic`
- Added support for `Endpoint Services`, `Change` and `Network Traffic` DataModels for the above mentioned eventtypes respectively.
- For below mentioned`MESSAGE_CODE`, `eventtype=cisco-ise-change` is introduced
    - `52002`, `60086`, `58022`, `58023`, `58024`, `60131`, `60132`, `60198`, `5232`, `5233`, `60085`, `60190`, `60197`, `60214`, `51100`, `60461`
- For below mentioned`MESSAGE_CODE`, `eventtype=cisco-ise-endpoint-service` is introduced
    - `11010`, `34127`, `34126`, `58001`, `58002`, `58005`, `11009`, `25004`, `34050`, `32000`, `60234`, `60235`, `87751`, `87604`, `13002`, `87608`, `87609`, `91004`, `91018`
- For below mentioned`MESSAGE_CODE`, `eventtype=cisco-ise-traffic` is introduced
    - `61025`
- Added support for CIM v4.19.0.
- Support for Cisco ISE product version 3.0

Fixed issues

Version 4.1.0 of the Splunk Add-on for Cisco ISE contains the following fixed issues.

If no issues appear below, no issues have yet been reported:

Known issues

Version 4.1.0 of the Splunk Add-on for Cisco ISE contains the following known issues.

If no issues appear below, no issues have yet been reported:

Third-party software attributions

Version 4.1.0 of the Splunk Add-on for Cisco ISE does not incorporate any third-party software or libraries.

Version 4.0.0

Version 4.0.0 of the Splunk Add-on for Cisco ISE was released on July 10, 2020.

About this release

Version 4.0.0 of the Splunk Add-on for Cisco ISE is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.2, 7.3, 8.0
CIM	4.15
Platforms	Platform independent
Vendor Products	Cisco ISE version 2.0, 2.4, and 2.7

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

Version 4.0.0 of the Splunk Add-on for Cisco ISE has the following new features.

- Added the new event type `cisco-ise-alert`
- Performance data model mapping has been removed for the `cisco-ise-system-statistics` event type.
- The authentication data model mapping has been removed for the following event types:
  - `cisco-ise-passed-authentication`
  - `cisco-ise-failed-authentication`
  - `cisco-ise-guest-authentication`
  - `cisco-ise-guest-authentication-failed`
- An authentication data model has been added for the `cisco-ise-authentication` event type.
- Change data model mapping has been removed for `cisco-ise-provision-succeeded` event type.
- Alert data model has been added for the `cisco-ise-alert` event type.
- Auto KV mode has been replaced with custom REGEX for field extractions in order to support different data formats and fix the broken extractions. As a result, search queries may take longer than before.
- Fixed broken field extractions.
- Removed the setup page, pxGrid Workflow actions, and EPS workflow actions.
- Index time of event has been changed to "Current".
- Added support for Splunk Connect for Syslog.
- Added support for CIM v4.15.
- Update for support for Cisco ISE version 2.7.
- Data Collection supports Syslog and Splunk Connect for Syslog.

Fixed issues

Version 4.0.0 of the Splunk Add-on for Cisco ISE contains the following fixed issues.

If no issues appear below, no issues have yet been reported:

Date resolved	Issue number	Description
2020-05-19	ADDON-25848	Cisco ISE: Splunk Cloud DATETIME_CONFIG problem

Known issues

Version 4.0.0 of the Splunk Add-on for Cisco ISE contains the following known issues.

If no issues appear below, no issues have yet been reported:

Third-party software attributions

Version 4.0.0 of the Splunk Add-on for Cisco ISE does not incorporate any third-party software or libraries.

Version 3.0.0

Version 3.0.0 of the Splunk Add-on for Cisco ISE is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x
CIM	4.14 and later
Platforms	Platform independent
Vendor Products	Cisco ISE version 1.x and 2.0

New features

Version 3.0.0 of the Splunk Add-on for Cisco ISE has the following new features.

- Support for Python3

Fixed issues

Version 3.0.0 of the Splunk Add-on for Cisco ISE contains the following fixed issues.

If no issues appear below, no issues have yet been reported:

Known issues

Version 3.0.0 of the Splunk Add-on for Cisco ISE contains the following known issues.

If no issues appear below, no issues have yet been reported:

Date filed	Issue number	Description
2020-03-26	ADDON-25848	Cisco ISE: Splunk Cloud DATETIME_CONFIG problem
2018-10-19	ADDON-19966	Issues with setup page on Splunk v7.2.0

Date filed	Issue number	Description
		Workaround: web.conf splunkdConnectionTimeout = 120

Third-party software attributions

Version 3.0.0 of the Splunk Add-on for Cisco ISE incorporates the following third-party software attributions:

- `pxGrid_search.jar` library, provided by Cisco and used by their permission.
- future
- configparser

Version 2.2.2

Version 2.2.2 of the Splunk Add-on for Cisco ISE was released on December 11, 2018.

About this release

Version 2.2.2 of the Splunk Add-on for Cisco ISE is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	6.6.x, 7.0.x, 7.1.x, 7.2.x
CIM	4.11
Platforms	Platform independent
Vendor Products	Cisco ISE version 1.x and 2.0

Known issues

Version 2.2.2 of the Splunk Add-on for Cisco ISE contains the following known issues.

If no issues appear below, no issues have yet been reported:

Date filed	Issue number	Description
2018-10-19	ADDON-19966	Issues with setup page on Splunk v7.2.0 Workaround: web.conf splunkdConnectionTimeout = 120

Third-party software attributions

Version 2.2.2 of the Splunk Add-on for Cisco ISE incorporates the `pxGrid_search.jar` library, provided by Cisco and used by their permission.

Version 2.2.0

Version 2.2.0 of the Splunk Add-on for Cisco ISE was released on June 8, 2016. This release is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.3 and later
CIM	4.3 and later
Platforms	Platform independent
Vendor Products	Cisco ISE version 1.x and 2.0

Migration from 2.1.1 to 2.2.0

There are no upgrade issues when upgrading from version 2.1.1 to 2.2.0.

Migration from 2.1.0 to 2.2.0

Version 2.1.1 of this add-on changed the timestamp extraction behavior. That release corrected the way that the Splunk platform selects the timestamp from among the three timestamps available in Cisco ISE data. This change may cause a time jump in your data at the upgrade point.

Migration from versions older than 2.1.0 to 2.2.0

If you have any version of the Splunk Add-on for Cisco ISE currently installed that is older than version 2.1.0, note that version 2.2.0 will not update or replace your current installation. Because the pre-2.1.0 community-supported versions of this add-on had a different folder structure, this add-on behaves as a new installation, not as an upgrade.

To migrate from any version prior to 2.1.0 to version 2.2.0:

1. Download and install version 2.2.0 of the add-on from Splunkbase.
2. Disable your previous version in the Splunk platform.
3. Enable version 2.2.0 of the add-on.
4. Create and adjust your local .conf files as needed to match your old configurations.
5. Verify your configurations work as expected.

'#Delete the older version of the add-on.

New features

Version 2.2.0 of the Splunk Add-on for Cisco ISE has the following new features.

Date	Issue number	Description
2016-02-18	ADDON-7816	This release of add-on now supports Cisco ISE version 1.x and 2.0.
2015-04-03	ADDON-3584	You can now customize the log level through the new `loglevel.conf` configuration file.

Fixed issues

Version 2.2.0 of the Splunk Add-on for Cisco ISE fixes the following issues.

Date	Issue number	Description

2015-05-05	ADDON-3929	Action values are not CIM-compliant with Authentication data model.
2016-05-06	ADDON-9326	Incorrect regex expressions in the `cisco-ise-action-failure-for-auth` and `cisco-ise-action-blocked` event type definitions.
2016-02-25	ADDON-7956	Tag expansions pull in unintended fields and negatively impact search performance.

Known issues

Version 2.2.0 of the Splunk Add-on for Cisco ISE contains the following known issues.

Date	Issue number	Description
2014-11-24	ADDON-2380	Workflow actions configuration limitations. pxGrid workflow action configuration not supported in `workflow_actions.conf`.
2015-07-10	ADDON-2610/ SPL-91709	Setup fails on Windows in Splunk Web when using Splunk platform 6.3 or earlier. Workaround: Upgrade to Splunk platform version 6.4 or set up `workflow_actions.conf` manually on Windows machines.
2017-11-10	ADDON-15925	Winsock error 10053 when trying to load the setup page of Cisco Identity Services. Workaround: Install the addon on Linux.

Third-party software attributions

Version 2.2.0 of the Splunk Add-on for Cisco ISE incorporates the `pxGrid_search.jar` library, provided by Cisco and used by their permission.

Version 2.1.2

Version 2.1.2 of the Splunk Add-on for Cisco ISE is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.0 and above
CIM	3.0 and above
Platforms	Platform independent
Vendor Products	Cisco ISE version 1.2 & 1.3

Migration from 2.1.1 to 2.1.2

There are no upgrade issues when upgrading from version 2.1.1 to 2.1.2.

Migration from 2.1.0 to 2.1.2

Version 2.1.1 of this add-on changed the timestamp extraction behavior. In that release, the way that the Splunk platform selects the timestamp from among the three timestamps available in Cisco ISE data was corrected. This may cause a time jump in your data at the upgrade point.

Migration from versions older than 2.1.0 to 2.1.2

If you have any version of the Splunk Add-on for Cisco ISE currently installed that is older than version 2.1.0, note that version 2.1.2 will not update or replace your current installation. Because the pre-2.1.0 community-supported versions of this add-on had a different folder structure, this add-on behaves as a new installation, not an upgrade.

To migrate from any version prior to 2.1.0 to version 2.1.2:

1. Download and install version 2.1.2 of the add-on from Splunkbase
2. Disable your previous version in the Splunk platform
3. Enable version 2.1.2 of the add-on
4. Create and adjust your local .conf files as needed to match your old configurations
5. Verify your configurations work as expected
6. Delete the older version of the add-on

Fixed issues

Version 2.1.2 of the Splunk Add-on for Cisco ISE fixes the following issues.

Date	Defect number	Description
2015-08-25	ADDON-5004	pxGrid_Search.jar file is corrupt.

Known issues

Version 2.1.2 of the Splunk Add-on for Cisco ISE has the following known issues.

Date	Defect number	Description
2015-05-05	ADDON-3929	Action values are not CIM-compliant with Authentication data model.
2014-11-24	ADDON-2380	Workflow actions configuration limitations. pxGrid workflow action configuration not supported in `workflow_actions.conf`.
2015-07-10	ADDON-2610/ SPL-91709	Setup fails on Windows in Splunk Web when using Splunk platform 6.3 or earlier. Workaround: Upgrade to Splunk platform version 6.4 or set up `workflow_actions.conf` manually on Windows machines.

Third-party software attributions

Version 2.1.2 of the Splunk Add-on for Cisco ISE incorporates the pxGrid_search.jar library, provided by Cisco and used by their permission.

Version 2.1.1

Version 2.1.1 of the Splunk Add-on for Cisco ISE was compatible with the following software, CIM versions, and platforms.

Splunk Enterprise versions	6.2, 6.1, 6.0
CIM	4.2, 4.1, 4.0, 3.0
Platforms	Platform independent
Vendor Products	Cisco ISE 1.2

Migration from 2.1.0 to 2.1.1

Version 2.1.1 of this add-on changes the timestamp extraction behavior. In this release, we are correcting the way that Splunk Enterprise selects the timestamp from among the three timestamps available in Cisco ISE data, which may cause a time jump in your data at the upgrade point.

Migration from versions older than 2.1.0 to 2.1.1

If you have any version of the Splunk Add-on for Cisco ISE currently installed that is older than version 2.1.0, note that version 2.1.1 will not update or replace your current installation. Because the pre-2.1.0 community-supported versions of this add-on had a different folder structure, this add-on behaves as a new installation, not an upgrade.

To migrate from any version prior to 2.1.0 to version 2.1.1:

1. Download and install version 2.1.1 of the add-on
2. Disable your previous version in Splunk Enterprise
3. Enable version 2.1.1 of the add-on
4. Create and adjust your local conf files as needed to match your old configurations
5. Verify your configurations work as expected
6. Delete the older version of the add-on

Fixed issues

Version 2.1.1 of the Splunk Add-on for Cisco ISE fixed the following issues.

Date	Defect number	Description
04/15/15	ADDON-3660	Stanza extract_vendor_action_ise in transforms.conf is not used in props.conf.
04/07/15	ADDON-3479	Add-on overrides Splunk Enterprise's default syslog timestamp configurations.
04/02/15	ADDON-3329	pxgremediate.py command does not return useful information.
03/31/15	ADDON-3423	Problems with authentication & dispatch of custom command, and improve logging.
03/31/15	ADDON-2512	Sourcetypes renamed in a way that broke backwards compatibility.
03/26/15	ADDON-3063	Authentication error received when invoking pxgremediate workflow (custom command). Workaround available from support.
03/26/15	ADDON-3079	Add-on contains *nix specific paths.
03/26/15	ADDON-3077	Potential command execution via malicious configuration file.

Known issues

Version 2.1.1 of the Splunk Add-on for Cisco ISE had the following known issues.

Date	Defect number	Description
08/19/15	ADDON-5004	pxGrid_Search.jar file is corrupt.
05/05/15	ADDON-3929	Action values are not CIM-compliant with Authentication data model.
04/01/15	ADDON-3560	Timestamp extraction behavior changes in this release, which impacts upgrades. In this release, we are correcting the way that Splunk Enterprise selects the timestamp from among the three timestamps available in Cisco ISE

		data, which may cause a time jump in your data at the upgrade point.
11/24/14	ADDON-2380	Workflow actions configuration limitations. pxGrid workflow action configuration not supported in `workflow_actions.conf`.
07/10/15	ADDON-2610/ SPL-86716	Setup fails on Windows in Splunk Web. Workaround: Set up `workflow_actions.conf` manually on Windows machines.

Third-party software attributions

Version 2.1.1 of the Splunk Add-on for Cisco ISE incorporates the pxGrid_search.jar library, provided by Cisco and used by their permission.

Version 2.1.0

Migration

If you have any previous version of the Splunk Add-on for Cisco ISE currently installed, note that version 2.1.0 will not update or replace your current installation. Because the previous community-supported versions of this add-on had a different folder structure, this add-on behaves as a new installation, not an upgrade.

To migrate from any previous version to version 2.1.0:

1. Download and install version 2.1.0 of the add-on
2. Disable your previous version in Splunk Enterprise
3. Enable version 2.1.0 of the add-on
4. Create and adjust your local conf files as needed to match your old configurations
5. Verify your configurations work as expected
6. Delete the older version of the add-on

New features

Version 2.1.0 of the Splunk Add-on for Cisco ISE included the following new features:

Resolved date	Issue number	Description
11/24/14	ADDON-1181	Normalize data to CIM Authentication and Change Analysis data models.
11/24/14	ADDON-2186	pxGrid remediation support with custom command.
10/27/14	ADDON-2035	Workflow actions to support ISE remediation
10/03/14	ADDON-1819	Pre-built panels for Cisco ISE

Known issues

Version 2.1.0 of the Splunk Add-on for Cisco ISE had the following known issues.

Date	Defect number	Description
02/02/15	ADDON-2610	Setup fails on Windows in Splunk Web. Workaround: Set up `workflow_actions.conf` manually on Windows machines.
01/23/15	ADDON-3063	Authentication error received when invoking pxgremediate workflow (custom command). Workaround available from support.

12/09/14	ADDON-2610	Setup fails on Windows machines. Workaround: set up `workflow_actions.conf` manually.
11/24/14	ADDON-2380	Workflow actions configuration limitations. pxGrid workflow action configuration not supported in `workflow_actions.conf`.
09/08/14	ADDON-1543	In multi-router installations, two different timestamps appear in Cisco ISE data, and the second one (after the IP address) is the correct one.

Third-party software attributions

Version 2.1.0 of the Splunk Add-on for Cisco ISE incorporates the pxGrid_search.jar library, provided by Cisco and used by their permission.