Splunk® Enterprise Security Installation and Upgrade Manual 6.6.2

Generated: 10/18/2021 11:15 pm

Table of Contents

Introduction

About Splunk Enterprise Security

Splunk Enterprise Security uses the Splunk platform's searching and reporting capabilities to provide the security practitioner with an overall view of their organization's security posture. Enterprise Security uses **correlation searches** to provide visibility into security-relevant threats and generate **notable events** for tracking identified threats. You can capture, monitor, and report on data from devices, systems, and applications across your environment.

This manual is written for a user capable of installing, configuring, and administering Splunk software. If you need training on the Splunk platform and Enterprise Security, see Education Courses for Enterprise Security Customers.

Other manuals for Splunk Enterprise Security:

- Release Notes
- Use Splunk Enterprise Security
- Administer Splunk Enterprise Security
- Use Cases
- REST API Reference

Share data in Splunk Enterprise Security

When Splunk Enterprise Security is deployed on Splunk Enterprise, the Splunk platform sends anonymized usage data to Splunk Inc. ("Splunk") to help improve Splunk Enterprise Security in future releases. For information about how to opt in or out, and how the data is collected, stored, and governed, see Share data in Splunk Enterprise.

How data is collected

Splunk Enterprise Security uses saved searches to collect anonymous usage data. These searches run in the background regardless of whether or not you opt-in to send usage data to Splunk, and do not have any significant impact on performance.

What data is collected

Splunk Enterprise Security collects the following basic usage information:

Name	Description	Example
`app.SplunkEnterpriseSecuritySuite.active_users`	Report the number of active users.	`{ "version": "1.0", "end": 1521483766, "begin": 1521396000, "data": { "analyst_count": 0, "count": 1, "admin_count": 1, "user_count": 0 }`

Name	Description	Example
		}

app.SplunkEnterpriseSecuritySuite.annotations_usage	Report the number of users that enable and start using annotations in correlation searches for the risk framework.	{
		"data": {
		"unique_annotation_count": 86,
		"unique_framework_count": 4,
		"searches_with_cis20": 200,
		"searches_with_kill_chain_phases": 176,
		"searches_with_mitre_attack": 119,
		"searches_with_nist": 199,
		"searches_with_annotations": 213
		},
		"version": "1.0"
		}

app.SplunkEnterpriseSecuritySuite.datamodel_distribution	Performs a data model audit to determine which models are the most heavily used.	{
		"data": {
		"size": 2265088,
		"datamodel": "Change_Analysis",
		"perc": 49.33
		},
		"version": "1.0"
		}

app.SplunkEnterpriseSecuritySuite.feature_usage	• Page Load Times reports the amount of time it takes for a page to load
	• Feature Usage: reports data about feature usage
		{
		"end": 1521483766,
		"begin": 1521396000,
		"version": "1.0",
		"data": {
		"count": 1,
		"avg_spent": 515,
		"view": "ess_home"
		}
		}

app.SplunkEnterpriseSecuritySuite.identity_manager	Reports statistics pertaining to the usage of the Assets and Identities Framework.	{ "data": { [-] "asset_blacklist_count": 0, "asset_count": 3, "asset_custom_count": 1, "asset_custom_fields": 0, "asset_enabled_count": 1, "asset_ldap_count": 0, "asset_search_count": 0, "identity_blacklist_count": 0,

Name	Description	Example
		"identity_count": 3, "identity_custom_count": 0, "identity_custom_fields": 0, "identity_enabled_count": 2, "identity_ldap_count": 0, "identity_search_count": 0, "total_blacklist_count": 0, "total_count": 6, "total_custom_count": 1, "total_enabled_count": 3, "total_ldap_count": 0, "total_search_count": 0 }, "version": 1.0 }

app.SplunkEnterpriseSecuritySuite.lookup_usage	Reports statistics pertaining to the usage of the Asset & Identity Manager, such as lookup table size and number of entries.	{
		"data": {
		"count": 0,
		"size": 22,
		"transform": "access_app_tracker"
		},
		"version": "1.0"
		}

app.SplunkEnterpriseSecuritySuite.riskfactors_usage	Reports how customers use the risk framework.	{
		{ [-]
		app: SplunkEnterpriseSecuritySuite
		component: app.SplunkEnterpriseSecuritySuite
		data: { [-]
		fields_info: [[-]
		{"fields_used": "dest_priority", "count": 1
		{"fields_used": "user_category", "count": 2
		{"fields_used": "user_priority", "count": 2
		{"fields_used": "user_watchlist", "count": 1
		]
		total: 5
		}
		deploymentID: 464150eb-1b95-528e-85ca-272ba
		eventID: AB7AC804-8711-459C-A649-0A2DD89622
		executionID: 1E895CC2-5C46-456F-9A79-86CC0E
		optInRequired: 3
		timestamp: 1603825511
		type: aggregate
		visibility: [[+]
		]
		}

app.SplunkEnterpriseSecuritySuite.risk_riskfactors_impact	Reports how the customers engage with risk framework.	{ [-] app: SplunkEnterpriseSecuritySuite component: app.SplunkEnterpriseSecuritySuite data: { [-] distinct_risk_object_count: 2 max_calc_risk_score: 100 max_risk_factor_add_matches: 0

Name	Description	Example
		max_risk_factor_mult_matches: 1 max_risk_score: 100 min_calc_risk_score: 100 min_risk_factor_add_matches: 0 min_risk_factor_mult_matches: 1 min_risk_score: 100 risk_factor_add_matches: 0 risk_factor_mult_matches: 0 risk_object_type: system } deploymentID: 3db462ee-7955-54b0-9a94-24bc1 eventID: 84949E43-2964-43CC-AA04-50F2C40826 executionID: 27E5957D-41F4-4C83-A1F1-DCF5C9 optInRequired: 3 timestamp: 1603851828 type: aggregate visibility: [[+]] }

app.SplunkEnterpriseSecuritySuite.search_actions	Reports what was searched for.	{
		"data": {
		"total_scheduled": 70,
		"action": "output_message",
		"is_adaptive_response": 1,
		"count": 6
		},
		"version": "1.0"
		}

app.SplunkEnterpriseSecuritySuite.search_execution	Reports average run time by search, to help gauge performance.	{
		"end": 1521483766,
		"begin": 1521396000,
		"data": {
		"avg_run_time": 0.75,
		"count": 2,
		"search_alias": "Access - Authentication
		},
		"version": "1.0",
		}

data.context	Reports how many times a given workbench panel was used, and the distribution of fields drilled into from workflow actions.	{
		component: app.session.rum.mark
		data: {
		app: SplunkEnterpriseSecuritySuite
		context: {
		field: lokloklok
		panels: [
		f2c5c990f8fbf4f173ed8ae17ac3463c53
		f2c5c990f8fbf4f173ed8ae17ac3463c53
		a7f1eed1b49d2391fbe7f6b6cb91a3c146
		]
		}
		hero: embedded workbench panel page
		page: ess_workbench_panel
		sourceLocation: controller mounted
		timeSinceOrigin: 17539.599999785423

Name	Description	Example

		<pre>transactionId: 9eb149d0-84d9-11ea-9a01-
		}
		deploymentID: 90dacf53-e620-5a99-8cd4-152
		eventID: 19c90580-816d-2dc5-13a8-5af7835
		experienceID: 6aa4e746-c8f0-234b-35b2-df
		optInRequired: 3
		timestamp: 1587588081
		userID:
		953b11dd9ec6593a941245c43738a191110c7e42f8e
		version: 3
		visibility: anonymous,support
		}</pre>

Planning

Deployment planning

Deploy Splunk Enterprise Security on a configured Splunk platform installation. Review the system and hardware requirements and the search head and indexer considerations before deploying Enterprise Security.

Available deployment architectures

You can deploy Splunk Enterprise Security in a single instance deployment or a distributed search deployment. Splunk Enterprise Security is also available in Splunk Cloud Platform. Before you deploy Splunk Enterprise Security on premises, familiarize yourself with the components of a Splunk platform deployment. See Components of a Splunk Enterprise deployment in the *Capacity Planning Manual*.

Single instance deployment

For a simple and small deployment, install Splunk Enterprise Security on a single Splunk platform instance. A single instance functions as both a search head and an indexer. Use forwarders to collect your data and send it to the single instance for parsing, storing, and searching.

You can use a single instance deployment for a lab or test environment, or a small system with one or two users running concurrent searches.

Distributed search deployments

A distributed search deployment is recommended for deploying and running Splunk Enterprise Security.

- Install Splunk Enterprise Security on a dedicated search head or search head cluster. A dedicated search head is not required for every implementation. It depends on the capacity of your specific environment and the workload of the apps you're already running, in addition to your Enterprise Security workload. See Introduction to capacity planning for Splunk Enterprise in the Splunk Enterprise *Capacity Planning* Manual.
- Improve search performance by using an index cluster and distributing the workload of searching data across multiple nodes. Using multiple indexers allows both the data collected by the forwarders and the workload of processing the data to be distributed across the indexers.
- Use forwarders to collect your data and send it to the indexers.

In a distributed search deployment, and to implement search head clustering, configure the search head to forward all data to the indexers. See Forward search head data to the indexer layer in the *Distributed Search* manual.

To properly scale your distributed search deployment with Splunk Enterprise Security, see Indexer scaling considerations for Splunk Enterprise Security.

Cloud deployment

Splunk Enterprise Security is available as a service in Splunk Cloud Platform. The Splunk Cloud Platform deployment architecture varies based on data and search load. Splunk Cloud Platform customers work with Splunk Support to set up, manage, and maintain their cloud infrastructure. For information on Splunk Cloud Platform deployments, see the Splunk Cloud Platform deployment types in the Splunk Cloud Platform *Admin Manual*.

Hybrid search deployment

A hybrid search configuration with Splunk Enterprise Security is not yet supported with Splunk Cloud Platform. You can set up an on-premises Splunk Enterprise Security search head to search indexers in another cloud environment. Any hybrid search deployment configuration must account for added latency, bandwidth concerns, and include adequate hardware to support the search load.

Splunk Enterprise system requirements

Splunk Enterprise Security requires a 64-bit OS install on all search heads and indexers. For the list of supported operating systems, browsers, and file systems, see System requirements for use of Splunk Enterprise on-premises in the Splunk Enterprise *Installation Manual*.

See the following to determine the compatibility of the Enterprise Security versions and Splunk platform versions:

- Splunk Products Version Compatibility Matrix in the *Splunk Products Version Compatibility Matrix* manual.
- Splunk Cloud Platform Service Details in the *Splunk Cloud Platform Service Description* manual.

For the details on how to upgrade Splunk Enterprise, and also the Splunk products version compatibility matrix, see About upgrading to 8.0 READ THIS FIRST in the Splunk Enterprise *Installation Manual*.

Hardware requirements

Splunk Enterprise Security requires minimum hardware specifications that you increase according to your needs and usage of Splunk Enterprise Security. These specifications also apply for a single instance deployment of Splunk Enterprise Security.

Machine role	Minimum CPU	Minimum RAM
Search head	16 physical CPU cores	32GB
Indexer	16 physical CPU cores	32GB

The minimum hardware specifications for search head cluster peers (search heads and indexers) to run Enterprise Security is the same as those required by standalone deployments (search heads and indexers).

Indexing is an I/O-intensive process. The indexers require sufficient disk I/O to ingest and parse data efficiently while responding to search requests. For the latest IOPS requirements to run Splunk Enterprise, see Reference Hardware: Indexer in the *Capacity Planning Manual*.

You might need to increase the hardware specifications of your own Enterprise Security deployment above the minimum hardware requirements depending on your environment. Depending on your system configuration, refer to the mid-range or high-performance specifications for Splunk platform reference hardware. See Mid-range specification and High-performance specification in the *Capacity Planning Manual*.

Splunk Enterprise Security search head considerations

Install Splunk Enterprise Security on a dedicated search head or a dedicated search head cluster. You can install only Common Information Model (CIM)-compatible apps or add-ons on the same search head as Splunk Enterprise Security. For example, the Splunk App for PCI Compliance (for Splunk Enterprise Security) or the Splunk Add-on for Facebook ThreatExchange can both be installed on the same search head as Splunk Enterprise Security.

All **real-time searches** in Splunk Enterprise Security use the indexed real-time setting to improve indexing performance. See About real-time searches and reports in the *Search Manual*. Disabling the indexed real-time search setting reduces the overall indexing capacity of your indexers. To review the performance implications of the types of real-time searches, see Known limitations of real-time searches in the *Search Manual*.

Splunk Enterprise Security requires the KV Store. For more information about KV Store, including the system requirements, see About the app key value store in the Splunk Enterprise *Admin Manual*. Splunk Enterprise Security stores some lookup files in the KV Store. In a search head cluster environment, syncing large KV Store lookups across the cluster members can fail and cause the KV Store to become stale. To mitigate this, you can increase the operations log size. See Prevent stale members by increasing operations log size in the Splunk Enterprise *Admin Manual*.

Splunk Enterprise Security and search head clustering

Splunk Enterprise Security supports installation on Linux-based search head clusters only. At this time, Windows search head clusters are not supported by Splunk Enterprise Security.

Search head clusters increase the search load on indexers. Add more indexers or allocate additional CPU cores to the indexers when implementing a search head cluster. See System requirements and other deployment considerations for search head clusters in the Splunk Enterprise *Distributed Search Manual* and Search head clustering architecture in the *Distributed Search Manual*.

Search head scaling considerations for Splunk Enterprise Security

Factor	Increase this specification
A large number of concurrent ad-hoc searches	Increase CPU cores Increase RAM
A high number of real-time searches being run A large number of users logging in at the same time	Increase CPU cores
A large number of enabled correlation searches	Increase RAM
Large asset and identity lookup files	Increase RAM

Indexer scaling considerations for Splunk Enterprise Security

Increase the number of indexers in your deployment to scale with increases in search load and search concurrency. Because a collection of indexers can serve more than one search head, additional search heads using the same indexers as a search head hosting Enterprise Security can affect the total performance of your indexer tier and reduce the resources available to Enterprise Security.

The Splunk platform uses indexers to scale horizontally. The number of indexers required in an Enterprise Security deployment varies based on the data volume, data type, retention requirements, search type, and search concurrency.

Work with Splunk Professional Services to estimate deployment architecture if you plan to ingest 1 terabyte (1TB) per day or more of data into Enterprise Security.

Performance test results

Review these performance test results to estimate the performance you can expect from your infrastructure based on the mix of data in your Splunk platform and Enterprise Security deployment. The indexers used for these performance tests match the reference hardware with 32GB of RAM and 16 CPU cores.

There are a few large factors to consider when sizing Splunk Enterprise Security.

- Correlation search load, based on the number of correlation searches and supporting searches enabled in your deployment.
- Data model acceleration load, based on the number of data models being accelerated, the type of data being modeled, the cardinality of the data being modeled, and the volume of data being accelerated.
- Search head cluster environment versus single search head environment.

Depending on the data mix, the ingest volume, and the searches enabled, the data model accelerations can lag behind the data ingestion. Using hardware similar to the AWS instance of i3en.12xlarge, we can simulate large customer system resource usage with approximately 24 indexers ingesting 625 GB per day to a total of 15 TB per day volume, based on the following lab example mix:

- 9 data models
- 10 major source types
- 60 out-of-the-box correlation searches
- 70 saved searches
- random navigation traffic on ES dashboards

Capacity planning is challenging due to the complexity of use cases, the data, and the architecture possibilities. Every situation is unique.

When scaling Splunk Enterprise with Splunk Enterprise Security to very high (15TB) levels of data volumes, some of the configurations that would normally be acceptable in a Splunk Enterprise deployment are no longer acceptable in a Splunk Enterprise deployment with Enterprise Security. You can work with your Splunk field architect to calculate and validate. The reason is that Enterprise Security ships with a number of default searches, including data model acceleration. These searches impact the overall cluster performance.

Because high volume Enterprise Security deployments run high numbers of searches that generate large amounts of results, the amount of work each peer must do can also become much greater than what you would see in a smaller deployment. As a result, memory consumption and runtimes of search jobs are key metrics to monitor and adjust for safe levels. Customers should pay careful attention to the styles and types of searches that are allowed to run on high volume Enterprise Security deployments, and enforce quality standards against the types of SPL commands, the timeframes, and intervals that are appropriate for scheduled searches within Enterprise Security.

Indexer clustering support

Splunk Enterprise Security supports both single site and multisite indexer cluster architectures. See The basics of indexer cluster architecture and Multisite cluster architecture in *Managing Indexers and Clusters of Indexers*.

A single site or multisite indexer cluster architecture can have one search head or one search head cluster with a running instance of Enterprise Security. Additional single instance search heads or additional search head clusters cannot run Enterprise Security.

For a multisite indexer cluster architecture, Splunk recommends the following:

- Enable summary replication. See Replicated summaries in *Managing Indexers and Clusters of Indexers*.
- Set the Enterprise Security search head to `site0` to disable search affinity. See Disable search affinity in *Managing Indexers and Clusters of Indexers*.

If you use indexer clustering, the method you use to deploy apps and configuration files to indexer peers is different. See Manage common configurations across all cluster peers and Manage app deployment across all cluster peers in the

Managing Indexers and Clusters of Indexers.

Data model accelerations

Splunk Enterprise Security accelerates data models to provide dashboard, panel, and correlation search results. Data model acceleration uses the indexers for processing and storage, storing the accelerated data in each index.

Limit data model acceleration for specific data models to specific indexes to improve performance of data model acceleration and reduce indexer load, especially at scale. See Set up the Splunk Common Information Model Add-on for more on restricting data models to specific indexes.

See Data model acceleration storage and retention to calculate the additional storage for data model acceleration.

Index TSIDX reduction compatibility

A retention policy for an index's TSIDX files is available in Splunk Enterprise 6.4.x. For more information, see Reduce tsidx disk usage in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual. Setting a retention policy for the TSIDX files does not affect the retention of data model accelerations.

Some searches provided with Enterprise Security do not work on buckets with reduced TSIDX files.

Panel/Search Name	Default time range	Workaround
Forwarder Audit panel: Event Count Over Time by Host	-30d	Set the TSIDX retention to a value greater than the time range.
Saved Search: Audit - Event Count Over Time By Top 10 Hosts	-30d	Set the TSIDX retention to a value greater than the time range.
Saved Search: Audit - Events Per Day - Lookup Gen	-1d	Set the TSIDX retention to a value greater than the default time range.
Saved Search: Endpoint - Index Time Delta 2 - Summary Gen	-1d	Set the TSIDX retention to a value greater than the default time range.

Using the deployment server with Splunk Enterprise Security

Splunk Enterprise Security includes apps and add-ons. If the deployment server manages those apps or add-ons, Enterprise Security will not finish installing.

- For add-ons included with Splunk Enterprise Security, deploy them using the Distributed Configuration Management tool. See Deploy add-ons included with Splunk Enterprise Security in this manual.
- For other apps and add-ons installed in your environment, deploy them with the deployment server if appropriate. See About deployment server and forwarder management in *Updating Splunk Enterprise Instances*.

If add-ons included with the Enterprise Security package are managed by a deployment server, remove the deployment client configuration before installing Enterprise Security.

1. Remove the `deploymentclient.conf` file containing references to the deployment server.
2. Restart Splunk services.

Virtualized hardware

If you install Splunk Enterprise Security in a virtualized environment, you need the same memory and CPU allocation as a non-virtualized bare-metal environment.

- Reserve all CPU and memory resources.
- Do not oversubscribe hardware.
- Test the storage IOPS across all Splunk platform indexer nodes simultaneously to ensure that the IOPS match the reference hardware specification used in your environment. See Reference Hardware in the *Capacity Planning Manual*

Insufficient storage performance is a common cause for poor search response and timeouts when scaling the Splunk platform in a virtualized environment.

- Use thick-provisioned storage. Thin provisioning storage might impact performance.

Monitoring Console

If you enable the Monitoring Console on an Enterprise Security search head, it must remain in standalone mode. For more on when and how to configure the Monitoring Console in a distributed environment, see Which instance should host the console? in *Monitoring Splunk Enterprise*.

Enterprise Security compatibility with other apps

Splunk Enterprise Security (ES) relies on the search knowledge and Common Information Model (CIM) support supplied by add-ons. The add-ons are responsible for defining the event processing necessary to optimize, normalize, and categorize security data for use with the CIM. Only CIM-compatible apps are compatible with Splunk Enterprise Security. Other apps and add-ons that are not CIM-compatible can include data knowledge that is not normalized for the CIM, preventing searches and dashboards that rely on those fields from functioning properly.

Only install apps and add-ons on the same search head with ES if they meet one of the following guidelines:

- Add-ons that are CIM-compatible and enrich data for use with ES.
- Apps that may or may not enrich data for ES, but whose primary purpose is to integrate with ES.

Splunk Enterprise Security and the SA-VMNetAppUtils component of the Splunk Add-on for VMware cannot be installed on the same search head. Conflicts with identically-named files can prevent some parts of Splunk Enterprise Security from working correctly.

Data source planning for Splunk Enterprise Security

The volume, type, and number of data sources influences the overall Splunk platform architecture, the number and placement of forwarders, estimated load, and impact on network resources.

Splunk Enterprise Security requires that all data sources comply with the Splunk Common Information Model (CIM). Enterprise Security is designed to leverage the CIM standardized data models both when searching data to populate dashboard panels and views, and when providing data for correlation searches.

Map add-ons to data sources

The add-ons included with Splunk Enterprise Security are designed to parse and categorize known data sources and other technologies for CIM compliance.

For each data source:

1. Identify the add-on: Identify the technology and determine the corresponding add-on. The primary sources for add-ons are the Technology-specific add-ons provided with Enterprise Security and the CIM-compatible content available on Splunkbase. If the add-on you want to use is not already compatible with the CIM, modify it to support CIM data schemas. For an example, see Use the CIM to normalize data at search time in the *Common Information Model Add-on Manual*.
2. Install the add-on: Install the add-on on the Enterprise Security search head. Install add-ons that perform index-time processing on each indexer. If the forwarder architecture includes sending data through a parsing or heavy forwarder, the add-on might be needed on the heavy forwarder. Splunk Cloud Platform customers must work with Splunk Support to install add-ons on search heads and indexers, but are responsible for on-premises forwarders.
3. Configure the server, device, or technology where necessary: Enable logging or data collection for the device or application and/or configure the output for collection by a Splunk instance. Consult the vendor documentation for implementation steps.
4. Customize the add-on where necessary: An add-on might require customization, such as setting the location or source of the data, choosing whether the data is located in a file or in a database, or other unique settings.
5. Set up a Splunk data input and confirm the source type settings: The README file of the add-on includes information about the source type setting associated with the data, and might include customization notes about configuring the input.

Considerations for data inputs

Splunk platform instances provide several types of input configurations to ingest data. Depending on the technology or source being collected, choose the input method that matches the infrastructure requirements based on the performance impact, ease of data access, stability, minimizing source latency, and maintainability.

- **Monitoring files**: Deploy a Splunk forwarder on each system hosting the files, and set the source type on the forwarder using an input configuration. If you have a large number of systems with identical files, use the Splunk Enterprise deployment server to set up standardized file inputs across large groups of forwarders.

- **Monitoring network ports**: Use standard tools such as a syslog server, or create listener ports on a forwarder. Sending multiple network sources to the same port or file complicates source typing. For more information, see the Splunk platform documentation.

    - For Splunk Enterprise, see Get data from TCP and UDP ports in Splunk Enterprise *Getting Data In*.
    - For Splunk Cloud Platform, see Get data from TCP and UDP ports in Splunk Cloud Platform *Getting Data In*.

- **Monitoring Windows data**: A forwarder can obtain information from Windows hosts using a variety of configuration options. For more information, see the Splunk platform documentation.

    - For Splunk Enterprise, see How to get Windows data into Splunk Enterprise in Splunk Enterprise *Getting Data In*.
    - For Splunk Cloud Platform, see Monitoring Windows data with Splunk Enterprise in Splunk Cloud

Platform *Getting Data In*.

- **Monitoring network wire data**: Splunk Stream supports the capture of real-time wire data. See About Splunk Stream in the Splunk Stream *Installation and Configuration Manual*.

- **Scripted inputs**: Use scripted inputs to get data from an API or other remote data interfaces and message queues. Configure the forwarder to call shell scripts, python scripts, Windows batch files, PowerShell, or any other utility that can format and stream the data that you want to index. You can also write the data polled by any script to a file for direct monitoring by a forwarder. For more information, see the Splunk platform documentation.

    - For Splunk Enterprise, see Get data from APIs and other remote data interfaces through scripted inputs in Splunk Enterprise *Getting Data In*.
    - For Splunk Cloud Platform, see Get data from APIs and other remote data interfaces through scripted inputs in Splunk Cloud Platform *Getting Data In*.

Collect asset and identity information

Splunk Enterprise Security compares asset and identity data with events in Splunk platform to provide data enrichment and additional context for analysis. Collect and add your asset and identity information to Splunk Enterprise Security to take advantage of the data enrichment. See Add asset and identity data to Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

Installation

Install Splunk Enterprise Security

Install Splunk Enterprise Security on an on-premises search head. Splunk Cloud Platform customers must work with Splunk Support to coordinate access to the Enterprise Security search head.

Splunk Enterprise platform considerations

Splunk Enterprise 7.2.0 uses Serialized Result Set (SRS) format by default. The exception is in searches that execute actions, for which we auto-detect whether to use CSV or SRS. This is handled in the `alert_actions.conf` file, but do not modify the `forceCsvResults` stanza without a thorough understanding of scripts or processes that access the results files directly.

A new `install_apps` capability is introduced in Splunk Enterprise v8. The change impacts the existing Enterprise Security `edit_local_apps` capability's functionality to install and upgrade apps. In ES, `enable_install_apps` is false by default. If you set `enable_install_apps=True` and you don't have the new `install_apps` and existing `edit_local_apps` capabilities, you will not be able to install and setup apps. This includes performing ES setup and installing other content packs or Technology Add-ons.

Installation prerequisites

- Review the Splunk platform requirements for Splunk Enterprise Security. See Deployment planning.
- If a deployment server manages any of the apps or add-ons included with Splunk Enterprise Security, remove the `deploymentclient.conf` file that contains references to the deployment server and restart Splunk services. If you do not do this, the installation will not complete.
- Your user account must have the admin role and the `edit_local_apps` capability. The admin role is assigned that capability by default.
- Approximately 1 GB of free space is required in the `/tmp/` directory for the installation or upgrade to complete. When installing or upgrading an app through either the CLI or Splunk Web UI, the `/tmp/` directory is utilized during the process.

Step 1. Download Splunk Enterprise Security

1. Log in to splunk.com with your Splunk.com user name and password.
2. Download the latest Splunk Enterprise Security product. You must be a licensed Enterprise Security customer to download the product.
3. Click **Download** and save the Splunk Enterprise Security product file to your desktop.
4. Log in to the search head as an administrator.

Step 2. Install Splunk Enterprise Security

The installer dynamically detects if you're installing in a single search head environment or search head cluster environment. The installer is also bigger than the default upload limit for Splunk Web.

1. Increase the Splunk Web upload limit to 1 GB by creating a file called `$SPLUNK_HOME/etc/system/local/web.conf` with the following stanza.
   [settings]
   max_upload_size = 1024

2. To restart Splunk from the Splunk toolbar, select **Settings > Server controls** and click **Restart Splunk**.
3. On the Splunk toolbar, select **Apps > Manage Apps** and click **Install App from File**.
4. Click **Choose File** and select the Splunk Enterprise Security product file.
5. Click **Upload** to begin the installation.
6. Click **Set up now** to start setting up Splunk Enterprise Security

There are a few differences after installing on a deployer in a SHC environment. See Install Splunk Enterprise Security in a search head cluster environment.

Step 3. Set up Splunk Enterprise Security

Set up Splunk Enterprise Security in a single search head environment.

1. Click **Start**.
2. If you are not using Secure Sockets Layer (SSL) in your environment, do one of the following steps when you see the SSL Warning message:
    1. Click **Enable SSL** to turn on SSL and start using `https://` for encrypted data transfer.
    2. Click **Do Not Enable SSL** to keep SSL turned off and continue using `http://` for data transfer.
3. The **Splunk Enterprise Security Post-Install Configuration** page indicates the status as it moves through the stages of installation.
4. Choose to exclude selected add-ons from being installed, or install and disable them. When the setup is done, the page prompts you to restart Splunk platform services.
5. If prompted to do so, click **Restart Splunk** to finish the installation.

If you enable SSL, you must change the Splunk Web URL to use https to access the search head after installing ES.

After the installation completes, review the installation log in: `$SPLUNK_HOME/var/log/splunk/essinstaller2.log`.

Step 4. Configure Splunk Enterprise Security

To continue configuring Splunk Enterprise Security, see the following:

1. Deploy add-ons included with Splunk Enterprise Security
2. Configure and deploy Indexes
3. Configure users and roles
4. Configure data models

For an overview of the data sources and collection considerations for Enterprise Security, see Data source planning.

Enterprise Security does not support Dark Theme.

Install Splunk Enterprise Security from the command line

Install Splunk Enterprise Security using the Splunk software command line. See About the CLI for more about the Splunk software command line.

1. Follow Step 1: Download Splunk Enterprise Security to download Splunk Enterprise Security and place it on the search head.

2. Start the installation process on the search head. Install with the `./splunk install app <filename>` command or perform a REST call to start the installation from the server command line.
   For example: `curl -k -u admin:password https://localhost:8089/services/apps/local -d filename="true" -d name="<file name and directory>" -d update="true" -v`

   > Do not use the following command ./splunk install app when upgrading the Splunk Enterprise Security app.

   You can upgrade the Splunk Enterprise Security app on the CLI using the same process as other Splunk apps or add-ons. For information on upgrading Splunk platform apps, see Manage apps and add-ons. After the Splunk Enterprise Security app is installed, run the `essinstall` command with the appropriate flags as shown in the next step.
3. On the search head, use the Splunk software command line to run the following command:
   ```
   splunk search '| essinstall' -auth admin:password
   ```
   You can also run this search command from Splunk Web and view the installation progress as search results.

   ```
   | essinstall
   ```

   > When installing from the command line, ssl_enablement defaults to "strict." If you don't have SSL enabled, the installer will exit with an error.

   If you run the search command to install Enterprise Security in Splunk Web, you can review the progress of the installation as search results. If you run the search command from the command line, you can review the installation log in: `$SPLUNK_HOME/var/log/splunk/essinstaller2.log`.

Test installation and setup of Splunk Enterprise Security

You can test the installation and setup of Splunk Enterprise Security by adding

1. Follow Step 1: Download Splunk Enterprise Security to download Splunk Enterprise Security and place it on the search head.
2. Start the installation process on the search head. Install with the `./splunk install app <filename>` command or perform a REST call to start the installation from the server command line.
   For example: `curl -k -u admin:password https://localhost:8089/services/apps/local -d filename="true" -d name="<file name and directory>" -d update="true" -v`
3. From Splunk Web, open the Search and Reporting app.
4. Type the following search to perform a dry run of the installation and setup.

   ```
   |essinstall --dry-run
   ```

Uninstall Splunk Enterprise Security

You can uninstall the ES app by removing SplunkEnterpriseSecuritySuite from the `$SPLUNK_HOME/etc/apps` folder structure. You can do this by recursively deleting the directory or moving it to `$SPLUNK_HOME/etc/disabled-apps` and restarting. By moving it to disabled-apps, it's available if you want to temporarily test and then move it back.

ES is a collection of apps, so removing a single app folder will not uninstall it. You need to remove or move all applicable apps in the suite.

Install Splunk Enterprise Security in a search head cluster environment

Splunk Enterprise Security has specific requirements and processes for implementing search head clustering.

- For an overview of search head clustering, see Search head clustering architecture in the *Distributed Search Manual*.
- For a complete list of search head clustering requirements, see System requirements and other deployment considerations for search head clusters in the *Distributed Search Manual*.

If you are installing Enterprise Security on an existing search head cluster environment which might have other apps deployed already, all of the steps in this section apply. Be careful to not delete or remove any existing content in the $SPLUNK_HOME/etc/shcluster/apps folder.

Prerequisites for installing Enterprise Security in a search head cluster environment

Splunk Enterprise Security supports installation on Linux-based search head clusters only. At this time, Windows search head clusters are not supported by Splunk Enterprise Security.

Before installing Enterprise Security in a search head cluster environment, verify that you have:

- One deployer
- The same version of Splunk Enterprise on the deployer and search head cluster nodes
- The same app versions of any other apps on the deployer and search head cluster nodes (not yet including Enterprise Security)
- The backup of `etc/shcluster/apps` on the deployer before installing Enterprise Security
- The backup of `etc/apps` from one of search head cluster nodes
- The backup of the KVstore from one of search head cluster nodes
- Verify on the deployer that your `server.conf shclustering` configuration is in `$SPLUNK_HOME/etc/system/local/server.conf` or is in an app that exports the server configuration globally via metadata:
  [server]
  export = system

Installing Enterprise Security in a search head cluster environment

The installer dynamically detects if you're installing in a single search head environment or search head cluster environment. The installer is also bigger than the default upload limit for Splunk Web. To install Enterprise Security on a search head cluster:

1. Prepare the deployer per the prerequisites.
2. Install Enterprise Security on the deployer.
    1. Increase the Splunk Web upload limit, for example to 1GB, by creating a file called `$SPLUNK_HOME/etc/system/local/web.conf` with the following stanza.
       [settings]
       max_upload_size = 1024
    2. On the Splunk toolbar, select **Apps > Manage Apps** and click **Install App from File**.
    3. Click **Choose File** and select the Splunk Enterprise Security product file.
    4. Click **Upload** to begin the installation.
    5. Click **Continue to app setup page**

Note the message that Enterprise Security is being installed on the deployer of a search head cluster environment and that technology add-ons will not be installed as part of the post-install configuration.

3. Click **Start Configuration Process**.
4. If you are not using Secure Sockets Layer (SSL) in your environment, do one of the following steps when you see the SSL Warning message:
    1. Click **Enable SSL** to turn on SSL and start using `https://` for encrypted data transfer.
    2. Click **Do Not Enable SSL** to keep SSL turned off and continue using `http://` for data transfer.

- Wait for the process to complete.
- Move SplunkEnterpriseSecuritySuite from `$SPLUNK_HOME/etc/apps` to `$SPLUNK_HOME/etc/shcluster/apps`

If you use the btool command line tool to verify settings, use it only after you move the SplunkEnterpriseSecuritySuite from $SPLUNK_HOME/etc/apps to $SPLUNK_HOME/etc/shcluster/appssearches directory. You must ensure that the SplunkEnterpriseSecuritySuite does not exist in the $SPLUNK_HOME/etc/apps directory. Otherwise, btool checks may cause errors because add-ons like SA-Utils that contain .spec files are not installed on the deployer.

The DA-ESS and SA apps are automatically extracted and deployed throughout the search head cluster.

- Use the deployer to deploy Enterprise Security to the cluster members. From the deployer, run this command: splunk apply shcluster-bundle --answer-yes -target <URI>:<management_port> -auth <username>:<password>

  For more information on using the deployer to distribute apps and configuration updates to search head cluster members, see Use the deployer to distribute apps and configuration updates.

To verify that Enterprise Security is deployed to the cluster members:

- From the GUI of a cluster member, you can check the **Help > About** menu to check the version number.
- From the CLI of a cluster member, you can check the `/etc/apps` directory to verify the supporting add-ons and domain add-ons for Enterprise Security: `DA-ESS-AccessProtection, DA-ESS-EndpointProtection, DA-ESS-IdentityManagement, DA-ESS-NetworkProtection, DA-ESS-ThreatIntelligence, SA-AccessProtection, SA-AuditAndDataProtection, SA-EndpointProtection, SA-IdentityManagement, SA-NetworkProtection, SA-ThreatIntelligence, SA-UEBA, SA-Utils, Splunk_DA-ESS_PCICompliance, SplunkEnterpriseSecuritySuite, Splunk_SA_CIM, Splunk_ML_Toolkit, and Splunk_SA_Scientific_Python_linux_x86_64 (or Splunk_SA_Scientific_Python_windows_x86_64 for windows)`
- From the CLI of a cluster member, you can check the `$SPLUNK_HOME/etc/apps/SplunkEnterpriseSecuritySuite/local/inputs.conf` file to see that the data model accelerations settings are enabled.

Although technology add-ons are bundled in the installer, they are not deployed as part of the installation process. You must deploy them manually if you want to use them. See Deploy add-ons included with Splunk Enterprise Security.

Installing Splunk Enterprise Security from the command line in a search head cluster environment

From the command line, the installer doesn't autodetect if it is being launched from a deployer. It is necessary to add a command line option: `'--deployment_type', default='search_head', choices=['search_head', 'shc_deployer'], help='select deployment type'`.

Installing Splunk Enterprise Security using the Splunk software command line. See About the CLI for more about the Splunk software command line.

1. Follow Step 1: Download Splunk Enterprise Security to download Splunk Enterprise Security and place it on the deployer.
2. Start the installation process on the deployer. Install with the `./splunk install app <filename>` command or perform a REST call to start the installation from the server command line.
   For example:
   curl -k -u admin:password https://localhost:8089/services/apps/local -d filename="true" -d name="<file name and directory>" -d update="true" -v
3. On the deployer, use the Splunk software command line to run the following command:
   splunk search '| essinstall --deployment_type shc_deployer' -auth admin:password
4. Restart with ./splunk restart only if SSL is changed from disabled to enabled or vicecersa.
5. Use the deployer to deploy Enterprise Security to the cluster members. From the deployer, run this command:
   splunk apply shcluster-bundle

Use the following table to identify the optimal value for `ssl_enablement` during your installation:

SSL mode	Description
strict	Default mode Ensure that SSL is enabled in the `web.conf` configuration file to use this mode. Otherwise, the installer exists with an error.
auto	Enables SSL in the `etc/system/local/web.conf` configuration file.
ignore	Ignores whether SSL is enabled or disabled.

If you run the search command to install Enterprise Security in Splunk Web, you can review the progress of the installation as search results. If you run the search command from the command line, you can review the installation log in: `$SPLUNK_HOME/var/log/splunk/essinstaller2.log`.

Managing configuration changes in a search head cluster

Some system configuration changes must be deployed using the deployer.

1. Instead of making the changes on a search head cluster member, make the changes on a deployer.
2. Migrate the necessary files to the search head cluster deployer.
3. Deploy the updated configuration to the search head cluster.

Configuration changes that must be deployed using the deployer:

Configuration change	File modified
Enable or disable indexed real-time searches on the General Settings page.	`inputs.conf`
Modify the indexed real-time disk sync delay on the General Settings page.	`inputs.conf`

Most configuration changes that you make in a search head cluster replicate automatically to other search head cluster members. For example:

- Add, modify, and disable threat intelligence sources
- Add, modify, and disable asset and identity source lists
- Changes to the user interface
- Changes to searches

See How configuration changes propagate across the search head cluster in the *Distributed Search Manual*.

Migrate an existing search head to a search head cluster

An Enterprise Security standalone search head or search head pool member cannot be added to a search head cluster. To migrate ES configurations to a search head cluster:

1. Identify any custom configurations and modifications in the prior ES installation. Check to make sure there is no local copy of `ess_setup.conf` that could conflict with the default one when you deploy Enterprise Security to the cluster.
2. Implement a new search head cluster.
3. Deploy the latest version of Enterprise Security on the search head cluster.
4. Review and migrate the customized configurations to the search head cluster deployer for replication to the cluster members.
5. Shut down the old ES search head.

For more information, see the topic Migrate from a standalone search head to a search head cluster in the Splunk Enterprise *Distributed Search Manual*.

For assistance in planning a Splunk Enterprise Security deployment migration, contact Splunk Professional Services.

Back up and restore Splunk Enterprise Security in a search head cluster environment

Back up and restore a Splunk Enterprise Security search head cluster (SHC) environment with at least three SHC nodes. All of the nodes in the SHC must be running the same version of Splunk Enterprise Security. Restoring an SHC environment might be necessary in the event of a disaster.

Take regular backups from the SHC, so that you have a backup from a time when the environment is healthy. For example, you could automate taking backups every hour. Choose a frequency of backups based on recovery point objectives.

To check if your environment is healthy, you can use one of the following methods:

- CLI command: `./splunk show shcluster-status â  verbose`
- API: `/services/shcluster/status?advanced=1`

In the output, look for the following fields:

Field	Description
dynamic_captain	Whether the cluster has a dynamically elected captain.
stable_captain	Whether the cluster captain is in a stable state.
service_ready_flag	Whether the cluster has enough members to support replication factor.
splunk_version	Whether all members, including the cluster master, are running Splunk version 7.1.0.
out_of_sync	Whether all nodes are currently in-sync.

Back up a search head cluster environment

Back up an SHC environment by backing up the KV store, the deployer, and the SHC nodes. The backup procedure does not require shutting down the SHC cluster or any node in the cluster.

Back up the KV store

To back up the KV store, run the following command from the CLI from the SHC node with the most recent data:

```
splunk backup kvstore -auth "admin:<password>"
```

This command creates an archive file in the `$SPLUNK_HOME/var/lib/splunk/kvstorebackup` directory. For example, the file might be named `kvdump_example.tar.gz`.

Back up the deployer and search head cluster nodes

1. On the deployer, back up the files in the `$SPLUNK_HOME/etc/shcluster` directory.
2. On the SHC node with the most recent data, note the GUID from the `shclustering` stanza from the `$SPLUNK_HOME/etc/system/local/server.conf` file. This information is necessary during the restore process.
3. On the SHC node with the most recent data, back up the files in the `$SPLUNK_HOME/var/run/splunk/snapshot/$LATEST_TIME-$CHECKSUM.bundle` bundle.
4. Create a `tar.gz` file from these backups.

Restore from a backup of a search head cluster environment

You need the following information to restore from a backup:

- The GUID from the `server.conf` file from one of the SHC members from before you begin restoring.

  After your restore the cluster, the restored cluster will have the same GUID as the cluster that was backed up.
- A backup of the deployer.
- A backup of the SHC node with the most recent data.
- A backup of the KV store from the SHC node with the most recent data.

The restore procedure requires the SHC to be shut down, but not the KV store.

Restore the deployer

1. On the deployer, extract the deployer backup file to the `$SPLUNK_HOME/etc/shcluster` directory.
2. Apply the bundle with the following command:
   ```
   splunk apply shcluster-bundle
   ```

Restore the search head cluster nodes

Complete the following steps on each SHC node that you want to restore:

1. Run the following command to stop Splunk Enterprise Security:
   ```
   splunk stop
   ```
2. Create a temporary folder and name it `temp`.
3. Extract the SHC node backup file to the `temp` directory.
4. Move the `config.bundle` file from the `temp` directory to the `$SPLUNK_HOME/etc` directory.
5. Extract the `config.bundle` file to the `$SPLUNK_HOME/etc` directory.

Restore the KV store

1. On an SHC node, check the `$SPLUNK_HOME/var/lib/splunk/kvstorebackup` directory to make sure that the `kvdump_example.tar.gz` backup file that you want to use to restore is there. If it is not in that directory, manually copy your tar.gz file to that location. Note that the KV store backup file is not automatically replicated across each SHC member.
2. Ensure that Splunk Enterprise Security is installed. The `collections.conf` file is necessary to complete the restore.
3. Run the following command to restore the KV store:
   `splunk restore kvstore -archiveName kvdump_example.tar.gz`
4. Restore the snapshot bundle by extracting the backup tar file from the `$SPLUNK_HOME/var/run/splunk/snapshot` directory to the `$SPLUNK_HOME/etc` directory.
5. Repeat these steps on each SHC node that you want to restore. Restoring the KV store on one SHC node does not cause the KV store to automatically replicate across each SHC member.

Entries that are present in both the current KV store and in the backup are updated and replaced by the entry in the backup. Collections that are in the current KV store but not in the backup are preserved, but not necessarily the documents inside of the collection.

Complete restoring the search head cluster environment

Finish restoring Splunk Enterprise Security from backup in an SHC environment.

1. In the `$SPLUNK_HOME/etc/system/local/server.conf` file, locate the `shclustering` stanza.
2. Update the field ID in this stanza with the GUID copied from the `server.conf` file during backup.
3. Run the following command to restart Splunk:
   `splunk restart`

Restore incident review history from internal audit logs

In the event that the backup process was not established prior to a data loss event with the KVStore, some of the information pertaining to incident review history can still be recovered using internal logs, as dictated by index _audit retention settings.

```
earliest=-30d index=_audit sourcetype=incident_review | rex "@@\w+,(?<rule
_name>[^,]+),(?<status>[^,]*),(?<owner>[^,]*),(?<urgency>[^,]*),(?<comment>.*),(?<user>[^,]+),
(?<something>[^,]+)" | eval time=_time | table comment owner rule_id rule_name status time urgency user |
outputlookup append=t incident_review_lookup_REMOVE_FOR_SAFETY
```

Deploy add-ons to Splunk Enterprise Security

The Splunk Enterprise Security package includes a set of add-ons, and is compatible with others.

- The add-ons that include "SA-" or "DA-" in the name make up the Splunk Enterprise Security framework. You do not need to take any additional action to deploy or configure these add-ons, because their installation and setup is handled as part of the Splunk Enterprise Security installation process. Do not disable any add-ons that make up the Splunk Enterprise Security framework.
- The rest of the add-ons include "TA-" in the name and are technology-specific and provide the CIM-compliant knowledge necessary to incorporate that source data into Enterprise Security.

For more about how the different types of add-ons interact with Splunk Enterprise Security, see About the ES solution

architecture on the Splunk developer portal. Technology-specific add-ons are supported differently than the add-ons that make up the Splunk Enterprise Security framework. See Support for Splunk Enterprise Security and provided add-ons in the *Release Notes* manual.

See Splunk Enterprise distributed deployments in the Splunk Machine Learning Toolkit *User Guide* if you're interested in the distributed apply feature of MLTK.

How you deploy the technology add-ons depends on the architecture of your Splunk platform deployment.

Prerequisite

Install Splunk Enterprise Security on your search head or search head cluster. See Install Enterprise Security. When you install Splunk Enterprise Security in a distributed environment, the installer installs and enables the add-ons included in the Enterprise Security package on the search head or search head cluster.

Steps

1. Determine which add-ons to install on forwarders
2. Deploy add-ons to forwarders
3. Deploy add-ons to indexers

Determine which add-ons to install on forwarders

Determine which add-ons to install on forwarders and which type of forwarder configuration each add-on requires by reviewing the documentation for the add-ons. Download add-ons from Splunkbase. Install add-ons that collect data on forwarders.

Most add-ons include input settings for a specific data source. Review the inputs.conf included with an add-on and deploy the add-on to a forwarder as needed. Some add-ons need to be deployed on forwarders installed directly on the data source system. Other add-ons require heavy forwarders. See the documentation or README file for each add-on for specific instructions.

- For add-ons with web-based documentation, follow the links below to determine where it needs to be installed and configured.
- For add-ons that do not have web-based documentation, see the README file included in the root folder of the add-on.

Deploy add-ons to forwarders

See Install an add-on in a distributed Splunk Enterprise deployment in the Splunk Add-ons documentation.

Technology-specific add-ons provided with Enterprise Security

Splunk Enterprise Security includes the technology add-on for UBA. See About the Splunk Add-on for Splunk UBA.

Deploy add-ons to indexers

Splunk recommends installing Splunk-supported add-ons across your entire Splunk platform deployment, then enabling and configuring inputs only where they are required. For more information, see Where to install Splunk add-ons in the Splunk Add-ons documentation.

The procedure that you use to deploy add-ons to your indexer can depend on your Splunk platform deployment. Select the option that matches your situation or preference.

Deployment situation	Procedure
Splunk Enterprise Security is running on Splunk Cloud Platform.	Contact Splunk Support and ask them to install the required add-ons to your indexers.
You prefer to deploy add-ons to the indexers manually.	See Install an add-on in a distributed Splunk Enterprise deployment.
Your indexers are clustered, you use the cluster master to deploy add-ons to cluster peers of your on-premises Splunk platform installation, and there is no additional deployment complexity.	Create the Splunk_TA_ForIndexers and manage deployment manually
Your indexers are not clustered, you use the deployment server to automatically manage indexer settings of your on-premises Splunk platform installation, and there is no additional deployment complexity.	This automatic procedure is deprecated. See the Release Notes.
Splunk Enterprise Security is running on a complex deployment, such as one Enterprise Security search head and one search head for other searches both using the same set of indexers.	Contact Splunk Professional Services for assistance with deploying add-ons to your indexers.

Create the Splunk_TA_ForIndexers and manage deployment manually

Use this procedure only if Splunk Enterprise Security is running on Splunk Enterprise rather than Splunk Cloud Platform, indexers are clustered, and there is no additional deployment complexity. If this does not match your deployment situation, see Deploy required add-ons to indexers to select a different deployment method.

Distributed Configuration Management collects the index-time configurations and basic index definitions into the Splunk_TA_ForIndexers package to simplify the deployment of add-on configurations to on-premises indexers. The Splunk_TA_ForIndexers includes all indexes.conf and index-time props.conf and transforms.conf settings from all enabled apps and add-ons on the search head, merges them into single indexes.conf, props.conf, and transforms.conf files, and places the files into one add-on for download. It works similar to a `./splunk cmd btool <conf_file_prefix> list` output.

This procedure deploys all add-ons that are enabled on your search head to your indexers. If you want to limit which add-ons you deploy to your indexers to only the subset that are strictly required to be on indexers, select Apps > Manage Apps and disable all add-ons that are not required on indexers before you begin this procedure, then re-enable them after you finish the procedure.

Before you deploy Splunk_TA_ForIndexers, make sure that existing add-ons installed on indexers are not included in the Splunk_TA_ForIndexers package. Deploying the same add-on twice might lead to configuration conflicts, especially if the add-ons are different versions.

1. On the Enterprise Security menu bar, select **Configure > General > General Settings**.
2. Scroll to **Distributed Configuration Management**, and click **Download Splunk_TA_ForIndexers** .
3. Select the contents for the package. You must select at least one of the following options to download the package.
    1. (Optional) Select the check box for **Include index time properties** to include the props.conf and transforms.conf files in the package.
    2. (Optional) Select the check box for **Include index definitions** to include the indexes.conf file in the package.
4. Click **Download the Package** to create and download the Splunk_TA_ForIndexers.

5. After the add-on downloads, you can modify the contents of the package.
   For example, modify indexes.conf to conform with site retention settings and other storage options.
6. Use the cluster master to deploy the Splunk_TA_ForIndexers or add-ons to the cluster peers. See Manage common configurations across all peers and Manage app deployment across all peers in *Managing Indexers and Clusters of Indexers*.

When you install a new add-on to use with Enterprise Security, repeat these steps to create an updated version of Splunk_TA_ForIndexers.

Integrate Splunk Stream with Splunk Enterprise Security

Enterprise Security integrates with Splunk Stream to capture and analyze network traffic data. Splunk Stream includes an app (splunk_app_stream) that you install on a search head and two forwarding options.

1. Install the Splunk App for Stream on the Enterprise Security search head.
   - For a Splunk Enterprise deployment, see Splunk Stream on-premise deployment architecture in the Splunk Stream *Installation and Configuration Manual*.
   - For a Splunk Cloud Platform deployment, see Splunk Stream for Cloud deployment architecture in the Splunk Stream *Installation and Configuration Manual*.
2. Activate the configuration template for Splunk Enterprise Security on the Splunk Stream forwarder that you use. You can use the Splunk Add-on for Stream (Splunk_TA_stream) or the independent Stream forwarder. See Use Stream configuration templates.

Use Stream in Enterprise Security

After setting up Splunk Stream, you can start a Stream capture job as a result of a correlation search. See Start a stream capture with Splunk Stream in *Administer Splunk Enterprise Security*. You can also start a stream capture job from a notable event on the Incident Review dashboard. See Start a Stream capture in *Use Splunk Enterprise Security*.

You can view and analyze Stream data events captured in Splunk Enterprise Security on the Protocol Intelligence dashboards. See Protocol Intelligence dashboards in '*Use Splunk Enterprise Security*.

Configure and deploy indexes

Splunk Enterprise Security implements custom indexes for event storage. The indexes are defined across the apps provided with Splunk Enterprise Security.

- In a single instance deployment, the installation of Enterprise Security creates the indexes in the default path for data storage.
- In a Splunk Cloud Platform deployment, customers work with Splunk Support to set up, manage, and maintain their cloud index parameters. See Manage Splunk Cloud Platform indexes in the *Splunk Cloud Platform Admin Manual*.
- In a distributed deployment, create the indexes on all Splunk platform indexers or search peers.

Index configuration

The indexes defined in Splunk Enterprise Security do not provide configuration settings to address:

- Multiple storage paths
- Accelerated data models
- Data retention
- Bucket sizing
- Use of volume parameters.

For detailed examples of configuring indexes, see indexes.conf.example in the Splunk Enterprise *Admin Manual*.

Indexes by app

You might see additional or fewer indexes, depending on your capabilities and which apps you have installed. The following are non-system indexes.

App context	Index	Description
DA-ESS-AccessProtection	`gia_summary`	Summary index used by the Geographically Improbable Access panel on the Access Anomalies dashboard.
DA-ESS-ThreatIntelligence	`ioc`	Unused in this release.
	`threat_activity`	Contains events that result from a threat list match.
SA-AuditAndDataProtection	`audit_summary`	Audit and Data Protection summary index.
SA-EndpointProtection	`endpoint_summary`	Endpoint protection summary index.
SA-NetworkProtection	`whois`	WHOIS data index.
SA-ThreatIntelligence	`notable`	Contains the notable events.
	`notable_summary`	Contains a stats summary of notable events used on select dashboards.
	`risk`	Contains the risk modifier events.
Splunk_DA-ESS_PCICompliance	`pci`	If PCI is installed, contains the PCI event data.
	`pci_posture_summary`	If PCI is installed, contains the PCI compliance status history.
	`pci_summary`	If PCI is installed, contains the PCI summary data.
Splunk_SA_CIM	`cim_summary`	Unused in this release.
	`cim_modactions`	Contains the adaptive response action events.
Splunk_TA_ueba	`ubaroute`	Does not contain event data. Used behind the scenes for routing to your UBA target.
	`ueba`	Contains UBA events.
SplunkEnterpriseSecuritySuite	`sequenced_events`	Contains sequenced event data, after the successful termination of a sequence template.

Add-ons can include custom indexes defined in an `indexes.conf` file. See About managing indexes in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

Index deployment

Splunk Enterprise Security includes a tool to gather the `indexes.conf` and index-time `props.conf` and `transforms.conf` settings from all enabled apps and add-ons on the search head and assemble them into one add-on. For more details, see Deploy add-ons included with Splunk Enterprise Security in this manual.

Configure users and roles

Splunk Enterprise Security uses the access control system integrated with the Splunk platform. The Splunk platform authorization allows you to add users, assign users to **roles**, and assign those roles custom **capabilities** to provide granular, role-based access control for your organization.

Splunk Enterprise Security relies on the admin user to run saved searches. If you plan to delete the admin user, update knowledge objects owned by that user before you do.

- For Splunk Enterprise, see Reassign one or more shared knowledge objects to a new owner in the *Knowledge Manager Manual*.
- For Splunk Cloud Platform, see Reassign one or more shared knowledge objects to a new owner in the *Knowledge Manager Manual*.

There are scenarios where it is still possible for an authenticated user to interact with certain core resources outside the control of the ES app, which can result in a lack of auditability. Make sure that all users with access to the ES app are trusted users that should have access to your ES related data, such as notable events and investigations.

Configuring user roles

Splunk Enterprise Security adds three roles to the default roles provided by Splunk platform. The new roles allow a Splunk administrator to assign access to specific functions in ES based on a user's access requirements. The Splunk platform administrator can assign groups of users to the roles that best fit the tasks the users will perform and manage in Splunk Enterprise Security. There are three categories of users.

User	Description	Splunk ES role
Security Director	Seeks to understand the current security posture of the organization by reviewing primarily the Security Posture, Protection Centers, and Audit dashboards. A security director does not configure the product or manage incidents.	`ess_user`
Security Analyst	Uses the Security Posture and Incident Review dashboards to manage and investigate security incidents. Security Analysts are also responsible for reviewing the Protection Centers and providing direction on what constitutes a security incident. They also define the thresholds used by correlation searches and dashboards. A Security Analyst must be able to edit notable events.	`ess_analyst`
Solution Administrator	Installs and maintains Splunk platform installations and Splunk Apps. This user is responsible for configuring workflows, adding new data sources, and tuning and troubleshooting the application.	`admin` or `sc_admin`

Each Splunk Enterprise Security custom role inherits from Splunk platform roles and adds capabilities specific to Splunk ES. Not all of the three roles custom to Splunk ES can be assigned to users.

Splunk ES role	Inherits from Splunk platform role	Added Splunk ES capabilities	Can be assigned to users
`ess_user`	user	Real-time search, list search head clustering, edit Splunk eventtypes in the Threat Intelligence supporting add-on, manage notable event suppressions.	Yes. Replaces the `user` role for ES users.
`ess_analyst`	user, ess_user, power	Inherits `ess_user` and adds the capabilities to create, edit, and own notable events and perform all transitions,	Yes. Replaces the `power` role for ES users.

Splunk ES role	Inherits from Splunk platform role	Added Splunk ES capabilities	Can be assigned to users
		and create and modify investigations.	
ess_admin	user, ess_user, power, ess_analyst	Inherits ess_analyst and adds several other capabilities.	**No**. You must use a Splunk platform admin role to administer an Enterprise Security installation.

See the capabilities specific to Splunk Enterprise Security for more details about which capabilities are assigned to which roles by default.

The Splunk platform admin role inherits all unique ES capabilities. In a Splunk Cloud Platform deployment, the Splunk platform admin role is named sc_admin. Use the admin or sc_admin role to administer an Enterprise Security installation.

Splunk platform role	Inherits from role	Added capabilities	Accepts user assignment
admin	user, ess_user, power, ess_analyst, ess_admin	All	Yes.
sc_admin	user, ess_user, power, ess_analyst, ess_admin	All	Yes.

ES expects that a user with the name and role of admin exists. If ES is installed on an on-premises Splunk Enterprise instance where the admin user's name is changed during the initial installation, then the scheduled searches included with ES are orphaned, disabled, and an error message prompts you to reassign them.

Role inheritance

All role inheritance is preconfigured in Enterprise Security. If the capabilities of any role are changed, other inheriting roles will receive the changes. For more information about roles, see the Splunk platform documentation.

- For Splunk Enterprise, see Add and edit roles in *Securing Splunk Enterprise*.
- For Splunk Cloud Platform, see Manage Splunk Cloud Platform roles in *Splunk Cloud Platform Admin Manual*.

Add capabilities to a role

Capabilities control the level of access that roles have to various features in Splunk Enterprise Security. Use the **Permissions** page in Enterprise Security to review and change the capabilities assigned to a role.

1. On the Splunk Enterprise Security menu bar, select **Configure > General > Permissions**.
2. Find the role you want to update.
3. Find the **ES Component** you want to add.
4. Select the check box for the component for the role.
5. Save.

Capabilities specific to Splunk Enterprise Security

Splunk Enterprise Security uses custom capabilities to control access to Splunk Enterprise Security-specific features. However, if you see list_inputs, this is a base capability that should not be removed.

Add capabilities on the permissions page in Splunk Enterprise Security to make sure that the proper access control lists (ACLs) are updated. The permissions page makes the ACL changes for you. If you add these custom capabilities on the Splunk platform settings page, you must update the ACLs yourself.

Capabilities are defined in the authorize.conf configuration file for Enterprise Security.

Function in ES	Description	Capability	ess_user	ess_analyst	ess_admin
Access data from Splunk UBA	Access data from Splunk Enterprise to Splunk UBA. See Set up the Splunk add-on for Splunk UBA in Splunk Enterprise Security.	edit_uba_settings			X
Adaptive Response Relay and associated KVStore collection	Write the Common Action Model (CAM) queue. See Set up an Adaptive Response Relay in Splunk Enterprise Security.	edit_cam_queue			X
Configuration checks	Allows you to run configuration checks.	edit_modinput_configuration_check			X
Create new notable events	Create ad-hoc notable events from search results. See Manually create a notable event in Splunk Enterprise Security.	edit_notable_events		X	X
Credential Manager	Manage credentials and certificates for Splunk Enterprise Security and other apps. Cannot be set on the Permissions page. See Manage credentials in Splunk Enterprise Security.	admin_all_objects list_storage_passwords list_app_certs edit_app_certs delete_app_certs			X
Data migrations	Allows you to perform one-time data migrations.	edit_modinput_data_migrator			X
Edit the Data Model Acceleration (DMA) modular input	Identify who can edit the Data Model Acceleration modular input. DMA is turned on for the required data models using a modular input by default.	edit_modinput_dm_accel_settings			X
Edit specific modinputs	Make changes to edit the modular name by using the "whois" feature.	edit_modinput_whois			X
Edit advanced search schedule settings	Edit the schedule priority and schedule window of correlation searches on Content Management.	edit_search_schedule_priority edit_search_schedule_window			X
Edit correlation searches	Edit correlation searches on Content Management. See Configure correlation searches in Splunk Enterprise Security. Users with this capability can also export content from Content Management as an app. See Export content as an	edit_correlationsearches schedule_search			X

Function in ES	Description	Capability	ess_user	ess_analyst	ess_admin
	app from Splunk Enterprise Security.				
Edit Distributed Configuration Management	Use distributed configuration management. See Deploy add-ons included with Splunk Enterprise Security.	edit_modinput_es_deployment_manager			X
Edit ES navigation	Make changes to the Enterprise Security navigation. See Customize the menu bar in Splunk Enterprise Security.	edit_es_navigation			X
Edit identity lookup configuration	Manage Asset and Identity lookup configurations. See Add asset and identity data to Splunk Enterprise Security, Enable asset and identity correlation in Splunk Enterprise Security, and Manage assets and identities in Splunk Enterprise Security.	edit_modinput_identity_manager			X
Edit Incident Review	Make changes to Incident Review settings. See Customize Incident Review in Splunk Enterprise Security.	edit_log_review_settings			X
Edit lookups	Create and make changes to lookup table files. See Create and manage lookups in Splunk Enterprise Security.	edit_lookups, edit_managed_configurations			X
Edit statuses	Make changes to the statuses available to select for investigations and notable events. See Manage notable event statuses.	edit_reviewstatuses			X
Edit notable event suppressions	Edit Splunk eventtypes in the Threat Intelligence supporting add-on, and create and edit notable event suppressions. See Create and manage notable event suppressions. The `ess_user` and `ess_analyst` roles don't have the default ability to edit suppressions through Splunk Web. However, they have the ability to perform read and write operations on eventtypes, so they can edit suppressions through the event types interface.	edit_suppressions			X

Function in ES	Description	Capability	ess_user	ess_analyst	ess_admin
Edit notable events	Make changes to notable events, such as assigning them and transition them between statuses. Statuses for Splunk ES investigations are stored in the reviewstatuses.conf file. See Triage notable events on Incident Review in Splunk Enterprise Security.	edit_notable_events		X	X
Edit per-panel filters	Permits the role to update per-panel filters on dashboards. See Configure per-panel filtering in Splunk Enterprise Security.	edit_per_panel_filters			X
Edit app permissions manager	Allows you to edit app permissions manager. Required for essinstall.	edit_modinput_app_permissions_manager			X
Edit intelligence downloads	Change intelligence download settings. See Download a threat intelligence feed from the Internet in Splunk Enterprise Security and Download an intelligence feed from the Internet in Splunk Enterprise Security.	edit_modinput_threatlist edit_modinput_threat_intelligence_manager			X
Edit threat intelligence collections	Upload threat intelligence and perform CRUD operations on threat intelligence collections using the REST API. See Upload a custom CSV file of threat intelligence in Splunk Enterprise Security and Threat Intelligence API reference.	edit_threat_intel_collections			X
Import content	Allows you to import content from installed applications.	edit_modinput_ess_content_importer			X
Migrate correlation searches	(Internal) Used by the background script to migrate correlation searches.	migrate_correlationsearches			X
Manage configurations	Make changes to the general settings or the list of editable lookups. See Configure general settings for Splunk Enterprise Security.	edit_managed_configurations			X
Manage all investigations	Allows the role to view and make changes to all investigations. See Manage security investigations in Splunk Enterprise Security.	manage_all_investigations			X
Manage Sequence	Allows the role to make changes to Sequence	edit_sequence_templates			X

Function in ES	Description	Capability	ess_user	ess_analyst	ess_admin
Templates	Templates, Sequence Template REST handlers, and related web pages. See Manage sequence templates in Splunk Enterprise Security.				
Manage analytics stories	Allows the role to make changes to analytics stories. See Manage analytics stories in Splunk Enterprise Security	edit_analyticstories		X	X
Manage your investigations	Create and edit investigations. Roles with this capability can make changes to investigations on which they are a collaborator. See Investigations in Splunk Enterprise Security.	edit_timeline		X	X
Own notable events	Allows the role to be an owner of notable events. See Assign notable events.	can_own_notable_events		X	X
Search-driven lookups	Create lookup tables that can be populated by a search. See Create search-driven lookups in Splunk Enterprise Security.	edit_managed_configurations schedule_search			X
Update app imports	Allows you to update app imports with all apps matching a given regular expression.	edit_modinput_app_imports_update			X

Adjust the concurrent searches for a role

Splunk platform defines a limit on concurrently running searches for the `user` and `power` roles by default. You may want to change those concurrent searches for some roles.

1. On the Splunk Enterprise Security menu bar, select **Configure > General > General Settings**.
2. Review the limits for roles and change them as desired.

Item	Description
Search Disk Quota (admin)	The maximum disk space (MB) a user with the admin role can use to store search job results.
Search Jobs Quota (admin)	The maximum number of concurrent searches for users with the admin role.
Search Jobs Quota (power)	The maximum number of concurrent searches for users with the power role.

To change the limits for roles other then `admin` and `power`, edit the `authorize.conf` file to update the default search quota. See the authorize.conf.example in the Splunk Enterprise *Admin* manual.

Configure the roles to search multiple indexes

The Splunk platform stores ingested data sources in multiple indexes. Distributing data into multiple indexes allows you to use role-based access control and vary retention policies for data sources. The Splunk platform configures all roles to

search only the `main` index by default. For more information about working with roles, see the Splunk platform documentation.

- For Splunk Enterprise, see About configuring role-based user access in the *Securing Splunk Enterprise* manual.
- For Splunk Cloud Platform, see Manage Splunk Cloud Platform users and roles in the *Splunk Cloud Platform Admin Manual*.

To allow roles in Splunk Enterprise Security to search additional indexes, assign the indexes that contain relevant security data to the relevant roles.

1. Select **Settings > Access Controls**.
2. Click **Roles**.
3. Click the role name that you want to allow to search additional indexes.
4. Select the desired **Indexes searched by default** and **Indexes** that this role can search. Do not include summary indexes, as this can cause a search and summary index loop.
5. Save your changes.
6. Repeat for additional roles as needed.

If you do not update the roles with the correct indexes, searches and other knowledge objects that rely on data from unassigned indexes will not update or display results.

For more information on the reasons for multiple indexes, see Why have multiple indexes? in Splunk Enterprise *Managing Indexers and Clusters of Indexers*.

Configure permissions for Machine Learning Toolkit SPL commands

No new capabilities are added to ES for using MLTK. To restrict permissions for MLTK SPL commands, see Change permissions in default.meta.conf in the Splunk Machine Learning Toolkit *User Guide*.

Configure data models for Splunk Enterprise Security

Splunk Enterprise Security leverages **data model acceleration** to populate dashboards and views and provide correlation search results. The data models are defined and provided in the Common Information Model add-on (Splunk_SA_CIM), which is included in the Splunk Enterprise Security installation. Enterprise Security also installs unique data models that only apply to Splunk Enterprise Security content.

Data model acceleration search load

A data model is accelerated through a scheduled summarization search process initiated on the search head. The summarization search runs on the indexers, searching newly indexed data while using the data model as a filter. The resulting matches are saved to disk alongside the index bucket for quick access.

On Splunk platform 6.3 and later, up to two simultaneous summarization searches can run per data model, per indexer. For more information, see Parallel summarization in the Splunk Enterprise *Capacity Planning Manual*. To adjust parallel summarization settings on Splunk Cloud Platform, file a support ticket.

Constrain data model searches to specific indexes

The Splunk Common Information Add-on allows you to constrain the indexes searched by a data model for improved performance. See Set up the Splunk Common Information Model Add-on in the Splunk Common Information Model

Add-on *User* manual.

Configure data model acceleration for CIM data models

The Splunk Common Information Add-on allows you to adjust your data model acceleration settings for each data model, including the backfill time, maximum concurrent searches, manual rebuilds, and scheduling priority. If you are using Splunk platform version 6.6.0, configure the tags whitelist setting to include any custom tags you use with CIM data models. See Accelerate CIM data models in the Splunk Common Information Model Add-on *User* manual.

Data model acceleration storage and retention

Data model acceleration uses the indexers for processing and storage, placing the accelerated data alongside each index. To calculate the additional storage needed on the indexers based on the total volume of data, use the formula:

Accelerated data model storage/year = Data volume per day * 3.4

This formula assumes that you are using the recommended retention rates for the accelerated data models.

For example, if you process 100GB/day of data volume for use with Enterprise Security, you need approximately 340GB of additional space available across all of the indexers to allow for up to one year of data model acceleration and source data retention.

Configuring storage volumes

By default, data model acceleration summaries reside in a predefined volume titled `_splunk_summaries` at the following path: `$SPLUNK_DB/<index_name>/datamodel_summary/<bucket_id>/<search_head_or_pool_id>/DM_<datamodel_app>_<datamodel_name>` . Data model acceleration storage volumes are managed in `indexes.conf` using the `tstatsHomePath` parameter. When configuring new storage volumes, the data model acceleration storage path defaults to the Splunk platform default index path of `$SPLUNK_HOME/var/lib/splunk` unless explicitly configured otherwise. The storage used for data model acceleration is not added to index sizing calculations for maintenance tasks such as bucket rolling and free space checks.

To manage the data model acceleration storage independently of index settings, you must define a new storage path with `[volume:]` stanzas. For an example of defining a volume and storing data model accelerations, see the Splunk platform documentation.

- For Splunk Enterprise, see Configure size-based retention for data models summaries in the Splunk Enterprise *Knowledge Manager Manual*.
- For Splunk Cloud Platform, see Configure size-based retention for data models summaries in the Splunk Cloud Platform *Knowledge Manager Manual*.

Data model default retention

The data model retention settings are contingent on the use case and data sources. A shorter retention uses less disk space and requires less processing time to maintain in exchange for limiting the time range of accelerated data.

Data Model	Summary Range
Alerts	All Time
Application State	1 month

Data Model	Summary Range
Authentication	1 year
Certificates	1 year
Change	1 year
Change Analysis	1 year
Compute Inventory	All Time
DLP (Data Loss Prevention)	1 year
Databases	All Time
Domain Analysis **(ES)**	1 year
Email	1 year
Endpoint	1 month
Identity Management	All Time
Incident Management **(ES)**	0
Interprocess Messaging	1 year
Intrusion Detection	1 year
Inventory	None
JVM (Java Virtual Machines)	All Time
Malware	1 year
Network Resolution (DNS)	3 months
Network Sessions	3 months
Network Traffic	3 months
Performance	1 month
Risk	All Time
Splunk Audit Logs	1 year
Splunk_CIM_Validation	All Time
Threat Intelligence **(ES)**	All Time
Ticket Management	1 year
Updates	1 year
Vulnerabilities	1 year
Web	3 months

You can use the following search to verify the current values:

```
| rest splunk_server=local count=0 /services/data/models | table title,acceleration.earliest_time
```

Use the **CIM Setup** page in the Splunk Common Information Model app to modify the retention setting for CIM data models. For more information, see Change the summary range for data model accelerations in the Splunk Common Information Model Add-on *User* manual. To change the summary range or other settings on a custom data model,

manually edit the `datamodels.conf` provided with the app or add-on.

- For instructions on how to edit these settings in Splunk Enterprise, see the datamodels.conf spec file in the Splunk Enterprise *Admin Manual*.
- If you are using Splunk Cloud Platform, file a support case to adjust these settings.

Data model acceleration rebuild behavior

In the Splunk platform, if the configuration of the data model structure changes, or the underlying search that creates the data model changes, a complete rebuild of the data model acceleration will initiate. Enterprise Security modifies the default behavior by applying data model configuration changes to the latest accelerations only, and prevents the removal of the prior accelerations. The indexers retain all existing accelerated data models with the prior configuration until the defined retention period is reached, or rolled with the index buckets. For best performance, do not change the manual rebuilds setting for any data models used by Splunk Enterprise Security.

- The rebuild configuration options are managed in the `datamodels.conf` file.

For more information about acceleration and rebuild behavior, see the Splunk platform documentation.

- For Splunk Enterprise, see Advanced configurations for persistently accelerated data models in the Splunk Enterprise *Knowledge Manager Manual*.
- For Splunk Cloud Platform, see Advanced configurations for persistently accelerated data models in the Splunk Cloud Platform *Knowledge Manager Manual*.

- Use the **Data Models management** page to force a full rebuild. Navigate to **Settings > Data Models**, select a data model, use the left arrow to expand the row, and select the **Rebuild** link.

- To review the acceleration status for all data models, use the Data Model Audit dashboard.

Data model acceleration enforcement

Enterprise Security enforces data model acceleration through a modular input. To disable acceleration for a data model in ES:

1. On the Splunk Enterprise toolbar, open **Settings > Data inputs** and select **Data Model Acceleration Enforcement Settings**.
2. Select a data model.
3. Uncheck the **Acceleration Enforced** option.
4. Save.

Data models used by Splunk Enterprise Security

For reference information about the data models used by Splunk Enterprise Security, see Data models used by ES in the Splunk developer portal.

Upgrading

Planning an upgrade of Splunk Enterprise Security

Plan an on-premises Splunk Enterprise Security upgrade. Splunk Cloud Platform customers must work with Splunk Support to coordinate upgrades to Enterprise Security.

Upgrade Splunk Enterprise to the selected version and then upgrade Enterprise Security to the selected version. If you are upgrading Splunk Enterprise and Enterprise Security at the same time, you don't have to do stepped upgrades.

Stepped upgrades are only necessary if you stop at different core upgrades along the way. For example, if you are upgrading from Splunk Enterprise 6.3 to Splunk Enterprise 7.3.4, you would not upgrade all the way to Enterprise Security to 6.4.1 because it is not supported on Splunk Enterprise 7.3.4. However, if you are upgrading from Splunk Enterprise 6.3 to Splunk Enterprise 8.1.3, then you can upgrade upgrade Enterprise Security all the way to 6.4.1.

Before you upgrade Splunk Enterprise Security

1. Review the compatible versions of the Splunk platform. See Splunk Enterprise system requirements.
2. Review the hardware requirements to make sure that your server hardware supports Splunk Enterprise Security. See Hardware requirements.
3. Review known issues with the latest release of Splunk Enterprise Security. See Known Issues in the Splunk Enterprise Security *Release Notes*.
4. Review deprecated features in the latest release of Splunk Enterprise Security. See Deprecated features in the Splunk Enterprise Security *Release Notes*.
5. Back up the search head, including the KV Store. The upgrade process does not back up the existing installation before upgrading. See Back up KV Store for instructions on how to back up the KV Store on the search head.
6. Approximately 1 GB of free space is required in the `/tmp/` directory for the upgrade to complete. When upgrading an app through either the CLI or Splunk Web UI, the `/tmp/` directory is utilized during the process.

Recommendations for upgrading Splunk Enterprise Security

Upgrade both the Splunk platform and Splunk Enterprise Security in the same maintenance window. See the Splunk Enterprise system requirements to verify which versions of Splunk Enterprise Security and Splunk Enterprise are supported with each other.

1. Upgrade Splunk Enterprise to a compatible version. See Upgrade your distributed Splunk Enterprise environment in the *Splunk Enterprise Installation Manual*.
2. Upgrade Splunk platform instances.
3. Upgrade Splunk Enterprise Security.
4. Review, upgrade, and deploy add-ons.
5. See the post-installation Version-specific upgrade notes.

Upgrading Enterprise Security deployed on a search head cluster is a multi-step process. The recommended procedure is detailed in Upgrade Enterprise Security on a search head cluster.

Upgrade-specific notes

- The upgrade will fail if a deployment server manages apps or add-ons included in the Enterprise Security package. Before starting the upgrade, remove the `deploymentclient.conf` file containing references to the

deployment server and restart Splunk services.
- The upgrade inherits any configuration changes and files saved in the app `/local` and `/lookups` paths.
- The upgrade maintains local changes to the menu navigation.
- After the upgrade, configuration changes inherited through the upgrade process might affect or override new settings. Use the ES Configuration Health dashboard to review configuration settings that might conflict with new configurations. See ES Configuration Health in the *User Manual*.
- The upgrade process is logged in `$SPLUNK_HOME/var/log/splunk/essinstaller2.log`
- Splunk Web might not start if you have AdvancedXML module folders from pre-4.0.x versions of Enterprise Security. Manually remove these files. For example, remove `$SPLUNK_HOME/etc/apps/SA-Utils/appserver/modules/SOLNLookupEditor`.

Upgrade notes for add-ons included with Splunk Enterprise Security:

- The upgrade process overwrites all prior or existing versions of apps and add-ons.
- The upgrade does not overwrite a newer version of an app or add-on installed in your environment.
- An app or add-on that was disabled in the previous version will remain disabled after the upgrade.
- The upgrade disables deprecated apps or add-ons. The deprecated app or add-on must be manually removed from the Enterprise Security installation. After the upgrade, an alert displays in Messages to identify all deprecated items.

Changes to add-ons

For a list of add-ons included with this release of Enterprise Security, see Technology-specific add-ons provided with Enterprise Security.

Upgrading distributed add-ons

Splunk Enterprise Security includes the latest versions of the included add-ons that existed when this version was released.

A copy of the latest add-ons are included with Splunk Enterprise Security. When upgrading Enterprise Security, review all add-ons and deploy the updated add-ons to indexers and forwarders as required. The Enterprise Security installation process does not automatically upgrade or migrate any configurations deployed to the indexers or forwarders. See Deploy add-ons included with Splunk Enterprise Security.

> You must migrate any customizations made to the prior versions of an add-on manually.

Upgrade Splunk Enterprise Security

This topic describes how to upgrade Splunk Enterprise Security on an on-premises search head from version 6.0.2 and higher or 6.1.1 and higher. Splunk Cloud Platform customers work with Splunk Support to coordinate upgrades to Enterprise Security.

Step 1. Review the planning topic

1. For an overview of the upgrade process and prerequisites, see Planning an upgrade in this manual.
2. Perform a full backup of the search head, including the KV Store, before upgrading. The upgrade process does not back up the existing installation before upgrading. See Back up KV Store for instructions on how to back up the KV Store on the search head.

To back out of the upgrade, you must restore the prior version of Splunk Enterprise Security from backup.

Step 2. Download Splunk Enterprise Security

1. Open splunk.com and log in with your Splunk.com ID. You must be a licensed Enterprise Security customer to download the product.
2. Download the latest Splunk Enterprise Security product.
3. Choose **Download** and save the Splunk Enterprise Security product file to your desktop.
4. Log in to the Enterprise Security search head as an administrator.

Step 3. Install the latest Splunk Enterprise Security

The installer dynamically detects if you're installing in a single search head environment or search head cluster environment. The installer is also bigger than the default upload limit for Splunk Web.

1. Increase the Splunk Web upload limit to 1 GB by creating a file called `$SPLUNK_HOME/etc/system/local/web.conf` with the following stanza.
   [settings]
   max_upload_size = 1024
2. To restart Splunk from the Splunk toolbar, select **Settings > Server controls** and click **Restart Splunk**.
3. On the Splunk Enterprise search page, select **Apps > Manage Apps** and choose **Install App from File**.
4. Select the Splunk Enterprise Security product file.
5. Click **Choose File** and select the Splunk Enterprise Security product file.
6. Click **Upgrade app** to overwrite the existing Splunk Enterprise Security installation.
7. Click **Upload** to begin the installation.
8. When prompted, configure Splunk Enterprise Security.
9. Click **Restart Splunk**.

If you do not run the setup procedure promptly after the file upload completes, Enterprise Security displays errors.

Step 4. Set up Splunk Enterprise Security

After Splunk Web returns after the restart, set up Splunk Enterprise Security.

1. Click **Continue to app setup page** to start the ES setup.
2. Click **Start**.
3. The **Splunk Enterprise Security Post-Install Configuration** page indicates the upgrade status as it moves through the stages of installation.

When the setup is complete, the page may prompt you to restart Splunk Platform services if you opted to enable SSL before the setup.

1. Click **Restart Splunk** to finish the installation.

For Enterprise Security version 6.4.1, you may see an error on the dashboard if you do not restart Splunk and navigate to the Incident Review page or the Investigation Dashboard.

Step 5. Validate the upgrade

The Splunk Enterprise Security upgrade process is now complete. Objects disabled during the upgrade process will automatically be enabled.

1. On the Enterprise Security menu bar, select **Audit > ES Configuration Health**.
2. Review potential conflicts and changes to the default settings. See ES Configuration Health in the *User Manual*.
3. Clear the browser cache of the browser you use to access Splunk Web to make sure that you access a fresh version of Splunk Web after upgrading. If you do not clear the browser cache, some pages might fail to load.

Splunk logs the upgrade in `$SPLUNKHOME$/var/log/splunk/essinstaller2.log`

Version-specific upgrade notes

Things to do after upgrading to specific versions of Enterprise Security.

After upgrading to version 6.6.0

When you upgrade the Splunk Enterprise Security app to versions 6.6.0 or higher, you will no longer have support for Glass Tables. Do not upgrade to ES 6.6.0 or higher if you need to continue using Glass Tables. For more information on this deprecated feature, see Deprecated features.

Additionally, if "Incident Review - Table Attributes" is changed before upgrading to ES 6.6.0, the Incident Review page does not display fields such as **Disposition**. As a workaround, check if the "table_attributes" in the `/etc/apps/SA-ThreatIntelligence/local/log_review.conf` configuration file exists. If the "table_attributes" in the `/etc/apps/SA-ThreatIntelligence/local/log_review.conf` configuration file exists, remove the "table_attributes" and revert to the default configuration values for ES 6.6.0. Manually add the following default fields to the "table attributes". For more information, see Change Incident Review Columns.

> You can customize the configuration file later, if required.

```
table_attributes = [\
{"field": "rule_title", "label": "Title"}
,\
{"field": "risk_object", "label": "Risk Object"}
,\
{"field": "risk_score", "label": "Aggregated Risk Score"}
,\
{"field": "risk_event_count", "label": "Risk Events"}
,\
{"field": "notable_type", "label": "Type"}
,\
{"field": "_time", "label": "Time"}
,\
{"field": "disposition_label", "label": "Disposition"}
,\
{"field": "security_domain", "label": "Security Domain"}
,\
{"field": "urgency", "label": "Urgency"}
,\
{"field": "status_label", "label": "Status"}
,\
{"field": "owner_realname", "label": "Owner"}
```

\
]

After upgrading to version 6.4.1

When you upgrade the Splunk Enterprise Security app to versions 6.0 or higher, you might see the issues mentioned in After upgrading to version 6.0. For complete details, see Manage asset and identity upon upgrade.

Upgrading to Enterprise Security 6.4.1 or higher does not allow you to remove existing fields using the Risk Factors Editor but only allows you to add fields to the risk data model. This prevents the mismatch between the default and local configuration of the risk data model. For more information on upgrade issues with the risk data model, see After upgrading from version 6.2.0 or lower to a version 6.3.0 or higher

After upgrading to version 6.4

When you upgrade the Splunk Enterprise Security app to versions 6.0 or higher, you might see the issues mentioned in After upgrading to version 6.0. For complete details, see Manage asset and identity upon upgrade.

Upgrading the Splunk Enterprise Security app to versions 6.4.0 or higher may cause the following issues:

- Threat intelligence manager is no longer available from the Splunk Enterprise menu bar at **Configure > Settings > Data inputs > Threat Intelligence Manager**.
- Threat intelligence uploads are no longer available from the Enterprise Security menu bar at **Configure > Data Enrichment > Threat Intelligence Uploads**.
- Health check warnings appear.

See Manage UI issues impacting threat intelligence after upgrading Splunk Enterprise Security. in the *Administer Splunk Enterprise Security* manual.

When you upgrade to Enterprise Security 6.4.0, notable actions for some correlation searches are disabled. If you want these correlation searches to generate notables, you must re-enable the notable actions for the correlation searches, see Enable notables for correlation searches in the *Administer Splunk Enterprise Security* manual.

When you upgrade to Enterprise Security 6.4.0 or higher, ensure that the email conventions that the identity lookups use to create a common unique key between different identity sources are configured as required. Note that only the **Email** convention is enabled by default. If you use the **Email Short** convention, make sure that the checkbox for **Email Short** is selected, otherwise you may lose data related to the **Email Short** convention during an upgrade. For more information on adding an identity input stanza for the lookup source, see Add an identity input stanza for the lookup source.

After upgrading to version 6.3

When you upgrade the Splunk Enterprise Security app to versions 6.0 or higher, you might see the issues mentioned in After upgrading to version 6.0. For complete details, see Manage asset and identity upon upgrade in the *Administer Splunk Enterprise Security* manual.

MLTK app version 5.2.0 is included in the ES installer. The previously generated models from MLTK 5.0 are compatible as-is. The previously generated models MLTK 4.x are not compatible and have to be regenerated. See Machine Learning Toolkit Overview in Splunk Enterprise Security for general information about models in MLTK 5.2.0.

After upgrading to version 6.2

When you upgrade the Splunk Enterprise Security app to versions 6.0 or higher, you might see the issues mentioned in After upgrading to version 6.0. For complete details, see Manage asset and identity upon upgrade.

After upgrading to Enterprise Security 6.2.0, you need to enable **Enforce props** in the Global Settings of Asset and Identity Management 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 ES 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. See Revise the enforcements used by the identity manager framework.

After upgrading to version 6.1.0

When you upgrade the Splunk Enterprise Security app to versions 6.0 or higher, you might see the issues mentioned in After upgrading to version 6.0. For complete details, see Manage asset and identity upon upgrade.

MLTK app version 5 is now included in the ES installer. The previously generated models from MLTK 4.x are not compatible and have to be regenerated. See Machine Learning Toolkit Overview in Splunk Enterprise Security for general information about models in MLTK 5. See Update Splunk MLTK models for Python 3 in the Splunk Enterprise *Python 3 Migration* manual for information about rebuilding models.

After upgrading to version 6.0

When you upgrade the Splunk Enterprise Security app to versions 6.0 or higher, you might see the following issues in Assets and Identities:

- The Asset and Identity Management navigation bar and page does not display if you have customized the menu bar in Splunk Enterprise Security. See Restore the default navigation or Recover the new view of Assets and Identities Navigation page.
- The Asset and Identity page merges the data for your assets and identities after the upgrade. For more information on how to avoid merged rows to display, see Avoid merged assets and identities data.
- The asset and identity collections, search previews, and search results may display differently from before the upgrade. To restore the previous view that you had prior to the upgrade, see Recover the new view of Assets and Identities Navigation page.
- The Asset and Identity page does not enable access to some of your previously saved macros. You may no longer be able to access saved macros if they were not documented for public use.

For complete details, see Manage asset and identity upon upgrade.

After upgrading to version 5.3.x

If you followed the default behavior and installed the technology add-ons that shipped with Enterprise Security in previous versions, after upgrading to version 5.3.x you will notice messages that state, "TA-<name> version <number> is lower than required." This is expected behavior with the recent installer enhancements. After upgrading, do one of the following:

- Update the technology add-ons manually. See Deploy add-ons included with Splunk Enterprise Security.
- Disable the modular input that manages these messages by going to **Settings > Data Inputs > Configuration Checker**, and disabling the **confcheck_es_app_version** input.

After upgrading to version 5.1.x

Manually delete the file `$SPLUNK_HOME/etc/apps/splunk_instrumentation/default/data/ui/views/search.xml`. After deleting the file, do one of the following:

- Refresh Splunk Web: `http(s)://yoursplunkurl.com:8000/en-US/debug/refresh?entity=data/ui/views`
- Refresh `splunkd`: `http(s)://yoursplunkurl.com:8089/services/data/ui/views/_reload`

After upgrading to version 5.0.x

- Select the **Edit Lookups** permission checkbox again. Because the **Edit Lookups** permission now includes an additional capability, the permission is not checked by default. Roles still have the **edit_lookups** capability. See Configure users and roles in the *Installation and Upgrade Manual*
- Enable the **Access - Geographically Improbable Access - Summary Gen** search to see data on the **Geographically Improbable Access** panel of the **Access Anomalies** dashboard or notable events produced by the **Geographically Improbable Access Detected** correlation search.

After upgrading from a version prior to 4.1.x

- Correlation search editor configurations might be inconsistent with pre-upgrade settings if the search migration process is still running. Search the internal index to look for successfully migrated searches and review the status of the migration operation.

```
index=_internal sourcetype=configuration_check file="confcheck_es_modactions*" migrated
```

- Enabled correlation searches that are not configured to create notable events revert to creating notable events. For example, a correlation search that by default created a notable event and a risk modifier that you configured to create only a risk modifier will, after upgrade, create both a risk modifier and a notable event.

    1. Before upgrading, note enabled correlation searches that do not create notable events using the following search.

    ```
    | rest splunk_server=local count=0 /services/saved/searches search="name=\"*-Rule\"" | where disabled=0 AND 'action.summary_index'=0 | table 'eai:acl.app',title
    ```

    2. After the upgrade is complete, update the affected correlation searches so that the searches no longer create notable events.

After upgrading from version 6.2.0 or lower to a version 6.3.0 or higher

Modifying risk factors using the Risk Factor Editor automatically creates corresponding field entries in the risk datamodel `Risk.json`. However, upgrading from enterprise Security version 6.2.0 or lower to a version 6.3.0 or higher may cause a mismatch if there is a discrepancy in the field entries of the local and the default configuration files of the risk data model and result in an error. Upgrading to Enterprise Security 6.4.1 or higher does not allow you to remove existing fields but only allows you to add fields to the risk data model. This prevents the mismatch between the local and the default configuration of the risk data model.

Test upgrade and setup of Splunk Enterprise Security

You can test the upgrade and setup of Splunk Enterprise Security before you perform the full upgrade. You must complete Step 1. Review the planning topic, Step 2. Download Splunk Enterprise Security, and the first two sub-steps of Step 3. Install the latest Splunk Enterprise Security before you can follow these steps.

1. From Splunk Web, open the Search and Reporting app.

2. Type the following search to perform a dry run of the upgrade and setup.

```
|essinstall --dry-run
```

Upgrade Splunk Enterprise Security in a search head cluster environment

Splunk Enterprise Security supports installation on Linux-based search head clusters (SHC) only. At this time, Windows search head clusters are not supported by Splunk Enterprise Security.

Upgrading Enterprise Security in a search head cluster environment

The installer dynamically detects if you're upgrading in a single search head environment or search head cluster environment. The installer is also bigger than the default upload limit for Splunk Web.

To upgrade Enterprise Security on a search head cluster deployer:

1. Prepare the deployer. See Prerequisites for installing Enterprise Security in a search head cluster environment.
2. Verify that you have the same version of Enterprise Security on the deployer and SHC nodes.
3. Increase the Splunk Web upload limit to 1GB by creating a file called `$SPLUNK_HOME/etc/system/local/web.conf` with the following stanza.
   [settings]
   max_upload_size = 1024
4. To restart Splunk from the Splunk toolbar, select **Settings > Server controls** and click **Restart Splunk**.
5. Install Enterprise Security on the deployer (this method is via the UI).
    1. On the Splunk toolbar, select **Apps > Manage Apps** and click **Install App from File**.
    2. Click **Choose File** and select the Splunk Enterprise Security product file.
    3. Check the checkbox for **Upgrade App**.
    4. Click **Upload**.
6. Click **Restart Now**.
7. Click the **Enterprise Security** app.
8. Click **Continue to app setup page**.

   Note the message that Enterprise Security is being installed on the deployer of a search head cluster environment and that technology add-ons will not be installed as part of the post-install configuration.
9. Click **Start Configuration Process**.

Deploy the changes to the cluster members

As of 7.3.0, Splunk Enterprise has four deployer modes for pushing application configuration changes to search head cluster members.

The previous behavior for pushing the app bundle from the deployer to the members was to merge the `$SPLUNK_HOME/shcluster/apps/<appname>/default` and `$SPLUNK_HOME/shcluster/apps/<appname>/local` folders of the deployer to overwrite the `$SPLUNK_HOME/etc/apps/<appname>/default` folder of each SHC member.

Although that merge behavior is still available as one of the configuration options, the default behavior is to duplicate `$SPLUNK_HOME/shcluster/apps/<appname>/default` along with `$SPLUNK_HOME/shcluster/apps/<appname>/local` on the SHC members. See the "Mode_merge_to_default" section of the Choose a deployer push mode in the Splunk Enterprise *Distributed Search Manual*.

In addition, lookups were previously preserved for all apps or for no apps. As of Splunk Enterprise 7.3.0, you're able to select the specific apps where you want to preserve lookups. See Preserve lookup files across app upgrades in the Splunk Enterprise *Distributed Search Manual*.

Splunk Enterprise 7.3.0 is not a requirement for upgrading, but you need Splunk Enterprise 7.3.0 or later if you want to take advantage of the deployer modes and the per-app lookup preservation.

To deploy the app to cluster members for Splunk Enterprise Security:

1. Choose a deployer push mode, such as `full` to configure system wide for the first time or `merge_to_default` to configure on a per-app basis. See the Choose a deployer push mode in the Splunk Enterprise *Distributed Search Manual*.
2. Use the deployer to deploy Enterprise Security to the cluster members. From the deployer, run this command: `splunk apply shcluster-bundle`

As of Enterprise Security 6.2.0, the default for the deployer's apply shcluster-bundle `-preserve-lookups` option is `true` to retain lookup file content generated on the search head cluster members. The `[shclustering]` stanza is now also included in the app.conf file of each bundled domain add-on (DA) and supporting add-on (SA) in Splunk Enterprise Security. The `-preserve-lookups true` argument, combined with `deployer_lookups_push_mode` in the app's app.conf file indicates how csv lookup files in the app are deployed. See shclustering in the Splunk Enterprise *Admin Manual*.

If you do not want to retain the lookup file content on cluster members for a particular app, you can comment out `deployer_lookups_push_mode` of `always_preserve` in the `[shclustering]` stanza of `$SPLUNK_HOME/shcluster/apps/<appname>/local` and it persists as your local setting from now on.

Validate the configuration on the search cluster

After you distribute the copy of Enterprise Security on the deployer to the search head cluster members, use the ES Configuration Health dashboard to compare the cluster-replicated knowledge objects to the latest installation of Enterprise Security.

1. Log in to Splunk Web on a search head cluster member.
2. Open Enterprise Security.
3. From the Enterprise Security menu bar, select **Audit > ES Configuration Health**.
4. Review potential conflicts and changes to the default settings.

See ES Configuration Health in *Use Splunk Enterprise Security*.