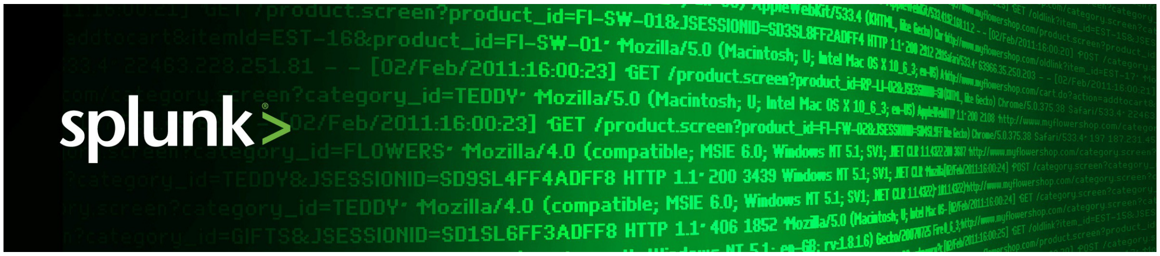


Splunk® Enterprise Installation Manual 7.2.4

Generated: 2/07/2019 3:34 pm

Table of Contents

Welcome to the Splunk Enterprise Installation Manual....................................1

What's in this manual..1

Plan your Splunk Enterprise installation..2

Installation overview..2

System requirements for use of Splunk Enterprise on-premises................4

Splunk Enterprise architecture and processes..13

Information on Windows third-party binaries distributed with Splunk Enterprise..16

Installation instructions..18

Secure your Splunk Enterprise installation..20

About securing Splunk Enterprise..20

Secure your system before you install Splunk Enterprise.........................20

Install Splunk Enterprise securely..20

More ways to secure Splunk Enterprise..22

Install Splunk Enterprise on Windows..24

Choose the Windows user Splunk Enterprise should run as....................24

Prepare your Windows network to run Splunk Enterprise as a network or domain user..27

Install on Windows..37

Install on Windows using the command line..43

Change the user selected during Windows installation............................55

Install Splunk Enterprise on Linux or Mac OS X...56

Install on Linux..56

Install on Mac OS X..59

Run Splunk Enterprise as a different or non-root user.............................62

Install Splunk Enterprise in virtual and containerized environments..........65

Deploy and run Splunk Enterprise inside a Docker container...................65

Start using Splunk Enterprise..67

Start Splunk Enterprise for the first time..67

What happens next?..72

Learn about accessibility to Splunk Enterprise...73

Table of Contents

Install a Splunk Enterprise license..75

About Splunk Enterprise licenses..75

Install a license..75

Upgrade or migrate Splunk Enterprise...77

How to upgrade Splunk Enterprise...77

About upgrading to 7.2 READ THIS FIRST...80

How to upgrade a distributed Splunk Enterprise environment..................93

Changes for Splunk App developers...99

Upgrade to 7.2 on UNIX..99

Upgrade to 7.2 on Windows...101

Migrate a Splunk Enterprise instance from one physical machine to another...103

Uninstall Splunk Enterprise..108

Uninstall Splunk Enterprise..108

Reference...111

PGP Public Key...111

Welcome to the Splunk Enterprise Installation Manual

What's in this manual

The *Installation Manual* provides the information that you need to install Splunk Enterprise.

- System requirements
- Licensing information
- Procedures for installing
- Procedures for upgrading from a previous version

Install the universal forwarder

To install the Splunk **universal forwarder**, see Install the universal forwarder software in the *Universal Forwarder* manual. The universal forwarder is a separate executable with its own set of installation procedures. For an introduction to forwarders, see About forwarding and receiving in the *Forwarding Data* manual.

Plan your Splunk Enterprise installation

Installation overview

Installing Splunk Enterprise on a host is the first step in realizing value from your data. Read this topic and the contents of this chapter before you begin an installation.

There are two ways you can install Splunk Enterprise:

- Download and install a Splunk Enterprise installation package
- Download the Splunk Enterprise Docker image and run Splunk Enterprise inside a Docker container

Containerized Splunk Enterprise provides a simplified and consistent way for you to quickly get started with Splunk Enterprise and gain hands-on experience with the software. While Splunk Enterprise Docker containers are portable across different environments and allow for complex and scalable deployments, in this release, Splunk only supports the standalone and single-server Splunk topology for container-based deployments. For information about Docker, see the Docker documentation.

Install Splunk Enterprise by using an installation package

1. See the system requirements for installation. Additional requirements for installation might apply based on the operating system on which you install Splunk Enterprise and how you use Splunk Enterprise.
2. (Optional) See Components of a Splunk Enterprise deployment to learn about the Splunk Enterprise ecosystem, and Splunk architecture and processes to learn what the installer puts on your machine.
3. See Secure your Splunk Enterprise installation and, where appropriate, secure the machine on which you will install Splunk Enterprise.
4. Download the installation package for your system from the Splunk Enterprise download page.
5. Perform the installation by using the installation instructions for your operating system. See Installation instructions.
6. (Optional) If this is the first time you have installed Splunk Enterprise, see the *Search Tutorial* to learn how to index data into Splunk software and search that data using the Splunk Enterprise search language.
7. (Optional) After you install Splunk Enterprise, calculate the amount of space your data takes up. See Estimate your storage requirements in the

Capacity Planning Manual.

8. To run Splunk Enterprise in a production environment and to understand how much hardware such an environment requires, see the *Capacity Planning Manual*.

Deploy and run Splunk Enterprise inside Docker containers

1. Confirm that your system meets the following requirements for container-based installation:
    1. See the Containerized computing platforms section in Supported Operating Systems for supported operating systems.
    2. Confirm that your system meets or exceeds the recommended hardware requirements. See Recommended hardware.
    3. Confirm that any disk volumes that you use to store Splunk Enterprise data inside a Docker container use one of the supported file systems. See Supported file systems.
2. See Secure your Splunk Enterprise installation and, where appropriate, secure the machine on which you want to install Splunk Enterprise.
3. Download and install Docker Enterprise or Community Edition Engine 17.06.2 or higher for your operating system.
4. Perform the installation. See Deploy and run Splunk Enterprise Docker containers for step-by-step installation instructions.
5. (Optional) Estimate the amount of space your Splunk Enterprise data will take up. See Estimate your storage requirements in the *Capacity Planning Manual*.
6. Create and mount volumes to the containers for storing data that Splunk Enterprise uses and generates, such as indexed data and configuration files.
   For instructions on configuring storage for data persistence, see Data Storage on Splunk Github.
7. To run Splunk Enterprise in a production environment and to understand how much hardware such an environment requires, see the *Capacity Planning Manual*.

Upgrade or migrate a Splunk Enterprise instance

In many cases, you can upgrade Splunk Enterprise over an existing version.

- To upgrade from an earlier version of Splunk Enterprise, see How to upgrade Splunk Enterprise in this manual for information and specific instructions.
- For information on migrating from one version to another, see the About upgrading - READ THIS FIRST topic for the version that you want to

upgrade to.
- To move a Splunk Enterprise instance from one host to another, see Migrate a Splunk instance.

System requirements for use of Splunk Enterprise on-premises

Splunk supports using Splunk Enterprise on several computing environments. Learn about the supported environments before you download the software.

The universal forwarder has its own set of hardware requirements. See Universal forwarder system requirements in the *Universal Forwarder* manual.

If you have ideas or requests for new features and you have a current Splunk contract, open a request with Splunk Support.

Supported Operating Systems

The following tables list the available computing platforms for Splunk Enterprise. The first table lists availability for *nix operating systems and the second lists availability for Windows operating systems.

Each table shows available computing platforms (operating system and architecture) and types of Splunk software. A bold **X** in a box that intersects the computing platform and Splunk software type you want means that Splunk software is available for that platform and type.

An empty box means that Splunk software is not available for that platform and type.

If you do not see the operating system or architecture that you are looking for in the list, the software is not available for that platform or architecture. This might mean that Splunk has ended support for that platform. See the list of deprecated and removed computing platforms in Deprecated Features in the *Release Notes*.

Some boxes contain characters other than a check mark. See the bottom of each table to learn what the characters mean and how it could impact your installation.

Confirm support for your computing platform

1. Find the operating system on which you want to install Splunk Enterprise in the **Operating system** column.
2. Find the computing architecture in the **Architecture** column that matches your environment.
3. Find the type of Splunk software that you want to use: Splunk Enterprise, Splunk Free, Splunk Trial, or Splunk Universal Forwarder.
4. If Splunk software is available for the computing platform and software type that you want, proceed to the download page to get it.

Unix operating systems

Operating system	Architecture	Enterprise	Free	Trial	Universal Forwarder
Solaris 10 and 11	x86 (64-bit)				**X**
	SPARC				**X**
Linux, all 2.6 kernel versions	x86 (64-bit)	D	D	D	D
Linux, all 3.x and 4.x kernel versions	x86 (64-bit)	**X**	**X**	**X**	**X**
PowerLinux, Little Endian kernel version 2.6 and higher (E)	PowerPC				**X**
zLinux, kernel version 2.6 and higher	s390x				**X**
FreeBSD 10 and 11	x86 (64-bit)				**X**
Mac OS X 10.11	Intel		D	D	D
macOS 10.12 and 10.13	Intel		**X**	**X**	**X**
AIX 7.1 and 7.2	PowerPC				**X**
ARM Linux	ARM				A

A: The software for this platform is available for download from splunk.com, but there is no official support for the platform.
D: Splunk supports this platform and architecture but might remove support in a future release. See Deprecated Features in the *Release Notes* for information on deprecation.
E: Support for PowerLinux on Big Endian kernels was removed.

Windows operating systems

The table lists the Windows computing platforms that Splunk Enterprise supports.

Operating system	Architecture	Enterprise	Free	Trial	Universal Forwarder
Windows Server 2008 R2 SP1	x86 (64-bit)				D
Windows Server 2012, Server 2012 R2, and Server 2016 (all installation options)	x86 (64-bit)	**X**	**X**	**X**	**X**
Windows 8.1	x86 (64-bit)		D	D	**X**
	x86 (32-bit)		D	D	**X**
Windows 10	x86 (64-bit)		**X**	**X**	**X**
	x86 (32-bit)		***	***	**X**

D: Splunk supports this platform and architecture but might remove support in a future release. See Deprecated Features in the *Release Notes* for information on deprecation.
*** Splunk supports but does not recommend using Splunk Enterprise on this platform and architecture.

Containerized computing platforms

Splunk offers official support for Splunk Enterprise and Universal Forwarder containers running in the following environments.

Operating system	Architecture	Container environment	Enterprise	Free	Trial	Universal Forwarder
Linux, 4.x kernel	x86 (64-bit)	Docker Enterprise or	**X**			**X**

Operating system	Architecture	Container environment	Enterprise	Free	Trial	Universal Forwarder
version		Community Edition 17.06.2 and higher				
zLinux, 4.x kernel version	s390x (64-bit)	Docker Enterprise or Community Edition 17.06.2 and higher				**X**

For container-based deployments of Splunk Enterprise and Universal Forwarder in environments that Splunk does not support, you can find support on Splunk Answers or through the open source community on GitHub for Splunk-Docker.

Splunk does not support Docker service-level or stack-level configurations such as swarm clusters or container orchestration. Consult Docker and Kubernetes documentation on how to build and manage Docker services.

Operating system notes

Windows

Some parts of Splunk Enterprise on Windows require elevated user permissions to function properly. See the following topics for information on the components that require elevated permissions and how to configure Splunk Enterprise on Windows:

- Splunk Enterprise architecture and processes
- Choose the Windows user Splunk Enterprise should run as
- Considerations for deciding how to monitor remote Windows data in *Getting Data In*

Operating systems that support the Monitoring Console

The Splunk Enterprise Monitoring Console works only on some versions of Linux and Windows. For information on supported platform architectures for the Monitoring Console, see Supported platforms in the *Troubleshooting Manual*. To learn about the other prerequisites for the Monitoring Console, see Monitoring Console setup prerequisites in *Monitoring Splunk Enterprise*.

Deprecated operating systems and features

As we update Splunk software, we sometimes deprecate and remove support of older operating systems. See Deprecated features in the Release Notes for information on which platforms and features have been deprecated or removed entirely.

Creating and editing configuration files on OSes that do not use UTF-8 character set encoding

Splunk software expects configuration files to be in ASCII or Universal Character Set Transformation Format-8-bit (UTF-8) format. If you edit or create a configuration file on an OS that does not use UTF-8 character set encoding, then ensure that the editor you use can save in ASCII or UTF-8.

IPv6 platform support

All Splunk-supported OS platforms can use IPv6 network configurations.

See Configure Splunk for IPv6 in the *Admin Manual* for details on IPv6 support in Splunk Enterprise.

Supported browsers

Splunk Enterprise supports the following browsers:

- Firefox (latest)
- Internet Explorer 11 (Splunk Enterprise does not support this browser in Compatibility Mode.)
- Safari (latest)
- Chrome (latest)

Recommended hardware

To evaluate Splunk Enterprise for a production deployment, use hardware that is typical of your production environment. This hardware should meet or exceed the recommended hardware capacity specifications.

For a discussion of hardware planning for production deployment, see Introduction to capacity planning for Splunk Enterprise in the *Capacity Planning* Manual.

Splunk Enterprise and virtual machines

If you run Splunk Enterprise in a virtual machine (VM) on any platform, performance decreases. This is because virtualization works by providing hardware abstraction on a machine into pools of resources. VMs that you define on the system draw from these resource pools. Splunk Enterprise needs sustained access to a number of resources, particularly disk I/O, for indexing operations. If you run Splunk Enterprise in a VM or alongside other VMs, indexing and search performance can degrade.

Splunk Enterprise and containerized infrastructures

Splunk officially supports deploying Splunk Enterprise inside Docker containers on the x86-64 architecture. For containerized deployments, your system must also meet or exceed the Recommended hardware capacity.

Docker images of Splunk Enterprise are also available at Docker Hub for developers to evaluate the deployment of Splunk on containerized infrastructures not covered by Splunk support. These Docker images are supported by the community. See https://hub.docker.com/r/splunk/splunk/.

For additional information related to Splunk Enterprise on containerized infrastructures, see Is Splunk supported on Kubernetes on the Splunk Answers site. Please post your questions and feedback for the Splunk product management team in the comments section of that post.

Recommended hardware capacity

The following requirements are accurate for a single instance installation with light to moderate use. For significant enterprise and distributed deployments, see the *Capacity Planning* Manual.

Platform	Recommended hardware capacity/configuration
Non-Windows platforms	2x six-core, 2+ GHz CPU, 12GB RAM, Redundant Array of Independent Disks (RAID) 0 or 1+0, with a 64 bit OS installed.
Windows platforms	2x six-core, 2+ GHz CPU, 12GB RAM, RAID 0 or 1+0, with a 64-bit OS installed.

RAID 0 disk configurations do not provide fault-tolerance. Confirm that a RAID 0 configuration meets your data reliability needs before deploying a Splunk Enterprise indexer on a system configured with RAID 0.

Maintain a minimum of 5GB of free hard disk space on any Splunk Enterprise instance, including forwarders, in addition to the space required for any indexes. See Estimate your storage requirements in *Capacity Planning* for a procedure on how to estimate the space you need. Failure to maintain this level of free space can degrade performance and cause operating system failure and data loss.

Hardware requirements for universal and light forwarders

The universal forwarder has its own set of hardware requirements. See Universal forwarder system requirements in the *Universal Forwarder* manual.

Supported file systems

If you run Splunk Enterprise on a file system that does not appear in this table, the software might run a startup utility named `locktest` to test the viability of the file system. If `locktest` fails, then the file system is not suitable for using with Splunk Enterprise.

Platform	File systems
Linux	ext3, ext4, btrfs, XFS, NFS 3/4
Solaris (universal forwarder only)	UFS, ZFS, VXFS, NFS 3/4
FreeBSD (universal forwarder only)	FFS, UFS, NFS 3/4, ZFS
Mac OS X	HFS, APFS, NFS 3/4
AIX	JFS, JFS2, NFS 3/4
Windows	NTFS, FAT32

Considerations regarding Network File System (NFS)

When you use Network File System (NFS) as a storage medium for Splunk indexing, consider all of the ramifications of file level storage.

Use block level storage rather than file level storage for indexing your data.

In environments with reliable, high-bandwidth, low-latency links, or with vendors that provide high-availability, clustered network storage, NFS can be an appropriate choice. However, customers who choose this strategy should work with their hardware vendor to confirm that their storage platform operates to the vendor specification in terms of both performance and data integrity.

If you use NFS, note the following:

- Do not use NFS to host hot or warm index **buckets**, because a failure in NFS can cause data loss. NFS works best with cold or frozen buckets.
- Do not use NFS to share cold or frozen index buckets amongst an indexer cluster, as this potentially creates a single point of failure.
- Splunk Enterprise does not support "soft" NFS mounts. These are mounts that cause a program attempting a file operation on the mount to report an error and continue in case of a failure.
- Only "hard" NFS mounts (mounts where the client continues to attempt to contact the server in case of a failure) are reliable with Splunk Enterprise.
- Do not disable attribute caching. If you have other applications that require disabling or reducing attribute caching, then you must provide Splunk Enterprise with a separate mount with attribute caching enabled.
- Do not use NFS mounts over a wide area network (WAN). Doing so causes performance issues and can lead to data loss.

*Considerations regarding system-wide resource limits on *nix systems*

Splunk Enterprise allocates system-wide resources like file descriptors and user processes on *nix systems for monitoring, forwarding, deploying, searching, and other things. The `ulimit` command controls access to these resources which must be set to acceptable levels for Splunk Enterprise to function properly on *nix systems.

The more tasks your Splunk Enterprise instance performs, the more resources it needs. You should increase the `ulimit` values if you start to see your instance run into problems with low resource limits. See I get errors about ulimit in splunkd.log in the *Troubleshooting Manual.*

The following table shows the system-wide resources that the software uses. It provides the minimum recommended settings for these resources for instances that are not forwarders, such as indexers, search heads, cluster masters, license masters, deployment servers, and Monitoring Consoles (MC).

System-wide Resource	ulimit invocation	Recommended min. value
Open files	`ulimit -n`	64000
User processes	`ulimit -u`	16000
Data segment size	`ulimit -d`	1073741824

On machines that run FreeBSD, you might need to increase the kernel parameters for default and maximum process stack size. The following table shows the parameters that must be present in `/boot/loader.conf` on the host.

System-wide Resource	Kernel parameter	Recommended value
Default process data size (soft limit)	`dfldsiz`	2147483648
Maximum process data size (hard limit)	`maxdsiz`	2147483648

On machines that run AIX, you might need to increase the systemwide resource limits for maximum file size (fsize) and resident memory size (rss). The following table shows the parameters that must be present in `/etc/security/limits` for the user that runs Splunk software.

System-wide Resource	ulimit invocation	Recommended value
Data segment size	`ulimit -d`	1073741824
Resident memory size	`ulimit -m`	536870912
Number of open files	`ulimit -n`	8192
File size limit	`ulimit -f`	`-1` (unlimited)

This consideration is not applicable to Windows-based systems.

Considerations regarding solid state disk drives

Solid state drives (SSDs) deliver significant performance gains over conventional hard drives for Splunk in "rare" searches - searches that request small sets of results over large swaths of data - when used in combination with bloom filters. They also deliver performance gains with concurrent searches overall.

Considerations regarding Common Internet File System (CIFS)/Server Message Block (SMB)

Splunk Enterprise supports the use of the CIFS/SMB protocol for the following purposes, on shares hosted by Windows hosts only:

- **Search head pooling** (Search head pooling is a deprecated feature.)
- Storage of cold or frozen **Index buckets**.

When you use a CIFS resource for storage, confirm that the resource has write permissions for the user that connects to the resource at both the file and share levels. If you use a third-party storage device, confirm that its implementation of CIFS is compatible with the implementation that your Splunk Enterprise instance runs as a client.

Do not index data to a mapped network drive on Windows (for example "`Y:\`" mapped to an external share.) Splunk Enterprise disables any index it encounters with a non-physical drive letter.

Considerations regarding environments that use the transparent huge pages memory management scheme

If you run Splunk Enterprise on a Unix machine that makes use of transparent huge memory pages, see Transparent huge memory pages and Splunk performance in the *Release Notes* before you attempt to install Splunk Enterprise.

This consideration is not applicable to Windows operating systems.

Further reading

See the Download Splunk Enterprise page to get the latest available version.

See the release notes for details on known and resolved issues in this release.

See Introduction to Capacity Planning for Splunk Enterprise in the *Capacity Planning* Manual for information on estimating capacity .

Splunk Enterprise architecture and processes

This topic discusses the internal architecture and processes of Splunk Enterprise at a high level. If you're looking for information about third-party components used in Splunk Enterprise, see the credits section in the Release notes.

Splunk Enterprise Processes

A Splunk Enterprise server installs a process on your host, `splunkd`.

`splunkd` is a distributed C/C++ server that accesses, processes and indexes streaming IT data. It also handles search requests. `splunkd` processes and indexes your data by streaming it through a series of pipelines, each made up of a series of processors.

- **Pipelines** are single threads inside the `splunkd` process, each configured with a single snippet of XML.

- **Processors** are individual, reusable C or C++ functions that act on the stream of IT data that passes through a pipeline. Pipelines can pass data to one another through **queues**.
- New for version 6.2, `splunkd` also provides the Splunk Web user interface. It lets users search and navigate data and manage Splunk Enterprise deployment through a Web interface. It communicates with your Web browser through REpresentational State Transfer (REST).
- `splunkd` runs a Web server on port 8089 with SSL/HTTPS turned on by default.
- It also runs a Web server on port 8000 with SSL/HTTPS turned off by default.

`splunkweb` installs as a legacy service on Windows only. Prior to version 6.2, it provided the Web interface for Splunk Enterprise. Now, it installs and runs, but quits immediately. You can configure it to run in "legacy mode" by changing a configuration parameter.

On Windows systems, `splunkweb.exe` is a third-party, open-source executable that Splunk renames from `pythonservice.exe`. Because it is a renamed file, it does not contain the same file version information as other Splunk Enterprise for Windows binaries.

Read information on other Windows third-party binaries that come with Splunk Enterprise.

Splunk Enterprise and Windows in Safe Mode

If Windows is in Safe Mode, Splunk services do not start. If you attempt to start Splunk Enterprise from the Start Menu while in Safe Mode, Splunk Enterprise does not alert you to the fact that its services are not running.

Additional processes for Splunk Enterprise on Windows

On Windows instances of Splunk Enterprise, in addition to the two services described, Splunk Enterprise uses additional processes when you create specific data inputs on a Splunk Enterprise instance. These inputs run when configured by certain types of Windows-specific data input.

splunk.exe

`splunk.exe` is the control application for the Windows version of Splunk Enterprise. It provides the command-line interface (CLI) for the program. It lets you start, stop, and configure Splunk Enterprise, similar to the *nix `splunk` program.

The `splunk.exe` binary requires an elevated context to run because of how it controls the `splunkd` and `splunkweb` processes. Splunk Enterprise might not function correctly if this program does not have the appropriate permissions on your Windows system. This is not an issue if you install Splunk Enterprise as the Local System user.

splunk-admon

`splunk-admon.exe` runs whenever you configure an Active Directory (AD) monitoring input. `splunkd` spawns `splunk-admon`, which attaches to the nearest available AD domain controller and gathers change events generated by AD. Splunk Enterprise stores these events in an index.

splunk-perfmon

`splunk-perfmon.exe` runs when you configure Splunk Enterprise to monitor performance data on the local Windows machine. This binary attaches to the Performance Data Helper libraries, which query the performance libraries on the system and extract performance metrics both instantaneously and over time.

splunk-netmon

`splunk-netmon` runs when you configure Splunk Enterprise to monitor Windows network information on the local machine.

splunk-regmon

`splunk-regmon.exe` runs when you configure a Registry monitoring input in Splunk. This input initially writes a baseline for the Registry in its current state (if requested), then monitors changes to the Registry over time.

splunk-winevtlog

You can use this utility to test defined event log collections, and it outputs events as they are collected for investigation. Splunk Enterprise has a Windows event log input processor built into the engine.

splunk-winhostmon

`splunk-winhostmon` runs when you configure a Windows host monitoring input in Splunk. This input gets detailed information about Windows hosts.

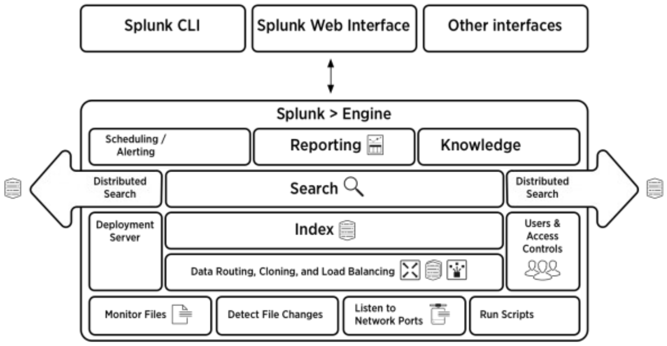
splunk-winprintmon

`splunk-winprintmon` runs when you configure a Windows print monitoring input in Splunk. This input gets detailed information about Windows printers and print jobs on the local system.

splunk-wmi

When you configure a performance monitoring, event log or other input against a remote computer, this program runs. Depending on how you configure the input, it either attempts to attach to and read Windows event logs as they come over the wire, or executes a Windows Query Language (WQL) query against the Windows Management Instrumentation (WMI) provider on the specified remote machine.

Architecture diagram



Information on Windows third-party binaries distributed with Splunk Enterprise

Learn about the third-party Windows binaries that come with the Splunk Enterprise and the Splunk universal forwarder packages.

For more information about the universal forwarder, see About forwarding and receiving data in the *Forwarding Data* Manual.

Third-party Windows binaries that ship with Splunk Enterprise

The following third-party Windows binaries ship with Splunk Enterprise. The Splunk Enterprise product includes these binaries, except where indicated.

The binaries provide functionality to Splunk Enterprise as shown in their individual descriptions. The binaries do not contain file version information or authenticode signatures (certificates that prove the binary file's authenticity). Additionally, Splunk Enterprise does not provide support for debug symbols related to third-party modules.

Binaries, apps, and scripts that do not ship with Splunk Enterprise have not been tested for Certified for Windows Server 2008 R2 (CFW2008R2) Windows Logo compliance.

Archive.dll

Libarchive.dll is a multi-format archive and compression library.

Both Splunk Enterprise and the Splunk universal forwarder include this binary.

Bzip2.exe

Bzip2 is a patent-free, high-quality data compressor. It typically compresses files to within 10% to 15% of the best available techniques (the prediction by partial matching (PPM) family of statistical compressors), while being about twice as fast at compression and six times faster at decompression.

Jsmin.exe

Jsmin.exe is an executable that removes white space and comments from JavaScript files, reducing their size.

Libexslt.dll

Libexslt.dll is the Extensions to Extensible Stylesheet Language Transformation (EXSLT) dynamic link C library developed for libxslt (a part of the GNU is Not Unix Network Object Model Environment (GNOME) project).

Both Splunk Enterprise and the Splunk universal forwarder include this binary.

Libxml2.dll

Libxml2.dll is the Extensible Markup Language (XML) C parser and toolkit library. This library was developed for the GNOME project but can be used outside of the GNOME platform.

Both Splunk Enterprise and the Splunk universal forwarder include this binary.

Libxslt.dll

Libxslt.dll is the XML Stylesheet Language for Transformations (XSLT) dynamic link C library developed for the GNOME project. XSLT itself is an XML language to define transformation for XML. Libxslt is based on libxml2, the XML C library developed for the GNOME project. It also implements most of the EXSLT set of processor-portable extensions functions and some of Saxon's evaluate and expressions extensions.

Both Splunk Enterprise and the Splunk universal forwarder include this binary.

Minigzip.exe

Minigzip.exe is the minimal implementation of the ?gzip? compression tool.

Openssl.exe

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and open source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library.

Both Splunk Enterprise and the Splunk universal forwarder include this binary.

Python.exe

Python.exe is the Python programming language binary for Windows.

Pythoncom.dll

Pythoncom.dll is a module that encapsulates the Object Linking and Embedding (OLE) automation API for Python.

Pywintypes27.dll

Pywintypes27.dll is a module that encapsulates Windows types for Python version 2.7.

Installation instructions

For detailed installation instructions for your operating system, choose one of the following.

- Windows
- Windows (from the command line)
- Linux

Full Splunk Enterprise is not available for macOS, but the trial and free versions are available.

- macOS

Splunk Enterprise availability has been removed for some operating systems

As of version 7.0.0, Splunk Enterprise is no longer available for the following operating system. To install and use Splunk Enterprise on this operating system, you must use a version prior to 7.0.0. The universal forwarder is available for installation on this platform.

- Solaris

The following operating systems have not had support for Splunk Enterprise since version 6.3.0. Universal forwarder instructions are available for the following platforms:

- FreeBSD
- AIX
- HP-UX

Secure your Splunk Enterprise installation

About securing Splunk Enterprise

When you set up and begin using your Splunk Enterprise installation or upgrade, perform some additional steps to ensure that Splunk Enterprise and your data are secure. Taking the proper steps to secure Splunk Enterprise reduces its attack surface and mitigates the risk and impact of most vulnerabilities.

This section highlights some of the ways that you can secure Splunk Enterprise before, during, and after installation. The *Securing Splunk Enterprise* manual provides more information about the ways you can secure Splunk Enterprise.

Secure your system before you install Splunk Enterprise

Before you install Splunk Enterprise, make your operating system secure. Harden all Splunk Enterprise server operating systems.

- If your organization does not have internal hardening standards, use the CIS hardening benchmarks.
- At a minimum, limit shell and command-line access to your Splunk Enterprise servers.
- Secure physical access to all Splunk Enterprise servers.
- Ensure that Splunk Enterprise end users practice physical and endpoint security.

Install Splunk Enterprise securely

Verify integrity and signatures for your Splunk Installation when you download and install Splunk Enterprise.

Verify Integrity

Verify your Splunk Enterprise download using hash functions such as Message Digest 5 (MD5) and Secure Hash Algorithm-512 (SHA-512) to compare the hashes. Use a trusted version of OpenSSL.

MD5

This procedure helps you compare the MD5 hash of the installation file you download from the Splunk website against the expected hash of the file. The tools you use to compare the files might be different based on the operating system that you run. You might need to download these tools before verifying the MD5 hash.

1. Download the installation package for the platform and version of Splunk software that you want.
2. On the "Thank you for downloading" page, click the link to the MD5 hash file for this package.
3. Open a shell prompt or Terminal window.
4. Print the contents of the MD5 hash file.

   ```
   cat splunk-x.x.x-xxxxxxxxxxxx-Linux-x86-64.tgz.md5
   MD5 (splunk-x.x.x-xxxxxxxxxxxx-Linux-x86_64.tgz) =
   c63c869754d420bb62f04f4096877481
   ```
5. Run the `md5` tool against the installer package.

   ```
   md5 splunk-x.x.x-xxxxxxxxxxxx-Linux-x86-64.tgz
   MD5 (splunk-x.x.x-xxxxxxxxxxxx-Linux-x86_64.tgz) =
   c63c869754d420bb62f04f4096877481
   ```
6. Compare the output of both commands.
7. If the hashes match, then you have confirmed that the installation package that you downloaded is the same as what is on the splunk.com website.

SHA512

1. Copy Link name of download

2. Append SHA512

3.
https://download.splunk.com/products/splunk/releases/6.4.3/windows/splunk-6.4.3-b03109c2bad4-

Verify Signatures

Verify the authenticity of the downloaded RPM package by using the Splunk GnuPG Public key.

1. Download the GnuPG Public key file. (This link is over Transport Layer Security (TLS).)

2. Install the key.

   ```
   rpm --import <filename>
   ```
3. Verify the package signature.

   ```
   rpm -K <filename>
   ```

More ways to secure Splunk Enterprise

After you install Splunk Enterprise, you have more options to secure your configuration.

Configure user authentication and role-based access control

Set up your users and use roles to control access. Splunk Enterprise lets you configure users in several ways. See the following information in *Securing Splunk Enterprise*.

- The built-in authentication system. See Set up user authentication with Splunk Enterprise native authentication.
- LDAP. See Set up user authentication with LDAP.
- A scripted authentication API for use with an external authentication system, such as Pluggable Authentication Modules (PAM) or Remote Access Dial-In User Server (RADIUS). See Set up user authentication with external systems.

After you configure users, you can assign roles in Splunk Enterprise that determine and control capabilities and access levels. See About role-based user access.

Use SSL certificates to configure encryption and authentication

Splunk Enterprise comes with a set of default certificates and keys that, when enabled, provide encryption and data compression. You can also use your own certificates and keys to secure communications between your browser and Splunk Web as well as data sent from forwarders to a **receiver**, such as an indexer.

See "About securing Splunk with SSL" in this manual.

Audit Splunk Enterprise

Splunk Enterprise includes audit features that let you track the reliability of your data.

- Monitor files and directories in *Getting Data In*
- Search for audit events in *Securing Splunk Enterprise*

Harden your Splunk Enterprise installation

See the following topics in *Securing Splunk Entrprise* to harden your installation.

- Deploy secure passwords across multiple servers
- Use Splunk Enterprise Access Control Lists
- Secure your service accounts
- Disable unnecessary Splunk Enterprise components
- Secure Splunk Enterprise on your network

Install Splunk Enterprise on Windows

Choose the Windows user Splunk Enterprise should run as

When you install Splunk Enterprise on Windows, the software lets you select the Windows user that it should run as.

The user you choose depends on what you want Splunk Enterprise to monitor

The user that Splunk Enterprise runs as determines what Splunk Enterprise can monitor. The Local System user has access to all data on the local machine by default, but nothing else. A user other than Local System has access to whatever data you want, but you must give the user that access before you install Splunk Enterprise.

About the Local System user and other user choices

The Windows Splunk Enterprise installer provides two ways to install it:

- As the Local System user
- As another existing user on your Windows computer or network, which you designate

To do any of the following actions with Splunk Enterprise, you must install it as a domain user:

- Read Event Logs remotely
- Collect performance counters remotely
- Read network shares for log files
- Access the Active Directory schema using Active Directory monitoring

The user that you specify must meet the following requirements. If the user does not satisfy these requirements, Splunk Enterprise installation might fail. Even if installation succeeds, Splunk Enterprise might not run correctly, or at all.

- Be a member of the Active Directory domain or forest that you want to monitor (when using AD)

- Be a member of the local Administrators group on the server on which you install Splunk Enterprise
- Be assigned specific user security rights

If you are not sure which user Splunk Enterprise should run as, then see Considerations for deciding how to monitor remote Windows data in the *Getting Data In* manual for information on how to configure the Splunk Enterprise user with the access it needs.

User accounts and password concerns

The user that you select to run Splunk Enterprise as also has unique password constraints.

If you have a password enforcement security policy on your Windows network, that policy controls the validity of any user passwords. If that policy enforces password changes, you must do one of the following to keep Splunk Enterprise services running:

- Before the password expires, change it, reconfigure Splunk Enterprise services on every machine to use the changed password, and then restart Splunk Enterprise on each machine.
- Configure the account that Splunk Enterprise uses so that its password never expires.
- Use a managed service account. See "Use managed service accounts" later in this topic.

Use managed service accounts

You can use a managed service account (MSA) to run Splunk Enterprise if you can meet all of the following conditions:

- You run Windows Server 2008 R2 or later, or Windows 8 or later in Active Directory
- At least one domain controller in your Active Directory runs Windows Server 2008 R2 or later

The benefits of using an MSA are:

- Increased security from the isolation of accounts for services.
- Administrators no longer need to manage the credentials or administer the accounts. Passwords automatically change after they expire. They do not have to manually set passwords or restart services associated with these

accounts.

- Administrators can delegate the administration of these accounts to non-administrators.

Some important things to understand before you install Splunk Enterprise with an MSA are:

- The MSA requires the same permissions as a domain account on the machine that runs Splunk Enterprise.
- The MSA must be a local administrator on the machine that runs Splunk Enterprise.
- You cannot use the same account on different machines, as you would with a domain account.
- You must correctly configure and install the MSA on the machine that runs Splunk Enterprise before you install Splunk Enterprise on the machine. See Service Accounts Step-by-Step Guide on MS Technet.

To install Splunk Enterprise using an MSA, see Prepare your Windows network for a Splunk Enterprise installation as a network or domain user.

Security and remote access considerations

Minimum permissions requirements

If you install Splunk Enterprise as a domain user, the machine that runs the instance requires that some default permissions change.

The `splunkd` and `splunkforwarder` services require specific user rights when you install Splunk Enterprise using a domain user. Depending on the sources of data you want to monitor, the Splunk Enterprise user might need additional rights. Failure to set these rights might result in a failed Splunk Enterprise installation, or an installation that does not function correctly.

Required basic permissions for the `splunkd` or `splunkforwarder` services

- Full control over the Splunk Enterprise installation directory.
- Read access to any files that you want to index.

Required Local/Domain Security Policy user rights assignments for the `splunkd` or `splunkforwarder` services

- Permission to log on as a service.
- Permission to log on as a batch job.

- Permission to replace a process-level token.
- Permission to act as part of the operating system.
- Permission to bypass traverse checking.

How to assign these permissions

This section provides guidance on how to assign the appropriate user rights and permissions to the Splunk Enterprise service account before you install. For procedures, see Prepare your Windows network for a Splunk Enterprise installation as a network or domain user.

Use Group Policy to assign rights to multiple machines

To assign the policy settings to a number of machines in your AD forest, you can define a Group Policy object (GPO) with these rights, and deploy the GPO across the forest.

After you create and enable the GPO, the machines in the forest pick up the changes, either during the next scheduled AD replication cycle (usually every 1.5 to 2 hours), or at the next boot time. Alternatively, you can force AD replication by using the `GPUPDATE` command-line utility on the machine that you want to update Group Policy.

When you set user rights with a GPO, those rights override identical Local Security Policy rights on a machine. You cannot change this setting. To retain the Local Security Policy rights, you must assign those rights within the GPO.

Troubleshoot permissions issues

The rights described are the rights that the `splunkd` and `splunkforwarder` services require to run. The data you want to access might require that you assign additional rights. Many user rights assignments and other Group Policy restrictions can prevent Splunk Enterprise from running. If you have problems, consider using a tool such as Process Monitor or the `GPRESULT` command line tool to troubleshoot GPO application in your environment.

Prepare your Windows network to run Splunk Enterprise as a network or domain user

You can prepare your Windows network to run Splunk Enterprise as a network or domain user other than the "Local System" user.

This can be different from the user that you use to install the software. Regardless of the user that you run Splunk Enterprise as, you must install the software with an account that has local administrator privileges on the installation machine.

These instructions have been tested for Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, and might differ for other versions of Windows.

The rights you assign by using these instructions are the minimum rights that are necessary for a successful Splunk Enterprise installation. You might need to assign additional rights, either within the Local Security Policy or a Group Policy object (GPO), or to the user and group accounts that you create, for Splunk Enterprise to access the data you want.

Security requirements and ramifications of changing system defaults through Group Policy

This procedure requires full administrative access to the host or Active Directory domain you want to prepare for Splunk Enterprise operations. Do not attempt to perform this procedure without this access.

The low-level access requirements for Splunk Enterprise operations necessitate these changes if you want to run Splunk Enterprise as a user other than the Local System user. You must make changes to your Windows network to complete this procedure. Making these changes can present a significant security risk.

To mitigate the risk, you can prevent the user that Splunk Enterprise runs as from logging in interactively, and limit the number of machines from where the user can log in. Alternatively, on Windows Server 2008 R2 and later, you can set up managed user accounts (MSAs) that further limit risk.

If you are not comfortable with or do not understand the security risks that come with this procedure, then do not perform it.

Configure Active Directory for running Splunk software as a domain user

The following procedures prepare your Active Directory for installations of Splunk Enterprise or the Splunk universal forwarder as a domain user.

To use PowerShell to configure your Active Directory for installation of Splunk Enterprise, see "Use PowerShell to configure your AD domain" later in this topic.

Prerequisites

You must meet the following requirements to perform this procedure:

- Your Windows environment runs Active Directory.
- You are a domain administrator for the AD domains that you want to configure.
- The installation hosts are members of this AD domain.

Create users

When you create users for running Splunk Enterprise, follow Microsoft best practices . See Microsoft Best Practices on MS TechNet.

1. Run the Active Directory Users and Computers tool by selecting **Start > Administrative Tools > Active Directory Users and Computers**.
2. Select the domain that you want to prepare for Splunk Enterprise operations.
3. Click **Action > New > User**
4. Enter the username for the new user and click **Next**.
5. Uncheck **User must change password at next logon**.
6. Click **Next**.
7. Click **Finish**.
8. (Optional) Repeat this procedure to create additional users.
9. (Optional) Quit Active Directory Users and Computers.

Create groups

This procedure creates the groups for users and machines that run Splunk Enterprise.

1. Run the Active Directory Users and Computers tool by selecting **Start > Administrative Tools > Active Directory Users and Computers**.
2. Select the domain that you want to prepare for Splunk Enterprise operations.
3. Double-click an existing container folder, or create an Organization Unit by selecting **New > Group** from the **Action** menu.
4. Select **Action > New > Group**.
5. Type a name that represents Splunk Enterprise user accounts, for example, Splunk Accounts.

6. Confirm that the **Group scope** is set to **Domain Local** and **Group type** is set to **Security**.
7. Click **OK** to create the group.
8. Create a second group and specify a name that represents Splunk Enterprise enabled computers, for example, Splunk Enabled Computers. This group contains computer accounts that receive permissions to run Splunk Enterprise as a domain user.
9. Confirm that the **Group scope** is **Domain Local** and the **Group type** is **Security**.

Assign users and computers to groups

This part of the procedure assigns users and computers that you created in the previous part.

1. Add the accounts to the **Splunk Accounts** group.
2. Add the computer accounts of the computers that will run Splunk Enterprise to the **Splunk Enabled Computers** group.
3. (Optional) Quit **Active Directory Users and Computers**.

Define a Group Policy object (GPO)

The Group Policy Object you create here will be distributed to all of the machines that run Splunk Enterprise. It assigns rights to the machines that make running Splunk Enterprise easier.

1. Run the **Group Policy Management Console (GPMC)** tool by selecting **Start > Administrative Tools > Group Policy Management**
2. In the tree view pane on the left, select **Domains**.
3. Click the **Group Policy Objects** folder.
4. In the **Group Policy Objects in <your domain>** folder, right-click and select **New**.
5. Type a name that describes the fact that the GPO will assign user rights to the servers you apply it to. For example, "Splunk Access."
6. Leave the **Source Starter GPO** field set to "(none)".
7. Click **OK** to save the GPO.
8. Remain in the GPMC. You will perform additional work there in the next section.

Add rights to the GPO

1. While still in the GPMC, right-click on the newly-created group policy object and select **Edit**.

2. In the **Group Policy Management Editor**, in the left pane, browse to **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment**.
    1. In the right pane, double-click on the **Act as part of the operating system** entry.
    2. In the window that opens, check the **Define these policy settings** checkbox.
    3. Click **Add User or Group?**
    4. In the dialog that opens, click **Browse?**
    5. In the **Select Users, Computers, Service Accounts, or Groups** dialog that opens, type in the name of the "Splunk Accounts" group you created earlier and click **Check Names?** Windows underlines the name if it is valid. Otherwise it tells you that it cannot find the object and prompts you for an object name again.
    6. Click OK to close the "Select Users?" dialog.
    7. Click OK again to close the "Add User or Group" dialog.
    8. Click OK again to close the rights properties dialog.
3. Repeat Steps 2a-2h for the following additional rights:
    - **Bypass traverse checking**
    - **Log on as a batch job**
    - **Log on as a service**
    - **Replace a process-level token**
4. Remain in the Group Policy Management Editor. You will perform additional work there in the next section.

Change Administrators group membership on each host

This procedure restricts who is a member of the Administrators group on the hosts to which you apply this GPO.

Confirm that all accounts that need access to the Administrators group on each host have been added to the Restricted Groups policy setting. Failure to do so can result in losing administrative access to the hosts on which you apply this GPO!

1. While still in the Group Policy Management Editor window, in the left pane, browse to **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups**.
    1. In the right pane, right-click and select **Add Group?** in the pop-up menu that appears.
    2. In the dialog that appears, type in **Administrators** and click OK.
    3. In the properties dialog that appears, click the **Add** button next to **Members of this group:**.

   4. In the **Add Member** dialog that appears, click **Browse?"**
   5. In the **Select Users, Computers, Service Accounts, or Groups** dialog that opens, type in the name of the "Splunk Accounts" group you created earlier and click **Check Names?** Windows underlines the name if it is valid. Otherwise it tells you that it cannot find the object and prompts you for an object name again.
   6. Click OK to close the **Select Users?** dialog.
   7. Click OK again to close the "Add User or Group" dialog.
   8. Click OK again to close the group properties dialog.
2. Repeat Steps 1a-1h for the following additional users or groups:
   - Domain Admins
   - any additional users who need to be a member of the Administrators group on every host to which you apply the GPO.
3. Close the Group Policy Management Editor window to save the GPO.
4. Remain in the GPMC. You will perform additional work there in the next section.

Restrict GPO application to select computers

This procedure controls which machines will actually receive the new GPO, and thus have their user rights assignments changed so that they can run Splunk Enterprise.

1. While still in the GPMC, in the GPMC left pane, select the GPO you created and added rights to, if it is not already selected. The GPMC displays information about the GPO in the right pane.
2. In the right pane, under **Security Filtering**, click **Add?**
3. In the **Select User, Computer, or Group** dialog that appears, type in "Splunk Enabled Computers" (or the name of the group that represents Splunk-enabled computers that you created earlier.)
4. Click **Check Names**. If the group is valid, Windows underlines the name. Otherwise, it tells you it cannot find the object and prompts you for an object name again.
5. Click OK to return to the GPO information window.
6. Repeat Steps 2-5 to add the "Splunk Accounts" group (the group that represents Splunk user accounts that you created earlier.)
7. Under **Security Filtering**, click the **Authenticated Users** entry to highlight it.
8. Click **Remove**. GPMC removes the "Authenticated Users" entry from the "Security Filtering" field, leaving only "Splunk Accounts" and "Splunk Enabled Computers."
9. Remain in the GPMC. You will perform additional work there in the next section.

Apply the GPO

Active Directory controls when Group Policy updates occur and GPOs get applied to hosts in the domain. Under normal circumstances, replication happens every 90-120 minutes. You must either wait this amount of time before attempting to install Splunk as a domain user, or force a Group Policy update by running `GPUPDATE /FORCE` from a command prompt on the host whose Group Policy you want to update.

1. While still in the GPMC, in the GPMC left pane, select the domain that you want to apply the GPO you created.
2. Right click on the domain, and select **Link an Existing GPO?** in the menu that pops up.

   If you only want the GPO to affect the OU that you created earlier, then select the OU instead and right-click to bring up the pop-up menu.
3. In the **Select GPO** dialog that appears, select the GPO you created and edited, and click **OK**. GPMC applies the GPO to the selected domain.
4. Close GPMC by selecting **File > Exit** from the GPMC menu.

Install Splunk with a managed system account

Alternatively, you can install Splunk Enterprise with a managed system account.

You can use the instructions in "Configure Active Directory for running Splunk software as a domain user" earlier in this topic to assign the MSA the appropriate security policy rights and group memberships.

When you grant file permissions to the MSA after installation, you might need to break NTFS permission inheritance from parent directories above the Splunk Enterprise installation directory and explicitly assign permissions from that directory and all subdirectories.

Windows grants the "Log on as a service" right to the MSA automatically if you use the Services control panel to make changes to Splunk services.

1. Create and configure the MSA that you plan to use to monitor Windows data.
2. Install Splunk from the command line and use the `LAUNCHSPLUNK=0` flag to keep Splunk Enterprise from starting after installation has completed.
3. After installation completes, use the Windows Explorer or the `ICACLS` command line utility to grant the MSA "Full Control" permissions to the Splunk Enterprise installation directory and all its sub-directories.

4. Change the default user for the `splunkd` and `splunkweb` service accounts, as described in the topic Correct the user selected during Windows installation.

   You must append a dollar sign ($) to the end of the username when completing this step for the MSA to work. For example, if the MSA is `SPLUNKDOCS\splunk1`, then you must enter `SPLUNKDOCS\splunk1$` in the appropriate field in the properties dialog for the service. You must do this for both the `splunkd` and `splunkweb` services.
5. Confirm that the MSA has the "**Log on as a service**" right.
6. Start Splunk Enterprise. It runs as the MSA configured above, and has access to all data that the MSA has access to.

Use PowerShell to configure your AD domain

You can use PowerShell to configure your Active Directory environment for Splunk Enterprise services. This option is available when you do not want to use the GUI-based administrative applications.

Create the Splunk user account

1. Open a PowerShell window.
2. Import the ActiveDirectory PowerShell module, if needed:

   ```
   > Import-Module ActiveDirectory
   ```
3. Create a new user:

   ```
   > New-ADUser ?Name <user> `
   -SamAccountName <user> `
   -Description ?Splunk Service Account? `
   -DisplayName ?Service:Splunk? `
   -Path ?<organizational unit LDAP path>? `
   -AccountPassword (Read-Host ?AsSecureString ?Account Password?) `
   -CannotChangePassword $true `
   -ChangePasswordAtLogon $false `
   -PasswordNeverExpires $true `
   -PasswordNotRequired $false `
   -SmartcardLogonRequired $false `
   -Enabled $true `
   -LogonWorkstations ?<server>? `
   ```

   In this example:

   - ♦ The command creates an account whose password cannot be changed, is not forced to change after first logon, and does not expire.

- ♦ *<user>* is the name of the user you want to create.
- ♦ *<organizational unit LDAP path>* is the name of the OU in which to put the new user, specified in X.500 format, for example: `CN=Managed Service Accounts,DC=splk,DC=com`.
- ♦ *<server>* is a single host or comma-separated list which specifies the host(s) that the account can log in from.

The `LogonWorkstations` argument is not required, but lets you limit which workstations a managed service account can use to log into the domain.

Configure the Splunk Enterprise server

After you have configured a user account, use PowerShell to configure the server with the correct permissions for the account to run Splunk Enterprise.

This is an advanced procedure. Improper changes to your AD can render it unusable. Perform these steps only if you feel comfortable doing so and understand the ramifications of using them, including problems that can occur due to typos and improperly-formatted files.

In the following examples:

- *<user>* is the name of the user you created that will run Splunk Enterprise.
- *<domain>* is the domain in which the user resides.
- *<computer>* is the remote computer you want to connect to in order to make changes.

To configure local security policy from PowerShell:

1. Connect to the machine that you wish to configure.
   - ♦ If you use the local machine, log in and open a PowerShell prompt, if you have not already.
   - ♦ If you connect to a remote machine, create a new `PSSession` on the remote host, as shown in the following examples.
   - ♦ You might need to disable Windows Firewall before you can make the remote connection. To do so, see Need to Disable Windows Firewall on MS TechNet (for versions of Windows Server up to Server 2008 R2, and Firewall with Advanced Security Administration with Windows PowerShell, also on MS TechNet.

   ```
   > Enter-PSSession -Computername <computer>
   ```
2. Add the service account to the local Administrators group.

```
> $group = [ADSI]?WinNT://<server>/Administrators,group?
> $group.Add(?WinNT://<domain>/<user>?)
```

3. Create a backup file that contains the current state of user rights settings on the local machine.

```
> secedit /export /areas USER_RIGHTS /cfg OldUserRights.inf
```

4. Use the backup to create a new user rights information file that assigns the Splunk Enterprise user elevated rights when you import it.

```
> Get-Content OldUserRights.inf `
| Select-String ?Pattern `
?(SeTcbPrivilege|SeChangeNotify|SeBatchLogon|SeServiceLogon|SeAssignPrimaryToken|
`
| %{ ?$_,<domain>\<user>? }
| Out-File NewUserRights.inf
```

5. Create a header for the new policy information file and concatenate the header and the new information file together.

```
> ( ?[Unicode]?, ?Unicode=yes? ) | Out-File Header.inf
> ( ?[Version]?, ?signature=`?`$CHICAGO`$`??, ?Revision=1?) |
Out-File ?Append Header.inf
> ( ?[Privilege Rights]? ) | Out-File ?Append Header.inf
> Get-Content NewUserRights.inf | Out-File ?Append Header.inf
```

6. Review the policy information file to ensure that the header was properly written, and that the file has no syntax errors in it.
7. Import the file into the local security policy database on the host.

```
> secedit /import /cfg Header.inf /db C:\splunk-lsp.sdb
> secedit /configure /db C:\splunk-lsp.sdb
```

Prepare a local machine or non-AD network for Splunk Enterprise installation

If you do not use Active Directory, follow these instructions to give administrative access to the user you want Splunk Enterprise to run as on the hosts on which you want to install Splunk Enterprise.

1. Give the user Splunk Enterprise should run as administrator rights by adding the user to the local Administrators group.
2. Start Local Security Policy by selecting **Start > Administrative Tools > Local Security Policy**.
3. In the left pane, expand **Local Policies** and then click **User Rights Assignment**.
    1. In the right pane, double-click on the **Act as part of the operating system** entry.

   2. Click **Add User or Group?**
   3. Click **Browse?**
   4. Type in the name of the "Splunk Computers" group you created earlier, and click **Check Names...** Windows underlines the name if it is valid. Otherwise it tells you that it cannot find the object and prompts you for an object name again.
   5. Click **OK**.
   6. Click **OK**.
   7. Click **OK**.

4. Repeat Steps 3a-3g for the following additional rights:
   - **Bypass traverse checking**
   - **Log on as a batch job**
   - **Log on as a service**
   - **Replace a process-level token**

After you have completed these steps, you can then install Splunk Enterprise as the desired user.

Install on Windows

You can install Splunk Enterprise on Windows with the Graphical User Interface (GUI)-based installer or from the command line. More options, such as silent installation, are available if you install from the command line. See Install on Windows from the command line for the command line installation procedure.

You cannot install or run the 32-bit version of Splunk Enterprise for Windows on a 64-bit Windows machine. You also cannot install Splunk Enterprise on a machine that runs an unsupported OS. For example, you cannot install Splunk Enterprise on a machine that runs Windows Server 2003. See System requirements. If you attempt to run the installer in such a way, it warns you and prevents the installation.

Note: If, rather than installing Splunk Enterprise, you want to install the Splunk **universal forwarder**, see Install a Windows universal forwarder from an installer in the *Universal Forwarder* manual. The universal forwarder is a separate executable from Splunk Enterprise and uses a different installer.

Upgrading?

If you plan to upgrade Splunk Enterprise, see How to upgrade Splunk Enterprise for instructions and migration considerations before proceeding.

Before you install

Choose the Windows user Splunk should run as

Before installing, see Choose the Windows user Splunk should run as to determine which user account Splunk should run as to address your specific needs. The user you choose has ramifications on what you must do prior to installing the software, and more details can be found there.

Disable or limit antivirus software if able

The Splunk Enterprise indexing subsystem requires high disk throughput. Any software with a device driver that intermediates between Splunk Enterprise and the operating system can restrict processing power available to Splunk Enterprise, causing slowness and even an unresponsive system. This includes anti-virus software.

You must configure such software to avoid on-access scanning of Splunk Enterprise installation directories and processes before you start a Splunk installation.

Consider installing Splunk software into a directory with a short path name

By default, the Splunk MSI file installs the software to `\Program Files\Splunk` on the system drive (the drive that booted your Windows machine.) While this directory is fine for many Splunk software installations, it might be problematic for installations that run in distributed deployments or that employ advanced Splunk features such as search-head or indexer clustering.

The Windows API has a path limitation of `MAX_PATH` which Microsoft defines as 260 characters including the drive letter, colon, backslash, 256-characters for the path, and a null terminating character. Windows cannot address a file path that is longer than this, and if Splunk software creates a file with a path length that is longer than `MAX_PATH`, it cannot retrieve the file later. There is no way to change this configuration.

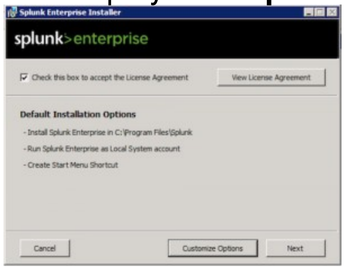
To work around this problem, if you know that the instance will be a member of a search head or indexer cluster, consider installing the software into a directory with a short path length, for example `C:\Splunk` or `D:\SPL`.

Install Splunk Enterprise via the GUI installer

The Windows installer is an MSI file.

Begin the installation

1. Download the Splunk installer from the Splunk download page.
2. To start the installer, double-click the `splunk.msi` file. The installer runs and displays the **Splunk Enterprise Installer** panel.



Splunk Enterprise Installer

☑ Check this box to accept the License Agreement

Default Installation Options

- Install Splunk Enterprise in C:\Program Files\Splunk
- Run Splunk Enterprise as Local System account
- Create Start Menu Shortcut

3. To continue the installation, check the "Check this box to accept the License Agreement" checkbox. This activates the "Customize Installation" and "Next" buttons.
4. (Optional) If you want to view the license agreement, click **View License Agreement**.

Installation Options

The Windows installer gives you two choices: Install with the default installation settings, or configure all settings prior to installing.

When you choose to install with the default settings, the installer does the following:

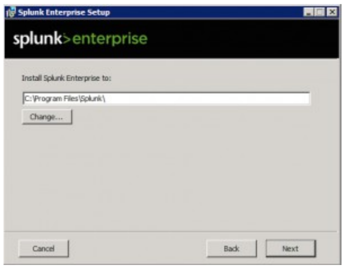
- Installs Splunk Enterprise in `\Program Files\Splunk` on the drive that booted your Windows machine.
- Installs Splunk Enterprise with the default management and Web network ports.
- Configures Splunk Enterprise to run as the Local System user.
- Prompts you to create a Splunk administrator password. You must do this before installation can continue.
- Creates a Start Menu shortcut for the software.

If you want to change any of these default installation settings, click **Customize Options** and proceed with the instructions in "Customize Options" in this topic.

Otherwise, click **Next**. You will be prompted for a password for the Splunk admin user. After you supply a password, installation begins and you can continue with the "Complete the install" instructions later in this topic.

Customize options during the installation

You can customize several options during the installation. When you choose to customize options, the installer displays the "Install Splunk Enterprise to" panel.



Install Splunk Enterprise to: C:\Program Files\Splunk\

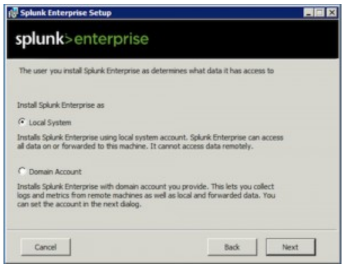
By default, the installer puts Splunk Enterprise into `\Program Files\Splunk` on the system drive. This documentation set refers to the Splunk Enterprise installation directory as `$SPLUNK_HOME` or `%SPLUNK_HOME%`.

Splunk Enterprise installs and runs two Windows services, `splunkd` and `splunkweb`. The `splunkd` service handles all Splunk Enterprise operations, and the `splunkweb` service installs to run only in legacy mode.

These services install and run as the user you specify on the "Choose the user Splunk Enterprise should run as" panel. You can choose to run Splunk Enterprise as the Local System user, or another user.

When the installer asks you the user that you want to install Splunk Enterprise as, you must specify the user name in `domain\username` format. The user must be a valid user in your security context, and must be an active member of an Active Directory domain. Splunk Enterprise must run under either the Local System account or a valid user account with a valid password and local administrator privileges. Failure to include the domain name with the user will cause the installation to fail.

1. Click **Change?** to specify a different location to install Splunk Enterprise, or click **Next** to accept the default value. The installer displays the "Choose the user Splunk Enterprise should run as" panel.



Splunk Enterprise Setup

The user you install Splunk Enterprise as determines what data it has access to

Install Splunk Enterprise as

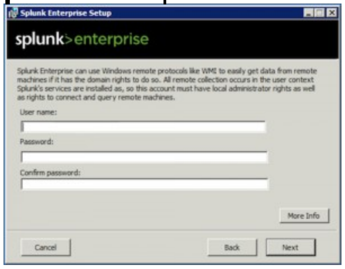
● Local System

Installs Splunk Enterprise using local system account. Splunk Enterprise can access all data on or forwarded to this machine. It cannot access data remotely.

○ Domain Account

Installs Splunk Enterprise with domain account you provide. This lets you collect logs and metrics from remote machines as well as local and forwarded data. You can set the account in the next dialog.

2. Select a user type and click **Next**.
3. If you selected the Local System user, proceed to Step 5. Otherwise, the installer displays the **Logon Information: specify a username and password** panel.



Splunk Enterprise Setup

Splunk Enterprise can use Windows remote protocols like WMI to easily get data from remote machines if it has the domain rights to do so. All remote collection occurs in the user context Splunk's services are installed as, so this account must have local administrator rights as well as rights to connect and query remote machines.

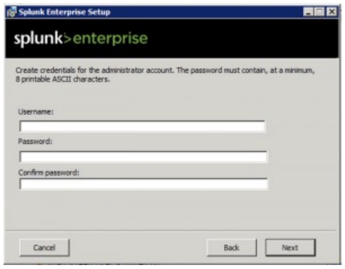
User name:

Password:

Confirm password:

4. Enter the Windows credentials that Splunk Enterprise uses to run on the machine and click **Next**.

   These credentials are different from the Splunk administrator credentials that you create in the next step.



Splunk Enterprise Setup

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

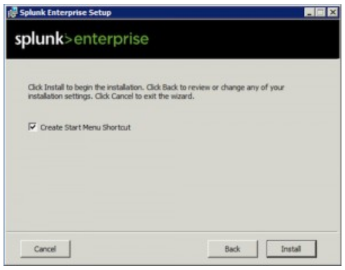
Username:

Password:

Confirm password:

5. Create credentials for the Splunk administrator user by entering a username and password that meets the minimum eligibility requirements as shown in the panel and click **Next**.

   You must perform this action as the installation cannot proceed without your completing it. If you do not enter a username, the installer creates the `admin` user during the installation process.
6. The installer displays the installation summary panel.



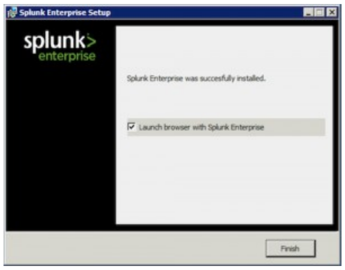
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

☑ Create Start Menu Shortcut

7. Click "Install" to proceed with the installation.

Complete the installation

The installer runs, installs the software, and displays the **Installation Complete** panel.



Splunk Enterprise was succesfully installed.

☑ Launch browser with Splunk Enterprise

If you specified the wrong user during the installation procedure, you will see two pop-up error windows explaining this. If this occurs, Splunk Enterprise installs itself as the Local System user by default. Splunk Enterprise does not start automatically in this situation. You can proceed through the final panel of the installation, but uncheck the "Launch browser with Splunk" checkbox to prevent your browser from launching. Then, use these instructions to switch to the correct user before starting Splunk.

1. (Optional) Check the boxes to **Launch browser with Splunk** and **Create Start Menu Shortcut**.
2. Click **Finish**. The installation completes, Splunk Enterprise starts and launches in a supported browser if you checked the appropriate box.

Avoid Internet Explorer Enhanced Security pop-ups in Splunk Web

If you use Internet Explorer to access Splunk Web, add the following URLs to the allowed Intranet group or fully trusted group to avoid getting "Enhanced Security" pop-ups:

- `quickdraw.splunk.com`

- the URL of your Splunk Enterprise instance

Install or upgrade license

If this is a new installation of Splunk Enterprise or switching from one license type to another, you must install or update your license. See Install a license.

Next steps

Now that you have installed Splunk Enterprise, you can find out how to start using Splunk Enterprise. See What happens next?

Alternatively, you can see the following topics in *Getting Data In* for help on adding Windows data:

- Monitor Windows Event Log data
- Monitor Windows Registry data
- Monitor WMI-based data
- Considerations for deciding how to monitor remote Windows data.

Install on Windows using the command line

You can install Splunk Enterprise on Windows from the command line.

Do not run the 32-bit installer on a 64-bit system. If you attempt this, the installer warns you and prevents installation.

If you want to install the Splunk **universal forwarder** from the command line, see Install a Windows universal forwarder from the command line" in the *Universal Forwarder* manual.

When to install from the command line

You can manually install Splunk Enterprise on individual machines from a command prompt or PowerShell window. Here are some scenarios where installing from the command line is useful:

- You want to install Splunk Enterprise, but do not want it to start right away
- You want to automate installation of Splunk Enterprise with a script
- You want to install Splunk Enterprise on a system that you will clone later

- You want to use a deployment tool such as Group Policy or System Center Configuration Manager
- You want to install Splunk Enterprise on a system that runs a version of Windows Server Core

Install using PowerShell

You can install Splunk Enterprise from a PowerShell window. The steps to do so are identical to those that you use to install from a command prompt.

Upgrading?

To upgrade Splunk Enterprise, see How to upgrade Splunk for instructions and migration considerations.

Splunk Enterprise does not support changing the management or Splunk Web ports during an upgrade.

Prerequisites to installing Splunk Enterprise on Windows

Choose the Windows user Splunk Enterprise should run as

Before you install, see Choose the Windows user Splunk Enterprise should run as to determine which user account Splunk Enterprise should run as to address your data collection needs. The user you choose has specific ramifications on what you need to do before you install the software.

Prepare your domain for a Splunk Enterprise installation as a domain user

The Windows network should be configured to support a Splunk Enterprise installation.

Before you install, see Prepare your Windows network for a Splunk Enterprise installation as a network or domain user for instructions about how to configure your domain to run Splunk Enterprise.

Disable or limit antivirus software if able

The Splunk Enterprise indexing subsystem requires high disk throughput. Any software with a device driver that intermediates between Splunk Enterprise and the operating system can restrict the processing power that is available to Splunk Enterprise. This can cause slowness and even an unresponsive system. This includes anti-virus software.

You must configure such software to avoid on-access scanning of Splunk Enterprise installation directories and processes before you start a Splunk installation

Have credentials for the Splunk administrator user ready

When you install Splunk Enterprise, you must create a username and password for the Splunk administrator user. The installer does not create credentials for the user by default. Think of a username and password combination and be ready to supply it when you perform the installation. If you do not supply at least a password during a silent installation, Splunk Enterprise can install without any users defined, which prevents login. You must then create a user-seed.conf file to fix the problem and restart the software.

Consider installing Splunk software into a directory with a short path name

By default, the Splunk MSI file installs the software to `\Program Files\Splunk` on the system drive (the drive that booted your Windows machine.) While this directory is fine for many Splunk software installations, it might be problematic for installations that run in distributed deployments or that employ advanced Splunk features such as search-head or indexer clustering.

The Windows API has a path limitation of `MAX_PATH` which Microsoft defines as 260 characters including the drive letter, colon, backslash, 256-characters for the path, and a null terminating character. Windows cannot address a file path that is longer than this, and if Splunk software creates a file with a path length that is longer than `MAX_PATH`, it cannot retrieve the file later. There is no way to change this configuration.

To work around this problem, if you know that the instance will be a member of a search head or indexer cluster, consider installing the software into a directory with a short path length, for example `C:\Splunk` or `D:\SPL`.

Install Splunk Enterprise from the command line

Invoke `msiexec.exe` to install Splunk Enterprise from the command line or a PowerShell prompt.

For 32-bit platforms, use `splunk-<...>-x86-release.msi`:

```
msiexec.exe /i splunk-<...>-x86-release.msi [<flag>]... [/quiet]
```

For 64-bit platforms, use `splunk-<...>-x64-release.msi`:

```
msiexec.exe /i splunk-<...>-x64-release.msi [<flag>]... [/quiet]
```

The value of `<...>` varies according to the particular release; for example, `splunk-6.3.2-aaff59bb082c-x64-release.msi`.

Command-line flags let you configure Splunk Enterprise at installation. Using command-line flags, you can specify a number of settings, including but not limited to:

- Which Windows event logs to index.
- Which Windows Registry hives to monitor.
- Which Windows Management Instrumentation (WMI) data to collect.
- The user Splunk Enterprise runs as. See Choose the Windows user Splunk Enterprise should run as for information about what type of user you should install your Splunk instance with.
- An included application configuration for Splunk to enable (such as the light forwarder.)
- Whether Splunk Enterprise should start automatically when the installation is finished.

Supported flags

The following is a list of the flags you can use when installing Splunk Enterprise for Windows from the command line.

The Splunk universal forwarder is a separate executable, with its own installation flags. See the supported installation flags for the universal forwarder in Install a Windows universal forwarder from the command line in the *Universal Forwarder* manual.

Flag	Purpose	Default
`AGREETOLICENSE=Yes|No`	Use this flag to agree to the EULA. You must set this flag to Yes to perform a silent installation. The flag does not work when you click the MSI to start installation.	`No`
`INSTALLDIR="<directory_path>"`	Use this flag to specify directory to install. The Splunk Enterprise	`C:\Program Files\Splunk`

Flag	Purpose	Default
	installation directory is referred to as $SPLUNK_HOME or %SPLUNK_HOME% throughout this documentation set.	
SPLUNKD_PORT=<port number>	Use this flag to specify alternate ports for splunkd and splunkweb to use. If you specify a port and that port is not available, Splunk Enterprise automatically selects the next available port.	8089
WEB_PORT=<port number>	Use this flag to specify alternate ports for splunkd and splunkweb to use. If you specify a port and that port is not available, Splunk Enterprise automatically selects the next available port.	8000

WINEVENTLOG_APP_ENABLE=1/0
WINEVENTLOG_SEC_ENABLE=1/0
WINEVENTLOG_SYS_ENABLE=1/0
WINEVENTLOG_FWD_ENABLE=1/0
WINEVENTLOG_SET_ENABLE=1/0
	Use these flags to specify whether or not Splunk Enterprise should index a particular Windows event log. You can specify multiple flags:
	Application log
	Security log
	System log
	Forwarder log
	Setup log
		0 (off)

REGISTRYCHECK_U=1/0
REGISTRYCHECK_BASELINE_U=1/0
	Use these flags to specify whether or not Splunk Enterprise should
	index events from
	capture a baseline snapshot of
	the Windows Registry user hive (HKEY_CURRENT_USER).
		0 (off)

Flag	Purpose	Default
	Note: You can set both of these at the same time.	

REGISTRYCHECK_LM=1/0
REGISTRYCHECK_BASELINE_LM=1/0
	Use these flags to specify whether or not Splunk Enterprise should
	index events from
	capture a baseline snapshot of
	the Windows Registry machine hive (HKEY_LOCAL_MACHINE).
	Note: You can set both of these at the same time.
		0 (off)

WMICHECK_CPUTIME=1/0
WMICHECK_LOCALDISK=1/0
WMICHECK_FREEDISK=1/0
WMICHECK_MEMORY=1/0
	Use these flags to specify which popular WMI-based performance metrics Splunk should index:
	CPU usage
	Local disk usage
	Free disk space
	Memory statistics
	Note: If you need this instance of Splunk Enterprise to monitor remote Windows data, then you must also specify the LOGON_USERNAME and LOGON_PASSWORD installation flags. Splunk Enterprise cannot collect any remote data that it does not have explicit access to. Additionally, the user you specify requires specific rights, administrative privileges, and additional permissions, which you must configure before installation. Read "Choose the Windows user Splunk Enterprise should run as" in this manual for additional
		0 (off)

Flag	Purpose	Default
	information about the required credentials. There are many more WMI-based metrics that Splunk can index. Review "Monitor WMI Data" in the Getting Data In Manual for specific information.	

`LOGON_USERNAME="<domain\username>"`
`LOGON_PASSWORD="<pass>"`
	Use these flags to provide domain\username and password information for the Windows user that Splunk Enterprise will run as. The `splunkd` and `splunkweb` services are configured with these credentials. For the `LOGON_USERNAME` flag, you must specify the domain with the username in the format "`domain\username`." Do not use this flag to set the Splunk administrator password.
	These flags are mandatory if you want this Splunk Enterprise installation to monitor any remote data. Review "Choose the Windows user Splunk Enterprise should run as" in this manual for additional information about which credentials to use.
		none

`SPLUNK_APP="<SplunkApp>"`	Use this flag to specify an included Splunk application configuration to enable for this installation of Splunk Enterprise. Currently supported options for `<SplunkApp>` are: `SplunkLightForwarder` and `SplunkForwarder`. These specify that this instance of Splunk will function as a light forwarder or heavy forwarder, respectively. Refer to the "About forwarding and receiving" topic in the *Forwarding Data* manual for more information.	none

Flag	Purpose	Default
	If you specify either the Splunk forwarder or light forwarder here, you must also specify FORWARD_SERVER="<server:port>". To install Splunk Enterprise with no applications at all, omit this flag. **Note:** The full version of Splunk Enterprise does not enable the universal forwarder. The universal forwarder is a separate downloadable executable, with its own installation flags.	
`FORWARD_SERVER="<server:port>"`	Use this flag only when you also use the `SPLUNK_APP` flag to enable either the Splunk heavy or light forwarder. Specify the server and port of the Splunk server to which this forwarder will send data.	none
`DEPLOYMENT_SERVER="<host:port>"`	Use this flag to specify a deployment server for pushing configuration updates. Enter the deployment server name (hostname or IP address) and port.	none
`LAUNCHSPLUNK=0/1`	Use this flag to specify whether or not Splunk software should start up after the installation completes, and automatically when the machine boots. **Note:** If you enable the Splunk Forwarder by using the `SPLUNK_APP` flag, the installer configures Splunk to start automatically, and ignores this flag.	`1` (on)
`INSTALL_SHORTCUT=0/1`	Use this flag to specify whether or not the installer should create a shortcut to Splunk on the desktop and in the Start Menu.	`1` (on)
`SPLUNKUSERNAME=<username>`	Create a username for the Splunk administrator user. If you specify a quiet	`admin`

Flag	Purpose	Default
	installation with the `/quiet` flag and do not specify this setting, then the software uses the default value of `admin`, but you must still specify a password with the `SPLUNKPASSWORD` or `GENRANDOMPASSWORD` flags for the installation to add the credentials successfully.	
`SPLUNKPASSWORD=<password>`	Create a password for the Splunk `admin` user. The password must meet eligibility requirements. If you specify a quiet installation with the `/quiet` flag and do not specify this flag or the `SPLUNKUSERNAME` flag, then the software installs without a user, and you must create one by editing the `user-seed.conf` configuration file.	N/A
`MINPASSWORDLEN=<positive integer>`	When using the `SPLUNKPASSWORD` flag to set a password, you can also set password eligibility requirements for password creation and modification. The `MINPASSWORDLEN` flag specifies the minimum length that a password must be to meet these eligibility requirements going forward. It cannot be set to 0 or a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.	`> 1`
`MINPASSWORDDIGITLEN=<integer>`	When using the `SPLUNKPASSWORD` flag to set a password, you can also set password eligibility requirements for password creation and modification. The `MINPASSWORDDIGITLEN` flag specifies the minimum number of numeral (0 through 9) characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing	`0`

Flag	Purpose	Default
	password you change must meet the new requirements after you set this flag.	
MINPASSWORDLOWERCASELEN=<integer>	When using the SPLUNKPASSWORD flag to set a password, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDLOWERCASELEN flag specifies the minimum number of lowercase ('a' through 'z') characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.	0
MINPASSWORDUPPERCASELEN=<integer>	When using the SPLUNKPASSWORD flag to set a password, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDUPPERCASELEN flag specifies the minimum number of uppercase ('A' through 'Z') characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.	0
MINPASSWORDSPECIALCHARLEN=<integer>	When using the SPLUNKPASSWORD flag to set a password, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDSPECIALCHARLEN flag specifies the minimum number of special characters that a password must contain to meet these eligibility requirements going forward. It cannot	0

Flag	Purpose	Default
	be set to a negative integer. The ':' (colon) character cannot be used as a special character. Any new password you create and any existing password you change must meet the new requirements after you set this flag.	
`GENRANDOMPASSWORD=1/0`	Generate a random password for the `admin` user and write the password to the installation log file. The installer writes the credentials to `%TEMP%\splunk.log`. After the installation completes, you can use the `findstr` utility to search that file for the word "PASSWORD". After you get the credentials, delete the installation log file, as retaining the file represents a significant security risk.	`0`

Silent installation

To run the installation silently, add `/quiet` to the end of your installation command string. If your system has User Access Control enabled (the default on some systems), you must run the installation as Administrator. To do this:

- When opening a command prompt or PowerShell window, right click on the app icon and select "Run As Administrator".
- Use this command window to run the silent install command.

Examples

The following are some examples of using different flags.

Silently install Splunk Enterprise to run as the Local System Windows user and set the Splunk administrator credentials to "SplunkAdmin/MyNewPassword"

```
msiexec.exe /I Splunk.msi SPLUNKUSER=SplunkAdmin
SPLUNKPASSWORD=MyNewPassword /quiet
```

Enable the Splunk heavy forwarder and specify credentials for the user Splunk Enterprise should run as

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder"
SPLUNKPASSWORD=MyNewPassword FORWARD_SERVER="<server:port>"
LOGON_USERNAME="AD\splunk" LOGON_PASSWORD="splunk123"
```

Enable the Splunk heavy forwarder, generate a random password for the default Splunk administrator user, enable indexing of the Windows System event log, and run the installer in silent mode

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder"
GENRANDOMPASSWORD=1 FORWARD_SERVER="<server:port>"
 WINEVENTLOG_SYS_ENABLE=1 /quiet
```

Where `"<server:port>"` are the server and port of the Splunk server to which this machine should send data.

Install Splunk Enterprise with verbose logging to C:\TEMP\SplunkInstall.log

```
msiexec.exe /I Splunk.msi /l*v C:\TEMP\SplunkInstall.log
```

See Command Line Options on Windows Dev Center for additional logging and command line options for `msiexec.exe`.

Avoid Internet Explorer (IE) Enhanced Security pop-ups

To avoid IE Enhanced Security pop-ups, add the following URLs to the allowed Intranet group or fully trusted group in IE:

- quickdraw.splunk.com
- the URL of your Splunk instance

Next steps

Now that you have installed Splunk Enterprise, **learn what happens next.**

You can also review this topic about considerations for deciding how to monitor Windows data in the Getting Data In manual.

Change the user selected during Windows installation

You can change the Windows user that Splunk Enterprise or a universal forwarder has been installed as prior to starting the software for the first time.

There are several scenarios where performing this task is helpful:

- If you selected "Domain user" during the Splunk Enterprise installation, and that user does not exist or you mistyped the information
- If you need to install a Splunk Enterprise instance as a managed system account (MSA)
- If you installed the software from a ZIP file and want to change the Windows user for the Splunk Enterprise services from the default SYSTEM user

You must perform this procedure before you start Splunk Enterprise. If Splunk Enterprise has started, then stop it, uninstall it, and reinstall it.

1. Run the Services tool. From the **Start** menu, click **Control Panel > Administrative Tools > Services**.
2. Find the `splunkd` and `splunkweb` (or `splunkforwarder` for the universal forwarder) services. These services must not be started. The Local System user owns them by default.
3. Right-click a service, and select **Properties**.
4. Click the **Log On** tab.
5. Click the **This account** button.
6. Fill in the correct domain\user name and password.
7. Click **Apply**.
8. Click **OK**.
9. (Optional) If you run Splunk Enterprise in legacy mode, repeat steps 2 through 6 for the second service.
10. Start the Splunk Enterprise services from the Service Manager or from the command-line interface.

Install Splunk Enterprise on Linux or Mac OS X

Install on Linux

You can install Splunk Enterprise on Linux using RPM or DEB packages or a tar file, depending on the version of Linux your host runs.

To install the Splunk **universal forwarder**, see Install a *nix universal forwarder in the *Universal Forwarder* manual. The universal forwarder is a separate executable, with a different installation package and its own set of installation procedures.

Upgrading Splunk Enterprise

If you are upgrading, see How to upgrade Splunk Enterprise for instructions and migration considerations before you upgrade.

Tar file installation

What to know before installing with a tar file

Knowing the following items helps ensure a successful installation with a tar file:

- Some non-GNU versions of `tar` might not have the `-C` argument available. In this case, to install in `/opt/splunk`, either `cd` to `/opt` or place the tar file in `/opt` before you run the `tar` command. This method works for any accessible directory on your host file system.
- Splunk Enterprise does not create the `splunk` user. If you want Splunk Enterprise to run as a specific user, you must create the user manually before you install.
- Confirm that the disk partition has enough space to hold the uncompressed volume of the data you plan to keep indexed.

Installation procedure

1. Expand the tar file into an appropriate directory using the `tar` command:

```
tar xvzf splunk_package_name.tgz
```

The default installation directory is `splunk` in the current working directory. To install into `/opt/splunk`, use the following command:

```
tar xvzf splunk_package_name.tgz -C /opt
```

RedHat RPM installation

RPM packages are available for Red Hat, CentOS, and similar versions of Linux.

The `rpm` package does not provide any safeguards when you use it to upgrade. While you can use the `--prefix` flag to install it into a different directory, upgrade problems can occur If the directory that you specified with the flag does not match the directory where you initially installed the software.

After installation, software package validation commands (such as `rpm -Vp <rpm_file>` might fail because of intermediate files that get deleted during the installation process. To verify your Splunk installation package, use the `splunk validate files` CLI command instead.

1. Confirm that the RPM package you want is available locally on the target host.
2. Verify that the Splunk Enterprise user account that will run the Splunk services can read and access the file.
3. If needed, change permissions on the file.
   ```
   chmod 744 splunk_package_name.rpm
   ```
4. Invoke the following command to install the Splunk Enterprise RPM in the default directory `/opt/splunk`.

   ```
   rpm -i splunk_package_name.rpm
   ```
5. (Optional) To install Splunk in a different directory, use the `--prefix` flag.

   ```
   rpm -i --prefix=/opt/new_directory splunk_package_name.rpm
   ```

Replace an existing Splunk Enterprise installation with an RPM package

- Run `rpm` with the `--prefix` flag and reference the existing Splunk Enterprise directory.

  ```
  rpm -i --replacepkgs --prefix=/splunkdirectory/
  splunk_package_name.rpm
  ```

Automate RPM installation with Red Hat Linux Kickstart

- If you want to automate an RPM install with Kickstart, edit the kickstart file and add the following.

  ```
  ./splunk start --accept-license
  ./splunk enable boot-start
  ```

  The `enable boot-start` line is optional.

Debian .DEB installation

Prerequisites to installation

- You can install the Splunk Enterprise Debian package only into the default location, `/opt/splunk`.
- This location must be a regular directory, and cannot be a symbolic link.
- You must have access to the root user or have sudo permissions to install the package.
- The package does not create environment variables to access the Splunk Enterprise installation directory. You must set those variables on your own.

If you need to install Splunk Enterprise somewhere else, or if you use a symbolic link for `/opt/splunk`, then use a tar file to install the software.

Installation procedure

- Run the `dpkg` installer with the Splunk Enterprise Debian package name as an argument.

  ```
  dpkg -i splunk_package_name.deb
  ```

Debian commands for showing installation status

Splunk package status:

```
dpkg --status splunk
```

List all packages:

```
dpkg --list
```

Information on expected default shell and caveats for Debian shells

Splunk Enterprise expects you to run commands from the `bash` shell. It expects `bash` to be available from `/bin/sh`.

On later versions of Debian Linux (for example, Debian Squeeze), the default shell is the `dash` shell.

Using the `dash` shell can result in zombie processes - processes that have completed execution, yet remain in the process table and cannot be killed or removed.

If you run Debian Linux, consider changing your default shell to be `bash`.

Next steps

Now that you have installed Splunk Enterprise:

- Start it and create administrator credentials. See Start Splunk Enterprise for the first time.
- Configure it to start at boot time. See Configure Splunk software to start at boot time.
- Learn what comes next. See what happens next?

Uninstall Splunk Enterprise

To learn how to uninstall Splunk Enterprise, see Uninstall Splunk Enterprise.

Install on Mac OS X

You can install Splunk Enterprise on Mac OS X with a DMG package or a tar file.

To install the Splunk **universal forwarder**, see Install a *nix universal forwarder in the *Universal Forwarder* manual. The universal forwarder is a separate executable, with its own set of installation procedures.

Upgrading?

If you are upgrading, review "How to upgrade Splunk Enterprise" for instructions and migration considerations before proceeding.

Installation options

The Mac OS installation package comes in two forms: a DMG package and a tar file.

If you require two installations in different locations on the same host, use the tar file. The DMG installer cannot install a second instance. If one exists, it removes that instance upon successful install of the second.

Graphical installation

1. Double-click on the DMG file. A **Finder** window containing splunk.pkg opens.
2. In the **Finder** window, double-click on splunk.pkg. The installer opens and displays the **Introduction**, which lists version and copyright information.
3. Click **Continue**. The **Select a Destination** window opens.
4. Choose a location to install Splunk Enterprise.
    - To install in the default directory, `/Applications/splunk`, click on the harddrive icon.
    - To select a different location, click **Choose Folder...**
5. Click **Continue**. The pre-installation summary displays. If you need to make changes:
    - Click **Change Install Location** to choose a new folder, or
    - Click **Back** to go back a step.
6. Click **Install**.
7. A window appears that prompts you for the credentials you used to log into your Mac. These are not your Splunk Enterprise instance or splunk.com credentials. Type in the password and click **OK** or **Install software.**
8. The installation begins. It might take a few minutes to complete.
9. When the install completes, click **Finish**. The installer places a shortcut on the Desktop.

Command line installation

To install Splunk Enterprise on Mac OS X from the command line, you must use the root user, or elevate privileges using the `sudo` command. **If you use `sudo`, your account must be an Administrator-level account.**

1. To mount the DMG file, run:
   ```
   sudo hdid splunk_package_name.dmg
   ```

The Finder mounts the disk image onto the desktop. The image is available under /Volumes/SplunkForwarder <version> (note the space).

2. To Install the software:
   - ♦ To the root volume:

```
cd /Volumes/SplunkForwarder\ <version>
sudo installer -pkg .payload/splunk.pkg -target /
```

There is a space in the disk image name. Use a backslash to escape the space or wrap the disk image name in quotes.

   - ♦ To a different disk of partition:

```
cd /Volumes/SplunkForwarder\ <version>
sudo installer -pkg .payload/splunk.pkg -target /Volumes\ Disk
```

There is a space in the disk image name. Use a backslash to escape the space or wrap the disk image name in quotes.

`-target` specifies a target volume, such as another disk, where Splunk will be installed in `/Applications/splunk`.

To install into a directory other than `/Applications/splunk` on any volume, see the graphical installation instructions.

tar file install

The tar file is a manual form of installation. When you install Splunk Enterprise with a tar file:

- Splunk Enterprise does not create the `splunk` user automatically. If you want it to run as a specific user, you must create the user manually before installing.
- Ensure that the disk partition has enough space to hold the uncompressed volume of the data you plan to keep indexed.

To install Splunk Enterprise on Mac OS X, expand the tar file into an appropriate directory using the `tar` command:

```
tar xvzf splunk_package_name.tgz
```

The default install directory is `splunk` in the current working directory. To install into `/Applications/splunk`, use the following command:

```
tar xvzf splunk_package_name.tgz -C /Applications
```

Next steps

Now that you have installed Splunk Enterprise:

- Start it, if it has not started already.
- Configure it to start at boot time. See Configure Splunk software to start at boot time.
- Learn what comes next.

Uninstall Splunk Enterprise

To learn how to uninstall Splunk Enterprise, see Uninstall Splunk Enterprise in this manual.

Run Splunk Enterprise as a different or non-root user

On *nix based systems, you can run Splunk Enterprise as a user other than root. This is a Splunk best practice and you should configure your systems to run the software as a non-root user where possible.

If you run Splunk software as a non-root user, confirm that the software can perform the following:

- Read the files and directories that you configure it to monitor. Some log files and directories might require root or superuser access to be indexed.
- Write to the Splunk Enterprise directory and execute any scripts configured to work with your alerts or scripted input. See Configure a script for an alert action in the *Alerting Manual* or Get data from APIs and other remote data interfaces through scripted inputs in *Getting data in*.
- Bind to the network ports it is listening on. Network ports below 1024 are reserved ports that only the root user can bind to.

Because network ports below 1024 are reserved for root access only, Splunk software can only listen on port 514 (the default listening port for syslog) if it runs as root. You can, however, install another utility (such as syslog-ng) to write your syslog data to a file and have Splunk monitor that file instead.

Set up Splunk software to run as a non-root user

1. Install Splunk software as the root user, if you have root access. Otherwise, install the software into a directory that has write access for the user that you want Splunk software to run as.
2. Change the ownership of the `$SPLUNK_HOME` directory to the user that you want Splunk software to run as.
3. Start the Splunk software.

Example instructions on how to install Splunk software as a non-root user

In this example, `$SPLUNK_HOME` represents the path to the Splunk Enterprise installation directory.

1. Log into the machine that you want to install Splunk software as root.
2. Create the `splunk` user and group.
   On Linux:
   ```
   useradd splunk
   groupadd splunk
   ```

   On Mac OS: You can use the **System Preferences > Accounts** System Preferences panel to add users and groups.
3. Install the Splunk software, as described in the installation instructions for your platform. See Installation instructions.

   Do not start Splunk Enterprise yet.
4. Run the `chown` command to change the ownership of the `splunk` directory and everything under it to the user that you want to run the software.

   ```
   chown -R splunk:splunk $SPLUNK_HOME
   ```

   If the `chown` binary on your system does not support changing group ownership of files, you can use the `chgrp` command instead. See the `man` pages on your system for additional information on changing group ownership.
5. Become the non-root user.

   ```
   su - <user>
   ```

   You can also log out of the root account and log in as that user.
6. Start the Splunk software.

   ```
   $SPLUNK_HOME/bin/splunk start
   ```

Use sudo to start or stop Splunk software as a different user

If you want to start Splunk Enterprise as the `splunk` user while you are logged in as a different user, you can use the `sudo` command.

```
sudo -H -u splunk $SPLUNK_HOME/bin/splunk start
sudo -H -u splunk $SPLUNK_HOME/bin/splunk stop
```

This example command assumes the following:

- That Splunk Enterprise has been installed in the default installation directory. If Splunk Enterprise is in an alternate location, update the path in the command accordingly.
- That your system has the `sudo` command available. If this is not the case, use `su` or get and install `sudo`.
- That you have already created the user that you want Splunk software to run as.
- That the `splunk` user has access to the `/dev/urandom` device to generate the certificates for the product.

Further reading

- To configure Splunk software to run at boot time as a non-root user, see Enable boot-start as a non-root user in the *Admin* Manual.
- To learn how to install Splunk Enterprise on Windows using a user that is not an administrator, see Choose the user Splunk Enterprise should run as.
- To learn how to change the Windows user that Splunk Enterprise services use, see Change the user selected during Windows installation.

Install Splunk Enterprise in virtual and containerized environments

Deploy and run Splunk Enterprise inside a Docker container

You deploy Splunk Enterprise inside a Docker container by downloading and launching the required Splunk Enterprise image in Docker. The image is an executable package that includes everything you need to run Splunk Enterprise. A container is a runtime instance of an image.

1. From a shell prompt, run the following command to download the required Splunk Enterprise image to your local Docker image library.

   ```
   docker pull splunk/splunk:latest
   ```
2. Run the downloaded Docker image.

   ```
   docker run -d -p 8000:8000 -e
   'SPLUNK_START_ARGS=--accept-license' -e
   'SPLUNK_PASSWORD=<password>' splunk/splunk:latest
   ```
   Where `<password>` is the new password you want to set for the Splunk Enterprise instance. For information on password requirements, see Configure a Splunk password policy in Authentication.conf in *Securing Splunk Enterprise*.

   `-p 8000:8000` exposes the default port of Splunk Enterprise inside the container to the outside world by mapping it to a port on the local host. In this case, the outside port is also 8000. If port 8000 is occupied by another service on the host, you can use the `-p` parameter to map the application port to another available port on the host, for example, `-p 9000:8000`.
3. The output of the `docker run` command is a hash of numbers and letters that represents the container ID of your new Splunk Enterprise deployment. Run the following command with the container ID to display the status of the container.

   ```
   docker ps -a -f id=<container_id>
   ```
4. When the status of the container becomes healthy, it means the container is already up and running. Open an Internet browser and access Splunk Enterprise inside the container through Splunk Web:

   ```
   localhost:8000
   ```

5. Log in to Splunk Enterprise inside the container using the username `admin` and the password you previously set when you ran the Docker image.

Administer Splunk Enterprise Docker containers

You can use the following Docker commands to manage containers.

- To see a list of your running containers with the command `docker ps`, just as you would in Linux.
- To stop your Splunk Enterprise container, use the following command.

```
docker container stop <container_id>
```

- To restart a stopped container, use the following command.

```
docker container start <container_id>
```

To learn more about Docker commands, see the Docker documentation.

Start using Splunk Enterprise

Start Splunk Enterprise for the first time

Before you begin using your new Splunk Enterprise upgrade or installation, take a few moments to make sure that the software and your data are secure.

As part of the initial startup process, Splunk Enterprise prompts you to create credentials for the administrator user. You can choose a username or use the default of `admin`. You can also enter a password. You must complete both steps for Splunk Enterprise to start and operate normally.

See the following topics in the *Securing Splunk* manual for more information:

- Hardening Standards
- Create secure administrator credentials

If you start Splunk Enterprise for the first time with the `--no-prompt` CLI argument, then the software does not prompt you to create the administrator credentials. If you do not create the credentials then Splunk Enterprise displays a message on login that there is no user. You must then manually create the credentials and restart Splunk Enterprise before you can log in. See "Create admin credentials manually" later in this topic for instruction on creating the credentials.

On Windows

You can start Splunk Enterprise on Windows using either the command line or the Services control panel. Using the command line offers more options.

From a command prompt or PowerShell window, run the following commands:

```
cd <Splunk Enterprise installation directory>\bin
splunk start
```

(For Windows users: in subsequent examples and information, replace `$SPLUNK_HOME` with `C:\Program Files\Splunk` if you have installed Splunk in the default location. You can also add `%SPLUNK_HOME%` as a system-wide environment variable by using the Advanced tab in the System Properties dialog box.)

On UNIX

1. Use the Splunk Enterprise command-line interface (CLI):

   ```
   cd <Splunk Enterprise installation directory>/bin
   ./splunk start
   ```
2. Create the Splunk Enterprise admin username. This is the user that you log into Splunk Enterprise with, not the user that you use to log into your machine or onto splunk.com. You can press Enter to use the default username of `admin`.

   ```
   This appears to be your first time running this version of Splunk.

   Create credentials for the administrator account.
   Characters do not appear on the screen when you type the password.

   Please enter an administrator username:
   ```
3. Create the password for the user that you just created. You use these credentials to log into Splunk Enterprise.

   ```
   Password must contain at least:
   * 8 total printable ASCII character(s).
   Please enter a new password:
   ```
4. If the default management and Splunk Web ports are already in use (or are otherwise not available), Splunk Enterprise offers to use the next available ports. You can either accept this option or specify a port to use.
5. You can optionally set the `SPLUNK_HOME` environment variable to the Splunk Enterprise installation directory. Setting the environment variable lets you refer to the installation directory later without having to remember its exact location:

   ```
   export SPLUNK_HOME=<Splunk Enterprise installation directory>
   cd $SPLUNK_HOME/bin
   ./splunk start
   ```
6. Splunk Enterprise displays the license agreement and prompts you to accept before the startup sequence continues.

On Mac OS X

Start Splunk Enterprise from the Finder

1. Double-click the **Splunk** icon on the Desktop to launch the helper application, entitled "Splunk's Little Helper".
2. Click **OK** to allow Splunk to initialize and set up the trial license.
3. (Optional) Click **Start and Show Splunk** to start Splunk Enterprise and direct your web browser to open a page to Splunk Web.

4. (Optional) Click **Only Start Splunk** to start Splunk Enterprise, but not open Splunk Web in a browser.
5. (Optional) Click **Cancel** to quit the helper application. This does not affect the Splunk Enterprise instance itself, only the helper application.

After you make your choice, the helper application performs the requested application and terminates. You can run the helper application again to either show Splunk Web or stop Splunk Enterprise.

The helper application can also be used to stop Splunk Enterprise if it is already running.

Start Splunk Enterprise from the command line

1. On macOS, the default Splunk Enterprise installation directory is `/Applications/splunk`.

   ```
   cd <Splunk Enterprise installation directory>/bin
   ./splunk start
   ```
2. Create the Splunk Enterprise admin username. This is the user that you log into Splunk Enterprise with, not the user that you use to log into your machine or onto splunk.com. You can press Enter to use the default username of `admin`.

   ```
   This appears to be your first time running this version of Splunk.

   Create credentials for the administrator account.
   Characters do not appear on the screen when you type the password.

   Please enter an administrator username:
   ```
3. Create the password for the user that you just created. You use these credentials to log into Splunk Enterprise.

   ```
   Password must contain at least:
   * 8 total printable ASCII character(s).
   Please enter a new password:
   ```

Other start options

Accept the Splunk license automatically when starting for the first time

1. Add the `--accept-license` option to the `start` command:

   ```
   $SPLUNK_HOME/bin/splunk start --accept-license
   ```
2. Create the Splunk Enterprise admin username. This is the user that you

log into Splunk Enterprise with, not the user that you use to log into your machine or onto splunk.com. You can press Enter to use the default username of `admin`.

```
This appears to be your first time running this version of Splunk.

Create credentials for the administrator account.
Characters do not appear on the screen when you type the password.

Please enter an administrator username:
```

3. Create the password for the user that you just created. You use these credentials to log into Splunk Enterprise.

```
Password must contain at least:
* 8 total printable ASCII character(s).
Please enter a new password:
```

4. The startup sequence displays:

```
Splunk> All batbelt. No tights.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration...  Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _blocksignature _internal
_introspection _thefishbucket history main msad msexchange perfmon
sf_food_health sos sos_summary_daily summary windows wineventlog
winevents
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                               [  OK
 ]

Waiting for web server at http://127.0.0.1:8000 to be
available... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
```

```
The Splunk web interface is at http://localhost:8000
```

Start Splunk Enterprise without prompting, or by answering "yes" to any prompts

There are two other `start` options: `no-prompt` and `answer-yes`.

- If you run `$SPLUNK_HOME/bin/splunk start --no-prompt`, Splunk Enterprise proceeds with startup until it has to ask a question. Then, it displays the question and why it has to quit, and quits. In this scenario, it does not prompt for administrator credentials. You must manually create the credentials and restart before you can log in. See "Create administrator credentials manually" later in this topic for the procedure.
- If you run `SPLUNK_HOME/bin/splunk start --answer-yes`, Splunk Enterprise proceeds with startup and automatically answers "yes" to all yes/no questions that it encounters during startup. It displays each question and answer as it continues.

If you run start Splunk Enterprise with all three options in one line, the following happens:

- The software accepts the license automatically and does not ask you to accept it.
- The software answers "yes" to any "yes/no" question.
- The software quits if it encounters a question that cannot be answered "yes" or "no".

Change where and how Splunk Enterprise starts

To learn how to change system environment variables that control how Splunk Enterprise starts and operates, see "Set or change environment variables" in the Admin manual.

Create administrator credentials manually

If you start Splunk Enterprise for the first time and use the `--no-prompt` CLI argument, Splunk Enterprise can start without an administrator user, which prevents login. To fix this problem, you must create the credentials and then restart Splunk Enterprise.

1. Stop Splunk Enterprise:

```
./splunk stop
```

2. With a text editor, create `$SPLUNK_HOME/etc/system/local/user-seed.conf`, substituting `$SPLUNK_HOME` for where you installed the software.
3. Within the file, add the following lines, substituting a password for `your new password`:

   ```
   [user_info]
   USERNAME = admin
   PASSWORD = <your new password>
   ```
4. Save the file and close it.
5. Restart Splunk Enterprise by following the instructions shown earlier in this topic.

For more information on administrator credential creation, including password management for automated installations, see Create a secure administrator password in *Securing Splunk Enterprise*.

Troubleshoot Splunk Enterprise not starting the first time

If you encounter a situation where Splunk Enterprise does not start, especially after an upgrade, confirm that you have not passed any illegal arguments to the Splunk CLI as part of the start process. If you have passed illegal arguments, rerun the `splunk start` command without the arguments.

Launch Splunk Web

With a supported web browser, navigate to:

```
http://<host name or ip address>:8000
```

Use whatever host and port you chose during installation.

What happens next?

Now that you have Splunk Enterprise installed on one server, here are some links to get started:

- Learn what Splunk Enterprise is, what it does, and how it's different.
- Learn how to add your data to Splunk Enterprise. See What Splunk software can monitor in *Getting Data In*.

- Learn how to add Splunk users and roles. See About users and roles in *Securing Splunk Enterprise*.
- Learn how to estimate storage requirements for your data. See Estimate your storage requirements in *Capacity Planning*.
- Learn how to plan your Splunk Enterprise deployment, from gigabytes to terabytes per day. See the Capacity Planning Manual.
- Learn how to search, monitor, report, and more. See the Search Tutorial.
- One big way that Splunk Enterprise differs from traditional technologies is that it **classifies and interprets data at search-time**. See What is Splunk Knowledge?.

If you downloaded Splunk Enterprise packaged with an **app** (for example, Splunk + WebSphere), go to Splunk Web and select the app in Launcher to go directly to the app setup page. To see more information about the setup and deployment for a packaged app, search for the app name on Splunkbase.

Learn about accessibility to Splunk Enterprise

Splunk is dedicated to maintaining and enhancing its accessibility and usability for users of assistive technology (AT), both in accordance with Section 508 of the United States Rehabilitation Act of 1973, and in terms of best usability practices. This topic discusses how Splunk addresses accessibility within the product for users of AT.

Accessibility of Splunk Web and the CLI

The Splunk Enterprise command line interface (CLI) is fully accessible, and includes a superset of the functions available in Splunk Web. The CLI is designed for usability for all users, regardless of accessibility needs, and Splunk therefore recommends the CLI for users of AT (specifically users with low or no vision, or mobility restrictions).

Splunk also understands that use of a GUI is occasionally preferred, even for non-sighted users. As a result, Splunk Web is designed with the following accessibility features:

- Form fields and dialog boxes have on-screen indication of focus, as supported by the Web browser.
- No additional on-screen focus is implemented for links, buttons or other elements that do not have browser-implemented visual focus.

- Form fields are consistently and appropriately labeled, and ALT text describes functional elements and images.
- Splunk Web does not override user-defined style sheets.
- Data visualizations in Splunk Web have underlying data available via mouse-over or output as a data table, such that information conveyed with color is available without color.
- Most data tables implemented with HTML use headers and markup to identify data as needed.
- Data tables presented using Flash visually display headers. Underlying data output in comma separated value (CSV) format have appropriate headers to identify data.

Accessibility and real-time search

Splunk Web does not include any blinking or flashing components. However, using real-time search causes the page to update. Real-time search is easily disabled, either at the deployment or user/role level. For greatest ease and usability, Splunk recommends the use of the CLI with real-time functionality disabled for users of AT (specifically screen readers). See How to restrict usage of real-time search in the *Search Manual* for details on disabling real-time search.

Keyboard navigation using Firefox and Mac OS X

To enable Tab key navigation in Firefox on Mac OS X, use system preferences instead of browser preferences. To enable keyboard navigation:

1. In the menu bar, click **[Apple icon] > System Preferences > Keyboard** to open the Keyboard preferences dialog.
2. In the Keyboard preferences dialog, click the **Keyboard Shortcuts** button at the top.
3. Near the bottom of the dialog, where it says **Full Keyboard Access,** click the **All controls** radio button.
4. Close the Keyboard preferences dialog.
5. If Firefox is already running, exit and restart the browser.

Install a Splunk Enterprise license

About Splunk Enterprise licenses

Splunk Enterprise takes in data from sources you designate and processes it so that you can analyze it. This process is called **indexing**. For information about the indexing process, see What Splunk Enterprise does with your data in *Getting Data In*.

Splunk Enterprise licenses specify how much data you can index per day.

For more information about Splunk licenses, see the following:

- How Splunk licensing works in the *Admin* manual.
- Types of Splunk Enterprise licenses in the *Admin* manual.
- More about Splunk Free in the *Admin* manual.

Install a license

After you install Splunk Enterprise, you must install a license within 60 days to continue using all of the features of the product.

Before you proceed, you might want to review these topics on licensing:

- See How Splunk licensing works in the *Admin Manual* for an introduction to Splunk licensing.
- See Allocate license volume in the *Admin Manual* for information about allocating license volume across Splunk Enterprise instances.
- See Types of Splunk software licenses in the *Admin Manual* to compare license types and learn which licenses can be combined, and which cannot.

Add a new license

If you install a Dev/Test license with an Enterprise license, the Enterprise license file will be replaced.

1. Navigate to **Settings > Licensing**.
2. Click **Add license**.

3. Either click **Choose file** and navigate to your license file and select it, or click **copy & paste the license XML directly...** and paste the text of your license file into the provided field.
4. Click **Install**. Splunk Enterprise installs your license.
5. If this is the first Enterprise license that you are installing, restart Splunk Enterprise.

License violations

License violations occur when you exceed the maximum daily indexing volume allowed for your license. If you exceed your licensed daily volume on any one calendar day, you receive a violation *warning*. The warning persists for 14 days. If you incur 5 or more warnings on an Enterprise license or 3 warnings on a Free license in a rolling 30-day period, you are in *violation* of your license.

Unless you have a Splunk Enterprise 6.5.0 or later "no-enforcement" license, Splunk Enterprise disables search for the offending license pools. Search capabilities return when you have fewer than 5 (Enterprise) or 3 (Free) warnings in the previous 30 days, or when you apply a temporary reset license (available for Enterprise only). To obtain a reset or "no-enforcement" license, contact your sales rep.

Summary indexing volume does not count against your license.

If you get a violation warning, you have until midnight (using the time on the license master) to resolve it before it counts against the total number of warnings within the rolling 30-day period.

During a license violation period:

- Splunk never stops indexing your data. Splunk only blocks search while you exceed your license.
- Splunk does not disable searches to the `_internal` index. This means that you can still access the Indexing Status dashboard or run searches against `_internal` to diagnose the licensing problem.

If you have license violations, see About license violations in the Admin Manual or Troubleshooting indexed data volume from the Splunk Community Wiki.

More licensing information is available in the "Manage Splunk licenses" chapter in the Admin Manual.

Upgrade or migrate Splunk Enterprise

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 7.2?

See Welcome to Splunk Enterprise 7.2 in the Release Notes for a full list of the new features that are available in 7.2.

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 7.2: 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 7.2:

- Upgrade on *nix
- Upgrade on Windows

Upgrade from 6.4 and earlier

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

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 this version.

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 this version.

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.

About upgrading to 7.2 READ THIS FIRST

Read this topic before you upgrade to learn important information and tips about the upgrade process to version 7.2 from a lower version.

Splunk App and Add-on Compatibility

Not all Splunk apps and add-ons are compatible with Splunk Enterprise version 7.2. Visit Splunkbase to confirm that your apps are compatible with Splunk Enterprise version 7.2.

If you use Enterprise Security version 5.0.x or lower, do not upgrade to Splunk Enterprise version 7.2. This version of Splunk Enterprise is not compatible with Splunk Enterprise Security versions 5.0.x and lower.

Upgrade clustered environments

To upgrade an indexer cluster, see Upgrade an indexer cluster in *Managing Indexers and Clusters of Indexers*. Those instructions supersede the upgrade material in this manual.

To upgrade a search head cluster, see Upgrade a search head cluster in *Distributed Search*. Those instructions supersede the upgrade material in this manual.

Upgrade paths

Splunk Enterprise supports the following upgrade paths to version 7.2 of the software:

- From version 6.5 or higher to 7.2 on full Splunk Enterprise.
- From version 6.5 or higher to 7.2 on Splunk universal forwarders.

If you run a version of Splunk Enterprise lower than 6.5:

1. Upgrade from your current version to version 6.5.
2. Upgrade to version 7.2.

See About upgrading to 6.5 - READ THIS FIRST for tips on migrating your instance to version 6.5.

Important upgrade information and changes

Here are some things that you should be aware of when installing the new version:

Significant tsidx performance improvements are turned off by default

Splunk Enterprise 7.2 introduces a change to the file format of tsidx index files, resulting in significant size reduction. The reduced file size leads to improved search performance through decreased I/O, improved utilization of SmartStore caches, and so on.

This change is beneficial under all circumstances. However, to upgrade multisite indexer clusters without search interruption, it is necessary to defer the format change until after the upgrade completes and all peer nodes can switch to the new format simultaneously. For this reason, Splunk Enterprise 7.2 ships with the feature turned off by default.

Turn this feature on, immediately after you complete your 7.2 upgrade.

To turn on the feature, edit `indexes.conf` on each indexer (or, in the case of indexer clusters, in the master node's configuration bundle). Set `tsidxWritingLevel` to 2. Make this change in the default section of the file, so that it applies to all indexes:

```
[default]
tsidxWritingLevel=2
```

Upgrades to App Key Value Store require database resynchronization in the event of a need to downgrade Splunk Enterprise

When you upgrade to version 7.2 of Splunk Enterprise, the database for App Key Value Store (also known as KV store) also gets upgraded. This can result in problems in a case where you need to downgrade from version 7.2 back to version 7.1.

If you need to downgrade Splunk Enterprise to version 7.1 or lower for any reason, then, before you start the downgrade, run the following command from a shell prompt or PowerShell window to resync KV Store for the lower version:

```
curl -u username:password -XPOST
https://<splunk>:8089/services/kvstore/resync/resync?featureCompatibilityVersion=3.4
```

You must run this command before you commence downgrade activities on the instance.

Splunk Enterprise uses a new cipher suite and message authentication code for inter-Splunk communication

Splunk Enterprise 7.2 introduces a new cipher suite and message authentication code (MAC) that replaces the existing cipher suite that was responsible for securely handling inter-Splunk communications.

The new suite and MAC are not compatible with the old suite. Splunk instances that run version 7.2 and higher of Splunk software have been configured by default to allow inter-Splunk communication using both the new and old suites. However, if you later configure a 7.2 or higher instance to run only the new suite and MAC, inter-Splunk communication between versions that run only the old suite is not possible. You cannot configure lower versions of Splunk software to use the new suite.

For more information about the changes, see Configure secure inter-Splunk communications with updated cipher suite and message authentication code in *Securing Splunk Enterprise*.

The new Splunk credentials scheme might affect scripted upgrades

Splunk Enterprise 7.1 introduced a new password scheme for Splunk software users. In version 7.2, the scheme has been extended to let you customize administrator credential creation for Splunk Enterprise instances.

This scheme includes additional settings and configuration options, which can affect how you upgrade if you use scripts to automate the upgrade process. You might need to change your upgrade scripts before performing scripted upgrades. Specifically, confirm that you do not pass any illegal arguments to the Splunk CLI for starting or restarting Splunk Enterprise during the upgrade, as this could result in a situation where Splunk Enterprise does not start after the upgrade has completed.

The new Splunk credentials scheme might affect new scripted installations

While the software retains existing credentials during an upgrade, if you perform scripted installations, those installations might be affected significantly by the new credential scheme. You might need to modify your scripts before you perform scripted installations with version 7.2 and higher of the software. Carefully read the following topics to understand the updated installation process:

- Install on Linux in the *Installation Manual*
- Install on Windows using the command line in the *Installation Manual*

For more information on the updated password policy, see Password best practices for administrators.

Additionally, your Splunk administrator might introduce password eligibility requirements that affect you if you change your password after an upgrade. See Configure Splunk password policies in *Securing Splunk Enterprise* for additional information.

The Splunk Web user interface has been updated significantly

Splunk Web has been refreshed with a new, improved look. While many user interface controls remain the same as they were in previous versions, the interface looks different than before, and some items have been relocated. This might cause confusion for those who have become accustomed to the previous interface.

Support for the ext2 (second extended) file system on Linux has been removed

(Originally introduced in version 7.1)

Support for the ext2 file system on Linux operating systems has been removed. If you still run an ext2 file system on a Linux machine that runs Splunk Enterprise, you must upgrade that filesystem on that machine to a minimum of ext3 before you upgrade Splunk Enterprise.

Data model searches now only use fields that have been defined within the data model

(Originally introduced in version 7.1)

When you upgrade to version 7.2 of Splunk Enterprise, data model searches can only use field names that have been defined within the data model. Splunk Enterprise no longer automatically extracts field names.

Additionally, if you have a data model search that references an automatically extracted field name that contains whitespace, you must work around the fact that data models do not allow field names that contain whitespace.

Scheduled views reaper might increase disk I/O and CPU usage on startup

(Originally introduced in version 7.1)

When you upgrade to version 7.2 of Splunk Enterprise, a new process that checks and removes orphaned scheduled views (saved searches or reports that generate PDFs on a schedule) runs. This happens when Splunk Enterprise starts, and might result in increased disk I/O and CPU usage on startup.

The default color scheme for choropleth maps has changed

(Originally introduced in version 7.1)

The color scheme for choropleth maps and single-value visualizations has changed in Splunk Enterprise 7.2. Existing visualizations will be retained through the upgrade, but any new visualizations that you create after an upgrade will use the new color scheme.

HTTP Event Collector now cleans up idle indexer ACK channels by default

(Originally introduced in version 7.1)

After an upgrade to version 7.2 of Splunk Enterprise, the HTTP Event Collector now cleans up any indexer ACK channels it finds that have an idle time of more than 'maxIdleTime' seconds, as defined by that setting in the inputs.conf configuration file, by default. While this results in improved HEC performance, you might experience a slight increase in network and CPU activity during the cleanup.

Modified navigation menus in default Splunk apps will be removed after upgrade

(Originally introduced in version 7.1)

After an upgrade to version 7.2 of Splunk Enterprise, any modifications that you have made to navigation menus in default Splunk apps will be removed.

As a reminder, you should not make edits to default apps or configurations, as they can be and, in nearly all cases, are removed after an upgrade. Edit local configurations rather than making modifications to Splunk default configurations and apps.

Stats percentile results might shift by a few percent

(Originally introduced in version 7.0)

Splunk software computes percentiles and median in stats and related commands (`tstats`, `streamstats`, `eventstats`, `chart`, `timechart`, `sistats`, `sichart`, `sitimechart`) using an approximation algorithm (unless you use the `exactperc` aggregation function). Before Splunk Enterprise 7.0, these commands used an approximation algorithm called `rdigest`. After you upgrade, the default digest behavior changes to `tdigest`, which has been shown to be more performant than `rdigest` in some cases, metrics data in particular.

Reports that use percentiles and medians might emit slightly different results upon an upgrade to Splunk Enterprise 7.0. The difference is usually small (less than 1%) but could be greater for highly skewed datasets. After the initial shift, `stats` continues using the new digest method and does not produce another shift unless you switch back to using the `rdigest` method.

If you want, you can revert the digest behavior globally in `limits.conf`. The behavior for `stats`, `tstats`, `streamstats`, `eventstats`, `chart`, and `timechart` are controlled by the setting in the `stats` stanza. The behavior for `sistats`, `sichart`, and `sitimechart` are controlled by the setting in the `sistats` stanza.

See limits.conf.spec in the *Admin Manual*.

The use of disabled lookups in searches or other lookups is no longer allowed

(Originally introduced in version 7.0)

You can no longer use a disabled lookup as part of a search or other lookup. After you upgrade, when you attempt to use a disabled lookup, you receive the error message `The lookup table '<lookup name>' is disabled`.

The ability to customize the number of reports retrieved might reduce browser performance

(Originally introduced in version 7.0)

You can now increase or decrease the number of reports that Splunk Web can retrieve at a time by modifying an entry in `web.conf`. If you increase the number of reports that can be retrieved after you upgrade, you might cause problems with browser performance due to the number of reports available.

SPL operator keywords can break saved searches

(Originally introduced in version 6.6)

As of version 6.6 of Splunk Enterprise, new SQL-style search processing language (SPL) keywords were introduced, such as `IN` and `OR`. These new keywords can potentially break existing saved searches after an upgrade if those searches contain these new keywords (for example, `search country=IN` or `search state=OR`.

Before you upgrade, review existing saved searches and add quotes around any searches that contain these new operators (for example, `search country="IN"` or `search state="OR"`.) For more information on these operators, see the search command usage information in the *Search Reference* Manual.

A new load-balancing scheme for forwarders is available

(Originally introduced in version 6.6)

All forwarder types now have a new scheme for balancing load between receiving indexers.

In addition to balancing load by time, they can also balance load by amount of data sent. The `autoLBVolume` setting in `outputs.conf` controls this setting.

See Choose a load balancing method in *Forwarding Data* for additional information.

Connectivity over SSL between version 7.0 and version 5.0 and lower is disabled by default

(Originally introduced in version 6.6)

Because of changes to the security ciphers in version 7.0 of Splunk Enterprise, instances of Splunk software that run on version 5.0 or less cannot connect to instances of version 7.0 or greater by default.

When you upgrade, any instances that run version 5.0 or lower no longer communicates with the upgraded instance over SSL. For a workaround, you can edit `inputs.conf` and `outputs.conf` on the sending instances to enable ciphers that allow communication between the instances.

For more information, see the Known Issues - Upgrade Issues page in the Splunk Enterprise 6.6.0 *Release Notes*.

Data model acceleration sizes on disk might appear to increase

(Originally introduced in version 6.6)

If you have created and accelerated a custom data model, the size that Splunk software reports it as being on disk has increased.

When you upgrade, data model acceleration summary sizes can appear to increase by a factor of up to two to one. This apparent increase in disk usage is the result of a refactoring of how Splunk software calculates data model acceleration summary disk usage. The calculation that Splunk software performs in version 7.0 is more accurate than in previous versions.

The number of potential data model acceleration searches has increased

(Originally introduced in version 6.6)

The default number of concurrent searches that are used for data model acceleration has been increased from two to three.

If you have an environment that uses data models, that have not yet been accelerated, Splunk software might run up to three searches to accelerate the data models. This can result in increased CPU, memory, and disk usage on the search heads that are accelerating the data models and can also cause more concurrent searches overall in an environment where the search heads are not clustered.

Security changes in SSL and TLS could affect customers who use LDAP

(Originally introduced in version 6.6)

If you have configured Splunk software to use the Lightweight Directory Access Protocol (LDAP) to authenticate, after an upgrade, changes in security settings for Secure Sockets Layer (SSL) and Transport Layer Security (TLS) could prevent the software from connecting to the LDAP server.

If that occurs, you can roll back the updated settings by doing the following:

1. Open `$SPLUNK_HOME/etc/openldap/ldap.conf` for editing with a text editor.
2. Comment the lines that begin with the following:

   ```
   #TLS_PROTOCOL_MIN ...
   #TLS_CIPHER_SUITE ...
   ```
3. Save the `ldap.conf` file and close it.
4. Restart Splunk software.

The 'autoLB' universal forwarder setting in outputs.conf is no longer configurable

(Originally introduced in version 6.6)

The `autoLB` setting, which controls how universal forwarders send data to indexers, and which only had a valid setting of `true`, has been locked to that value. Since auto-loadbalancing is the only way that forwarders can send data, there is no longer a reason to make that setting configurable. Universal forwarders will now ignore attempts to configure the setting to anything other than `true`.

You might notice an error about a bad configuration for `autoLB` during the startup check. You can safely ignore this error.

The 'compressed' settings on a forwarder and a receiving indexer no longer must match for the instances to communicate

(Originally introduced in version 6.6)

Forwarders and indexers now auto-negotiate their connections. After an upgrade, it is no longer necessary for you to confirm that the `compressed` setting in an `outputs.conf` stanza on the forwarder matches the corresponding `compressed` setting in a `splunktcp://` stanza in `inputs.conf` on the receiver for the forwarder-receiver connection to work.

Indexers in a distributed Splunk environment now respect the INDEXED setting in fields.conf on search heads only

(Originally introduced in version 6.6)

To better align with documented best practice, the way that indexers handle the `INDEXED` setting in `fields.conf` has changed.

Indexers now respect the setting as it has been configured on search heads only. When you upgrade, if you have only configured this setting in `fields.conf` on indexers, you must configure it on the search heads if it is not there.

Use different settings for better data distribution between indexers in a load-balanced forwarder configuration

(Originally introduced in version 6.6)

If you have a setup where universal forwarders have been configured to send data to indexers in a load-balanced scheme, you should replace configurations that have `forceTimeBasedAutoLB` with those that use `EVENT_BREAKER_ENABLE` and `EVENT_BREAKER` instead. For more information about these new settings, see Configure load balancing for Splunk Enterprise in the *Universal Forwarder Manual*.

Protection for the '/server/info' REST endpoint is now on by default

(Originally introduced in version 6.6)

In version 6.5 of Splunk Enterprise, a setting was introduced to require authentication to access the `server/info` REST endpoint.

After you upgrade, this protection is enabled by default.

Memory usage on indexers increases during indexing operations

(Originally introduced in version 6.5)

When you upgrade to version 7.0 of Splunk Enterprise, the amount of memory that indexers use during indexing operations increases. If you have configured an indexer with parallelization (multiple indexing pipelines), the usage increase can be significant.

Indexers that have been configured with a single indexing pipeline, which is the default for a Splunk Enterprise installation, see memory usage increases of up to 10%. Indexers that have two pipeline sets see increases of up to 15%. Indexers that have been configured with four indexing pipelines see increases of up to 25%.

Confirm that your indexers meet or exceed the minimum hardware specifications that the *Capacity Planning Manual* details before you perform an upgrade. See Reference hardware for memory details for each host.

The free version of Splunk now includes App Key Value Store

(Originally introduced in version 6.5)

When you upgrade to version 7.0 of Splunk Enterprise, the free version of Splunk Enterprise gets access to the App Key Value Store feature.

This change results in processes running on your host that support App Key Value Store. These processes might result in extra memory or disk space usage.

The instrumentation feature adds an internal index and can increase disk space usage

(Originally introduced in version 6.5)

The instrumentation feature of Splunk Enterprise, which lets you share Splunk Enterprise performance statistics with Splunk after you opt in, includes a new internal index which can cause disk space usage to rise on hosts that you upgrade. You can opt out of sharing performance data by following the instructions at Share data in Splunk Enterprise in the *Admin Manual*.

Certain JSChart limits have been increased which might reduce performance in older browsers

(Originally introduced in version 6.5)

The number of series, results, and data points that a JSChart chart element can display has been increased.

The number of series has doubled from 50 to 100. The number of results that can be displayed has increased from 1000 to 10,000. The number of total data points has increased from 20,000 to 50,000.

If you have not already changed the defaults for these JSChart elements, then you will see more data points on your JSChart elements after an upgrade. If you use an older browser to interact with Splunk Enterprise, you might also see slightly reduced performance.

A new capability 'deleteIndexesAllowed' has been added that inhibits index deletion

(Originally introduced in version 6.5)

A new user capability, `deleteIndexesAllowed`, has been added. Non-administrator user roles must hold this capability before they can delete indexes. After you upgrade, you can assign this capability to any non-administrator user roles so that they can delete indexes.

User roles must also hold the "delete_by_keyword" capability to delete indexes.

Windows-specific changes

The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cipher suites in version 7.2 are not supported on Windows Server 2008 R2

(Originally introduced in version 6.6)

The TLS and SSL cipher suites that come with version 7.2 of Splunk Enterprise do not support Windows Server 2008 R2 by default. If you upgrade, and you used SSL and TLS to handle forwarder-to-indexer communication or alert actions, those actions will not work until you make updates to both Windows and Splunk Enterprise configurations.

See About TLS encryption and cipher suites in *Securing Splunk Enterprise* for instructions on how to configure Windows Server 2008 R2 and Splunk Enterprise to use the new cipher suites.

The Windows Event Log monitoring input has improved performance, new settings, and changes in behavior

(Originally introduced in version 6.6)

The Windows Event Log monitoring input now has improved performance. Owing to improved efficiencies in how the input retrieves and processes events, it provides up to twice the performance as previous versions. To improve performance further, several new input settings have been added. Also, the input now respects the `checkpointInterval` setting in an Event Log monitoring stanza. For additional information about the changes, see Monitor Windows Event Log data in *Getting Data In.*

Before you upgrade:

- Review your Event Log monitoring input stanzas and confirm that the `checkpointInterval` setting is not set to something very large. Large settings might result in a large number of duplicate events after Splunk Enterprise restarts from a crash. If you have not already set `checkpointInterval` then you do not need to set it now.
- Confirm that the machines that retrieve Windows Event Log data meet or exceed the minimum requirements as described in System Requirements for user of Splunk Enterprise on-premises. In particular, if the timely arrival of Event Log events is critical for your organization, any machines that use the input must conform with those requirements.

The Windows universal forwarder installation package no longer includes the Splunk Add-on for Windows

(Originally introduced in version 6.5)

The installation package for the universal forwarder no longer includes the Splunk Add-on for Windows. If you need the add-on, you must download and install it separately.

The installer does not delete existing installations of the add-on.

Support for Internet Explorer versions 9 and 10 has been removed

(Originally introduced in version 6.5)

Microsoft has announced that support for all versions of Internet Explorer below version 11 has ended as of January 12, 2016. Owing to that announcement, Splunk has ended support for Splunk Web for these same versions. This might result in a suboptimal browsing experience in lower versions of Internet Explorer.

When you upgrade, also upgrade the version of Internet Explorer that you use to 11 or higher. An alternative is to use another browser that Splunk supports.

Learn about known upgrade issues

To learn about any additional upgrade issues for Splunk Enterprise, see the Known Issues - Upgrade Issues page in the *Release Notes*.

How to upgrade a distributed Splunk Enterprise environment

Distributed Splunk Enterprise environments vary widely. Some have multiple indexers or search heads, some have search head pools, and others have indexer- and search-head clusters. These types of environments present challenges over upgrading single-instance installations.

Determine the upgrade procedure to follow for your type of environment

Depending on the kind of distributed environment you have, you might have to follow separate instructions to complete the upgrade. This topic provides guidance on how to upgrade distributed environments that do not have any clustered elements like index- or search-head clusters. It also has information on how to upgrade environments that use the deprecated **search head pool** feature. Environments with clustered elements, such as indexer clusters and search head clusters, have different upgrade procedures in different topics.

- To upgrade a distributed environment that has a search head pool or does not have any clustered elements, follow the procedures in this topic.
- To upgrade an environment with index clusters, see Upgrade an indexer cluster in *Managing Indexers and Clusters of Indexers*.
- To upgrade an environment with search head clusters, see Upgrade a search head cluster in *Distributed Search*.
- If you have additional questions about upgrading your distributed Splunk Enterprise environment, log a case at the Splunk Support Portal.

Cross-version compatibility between distributed components

While there is some range in compatibility between various Splunk software components, they work best when they are all at a specific version. If you have to upgrade one or more components of a distributed deployment, you should confirm that the components you upgrade remain compatible with the components that you don't.

- For information on compatibility between differerent versions of **search heads** and **search peers** (indexers), see System requirements and other deployment considerations for distributed search in *Distributed Search*.
- For information on compatibility between indexers and forwarders, see Compatibility between forwarders and indexers in *Forwarding Data*.

Test apps prior to the upgrade

Before you upgrade a distributed environment, confirm that Splunk apps work on the version of Splunk Enterprise that you want to upgrade to. You must test apps if you want to upgrade a distributed environment with a search head pool, because search head pools use shared storage space for apps and configurations.

When you upgrade, the migration utility warns of apps that need to be copied to shared storage for pooled search heads when you upgrade them. It does not copy them for you. You must manually copy updated apps, including apps that ship with Splunk Enterprise (such as the Search app) - to shared storage during the upgrade process. Failure to do so can cause problems with the user interface after you complete the upgrade.

1. On a reference machine, install the full version of Splunk Enterprise that you currently run.
2. Install the apps on this instance.

3. Access the apps to confirm that they work as you expect.
4. Upgrade the instance.
5. Access the apps again to confirm that they still work.

If the apps work as you expect, move them to the appropriate location during the upgrade of your distributed environment:

- If you use non-pooled search heads, move the apps to `$SPLUNK_HOME/etc/apps` on each search head during the search head upgrade process.
- If you use pooled search heads, move the apps to the shared storage location where the pooled search heads expect to find the apps.

Upgrade a distributed environment with multiple indexers and non-pooled search heads

This procedure upgrades the search head tier, then the indexing tier, to maintain availability.

Prepare the upgrade

1. Confirm that any apps that the non-pooled search heads use will work on the upgraded version of Splunk, as described in "Test your apps prior to the upgrade" in this topic.
2. (Optional) If you use a **deployment server** in your environment, disable it temporarily. This prevents the server from distributing invalid configurations to your other components.
3. (Optional) Upgrade the deployment server, but do not restart it.

Upgrade the search heads

1. Disable one of the search heads.
2. Upgrade the search head. Do not let it restart.
3. After you upgrade the search head, place the confirmed working apps into the `$SPLUNK_HOME/etc/apps` directory of the search head.
4. Re-enable and restart the search head.
5. Test apps on the search head for operation and functionality.
6. If there are no problems with the search head, then disable and upgrade the remaining search heads, one by one. Repeat this step until you have reached the last search head in your environment.
7. (Optional) Test each search head for operation and functionality after you bring it up.

8. After you upgrade the last search head, test all of the search heads for operation and functionality.

Upgrade the indexers

1. Disable and upgrade the indexers, one by one. You can restart the indexers immediately after you upgrade them.
2. Test search heads to ensure that they find data across all indexers.
3. After you upgrade all indexers, restart your deployment server.

Upgrade a distributed environment with multiple indexers and pooled search heads

If your distributed environment has **pooled search heads**, the process to upgrade the environment becomes significantly more complex. If your organization has restrictions on downtime, use a maintenance window to perform this upgrade.

Following are the key concepts to upgrade this kind of environment.

- Pooled search heads must be enabled and disabled as a group.
- The version of Splunk Enterprise on all pooled search heads must be the same.
- You must test apps and configurations that the search heads use prior to upgrading the search head pool.

If you have additional concerns about this guidance here, you can log a case through the Splunk Support Portal.

To upgrade a distributed Splunk environment with multiple indexers and pooled search heads:

Prepare the upgrade

See "Configure search head pooling" in the *Distributed Search* manual for instructions on how to enable and disable search head pooling on each search head.

1. Confirm that any apps that the pooled search heads use will work on the upgraded version of Splunk Enterprise, as described in "Test your apps prior to the upgrade" in this topic.
2. If you use a **deployment server** in your environment, disable it temporarily. This prevents the server from distributing invalid

configurations to your other components.

3. Upgrade your deployment server, but do not restart it.
4. Designate a search head in your search head pool to upgrade as a test for functionality and operation.
5. For the remainder of these instructions, refer to that search head as "Search Head #1."

Note: You must remove search heads from a search head pool temporarily before you upgrade them. This must be done for several reasons:

- To prevent changes to the apps and user objects hosted on the search head pool shared storage.
- To stop the inadvertent migration of local apps and system settings to shared storage during the upgrade.
- To ensure that you have a valid local configuration to use as a fallback, should a problem occur during the upgrade.

If problems occur as a result of the upgrade, search heads can be temporarily used in a non-pooled configuration as a backup.

Upgrade the search head pool

Caution: Remove each search head from the search head pool before you upgrade it, and add it back to the pool after you upgrade. While you don't need to confirm operation and functionality of each search head, only one search head at a time can be up during the upgrade phase.

1. Bring down all of the search heads in your environment. At this point, searching capability becomes unavailable, and remains unavailable until you restart all of the search heads after upgrading.
2. Place the confirmed working apps in the search head pool shared storage area.
3. Remove Search Head #1 from the search head pool.
4. Upgrade Search Head #1.
5. Restart Search Head #1.
6. Test the search head for operation and functionality. In this case, "operation and functionality" means that the instance starts and that you can log into it. It does not mean that you can use apps or objects hosted on shared storage. It also does not mean distributed searches will run correctly.
7. If the upgraded Search Head #1 functions as desired, bring it down.
8. Copy the apps and user preferences from the search head to the shared storage.

9. Add the search head back to the search head pool.
10. Restart the search head.
11. Upgrade the remaining search heads in the pool with this procedure, one by one.

Restart the search heads

1. After you have upgraded the last search head in the pool, restart all of them.
2. Test all search heads for operation and functionality across all of the apps and user objects that are hosted on the search head pool.
3. Test distributed search across all of your indexers.

Upgrade the indexers

For information on version compatibility between search heads and indexers, see System requirements and other deployment considerations for distributed search in *Distributed Search*.

1. (Optional if you do not have downtime concerns) Choose an indexer to keep the environment running, and designate it as "Indexer #1".
2. (Optional if you do not have downtime concerns) Choose a second indexer to upgrade, and designate it as "Indexer #2."
3. If you need to maintain uptime, bring down all of the indexers except Indexer #1. Otherwise, bring all indexers down and continue at Step 7.
4. Upgrade Indexer #2.
5. Bring up Indexer #2 and test for operation and functionality.
6. Once you have confirmed proper operation on Indexer #2, bring down Indexer #1.
7. Upgrade Indexer #1 and all of the remaining indexers, one by one. You can restart the indexers immediately after you upgrade them.
8. Confirm operation and functionality across all of the indexers.
9. Restart the deployment server, and confirm its operation and functionality.

Upgrade forwarders

When you upgrade your distributed environment, you can also upgrade any universal forwarders in that environment. This is not required, however, and you might want to consider whether or not you need to. Forwarders are always compatible with later versions of indexers.

To upgrade universal forwarders, see the following topics in the *Universal Forwarder* manual.

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

Changes for Splunk App developers

If you develop apps for the Splunk platform, read this topic to find out what changes we've made to how the software works with apps in version 7.x, and how to migrate any existing apps to work with the new version.

Changes

- Updated Splunk Web user interface
- For other changes, or to learn more about Splunk app development, visit the Splunk Dev portal.

Visit the Splunk Dev portal

To learn more about Splunk app development, visit the Splunk Dev portal.

Upgrade to 7.2 on UNIX

Before you upgrade

Before you upgrade, see About upgrading to 7.2: READ THIS FIRST for information on changes in the new version that can impact you if you upgrade from an existing version.

Splunk Enterprise does not provide a means of downgrading to previous versions. If you need to revert to an older Splunk release, uninstall the upgraded version and reinstall the version you want.

Back your files up

Before you perform the upgrade, **back up all of your files**, including Splunk Enterprise configurations, indexed data, and binaries.

For information on backing up data, see Back up indexed data in the *Managing Indexers and Clusters Manual*.

For information on backing up configurations, see Back up configuration information in the *Admin Manual*.

How upgrading works

To upgrade a Splunk Enterprise installation, you must install the new version directly on top of the old version (into the same installation directory.) When Splunk Enterprise starts after an upgrade, it detects that the files have changed and asks whether or not you want to preview the migration changes before it performs the upgrade.

If you choose to view the changes before proceeding, the upgrade script writes the proposed changes to the `$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>` file.

Splunk Enterprise does not change your configuration until after you restart it.

Upgrade Splunk Enterprise

1. Open a shell prompt on the machine that has the instance that you want to upgrade.
2. Change to the `$SPLUNK_HOME/bin` directory.
3. Run the `$SPLUNK_HOME/bin/splunk stop` command to stop the instance.
4. Confirm that no other processes can automatically start Splunk Enterprise.
5. To upgrade and migrate, install the Splunk Enterprise package directly over your existing deployment.
    - If you use a `.tar` file, expand it into the same directory with the same ownership as your existing Splunk Enterprise instance. This overwrites and replaces matching files but does not remove unique files. `tar xzf splunk-7.x.x-<version-info>.tgz -C /splunk/parent/directory`
    - If you use a package manager, such as RPM, type `rpm -U splunk_package_name.rpm`
    - If you use a .dmg file on Mac OS X, double-click it and follow the instructions. Specify the same installation directory as your existing installation.
6. Run the `$SPLUNK_HOME/bin/splunk start` command.
   Splunk Enterprise displays the following output.

   ```
   This appears to be an upgrade of Splunk.
   --------------------------------------------------------------------------------
   Splunk has detected an older version of Splunk installed on this
   machine. To
   finish upgrading to the new version, Splunk's installer will
   automatically
   ```

```
update and alter your current configuration files. Deprecated
configuration
files will be renamed with a .deprecated extension.
You can choose to preview the changes that will be made to your
configuration
files before proceeding with the migration and upgrade:
If you want to migrate and upgrade without previewing the changes
that will be
made to your existing configuration files, choose 'y'.
If you want to see what changes will be made before you proceed
with the
upgrade, choose 'n'.
Perform migration and upgrade without previewing configuration
changes? [y/n]
```

7. Choose whether or not you want to run the migration preview script to see proposed changes to your existing configuration files, or proceed with the migration and upgrade right away. If you choose to view the expected changes, the script provides a list.
8. After you review these changes and are ready to proceed with migration and upgrade, run `$SPLUNK_HOME/bin/splunk start` again.

Upgrade and accept the license agreement simultaneously

After you place the new files in the Splunk Enterprise installation directory, you can accept the license and perform the upgrade in one command.

- To accept the license and view the expected changes (answer 'n') before continuing the upgrade, use the following command.

  ```
  $SPLUNK_HOME/bin/splunk start --accept-license --answer-no
  ```

- To accept the license and begin the upgrade without viewing the changes (answer 'y').

  ```
  $SPLUNK_HOME/bin/splunk start --accept-license --answer-yes
  ```

Upgrade to 7.2 on Windows

You can upgrade with either the GUI installer or the `msiexec` utility on the command line as described in "Install on Windows via the command line".

Splunk does not provide a means of downgrading to previous versions.

After you upgrade Splunk Enterprise, if you need to downgrade, you must uninstall the upgraded version and then reinstall the previous version of Splunk Enterprise that you were using. Do not attempt to install over an upgraded installation with an installer from a previous version, as this can result in a corrupt instance and data loss.

Before you upgrade

Before you upgrade, see About upgrading to 7.2: READ THIS FIRST for information on changes in the new version that can impact you if you upgrade from an existing version.

Splunk Enterprise does not provide a means of downgrading to previous versions. If you need to revert to an older Splunk release, uninstall the upgraded version and reinstall the version you want.

The Windows domain user must match what you specified at installation

If you installed Splunk Enterprise with a domain user, you must specify the same domain user explicitly during an upgrade. If you do not, Splunk Enterprise installs the upgrade as the Local System user. If you do not do this, or you specify the wrong user accidentally during the upgrade, then see Correct the user selected during installation to switch to the correct user before you start Splunk Enterprise.

Changing Splunk Enterprise ports during an upgrade is not supported

Splunk Enterprise does not support changing the management or Splunk Web ports when you upgrade. If you need to change these ports, do so either before or after you upgrade.

Back your files up

Before you upgrade, back up all of your files, including Splunk Enterprise configurations, indexed data, and binaries.

- For information on backing up data, see Back up indexed data in the *Managing Indexers and Clusters Manual*.
- For information on backing up configurations, see Back up configuration information in the *Admin Manual*.

Keep copies of custom certificate authority certificates

When you upgrade on Windows, the installer overwrites any custom certificate authority (CA) certificates that you have created in `%SPLUNK_HOME%\etc\auth`. If you have custom CA files, back them up before you upgrade. After the upgrade, you can restore them into `%SPLUNK_HOME%\etc\auth`. After you have restored the certificates, restart Splunk Enterprise.

Upgrade Splunk Enterprise using the GUI installer

1. Download the new MSI file from the Splunk download page.
2. Double-click the MSI file. The installer runs and attempts to detect the existing version of Splunk Enterprise installed on the machine. When it locates the older version, it displays a pane that asks you to accept the licensing agreement.
3. Accept the license agreement. The installer then installs the updated Splunk Enterprise. This method of upgrade retains all parameters from the existing installation. By default, the installer restarts Splunk Enterprise when the upgrade completes and places a log of the changes made to configuration files during the upgrade in `%TEMP%`.

Upgrade using the command line

1. Download the new MSI file from the Splunk download page.
2. Install the software, as described in Install on Windows via the command line.
   - If Splunk runs as a user other than the Local System user, specify the credentials for the user in your command-line instruction with the `LOGON_USERNAME` and `LOGON_PASSWORD` flags.
   - You can use the `LAUNCHSPLUNK` flag to specify whether Splunk Enterprise should start up automatically or not when the upgrade finishes, but you cannot change any other settings.
   - Do not change the network ports (`SPLUNKD_PORT` and `WEB_PORT`) at this time.
3. Depending on your specification, Splunk Enterprise might start automatically when you complete the installation.

Migrate a Splunk Enterprise instance from one physical machine to another

Important: These migration instructions are for on-premises Splunk Enterprise instances only.
If you are a Splunk Cloud customer or want to migrate your data from Splunk Enterprise to Splunk Cloud, do not use these instructions. Contact Professional Services for assistance.

You can migrate a Splunk Enterprise instance from one server, operating system, architecture, or filesystem to another, while maintaining the indexed data, configurations, and users. Migrating an instance of Splunk Enterprise different than upgrading one, which is merely installing a new version on top of an older one.

Do not attempt to migrate a Splunk Enterprise installation to Splunk Cloud using these instructions. Doing so could result in data loss. Speak with Professional Services or your Splunk Cloud representative for information and instructions.

When to migrate

There are a number of reasons to migrate a Splunk Enterprise install:

- Your Splunk Enterprise installation is on a host that you wish to retire or reuse for another purpose.
- Your Splunk Enterprise installation is on an operating system that either your organization or Splunk no longer supports, and you want to move it to an operating system that does have support.
- You want to switch operating systems (for example, from *nix to Windows or vice versa)
- You want to move your Splunk Enterprise installation to a different file system.
- Your Splunk Enterprise installation is on 32-bit architecture, and you want to move it to a 64-bit architecture for better performance.
- Your Splunk Enterprise installation is on a system architecture that you plan to stop supporting, and you want to move it to an architecture that you do support.

Considerations for migrating Splunk Enterprise

While migrating a Splunk Enterprise instance is simple in many cases, there are some important considerations to note when doing so. Depending on the type, version, and architecture of the systems involved in the migration, you might need to consider more than one of these items at a time.

When you migrate a Splunk Enterprise instance, note the following.

Differences in Windows and Unix path separators

The path separator (the character used to separate individual directory elements of a path) on *nix and Windows is different. When you move index files between these operating systems, you must confirm that the path separator you use is correct for the target operating system. You must also make sure that you update any Splunk configuration files (in particular, `indexes.conf`) to use the correct path separator.

For more information about how path separators can impact Splunk Enterprise installations, see Differences between *nix and Windows in Splunk operations in the *Admin* manual.

Windows permissions

When moving a Splunk Enterprise instance between Windows hosts, make sure that the destination host has the same rights assigned to it that the source host does. This includes but is not limited to the following:

- Ensure that the file system and share permissions on the target host are correct and allow access for the user that runs Splunk Enterprise.
- If Splunk Enterprise runs as an account other than the Local System user, that the user is a member of the local Administrators group and has the appropriate Local Security Policy or Domain Policy rights assigned to it by a Group Policy object

Architecture changes

If you downgrade the architecture that your Splunk Enterprise instance runs on (for example, 64-bit to 32-bit), you might experience degraded search performance on the new host due to the larger files that the 64-bit operating system and Splunk Enterprise instance created.

Distributed and clustered Splunk environments

When you want to migrate data on a distributed Splunk instance (that is, an indexer that is part of a group of search peers, or a search head that has been configured to search indexers for data), you should remove the instance from the distributed environment before attempting to migrate it.

Bucket IDs and potential bucket collision

If you migrate a Splunk Enterprise instance to another Splunk instance that already has existing indexes with identical names, you must make sure that the individual buckets within those indexes have bucket IDs that do not collide. Splunk Enterprise does not start if it encounters indexes with buckets that have colliding bucket IDs. When you copy index data, you might need to rename the copied bucket files to prevent this condition.

How to migrate

When you migrate on *nix systems, you can extract the tar file you downloaded directly over the copied files on the new system, or use your package manager to upgrade using the downloaded package. On Windows systems, the installer updates the Splunk files automatically.

1. Stop Splunk Enterprise on the host from which you want to migrate.
2. Copy the entire contents of the $SPLUNK_HOME directory from the old host to the new host.
3. Install the appropriate version of Splunk Enterprise for the target platform.
4. Confirm that index configuration files (indexes.conf) contain the correct location and path specification for any non-default indexes.
5. Start Splunk Enterprise on the new instance.
6. Log into Splunk Enterprise with your existing credentials.
7. After you log in, confirm that your data is intact by searching it.

How to move index buckets from one host to another

If you want to retire a Splunk Enterprise instance and immediately move the data to another instance, you can move individual buckets of an index between hosts, as long as:

When you copy individual bucket files, you must make sure that no bucket IDs conflict on the new system. Otherwise, Splunk Enterprise does not start. You might need to rename individual bucket directories after you move them from the source system to the target system.</code>

1. Roll any hot buckets on the source host from hot to warm.
2. Review indexes.conf on the old host to get a list of the indexes on that host.
3. On the target host, create indexes that are identical to the ones on the source system.
4. Copy the index buckets from the source host to the target host.

5. Restart Splunk Enterprise.

Uninstall Splunk Enterprise

Uninstall Splunk Enterprise

Learn how to remove Splunk Enterprise from a host by following the procedures in this topic.

Prerequisites

1. If you configured Splunk Enterprise to start on boot, remove it from your boot scripts before you uninstall.

   ```
   ./splunk disable boot-start
   ```
2. Stop Splunk Enterprise. Navigate to `$SPLUNK_HOME/bin` and type `./splunk stop` (or just `splunk stop` on Windows).

Uninstall Splunk Enterprise with your package management utilities

Use your local package management commands to uninstall Splunk Enterprise. In most cases, files that were not originally installed by the package will be retained. These files include your configuration and index files which are under your installation directory.

In these instructions, `$SPLUNK_HOME` refers to the Splunk installation directory. On Windows, this is `C:\Program Files\Splunk` by default. For most Unix platforms, the default installation directory is `/opt/splunk`. On Mac OS X, it is `/Applications/splunk`.

RedHat Linux

```
rpm -e splunk_product_name
```

Debian Linux

```
dpkg -r splunk
```

Remove all Splunk files, including configuration files

```
dpkg -P splunk
```

Other things you might want to delete

- If you created any indexes and did not use the Splunk Enterprise default path, you must delete those directories as well.
- If you created a user or group for running Splunk Enterprise, you should also delete them.

Windows

- Use the **Add or Remove Programs** option in the Control Panel. In Windows 7, 8.1, and 10, and Windows Server 2008 R2 and 2012 R2, that option is available under **Programs and Features.**
- (Optional) You can also uninstall Splunk Enterprise from the command line by using the `msiexec` executable against the Splunk installer package.

  ```
  msiexec /x splunk-<version>-x64.msi
  ```

Under some circumstances, the Microsoft installer might present a reboot prompt during the uninstall process. You can safely ignore this request without rebooting.

Uninstall Splunk Enterprise manually

If you can't use package management commands, use these instructions to uninstall Splunk Enterprise.

1. Stop Splunk Enterprise.

   ```
   $SPLUNK_HOME/bin/splunk stop
   ```
2. Find and `kill` any lingering processes that contain "splunk" in their name.
   For Linux

   ```
   kill -9 `ps -ef | grep splunk | grep -v grep | awk '{print $2;}'`
   ```

   For Mac OS

```
kill -9 `ps ax | grep splunk | grep -v grep | awk '{print $1;}'`
```

3. Remove the Splunk Enterprise installation directory, `$SPLUNK_HOME`.
   For Linux

   ```
   rm -rf /opt/splunk
   ```

   For Mac OS

   ```
   rm -rf /Applications/splunk
   ```

   You can also remove the installation directory by dragging the folder into the Trash.
4. Remove any Splunk Enterprise datastore or indexes outside the top-level directory, if they exist.

   ```
   rm -rf /opt/splunkdata
   ```
5. Delete the `splunk` user and group, if they exist.
   For Linux
   ```
   userdel splunk
   groupdel splunk
   ```

   For Mac OS
   Use the **System Preferences > Accounts** panel to manage users and groups.

   For Windows
   Open a command prompt and run the command `msiexec /x` against the msi package that you used to install Splunk Enterprise. If you don't have that package, get the correct version from the download page.

Reference

PGP Public Key

You can copy the Pretty Good Privacy (PGP) public key for Splunk software from this page or download the file using HTTPS. The Gnu Privacy Guard (GPG) keyid and instructions to install the PGP public key are also available.

This PGP public key is used to sign packages of Splunk software that are released on or after August 15, 2018.

PGP public key block

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFtbebEBEADjLzD+QXyTqLwT2UW1Dle5MpBj+C5cbaCIpFEhl+KemcnUKHls
TlCxEpzJczZPiYtcp+wtKCaNG/zoEvYCQ0jKk6Wgoa2cLkDeHtNiuBCHrztgeDTe
FpPT+xmtLoJvu1T0JV/iPG7p5FBGYKOKApnd/awRRC47plCGfVA3VVdQP8jhpMZV
T9C86hWbNo/NRjNH69x1xAe/9POc8KmVxZQb+KGG5tulGIWa7jlTMw850HZwFcft
F13DiAVgCj516K8oZBb5bjgu2ZvpCtMRbCmrzx26ilcB7VJRsTaB6G8MqRzVgLuj
11dTG2XMuBw+3UcjAlZ/y6Cut0Gc5FHIKqwMVXf29y9uXddvIqQnkE0AkOj6flm6
OElvmq7v+NVYLRb9XTy0oWTwOtyGTTso2xwZ8itDT4rIWeta0FxtQPt8Kq369ZGy
CbKl1PU9IrKAeST0AkXyfQXqPc0IzHxz3AhOLzvwm/9/0OWs0ONbxdyTCxQjrhe6
1YBoVv2T5K27fTp7rMFEstyU0NFI3J5P/oxg5ts6y2lCMUB7Q71yAOWVZPgucOAH
7iiNmvrytuGT0c8TfJku1cneajW9jmNvKVD/r3qj6YTAL3mqC0yYx3PiLyUVm8OZ
q90hpFHAI7zV1u6zMqV4EkWg5tEknMWcjQnyIfn0Jx8LedDjbTM8Dt9VKQARAQAB
tCFTcGx1bmssIEluYy4gPHJlbGVhc2VAc3BsdW5rLmNvbT6JAk4EEwEIADgWIQRY
wzMQt6NUwSedtmle+gHts81EIAUCW1t5sQIbAwULCQgHAgYVCAkKCwIEFgIDAQIe
AQIXgAAKCRBe+gHts81EIEsUD/9urCsBW40ahPr1gBsu6TlFbVWFN6TK7NpByecr
KzhDlOGJbh7g1u1qRO88ncUb/iPFfBjpJJ0RbskrZQKVVbmnhLeNPw4oqHq4kNmN
Kc8iV9tynw55Ww5Y0cJoeWrx9Ireub3+1GhKzUomIK0TuQtMULmW7Tdwm46iEDgC
qox2hOutlMFjrT9XOFnluCeyi8HL9m6xUlvvsxYxqWIzWUvoWH3AwpGSPMwg/nzH
Vl1Wz9IJOLqjQFBiA1Vmb/UEkP60JAtXWtNKJ7OqTLag29XBSaJO1NiQFZYb8uCU
GSqNOKYUwiO3ZivmVYlXBT7fC2uHpU45g/d2PrRKgVvIOC9xKiG8+jh/WuWlTl4i
vVjAIEnIFwO8Nig7uoR9xi+0ZxzkP00tGO2Cgv0cFf3TYQrSgrD7QDRBN2az4HtF
WvxJuOYjNLl7mp+Lx0Aj9wtb1WkYNBV0NMXThhnZsDU6Uo6ijJa2uBwkT8MljCHX
n7DjVFZYoZ6m2cwUdR5XSwfpSq0lA7LcSbef4CIC1H0mVxVzeB2B6xGxpVIMNGs4
B1RXW1amVeKmv9ZbTAQpGNVMyGJ8oOhksBFL2Ng0Z5kA9aCuwr1OjyrxBdglfGd/
wmEGIX2cLNNvS+Elh4JzFuKsURWbJ8qFl7cQvKQkS+UTwu7e3CCp8VztfRqPvgQi
A+2oI7kCDQRbW3mxARAAtoBTC9nNiY3301QKzTyPvudD3XI03RZTXVsSHVP4yV0x
fobD2aRhMjxwRjrajZnMCEFKB7yYtsbyiRfznLoycFBse6p4y9gguWEIgaW6TTQP
zQTEgi6AKt38nqDN42L/WurNhAKq9R5X/85vr2t6b18Yp2kw62okbuTtVLjuNwzh
tnZE/HziWVbtBy0KfZ0c6QMUHn7j0U67+QJeIzLcQuBn4qnb177TRtnqNZ9aFTXX
mnUA7qTOAvL+wsoyOcuOboj4N45H5s/izPSiXkoUM1ITuuUI3QHi46zw5cEvSLg+
WImwwZCN4tC275abjxW7XbirglV1EOlCWoALIOAh1BwXDA/JJGwbGOp+ueE7askJ
```

```
TiAtP9EM1mJSWnbE9uKDUvEMIaavwtt0kWmQOrB4HFY0AsTOnCxWQYCOb0CDImyq
ScblC3tqvoZzbjPBHQFvxClzxfGdmvQwoxr2WRfsspLPuG1FzgmmX29/WaOV747W
TwJP9xw1OtJmAkq/+CH6J12PmXHy9sJRdk6d1PPEuHjJ588U3Kwc7B5uAtgnwQO8
aS4zPM45y6+J1D2SdM0ydwuqQ9z9wwa022EGTa89k5Vfigx+C/VaDMa1Bu/NSkZ8
7S0NpQGbRwDp76gSKvV1T/15hYVg2nOsI1hTVmM8hVZQO3kO4zFjl0rNNjwWor0A
EQEAAYkCNgQYAQgAIBYhBFjDMxC3o1TBJ522aV76Ae2zzUQgBQJbW3mxAhsMAAoJ
EF76Ae2zzUQg26YP/0dj63ldEluB8L7+dFm9stebcmpgxAugmntdlprDkGi6Rhfd
ks7ufF+mny731GZPcJWIYKi797qerG5O1AI4siaK9FRKzw4PLIGvhOoNg2wrSP/+
7qTFf+ZbT7H5VpIqwcnnnRT05pi1KiMIXW82h47daFYVNhQPbV4+USHwFG7r3Lku
XdiS4hrcoe+Y/a9zGVAdU9QwrT8CuNAw8SYNYx1rJECHiMxmMaEw42a5NARoFdbh
swnR6Mwy5sPhzOHjSI/ZPyM/W9TKAoXfmDQSGDrvnU6NAdpIbP1Ab1FtMjuARfRg
8ndqfm/n8MIvAxjzoBBZkdV5HLOndX3fLVNewnvSWQx9OlV4a7+dKXeQ8TueOMq+
XMA4RKsh3gEMJWbVRZwZnxy+3UKGJD3el0+C7m483ptR8Tj8qBq5KELO0vkcq8+a
eHIbzmQSsj9iAdNfGVLYhimzpZy5NCTl2sgmy4g33pd1jMtUzdFZhvelVzMNlkLZ
AmAJX7yZLQwLsXDEpffgp2S/U8vYAZNTdeZqKvmvCCO+fweRRC7NnnPJQ7nVhL7r
VDxHuk8oMqBQIUdE7Z+WDfyagMMhJWbeMNnnhTZdoPmpXEGkjUKwPDYl+GmF50c1
6vjXtbrcP42pu2IQxiqiaTSLei8LRwPck1eE+78sSUxjVuWRuThoYRhGYoXt
=ivRW
-----END PGP PUBLIC KEY BLOCK-----
```

GPG key ID

The GPG public key ID is `key ID b3cd4420`.

Install the PGP public key

1. Copy and paste the key into a file, or download the file using HTTPS.
2. Install the key with the RPM package manager:

```
rpm --import <filename>
```