Splunk® Enterprise Installation Manual 7.1.0

How to upgrade Splunk Enterprise

Generated: 5/21/2018 3:54 am

How to upgrade Splunk Enterprise

Upgrading a single Splunk Enterprise instance is straightforward. In many cases, you upgrade the software by installing the latest package over your existing installation. When you upgrade on Windows systems, the installer package detects the version that you have previously installed and offers to upgrade it for you.

Splunk Enterprise must be upgraded with a user account that has administrative privileges and that can write to the instance directory and all of its subdirectories.

What's new and awesome in 7.1?

See Welcome to Splunk Enterprise 7.1 in the Release Notes for a full list of the new features that are available in 7.1.

See Known issues in the Release Notes for a list of issues and workarounds in this release.

Back up your existing deployment

Always back up your existing Splunk Enterprise deployment before you perform any upgrade or migration.

You can manage upgrade risk by using technology that lets you restore your Splunk Enterprise installation and data to a state prior to the upgrade, whether that is external backups, disk or file system snapshots, or other means. When backing up your Splunk Enterprise data, consider the $SPLUNK_HOME directory and any indexes outside of it.

For more information about backing up your Splunk Enterprise deployment, see Back up configuration information in the *Admin Manual* and Back up indexed data in *Managing Indexers and Clusters of Indexers*.

Choose the proper upgrade procedure based on your environment

The way that you upgrade Splunk Enterprise differs based on whether you have a single Splunk Enterprise instance or multiple instances connected together. The differences are significant if you have configured a cluster of instances.

Upgrade distributed environments

If you want to upgrade a distributed Splunk Enterprise environment, including environments that have one or more **search head pools**, see How to upgrade a distributed Splunk Enterprise environment.

Upgrade clustered environments

There are special requirements for upgrading an indexer cluster or a search head cluster. The following topics have upgrade instructions that supersede the instructions in this manual:

- To upgrade an indexer cluster, see Upgrade an indexer cluster in the *Managing Indexers and Clusters of Indexers*.
- To upgrade a search head cluster, see Upgrade a search head cluster in *Distributed Search*.

Important upgrade information and changes

See About upgrading to 7.1: READ THIS FIRST for migration tips and information that might affect you when you upgrade.

Upgrade from 6.5 and later

Splunk supports a direct upgrade from versions 6.5 and later of Splunk Enterprise to version 7.1:

- Upgrade to 7.1 on *nix
- Upgrade to 7.1 on Windows

Upgrade from 6.4 and earlier

Splunk does not support directly upgrading from version 6.4 and earlier of Splunk Enterprise to version 7.1.

Upgrade from versions 6.0, 6.1, 6.2, 6.3, and 6.4

If you run versions 6.0, 6.1, 6.2, 6.3, or 6.4 of Splunk Enterprise, upgrade to version 6.5 first before attempting an upgrade to version 7.1.

Upgrade from version 5.0

If you run versions 5.0 of Splunk Enterprise, upgrade to version 6.5 first before attempting an upgrade to version 7.1.

Get and install the "no-enforcement" license

A Splunk license that does not block search after a license has been in violation is available.

This license is standard on all new installations of Splunk Enterprise. If you want to use this license type after an upgrade, you must get and install it on your Splunk Enterprise instance separately. Your instance must run Splunk Enterprise 6.5.0 or later. If you have a distributed deployment, the Splunk Enterprise instance that acts as your license master must run 6.5.0 or later. You do not need to upgrade the rest of your deployment to 6.5.0 for a no-enforcement license to work. You must have a contract in good standing with Splunk to take advantage of this new license type.

For additional information about the new license, see Types of Splunk software licenses in the *Admin Manual*.

Enable the new license behavior:

1. Upgrade your Splunk Enterprise environment (single instance or license master, at minimum) to 6.5.0 or later.
2. Contact your sales representative, who can confirm your details and, along with Splunk Support, issue you a no-enforcement license key.
3. Apply the key to your Splunk Enterprise instance or, in the case of a distributed deployment, your license master instance.
4. Restart Splunk Enterprise on the individual host or license master for the new license to take effect.

Upgrade universal forwarders

Upgrading universal forwarders is a different process than upgrading Splunk Enterprise. Before upgrading your universal forwarders, see the appropriate upgrade topic in the *Universal Forwarder Manual* for your operating system:

- Upgrade the Windows universal forwarder
- Upgrade the universal forwarder for *nix systems

To learn about interoperability and compatibility between indexers and forwarders, see Compatibility between forwarders and indexers in *Forwarding Data*.

Replace lost package manifest files

Splunk installation packages have manifest files that Splunk software needs to run. The manifest files exist in the root of the Splunk installation and end in `-manifest`. If the files are not present (for example, if you have deleted them) then Splunk software cannot run as it cannot verify that it is a valid installation.

If you delete those files in the process of upgrading, or for any reason, you can restore them with the following procedure:

1. Download an identical copy of the Splunk installer that you downloaded previously. This copy must be the same version and architecture, as manifest files are specific to each version.
2. Extract the files to a directory that is not your existing Splunk installation.
3. Copy the files from this directory to the root directory of your Splunk installation.
4. Start Splunk Enterprise and confirm that it starts normally.