Splunk® Enterprise Installation Manual 6.6.2

Generated: 8/04/2017 8:59 am

Table of Contents

Table of Contents

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.

Installation basics

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*.

Upgrade or migrate a Splunk Enterprise instance

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

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

Before you download and install Splunk Enterprise for on-premises use, learn about the computing environments that Splunk supports.

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

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

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

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

Supported server hardware architectures

Splunk offers support for 32- and 64-bit architectures on several platforms.

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 has a matrix of boxes that define available computing platforms (operating system and architecture) and types of Splunk software. A '?' (check mark) in a box that intersects your computing platform and Splunk software type 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 have other characters. 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)	D	D	D	?
	SPARC				?
Linux, kernel version 2.6 and later	x86 (64-bit)	?	?	?	?
	x86 (32-bit)				D
Linux, kernel version 3.x and later	x86 (64-bit)	?	?	?	?
	x86 (32-bit)				D
PowerLinux, kernel version 2.6 and later (includes Big Endian and Little Endian versions)	PowerPC				?
zLinux, kernel version 2.6 and later	s390x				?
FreeBSD 9	x86 (64-bit)				?
FreeBSD 10	x86 (64-bit)				?
Mac OS X 10.10	Intel		D	D	D

Mac OS X 10.11 and macOS 10.12	Intel	?	?	?
AIX 7.1 and 7.2	PowerPC			?
HP/UX? 11i v3	Itanium			D
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.
? You must use gnu `tar` to unpack the HP/UX installation archive.

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	x86 (64-bit)	D	D	D	D
Windows Server 2012, Server 2012 R2, and Server 2016	x86 (64-bit)	?	?	?	?
Windows 8, 8.1, and 10	x86 (64-bit)		?	?	?
	x86 (32-bit)		***	***	?

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.

Operating system notes

Windows

Certain 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 architecture and processes.
- Choose the user Splunk 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 certain versions of Linux, Solaris, 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.

Support for some *nix operating systems has ended

Splunk has ended support for Splunk Enterprise on FreeBSD, AIX, HP-UX, and 32-bit versions of the Linux kernel. There are still universal forwarder packages available for these platforms, and installation instructions have been updated to install the universal forwarder for those systems:

- Install the universal forwarder on FreeBSD
- Install the universal forwarder on AIX
- Install the universal forwarder on HP-UX

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 except:

- AIX
- HP/UX on PA-RISC architecture

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 *Capacity Planning*.

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 system 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.

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

Capacity Planning.

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 those 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	ext2, ext3, ext4, btrfs, XFS, NFS 3/4
Solaris	UFS, ZFS, VXFS, NFS 3/4
FreeBSD	FFS, UFS, NFS 3/4, ZFS
Mac OS X	HFS, NFS 3/4
AIX	JFS, JFS2, NFS 3/4
HP-UX	VXFS, 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** as 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`	8192
User processes	`ulimit -u`	1024
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 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 before you attempt to install Splunk Enterprise.

This consideration is not applicable to Windows operating systems.

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
- Solaris
- Mac OS X

No support for full Splunk Enterprise on AIX, FreeBSD, and HP-UX

As of Version 6.3.0, Splunk Enterprise is no longer available for the following operating systems. To install and use Splunk Enterprise on these operating systems, you must use a version prior to 6.3.0.

The universal forwarder is available for installation on these platforms. See the following links for universal forwarder installation instructions:

- 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 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 provides an opportunity to 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 for an installation as a network or domain user

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

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.

Prepare Active Directory for Splunk installation as a domain user

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 "Prepare your Active Directory to run Splunk Enterprise services as a domain account" 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 system. You also cannot install Splunk Enterprise on a machine that runs an unsupported OS (for example, 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.

Install the universal forwarder

If 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 installer from the Splunk Enterprise 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. To start the installer, double-click the `splunk.msi` file. The installer runs and displays the **Splunk Enterprise Installer** panel.

2. To continue the installation, check the "Check this box to accept the License Agreement" checkbox. This activates the "Customize Installation" and "Install" buttons.
3. (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 system drive (the drive that booted your Windows system.)
- Installs Splunk Enterprise with the default management and Web ports.
- Configures Splunk Enterprise to run as the Local System user.
- Creates a Start Menu shortcut for the software.

If you want to change any of these default installation settings, click the "Customize Options" button and proceed with the instructions in "Customize Options" in this topic. Otherwise, click the "Install" button to install the software with the defaults and continue with "Complete the install" 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.

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.

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.

4. Specify user credentials and click **Next**. The installer displays the installation summary panel.

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

Complete the installation

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

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.

Before you install

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

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 Deploy 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. This flag must be set to Yes for a silent installation.	No
INSTALLDIR="<directory_path>"	Use this flag to specify directory to install. Splunk's installation directory is referred to as $SPLUNK_HOME or %SPLUNK_HOME% throughout this documentation set.	C:\Program Files\Splunk
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 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 will automatically select 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 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 should index events from	0 (off)

	capture a baseline snapshot of the Windows Registry user hive (`HKEY_CURRENT_USER`). **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 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 to monitor remote Windows data, then you must also specify the `LOGON_USERNAME` and `LOGON_PASSWORD` installation flags. Splunk 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
		`0` (off)

	Windows user Splunk should run as" in this manual for additional 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 user that Splunk 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`."
	
	These flags are mandatory if you want this Splunk Enterprise installation to monitor any remote data. Review "Choose the Windows user Splunk 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. 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. If you specify either the Splunk forwarder or light forwarder here, you must also specify	none

	FORWARD_SERVER="<server:port>". To install Splunk Enterprise with no applications at all, omit this flag. **Note:** The full version of Splunk 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 should start up automatically on system boot. **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)

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 user

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

Enable the Splunk heavy forwarder, enable indexing of the Windows System event log, and run the installer in silent mode

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder"
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.

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

What's next?

Now that you've installed Splunk Enterprise, **what comes 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 Unix, 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?

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

Tar file installation

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

To install Splunk Enterprise on a Linux system, 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.

1. Confirm that the RPM package you want is available locally on the target host.
2. Verify that the Splunk Enterprise user (the 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 that references 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
```

Note: The `enable boot-start` line is optional.

Debian .DEB install

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.

- 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 </code>/bin/sh</code>.

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.

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

Next steps

Now that you have installed Splunk Enterprise:

- Start it, if it has not started already. 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 comes next?

Uninstall Splunk Enterprise

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

Install on Solaris

You can install Splunk Enterprise on Solaris with a PKG packages, 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, see How to upgrade Splunk for instructions and migration considerations before proceeding.

Install Splunk

Splunk Enterprise for Solaris is available as a PKG file or a tar file.

PKG file install

The PKG installation package includes a request file that prompts you to answer a few questions before Splunk installs.

```
pkgadd -d ./splunk_product_name.pkg
```

A list of the available packages is displayed.

- Select the packages you wish to process (the default is "all").

The installer then prompts you to specify a base installation directory.

- To install into the default directory, `/opt/splunk`, leave this blank.

tar file install

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

- Some non-GNU versions of `tar` might not have the `-C` argument available. In this case, if you want to install in `/opt/splunk`, either `cd` to `/opt` or place the tar file in `/opt` before running the `tar` command. This method will work for any accessible directory on your machine's filesystem.
- If the `gzip` binary is not present on your system, you can use the `uncompress` command instead.
- 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 a Solaris system, expand the tar file into an appropriate directory using the `tar` command:

```
tar xvzf splunk_package_name.tar.Z
```

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

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

What gets installed

To learn more about the Splunk Enterprise package and what it installs, run the following command:

```
pkginfo -l splunk
```

To list all packages that have been installed on the host:

```
pkginfo
```

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.

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**. The installation begins. It might take a few minutes to complete.
7. When your 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 /
```

Note: 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
```

Note: 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.

Install the universal forwarder on FreeBSD

Important: Splunk does not offer an installation package for Splunk Enterprise on FreeBSD. There is a universal forwarder installation package for FreeBSD versions 9 and 10.

To use Splunk Enterprise on FreeBSD, you must download an older version of the Splunk software. See the previous releases page.

Basic installation

These instructions install the universal forwarder in the default directory, `/opt/splunkforwarder`. If `/opt` does not exist and you have not created it, you might receive an error message. There is no current version of Splunk Enterprise that is available for FreeBSD.

FreeBSD best practices maintain a small root filesystem. You might want to create a symbolic link to another filesystem and install Splunk there, rather than attempting to install in `/opt`.

1. Confirm that the `/opt/splunkforwarder` directories exist. If they do not, create them or link to another file system from there.
2. Install the universal forwarder on FreeBSD using the Intel installer:
   `pkg_add splunkforwarder-intel.tgz`

   To install Splunk Enterprise in a different directory:

```
pkg_add -v -p /usr/splunk splunkforwarder-intel.tgz
```

Tar file installation

The tar file is a manual form of installation.

These instructions are for installing the universal forwarder tar file only. There is no current version of Splunk Enterprise available for FreeBSD.

When you install the universal forwarder with a tar file:

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

Expand the universal forwarder tar file into an appropriate directory using the `tar` command. The default install directory is `splunkforwarder` in the current working directory.

```
tar xvzf splunkforwarder.tgz
```

To install into `/opt/splunkforwarder`, execute:

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

After you install

To ensure that the forwarder functions properly on FreeBSD, you must perform some additional activities after installation. This includes setting process and virtual memory limits.

The figures below represent a host with 2GB of physical memory. If your host has less than 2 GB of memory, reduce the values accordingly.

1. Add the following to `/boot/loader.conf`
   ```
   kern.maxdsiz="2147483648" # 2GB
   kern.dfldsiz="2147483648" # 2GB
   machdep.hlt_cpus=0
   ```
2. Add the following to `/etc/sysctl.conf`:
   ```
   vm.max_proc_mmap=2147483647
   ```
3. Restart FreeBSD for the changes to take effect.

Next steps

Now that you have installed the Splunk universal forwarder, visit the *Universal Forwarder* manual to:

- Learn how to configure it to get and forward data.
- Configure it to start at boot time. See Configure Splunk software to start at boot time.
- Learn the what commands you can issue to it.

Install the universal forwarder on AIX

Important: Splunk does not offer an installation package for Splunk Enterprise on AIX. There is a universal forwarder installation package for AIX versions 7.1 and 7.2.

To use Splunk Enterprise on AIX, you must download an older version of the Splunk software.

Prerequisites

The user that you install the universal forwarder as must have permission to read `/dev/random` and `/dev/urandom` or the installation will fail.

Basic installation

The AIX universal forwarder installer comes in tar file form. There is no current version of Splunk Enterprise available for AIX.

When you install with the tar file:

- Splunk Enterprise does not create the `splunk` user automatically. If you want Splunk Enterprise to run as a specific user, you must create the user manually.
- Confirm that the disk partition that you install into has enough space to hold the uncompressed volume of the data you want to keep indexed.
- Use GNU `tar` to unpack the tar files, as AIX `tar` can fail to unpack long file names, fail to overwrite files, among other things. If you must use the system tar, confirm the `tar` output for error messages. GNU `tar` comes as part of the AIX Toolbox for Linux Applications package (usually as `/opt/freeware/bin/tar`.)

To install the universal forwarder on an AIX system, expand the tar file into an appropriate directory. The default installation directory for the universal forwarder is `/opt/splunkforwarder`.

Startup options

The first time you start the universal forwarder after a new installation, you must accept the license agreement. To start the forwarder and accept the license in one step:

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

Note: There are two dashes before the `accept-license` option.

Next steps

To configure the forwarder to start automatically at boot time, see Enable boot-start as a non-root user.

See the *Universal Forwarder* manual to:

- Learn how to configure it to get and forward data.
- Learn the what commands you can issue to it.

Install the universal forwarder on HP-UX

Important: Splunk does not offer an installation package for Splunk Enterprise on HP-UX. There is a universal forwarder installation package for HP-UX version 11i v3.

To use Splunk Enterprise on HP-UX, you must download an older version of the Splunk software.

Basic installation

To install the universal forwarder on an HP-UX system, expand the tar file with GNU `tar` into an appropriate directory. The default installation directory is `/opt/splunkforwarder`.

When you install with the tar file:

- The forwarder does not create the `splunk` user automatically. If you want the forwarder to run as a specific user, you must create the user manually.
- Be sure the disk partition has enough space to hold the uncompressed volume of the data you plan to keep indexed.

Next steps

Now that you have installed the Splunk universal forwarder, visit the *Universal Forwarder* manual to:

- Learn how to configure it to get and forward data.
- Configure it to start at boot time. See Configure Splunk software to start at boot time.
- Learn the what commands you can issue to it.

Run Splunk Enterprise as a different or non-root user

Important: This topic is for non-Windows operating systems only.

- To configure Splunk software to run at boot time as a non-root user, see Enable boot-start as a non-root user.
- 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.

You can run Splunk Enterprise as any user on the local system. It is a Splunk best practice to run Splunk software as a non-root user.

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

- 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.
- 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 procedure, `$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, Solaris, and FreeBSD:
   ```
   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 [Chooseyourplatform|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.

Additional privileges and network ports required for installation on Solaris 10

When installing Splunk Enterprise on Solaris 10 as the `splunk` user, you must set additional privileges to start `splunkd` and bind to reserved ports.

To start `splunkd` as the `splunk` user on Solaris 10, run:

```
usermod -K defaultpriv=basic,net_privaddr,proc_exec,proc_fork splunk
```

To allow the `splunk` user to bind to reserved ports on Solaris 10, run (as root):

```
usermod -K defaultpriv=basic,net_privaddr splunk
```

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. For more information, see Hardening Standards in the *Securing Splunk Enterprise* manual.

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. In a command prompt, go to `C:\Program Files\Splunk\bin` and type:

```
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

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

```
<Splunk Enterprise installation directory>/bin/splunk start
```

Splunk Enterprise then displays the license agreement and prompts you to accept before the startup sequence continues.

You can optionally set the `SPLUNK_HOME` environment variable to the Splunk Enterprise installation directory so that you can start the software as follows:

```
export SPLUNK_HOME=<Splunk Enterprise installation directory>
$SPLUNK_HOME/bin/splunk start
```

Setting the environment variable lets you refer to the installation directory later without having to remember its exact location.

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

To start Splunk Enterprise from the command line interface, run the following command from `$SPLUNK_HOME/bin` directory (where $SPLUNK_HOME is the directory into which you installed Splunk, by default `/Applications/splunk`):

```
./splunk start
```

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.

Other start options

To accept the license automatically when you start Splunk Enterprise for the first time, add the `accept-license` option to the `start` command:

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

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
```

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 requires you to answer a question. Then, it displays the question, why it is quitting, and quits.
- If you run `SPLUNK_HOME/bin/splunk start --answer-yes`, Splunk Enterprise proceeds with startup and automatically answers "yes" to all yes/no questions. It displays the question and answer as it continues.

If you run start with all three options in one line, for example:

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

- Splunk does not ask you to accept the license.

- Splunk answers yes to any yes/no question.
- Splunk quits when it encounters a non-yes/no question.

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.

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.

The first time you log in to Splunk Enterprise, the default login details are:
Username - *admin*
Password - *changeme*

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. We call this process **indexing**. For information about the indexing process, refer to What Splunk Enterprise does with your data in the *Getting Data In* manual.

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

For more information about Splunk licenses, begin by reading:

- 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 Groups, stacks, pools, and other terminology in the *Admin Manual* for more information about Splunk license terms.
- 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 6.6?

See Meet Splunk Enterprise 6.6 in the Release Notes for a full list of the new features that are available in 6.6.

See the 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 the *Managing Indexers and Clusters Manual*.

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 deployment.

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 Manual*.
- To upgrade a search head cluster, see Upgrade a search head cluster in the *Distributed Search Manual*.

Important upgrade information and changes

See About upgrading to 6.6: READ THIS FIRST for specific migration tips and information that might affect you when you upgrade.

Upgrade from 6.0 and later

Splunk Enterprise supports a direct upgrade from versions 6.0 and later to version 6.6.

- Upgrade to 6.6 on *nix
- Upgrade to 6.6 on Windows

Upgrade from 5.0 and earlier

Upgrading directly to version 6.6 from version 5.0 and earlier is not officially supported.

- If you run version 5.0, upgrade to version 6.3 first before attempting an upgrade to 6.6.
- If you run version 4.3, upgrade to version 6.0 first before attempting an

upgrade to 6.6.
- If you run a version earlier than 4.3:
    - Upgrade to version 4.3.
    - Then upgrade to version 6.0.
    - Then upgrade to version 6.6.

See About upgrading to 4.3 READ THIS FIRST for specific details on how to upgrade to version 4.3.

Get and install the "no-enforcement" license

A new license type 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*.

To 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 will 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 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 Indexer and universal forwarder compatibility in the *Forwarding Data Manual*.

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 can not 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 6.6 READ THIS FIRST

Read this topic before you upgrade to learn important information and tips about the upgrade process to version 6.6 from an earlier version.

Splunk App and Add-on Compatibility

Not all Splunk apps and add-ons are compatible with Splunk Enterprise version 6.6. Visit Splunkbase to confirm that your apps are compatible with Splunk Enterprise version 6.6.

Upgrade clustered environments

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

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

Upgrade paths

Splunk Enterprise supports the following upgrade paths to version 6.6 of the software:

- From version 6.0 or later to 6.6 on full Splunk Enterprise.
- From version 5.0 or later to 6.6 on Splunk universal forwarders.

If you run a version of Splunk Enterprise prior to 6.0, upgrade to 6.0 first, then upgrade to 6.6. Users of Splunk Enterprise 5.0 can upgrade to 6.3 before upgrading to 6.6. See About upgrading to 6.0 - READ THIS FIRST for tips on migrating your instance to version 6.0.

Important upgrade information and changes

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

Customers who run version 6.4.7 of Splunk Enterprise might reintroduce software defects by upgrading to version 6.6.0 or 6.6.1

Some defects that Splunk fixed in version 6.4.7 are not yet fixed in version 6.6.0 or 6.6.1. If you run version 6.4.7 of Splunk Enterprise, you might reintroduce those defects by upgrading to version 6.6.0 or 6.6.1.

Consider waiting for version 6.6.2 to arrive before upgrading from version 6.4.7.

This notice applies only to customers that run version 6.4.7 and want to upgrade to version 6.6.0 or 6.6.1. It does not apply to those who run version 5.x or any other version of 6.x.

A new load-balancing scheme for forwarders is available

As of version 6.6 of Splunk Enterprise, 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 6.6 and version 5.0 and earlier is disabled by default

Because of changes to the security ciphers in version 6.6 of Splunk Enterprise, instances of Splunk software that run on version 5.0 or less cannot connect to instances of version 6.6 or greater by default.

When you upgrade, any instances that run version 5.0 or earlier will no longer communicate with the upgraded instance over SSL. To work around the problem, 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 *Release Notes*.

Data model acceleration sizes on disk might appear to increase

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 6.6 is more accurate than in previous versions.

The number of potential data model acceleration searches has increased

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 a number of data models, and those models 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

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

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

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

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

If you have 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

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 will be enabled by default.

Memory usage on indexers increases during indexing operations

(Originally introduced in version 6.5)

When you upgrade to version 6.6 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 6.6 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 a new 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 performance data in the *Admin Manual*.

Distributed search now defaults to a single protocol

(Originally introduced in version 6.4)

In an effort to reduce the potential of problems when search heads connect to search peers, several settings have been added or changed in `distsearch.conf` that control this process.

- The `trySSLFirst` setting no longer has any meaning in the context of search head-to-search peer connections.
- A new setting `defaultUriScheme` controls what protocol search heads use to connect to search peers, and can be configured to `http` or `https`. This setting acts as the default connection scheme for any peers that you add to a search head after you configure the setting.

After you upgrade, review `distsearch.conf` to confirm that the file has been updated with the new variables.

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 have 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. And 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 has been added that requires non-administrator user roles to hold it before they can delete indexes. After you upgrade, you must assign this capability to any non-administrator user roles before they can delete any indexes.

User roles must also have the "delete_by_keyword" capability.

Migration time might increase significantly if there are a large number of data model or report acceleration summaries

(Originally introduced in version 6.4)

When you upgrade to version 6.6 of Splunk Enterprise, the software generates checksums for data model and report acceleration summaries as part of the migration. This action is for better compatibility with indexes on indexer clusters, but happens on all deployments. If your deployment has a large number of existing data model or report acceleration summaries, the checksum generation process might take a long time. Splunk Enterprise generates entries in `migration.log` during the process:

```
Generating checksums for datamodel and report acceleration bucket
summaries for all indexes.
If you have defined many indexes and summaries, summary checksum
generation may take a long time.
Processed 1000 out of 10007 configured indexes.
Processed 2000 out of 10007 configured indexes.
[...]
```

```
Processed 10000 out of 10007 configured indexes.
Finished generating checksums for datamodel and report acceleration
bucket summaries for all indexes.
```

The working directory for the inputcsv, outputcsv, and streamedcsv search commands has changed

(Originally introduced in version 6.4)

The working directory for the `inputcsv`, `outputcsv`, and `streamedcsv` search commands has changed. When you execute these search commands after an upgrade, Splunk Enterprise stores and reads the files they create in `$SPLUNK_HOME/var/run/splunk/csv`, rather than `$SPLUNK_HOME/var/run/splunk`.

The upgrade process moves any existing working files to the new directory and logs the following message to `migration.log`:

```
Creating $SPLUNK_HOME/var/run/splunk/csv and moving inputcsv/outputcsv
files into the created directory.
```

Note the following migration issues:

- Apps, add-ons, or scripts that use the commands or that reference the old working directory could be negatively affected when you upgrade due to the changed directory location.
- You must manually migrate any files that you use in conjunction with `inputcsv` that do not end with the `.csv` file extension, or that are in a subdirectory.
- If you have a component that is external to Splunk Enterprise that uses the `outputcsv` command, you must manually update the paths of any files or scripts in that component that use the command.
- Additionally, if the component contains files that `outputcsv` has generated, and those files either do not end in `.csv` or are in a subdirectory, you must migrate those files to the new working directory manually.

Search commands that exist only in a user context will no longer execute

(Originally introduced in version 6.4)

If you have any search commands that run in the context of a specific Splunk Enterprise user (meaning that the commands have been defined in a `commands.conf` only for that user, for example, `$SPLUNK_HOME/etc/users/alice/local/commands.conf`), those commands will no longer be available for execution after you upgrade.

To fix the problem, move the command configurations to either the app level (put the configurations into `$SPLUNK_HOME/etc/apps/<app_name>/local/commands.conf`) or the system level (`$SPLUNK_HOME/etc/system/local/commands.conf`).

Confirm that the introspection directory has the correct permissions

(Originally introduced in version 6.4)

If you run Splunk Enterprise on Linux as a non-root user, and use an RPM to upgrade, the RPM writes the `$SPLUNK_HOME/var/log/introspection` directory as root. This can cause errors when you attempt to start the instance later. To prevent this, `chown` the `$SPLUNK_HOME/var/log/introspection` directory to the user that Splunk Enterprise runs as after upgrading and before restarting Splunk Enterprise.

The Splunk Web visualizations editor changes take precedence over existing 'rangemap' configurations for single-value visualizations

(Originally introduced in version 6.4)

If you use the `rangemap` search command to define ranges and colors for single-value visualizations on dashboards, use the Format editor instead when you upgrade. Changes that you make with the Format editor to these visualizations override the `rangemap` configurations. Going forward, generate new single value visualizations by using a query that does not contain the `rangemap` command, and then use the Format editor to configure ranges, colors, or any additional settings.

Any changes that you make with the editor to single-value visualizations that were generated with `= rangemap` override edits that you make to the `range map` command. Additionally, while the editor attempts to preserve the existing configuration, it no longer recognizes `rangemap` as a valid command to generate these types of visualizations.

Splunk Enterprise now limits the addition of search peers with a large time skew

(Originally introduced in version 6.4)

When you upgrade to Splunk Enterprise 6.6, you will no longer be able to use Splunk Web to add search peers with a time skew of more than 10 minutes from the search head where you add the peers.

You can change this setting by editing `limits.conf` on the search head and setting the `addpeer_skew_limit` to a positive integer that is lower than its default of 600 (seconds).

Splunk Enterprise support for running multiple searches on a single process could increase memory usage

(Originally introduced in version 6.4)

As of version 6.6, Splunk Enterprise can launch multiple searches on a single process on *nix hosts.

When you upgrade, you should see improved search performance, but you might also see increased memory usage.

This change is not applicable on Windows instances of Splunk Enterprise.

Support for the Deployment Monitor app has been removed

(Originally introduced in version 6.3)

Support for the Splunk Deployment Monitor App has been removed. When you upgrade to Splunk Enterprise 6.6, use the monitoring console instead to monitor your distributed deployment. See *Monitoring Splunk Enterprise*.

Data block signing has been removed

(Originally introduced in version 6.3)

Data block signing has been removed from Splunk Enterprise.

Accelerated custom data model summaries will rebuild on upgrade

(Originally introduced in version 6.3, can happen on upgrades from 6.3)

)When you upgrade to Splunk Enterprise 6.6, any accelerated custom data model summaries that are present on the instance - such as those created by the Splunk App for Enterprise Security - will be rebuilt. This is because of optimizations to data model searches that have been made, which make the searches incompatible with previously generated summaries.

During the rebuild process, CPU, memory, and disk I/O usage on indexers with the summaries will increase significantly. Searches that rely on those data model

summaries will be very slow and might not work fully.

If you need to prevent Splunk Enterprise from automatically rebuilding these summaries on upgrade, make the following changes to your Splunk Enterprise configuration before starting an upgrade:

In `datamodels.conf`:

```
acceleration.manual_rebuilds = true
```

In `limits.conf`:

```
[tstats]
allow_old_summaries = true
```

There is now a limit on the number of learned source types

(Originally introduced in version 6.3)

For all versions of Splunk Enterprise, the number of source types that an instance can learn in the process of monitoring and indexing files has been limited.

To reduce instances where CPU and memory usage spiked during such operations, a new attribute that controls how many source types an instance learns when it monitors files and analyzes file contents has been created. The limit is 1000, and you can change this setting by editing the following attribute in `limits.conf` and restarting Splunk Enterprise:

```
learned_sourcetypes_limit = <number>
```

While this setting should prevent memory and CPU spikes, continue to use `props.conf` and `inputs.conf` to define and apply source types.

Parallel summarization for data model summaries has been enabled

(Originally introduced in version 6.3)

The number of searches that the Splunk platform runs at a time to generate summary files for data models has changed.

When you upgrade to Splunk Enterprise 6.6, the software runs two concurrent search jobs to generate the summary files, instead of one. This change is called "parallel summarization." It might result in an increase in CPU and memory

usage on the instance that contains the data models while the search jobs run, but results in faster availability of data model summaries.

You can change this setting back to the previous default for individual data models. See Parallel summarization in the *Knowledge Manager Manual*.

You must now enable access to Splunk Enterprise debugging endpoints

(Originally introduced in version 6.3)

Splunk Enterprise used to allow access to debugging endpoints by default. This is no longer the case. When you upgrade, you won't be able to access the debugging endpoints until you make a change in `web.conf` and restart Splunk Enterprise:

```
[settings]
enableWebDebug = true
```

Migration from search head pooling to search head clustering

If you want to migrate to search head clustering from a standalone search head, or from search head pooling, which has been deprecated, you must follow specific instructions and use new Splunk Enterprise instances for search head cluster members. See the following topics in the *Distributed Search* manual for more information on migrating to search head clustering:

- Migrate from standalone search heads
- Migrate from search head pooling

Search head clusters now respect user- and role-based search quotas

(Originally introduced in version 6.3)

When you upgrade to Splunk Enterprise 6.6, any search head clusters that you have deployed will respect and enforce search quotas that are in place for users and roles. This might result in some searches not executing, depending on the number of concurrent searches that are active. To defeat this feature, set the following attributes in `limits.conf`:

```
shc_role_quota_enforcement = false
shc_local_quota_check = true
```

The App Key Value Store service might increase disk space usage

(Originally introduced in version 6.2)

The App Key Value Store (or KV Store) service, which provides a way for you to maintain the state of your application by storing and retrieving data within it, might cause an increase in disk usage on the instance, depending on how many apps you run. You can change where the KV Store service puts its data by editing `server.conf`, and you can restore data used by KV Store with the `splunk clean` CLI command. See About the app key value store in the Admin manual.

Splunk Enterprise now identifies search commands that could negatively impact performance

In an effort to improve security and performance, some Search Processing Language (SPL) commands have been tagged with a variable that prompts Splunk Enterprise to warn you about performance impact when you use them in a search query. After an upgrade, you might see a warning message that a search that you run has commands that might have risky side effects.

Results for unaccelerated data models now match results from accelerated data models

(Originally introduced in version 6.2)

The way that unaccelerated data models query indexes for events has changed.

These models now query all indexes, rather than just the default index. This means that the number of results you see for unaccelerated data models should now match the number of results you see for accelerated data models.

After you upgrade, you might see more results for an unaccelerated data model than you did prior to upgrading.

New installed services open additional network ports

(Originally introduced in version 6.2)

Splunk Enterprise installs and runs two additional services: App Key Value Store and App Server. This opens two network ports by default on the local machine: 8065 (for App Server) and 8191 (for App Key Value Store.) Confirm that no firewall block these ports. The App Key Value Store service also starts an additional process, `mongod`. If needed, you can disable App Key Value Store by

editing `server.conf` and changing the `dbPath` attribute to a valid path on a file system that the Splunk Enterprise instance can reach. See About the app key value store in the *Admin* manual.

Formatting for single-value visualizations has changed

(Originally introduced in version 6.3)

The formatting for single-value visualizations has changed in that these visualizations have been redesigned to be as readable as possible from a distance. When you upgrade, dashboards that use these visualizations might be impacted by very large letters or numbers.

To work around the problem, you can either:

- Make use of the new time context if you show a numeric value that you can query over time.
- Use Simple XML to reduce the single value panel height from its default of 115 pixels. Or,
- Replace the single value panel with a custom HTML panel.

See this post on Splunk Answers for additional information prior to upgrading.

New default values for some attributes can impact Splunk operations over SSL

(Originally introduced in version 6.3)

There are new defaults which can possibly impact running Splunk Enterprise over SSL:

- The `supportSSLv3Only` attribute, which controls how Splunk Enterprise handles SSL clients, now has a default setting of `true`. This means that only clients who can speak the SSL v3 protocol can connect to the Splunk Enterprise instance.
- The `cipherSuite` attribute, which controls the encryption protocols that can be used during an SSL connection, now has a default setting of `TLSV1+HIGH:@STRENGTH`. This means that only clients that possess a Transport Layer Security (TLS) v1 cipher with a 'high' encryption suite can connect to a Splunk Enterprise instance.

Login page customization has changed

Login page customization has changed as of version 6.6 of Splunk Enterprise. To learn how the new customization process works, see Customize the login page in *Developing Views and Apps for Splunk Web*.

Windows-specific changes

The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cipher suites in version 6.6 are not supported on Windows Server 2008 R2

The TLS and SSL cipher suites that come with version 6.6 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 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

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 a reasonable one (meaning, you have not set it 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 the system

requirements page in this manual. 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.

Splunk does not expect any other impacts to occur as a result of an upgrade.

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 to use 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 earlier versions of Internet Explorer.

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

The Windows host monitoring input no longer monitors application state

(Originally introduced in version 6.3)

The Windows host monitor input has been modified to no longer monitor the state of installed applications.

Due to a bug in the system call that Splunk Enterprise uses to monitor application state, the Windows Installer service attempts to reconfigure all installed applications.

When you upgrade, any Windows host monitoring input stanzas that reference the "Application" attribute will no longer function. To get application state data, use the Windows Event Log monitor and search for Event ID Nos. 11707 (for installation) or 11724 (for uninstallation/removal.)

Alternatively, you can use a PowerShell script (`Get-WmiObject -Class Win32_Product | Format-List -Property Name,InstallDate,InstallLocation,PackageCache,Vendor,Version,IdentifyingNum`) or the Windows Management Instrumentation Command-line interface (WMIC). For example: `wmic product get name,version,installdate`

New installation and upgrade procedures

(Originally introduced in version 6.2)

The Windows version of Splunk Enterprise has a more streamlined installation and upgrade workflow. The installer now assumes specific defaults (for new installations) and retains existing settings (for upgrades) by default. To make any changes from the default on installations, you must check the "Customize options" button. During upgrades, your only option is to accept the license agreement. See Installation options."

Changes have been made to support more granular authorization for Windows inputs

(Originally introduced in version 6.4)

Splunk Enterprise has been updated to allow for more control when using Windows inputs like Network Monitoring and Host Monitoring. If you use Splunk Enterprise as a user with a role that does not inherit from other roles, it is possible that the user might not be able to access certain Windows inputs.

The Splunk Web service installs but does not run

(Originally introduced in version 6.2)

The `splunkd` service handles all Splunk Web operations. However, on Windows instances, the installer still installs the `splunkweb` service, although the service quits immediately on launch when operating in normal mode. You can configure the service to run in legacy mode by changing a configuration parameter in `web.conf`. See Start Splunk Enterprise on Windows in legacy mode in the Admin manual.

Do not run Splunk Web in legacy mode permanently. Use legacy mode to temporarily work around issues introduced by the new integration of the user interface with the main splunkd service. After you correct the issues, return Splunk Web to normal mode as soon as possible.

No support for enabling Federal Information Processing Standards (FIPS) after an upgrade

There is no supported upgrade path from a Splunk Enterprise system with enabled Secure Sockets Layer (SSL) certificates to a system with FIPS enabled. If you need to enable FIPS, you must do so on a new installation.

The default behavior for translating security identifiers (SID) and globally unique identifiers (GUIDs) when monitoring Windows Event Log data has changed

(Originally introduced in version 6.2)

The `etc_resolve_ad_obj` attribute, which controls whether or not Splunk Enterprise attempts to resolve SIDs and GUIDs when it monitors event log channels, is now disabled by default for all channels. When you upgrade, any `inputs.conf` monitor stanzas that do not explicitly define this attribute will no longer perform this translation.

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

How Splunk Web procedures have changed from version 5 to version 6

Use this topic to learn about some of the major differences in how to accomplish tasks using the Splunk Web user interface from version 5.x to version 6.x.

What's changed?

Procedure/Task	How you used to do it	How you do it now
First time login to Splunk Enterprise	In 5.x, the Splunk Enterprise launcher has two tabs: Welcome and Splunk Home. In Welcome, you can Add data and Launch search app.	In 6.x, Splunk Enterprise launches with Home. The main parts of Home include the Splunk Enterprise navigation bar, the Apps panel, the Explore Splunk Enterprise panel, and a custom default dashboard (not shown here).
Returning to Home	In 5.x, to return to Home/Welcome you selected the Home app from the App menu.	In 6.x, you click the Splunk logo in the upper left of the navigation bar. Doing so always returns you to Home.

Edit account information	In 5.x you accessed your account information (change full name, email address, default app, timezone, password) under Manager > Users and authentication > Your account.	In 6.x, you access account information directly from the Splunk navigation under Administrator > Edit Account.
Logout from Splunk Enterprise	In 5.x, you clicked the "Logout" button on the navigation bar.	In 6.x, you select Administrator > Logout. (If you are not logged in as Administrator, Splunk Enterprise displays the full name of the logged in user. Click this name to bring up the "Logout" menu option)
Manager/Settings	In 5.x, you edited all objects and system configurations from the Manager page or from the "Administrator" link on the navigation bar.	In 6.x, you access these configurations directly from the Settings menu. There is no separate Manager page.
Manage Apps: Edit permissions for installed apps, create a new app, or browse Splunk Apps for community apps	In 5.x, you used Manager -> Apps or selected from the App menu.	In 6.x, you use the Apps menu on the navigation bar or the gear icon beside the word Apps on the Home page.

Search	Summary, Search Searches & Reports Dashboards & Views	Search Reports Dashboards
Extract fields or show source	In the search results, click on the arrow to the left of the timestamp of an event and select Extract Fields or Show Source.	In the search results, click on the arrow to the left of the timestamp of an event and then click Event Actions. Select Extract Fields or Show Source.
Find the list of alerts	In the navigation bar, you selected "Alerts".	In the navigation bar, you select Activity > Triggered Alerts.
Find the timeline	In 5.x, the timeline was always visible as part of the dashboard after you ran a search. You can hide the timeline.	In 6.x, you can only view the timeline if you're looking at the Events tab after you run a search.

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 6.6, and how to migrate any existing apps to work with the new version.

Changes

- Self-service app management in Splunk Cloud now includes app update,

a bigger set of vetted apps, and support for multiple search heads.
- Mod Setup, a new framework for building setup screens in your apps.
- Updates to Add-On Builder and the App Packaging Toolkit.

Visit the Splunk Dev portal

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

Upgrade to 6.6 on UNIX

Before you upgrade

Before you upgrade, see About upgrading to 6.6: 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 host 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 zxf splunk-6.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 6.6 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 6.6: 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

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. An upgrade is a form of migration.

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.

Endianness

If you indexed data with a version of Splunk Enterprise earlier than 4.2, the index files that comprise that data are sensitive to operating system endianness, which is the way the system organizes the individual bytes of a binary file (or other data structure).

Some operating systems are *big-endian* (meaning they store the most significant byte of a word in computer memory first), and others are *little-endian* (meaning they store the least significant byte first). These operating systems create binary files of the same endianness. Index bucket files are binary, and thus, for versions of Splunk Enterprise earlier than 4.2, are the same endianness of the operating system that created them.

For a listing of processor architectures and the endianness they use, see the Endianness article on Wikipedia.

When you migrate a pre-4.2 Splunk Enterprise instance, in order for the destination system to be able to read the migrated data, you must transfer index files between systems with the same kind of endianness (for example, a NetBSD system running on a SPARC processor to a Linux system also running on a SPARC processor.)

If you can't move index between systems with the same endianness (for example, when you want to move from a system that is big-endian to a system that is little-endian), you can move the data by forwarding it from the big-endian system to the little-endian system. Then, after you have forwarded all the data, you can retire the big-endian system.

Index files that Splunk Enterprise versions 4.2 and later create are not sensitive to host endianness.

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:

- The source and target hosts have the same endianness.
- You do not restore a bucket created by a 4.2 or later version of Splunk Enterprise to a version less than 4.2.

Note: 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.

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.

Migrate to the new Splunk Enterprise licenser

Learn how to migrate your license configuration from a Splunk Enterprise deployment that runs a version earlier than 4.2 to the 4.2 and later licenser model by following the procedures in this topic.

Note: This topic does not cover the upgrade of an entire Splunk Enterprise deployment. See How to upgrade Splunk before you upgrade your Splunk Enterprise deployment.

Before you proceed, see the following:

- How Splunk licensing works in the *Admin Manual* for an introduction to Splunk licensing.
- Groups, stacks, pools, and other terminology in the *Admin Manual* for more information about Splunk license terms.

Old licenses

Migrating from an older version of Splunk Enterprise most likely puts you in one of these two categories:

- If you run Splunk Enterprise 4.0 or later, your license will work in 4.2 and later.
- If you migrate from a version of Splunk Enterprise that is older than 4.0, you must contact your Splunk Sales representative and arrange for a new license. See What to expect when upgrading to 4.0 before proceeding with the migration. Depending on how old your version of Splunk Enterprise is, you might want to migrate in multiple steps (for example, first to 4.0, then 4.1, 4.2, and finally 5.0+) to maintain your configurations.

Migrating search heads

If your search heads used old forwarder licenses, they will be automatically converted to be in the Download-trial group. Before you proceed, add your search heads to an established Enterprise license pool. Even if they have no indexing volume, this practice enables Enterprise features, especially alerting and authentication.

Migrate a standalone instance

If you've got a single 4.1.x Splunk Enterprise indexer and it has a single license installed on it, you can just proceed as normal with your upgrade. See How to upgrade Splunk for instructions, and be sure to read the "READ THIS FIRST" documentation prior to migrating.

Your existing license will work with the new licenser, and will show up as a valid **stack**, with the indexer as a member of the default pool.

Migrate a distributed indexing deployment

If you've got multiple 4.1.x indexers, each with their own licenses, follow these high-level steps **in this order** to migrate the deployment:

1. Designate one of your Splunk Enterprise instances as the **license master**. A **search head** is a good choice if one is available.
2. Install or upgrade the Splunk Enterprise instance you have chosen to be the license master, following the standard instructions in this manual.
3. Configure the license master to accept connections from the indexers as

desired.

4. Upgrade each indexer one at a time, following these steps:
    1. Upgrade an indexer to 5.0 following the instructions in this manual. It will operate as a stand-alone license master until you perform the following steps.
    2. Make a copy of the indexer Enterprise license file. You can locate license files for 4.2 and earlier in `$SPLUNK_HOME/etc/splunk.license` on each indexer.)
5. install the license onto the license master, adding it to the stack and pool to which you want to add the indexer.
6. Configure the indexer as a **license slave** and point it at the license master.
7. On the license master, confirm that the license slave connects as expected by navigating to **Manager > Licensing** and looking at the list of indexers associated with the appropriate pool.
8. Once you confirm that the license slave connects as expected, proceed to upgrade the next indexer, following the same steps.

Migrate forwarders

If you have deployed **light forwarders**, review the information in Migrate from a light forwarder in the *Universal Forwarder* Manual. You can upgrade your existing light forwarders to the universal forwarder as the universal forwarder includes its own license.

If you have deployed a heavy forwarder (a full instance of Splunk that performs indexing before forwarding to another Splunk Enterprise instance), you can treat it like an indexer--add it to a license pool along with the other indexers.

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.</br>

   ```
   ./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
```

FreeBSD

```
pkg_delete splunk
```

Uninstall Splunk Enterprise from a different location

```
pkg_delete -p /usr/splunk splunk
```

Solaris

```
pkgrm splunk
```

HP-UX

1. Stop Splunk Enterprise.

   ```
   $SPLUNK_HOME/bin/splunk stop
   ```
2. If you enabled boot-start, run the following command as the root user.

   ```
   $SPLUNK_HOME/bin/splunk disable boot-start
   ```
3. Delete the Splunk installation directories.

   ```
   rm -rf $SPLUNK_HOME
   ```

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
```

Note: 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 and Solaris:

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

   For FreeBSD and Mac OS

   ```
   kill -9 `ps ax | grep splunk | grep -v grep | awk '{print $1;}'`
   ```
3. Remove the Splunk Enterprise installation directory, `$SPLUNK_HOME`.

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

   On Mac OS, 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, Solaris, and FreeBSD:
   ```
   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

This topic includes the PGP public key and installation instructions. You can also download the file using HTTPS.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.1 (GNU/Linux)

mQGiBEbE21QRBADEMonUxCV2kQ2oxsJTjYXrYCWCtH5/OnmhK5lT2TQaE9QUTs+w
nM3sVInQqwRwBDH2qsHgqjJS0PIE867n+lVuk0gSVzS5SOlYzQjnSrisvyN452MF
2PgetHq8Lb884cPJnxR6xoFTHqOQueKEOXCovz1eVrjrjfpnmWKa/+5X8wCg/CJ7
pT7OXHFN4XOseVQabetEbWcEAIUaazF2i2x9QDJ+6twTAlX2oqAquqtBzJX5qaHn
OyRdBEU2g4ndiE3QAKybuq5f0UM7GXqdllihVUBatqafySfjlTBaMVzd4ttrDRpq
Wya4ppPMIWcnFG2CXf4+HuyTPgj2cry2oMBm2LMfGhxcqM5mpoyHqUiCn7591Ra/
J2/FA/0c2UAUh/eSiOn89I6FhFOicT5RPtRpxMoEM1Di15zJ7EXY+xBVF9rutqhR
5OI9kdHibYTwf4qjOOPOA7237N1by9GiXY/8s+rDWmSNKZB+xAaLyl7cDhYMv7CP
qFTutvE8BxTsF0MgRuzIHfJQE2quuxKJFs9lkSFGuZhvRuwRcrQgS2ltIFdhbGxh
Y2UgPHJlbGVhc2VAc3BsdW5rLmNvbT6IXgQTEQIAHgUCRsTbVAIbAwYLCQgHAwID
FQIDAxYCAQIeAQIXgAAKCRApYLH9ZT+xEhsPAKDimP8sdCr2ecPm8mre/8TK3Bha
pQCg3/xEickiRKKlpKnySUNLR/ZBh3m5Ag0ERsTbbRAIAIdfWiOBeCj8BqrcTXxm
6MMvdEkjdJCr4xmwaQpYmS4JKK/hJFfpyS8XUgHjBz/7zfR8Ipr2CU59Fy4vb5oU
HeOecK9ag5JFdG2i/VWH/vEJAMCkbN/6aWwhHt992PUZC7EHQ5ufRdxGGap8SPZT
iIKY0OrX6Km6usoVWMTYKNm/v7my8dJ2F46YJ7wIBF7arG/voMOg1Cbn7pCwCAtg
jOhgjdPXRJUEzZP3AfLIc3t5iq5n5FYLGAOpT7OIroM5AkgbVLfj+cjKaGD5UZW7
SO0akWhTbVHSCDJoZAGJrvJs5DHcEnCjVy9AJxTNMs9GOwWaixfyQ7jgMNWKHJp+
EyMAAwYH/RLNK0HHVSByPWnS2t5sXedIGAgm0fTHhVUCWQxN3knDIRMdkqDTnDKd
qcqYFsEljazI2kx1ZlWdUGmvU+Zb8FCH90ej8O6jdFLKJaq50/I/oY0+/+DRBZJG
3oKu/CK2NH2VnK1KLzAYnd2wZQAEja4O1CBV0hgutVf/ZxzDUAr/XqPHy5+EYg96
4Xz0PdZiZKOhJ5g4QjhhOL3jQwcBuyFbJADw8+Tsk8RJqZvHfuwPouVU+8F2vLJK
iF2HbKOUJvdH5GfFuk6o5V8nnir7xSrVj4abfP4xA6RVum3HtWoD7t//75gLcW77
kXDR8pmmnddm5VXnAuk+GTPGACj98+eISQQYEQIACQUCRsTbbQIbDAAKCRApYLH9
ZT+xEiVuAJ9INUCilkgXSNu9p27zxTZh1kL04QCg6YfWldq/MWPCwa1PgiHrVJng
p4s=
=Mz6T
-----END PGP PUBLIC KEY BLOCK-----
```


Install the key

1. Copy and paste the key into a file, or download the file using HTTPS.

2. Install the key using:

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