



## **Splunk Installation Manual**

**Version: 3.4.9**

**Generated: 11/22/2009 03:06 am  
Copyright Splunk, Inc. All Rights Reserved**

# Table of Contents

<b><u>Read This First</u></b> .....	<b>1</b>
<u>What's in the Installation Manual?</u> .....	1
<u>System requirements</u> .....	1
<b><u>Step by Step Installation</u></b> .....	<b>4</b>
<u>Before you install</u> .....	4
<u>AIX installation</u> .....	6
<u>FreeBSD installation</u> .....	7
<u>Linux installation</u> .....	10
<u>Mac OS installation</u> .....	13
<u>Solaris installation</u> .....	16
<u>Windows installation</u> .....	19
<u>Windows installation via the commandline</u> .....	23
<u>Startup options</u> .....	27
<u>License management</u> .....	29
<u>Install Splunk Enterprise Manager</u> .....	32
<b><u>Splunk forwarder, light forwarder, and other configurations</u></b> .....	<b>33</b>
<u>Enable the Splunk forwarder or light forwarder</u> .....	33
<u>Commandline installation for Splunk forwarder or light forwarder on Windows</u> .....	36
<u>Enable Splunk desktop configuration</u> .....	37
<u>Enable the Splunk light forwarder via the deployment server</u> .....	39
<b><u>Advanced Installation Topics</u></b> .....	<b>40</b>
<u>Configure Splunk before startup</u> .....	40
<u>Run Splunk as non-root user</u> .....	41
<u>Disable update checker</u> .....	42
<u>Configure SELinux</u> .....	43
<u>Uninstall Splunk manually</u> .....	43
<b><u>Upgrade Instructions</u></b> .....	<b>45</b>
<u>Upgrade and migrate to 3.3 and later</u> .....	45
<u>Upgrade Splunk on Windows</u> .....	46
<u>Migration considerations</u> .....	48
<u>Migrate your 32-bit Splunk Windows installation to 64-bit</u> .....	50
<u>Migrate your Windows saved searches to 3.3.x and later</u> .....	52
<u>Migrate bundles to new application directory structure</u> .....	53
<b><u>Help</u></b> .....	<b>54</b>
<u>Getting Help</u> .....	54
<b><u>Reference</u></b> .....	<b>56</b>
<u>File Manifest</u> .....	56
<u>PGP Public Key</u> .....	56

# Read This First

## What's in the Installation Manual?

### What's in the Installation Manual?

Use this guide to install or upgrade Splunk, configure options for startup, and learn about configuring the Splunk light forwarder and other useful applications.

### Find what you need

You can use the table of contents to the left of this panel, or simply search for what you want in the search box in the upper right.

If you're interested in more specific scenarios and best practices, you can visit the Splunk Community Wiki to see how other users Splunk IT.

## System requirements

### System requirements

Before you download and install the Splunk software, read the following sections for the supported system requirements. If you have ideas or requests for new features to add to future releases, email Splunk Support. Also, you can follow our Product Roadmap.

Refer to the download page for the latest version to download. Check the release notes for details on known and resolved issues.

**Caution:** Splunk does not provide a direct upgrade path to version 3.2.x from versions earlier than 3.0. You cannot upgrade directly from 2.x to 3.2. If you are upgrading from an earlier version of Splunk, refer to the upgrade and migration instructions for upgrading to 3.0 and upgrade to 3.0 or 3.1 before proceeding.

### Host operating system

- Linux 2.6+ kernel Linux distributions (x86 and x86\_64) and major 2.4+ kernel Linux distributions with NPTL (x86)
- Solaris 8, 9 & 10 / Sparc
- Solaris 9 & 10 / x86
- Mac OS X 10.4+ / x86 and PPC
- FreeBSD 6.1 (6.2 for 64-bit versions) or later
- AIX 5.2 and 5.3
  - ◆ AIX 5.4 has not yet been tested by Splunk. If you want to give it a try, please install it on a test server and send us feedback.
- 32-bit: Windows 2000, XP, Windows Server 2003, Vista, Windows Server 2008
- 64-bit: Windows Server 2003, Vista, Windows Server 2008

**Important:** Running the 64-bit version of Splunk for Windows on a 32-bit platform is not recommended. If you can run Splunk on 64-bit hardware, we strongly recommend it. The

performance is greatly improved over the 32-bit version.

**Note:** Splunk is certified to run on English versions of Windows only. Non-English operating systems are not supported.

**Note:** Windows registry monitoring is not supported on Windows 2000 due to an issue with a Windows 2000 DLL.

**Client operating system / browser (for access to Splunk Web)**

- AIX, BSD and Linux: Firefox 1.5 or 2.0; Adobe Flash 9 or higher
- Mac OS X: Firefox 1.5 or 2.0; Adobe Flash 9 or higher
- Windows: Internet Explorer 6 or 7 or Firefox 1.5 or 2.0; Adobe Flash 9 or higher

You can verify your installed version of Flash [here](#)

**Hardware capacity requirements**

Splunk is a high-performance application. If you are performing a comprehensive evaluation of Splunk for production deployment, we recommend that you use hardware typical of your production environment; this hardware should **meet or exceed** the recommended hardware capacity specifications below.

**Note:** Running Splunk in virtual machine (VM) mode on any platform will degrade performance.

**Recommended and minimum hardware capacity**

<b>Platform</b>	<b>Recommended hardware capacity</b>	<b>Minimum supported hardware capacity</b>
Non-Windows platforms	2x3.4 GHz CPU, 4 GB RAM	1x1.4 GHz CPU, 1 GB RAM
Windows platforms	Multi-core Xeon or equivalent at 3Ghz, 4GB RAM	Pentium 4 or equivalent at 2Ghz, 2GB RAM

**Note:** Use the minimum supported hardware guidelines for personal use of Splunk. We recommend you use the Splunk desktop application/configuration when using Splunk on desktops or laptops.

**Important:** For all installations including forwarders, a minimum of 2GB hard disk space for your Splunk installation is required **in addition to the space required for your index**. Refer to this topic on estimating your index size requirements in the Splunk Community area of the KnowledgeBase for some planning information.

**Important:** The minimum requirements for Splunk apply to all configurations other than Splunk light forwarder instances.

## Hardware requirements for Splunk light forwarders

Recommended	Dual Core 1.5Ghz+ processor, 1GB+ RAM
Minimum	1.0 Ghz processor, 512MB RAM

For more information on deployment planning, refer to the Deployment section of the Splunk community KnowledgeBase.

### Supported server hardware architectures

32 and 64-bit architectures are supported for some platforms. See the download page page for details.

### Supported file systems

Platform	File systems
Linux	ext2/3, reiser3, XFS
Solaris	UFS, ZFS, VXFS
FreeBSD	FFS, UFS
Mac OS X	HFS
AIX	JFS, JFS2, NFS 3/4
Windows	NTFS, FAT32

**Note:** Most other file systems are supported. If you run Splunk on a filesystem that is not listed above, Splunk may run a startup utility named `locktest`. Locktest is a program that tests the start up process. If `locktest` runs and fails, the filesystem is not suitable for running Splunk.

**Note:** On FreeBSD, mounting as `nullfs` is not supported.

### Storage and performance notes

For some tools for estimating your index size, refer to this topic on the Splunk Wiki.

For more information on ways to reduce your index density, click [here](#)

# Step by Step Installation

## Before you install

### Before you install

Before installing Splunk on your system:

- Read the system requirements.
- Check the release notes for details on known and resolved issues.
- Refer to the download page for the latest version to download.
- If you are upgrading, review the upgrade documentation later in this manual and check the migration documentation for any migration considerations before proceeding.

Some platform-specific installers come in both a package form and a tarball. Follow the instructions for your specific package or tarball.

Note: If you have a system maintenance process that periodically compresses files on your filesystem, you must disable this for your Splunk installation and index directories. There are many static files that are required for normal operation and must not be compressed.

### Installing as root

Splunk must run as `root` or as a member of the `splunk` group. When installing from any type of package manager that isn't a tarball, you must install as `root`. When you install Splunk with root privileges, it creates the user `splunk` and group `splunk` (if they do not already exist). If you do not install Splunk with root privileges, it won't attempt to create users or groups.

Splunk can run as any user on the local system. However, the user Splunk runs as must have access rights to read all the data inputs you define. Keep in mind that some files and directories may be in privileged locations and therefore will not be indexed if you don't have the correct ownership settings.

### Running Splunk on Windows

To *install* Splunk, you must have local administrator privileges in order to bind the ports required for `splunkd` to `splunkweb` communication. During the install process, you will have the option to select which account `splunkd` and `splunkweb` will run as consistently.

**Splunk strongly recommends that you run Splunk as the local system account if you do not need to collect data from other machines**

If you would like to collect data from additional machines remotely - for example, WMI polling of event logs, or collection IIS logs through a file share - you must install Splunk using a domain service account that you create. This account needs administrator-like permissions on the local box, and sufficient privileges on the target machines to collect your desired data. For more information on WMI polling permission setting, please refer to the WMI documentation.

You can run Splunk as another account besides local system or the local administrator. However, you must grant the following rights to the service account:

- Full control over Splunk's installation directory
- Read access to any flat-file directory (to read whatever files you are configuring it to monitor).
- Permission to log on as a service
- Permission to log on as a batch job.
- Replace a process-level token.
- Permission to act as part of the operating system.
- Permission to bypass traverse checking.

You must allow this account additional, specific permissions if you want to collect the registry or event logs.

Splunk Web's service does not require as many permissions as `splunkd` to function, and can be safely reduced to:

- Full control over Splunk's install directory
- Log on as a service

**Note:** When installing Splunk using domain account user, you must enable NetBIOS to validate the account authentication.

#### Disabling update checker

Splunk Web is configured to check for new versions of itself. If you are running Splunk on a LAN that is not connected to the rest of the Web, you will want to disable this feature.

#### What ports Splunk uses

Splunk uses two network ports by default; ports 8000 (Splunk Web) and 8089 (management port) are opened initially. You can also enable SSL for Splunk Web after you install.

#### What gets installed

For a complete list of files that Splunk installs, refer to the file manifest for your platform, located in `$SPLUNK_HOME`, at the same level as the `/etc` directory.

#### Advanced installation topics

Before you start Splunk for the first time, review the topics under Advanced Installation. The topics include configuring Splunk to start at boot time, bind to an IP, and run as a non-root user.

# AIX installation

## AIX installation

This topic will guide you through installing Splunk on the AIX platform.

**Note:** If you are upgrading, review the upgrade documentation later in this manual and check the migration documentation for any migration considerations before proceeding.

## Install Splunk

The AIX install comes in tarball form only. We plan to provide a native install package in a later release.

When installing with the tarball:

- Splunk does not create the `splunk` user automatically. If you want Splunk 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.

To install Splunk on an AIX system, expand the tarball into an appropriate directory. The default install directory is `/opt/splunk`.

For **AIX 5.3**, check to make sure your service packs are up to date. Splunk requires the following service level:

```
$ oslevel -r  
5300-005
```

## Start Splunk

Splunk can run as any user on the local system. If you run Splunk as a non-root user, make sure that Splunk has the appropriate permissions to read the inputs that you specify. Refer to the instructions for running Splunk as a non-root user for more information.

To start Splunk from the command line interface, run the following command:

```
`${SPLUNK_HOME}/bin/splunk start
```

By convention, this document uses:

- ``${SPLUNK_HOME}` to identify the path to your Splunk installation.
- ``${SPLUNK_HOME}/bin/`` to indicate the location of the command line interface.

## Startup options

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

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

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

For more information, refer to Splunk startup options

If this is an upgrade to 3.2 or later, you have the option of reviewing changes to be made to your configuration files during migration. Refer to the upgrade instructions for more details.

## Launch Splunk Web and log in

After you start Splunk and accept the license agreement,

1. In a browser window, access Splunk Web at `http://<hostname>:port`.

- `hostname` is the host machine.
- `port` is the port you specified during the installation (the default port is 8000).

2. If you are running Splunk with a Free license, Splunk Web launches without prompting you for login information. If you are running Splunk with an Enterprise license, Splunk Web prompts you for login information (default, username `admin` and password `changeme`) before it launches.

## Manage your license

If you are performing a new installation of Splunk or switching from one license type to another, you must update your license.

## Uninstall Splunk

Use your local package management commands to uninstall Splunk. 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.

If you can't use package management commands, follow the instructions for manually uninstalling Splunk components.

# FreeBSD installation

## FreeBSD installation

This topic will guide you through installing Splunk on the FreeBSD platform.

**Note:** If you are upgrading, review the upgrade documentation later in this manual and check the migration documentation for any migration considerations before proceeding.

### Install Splunk

The FreeBSD builds comes in two forms: an installer (5.4-intel) and a tarball (i386). Both are TGZ files.

#### Basic install

To install FreeBSD using the intel installer:

```
pkg_add splunk_package_name-5.4-intel.tgz
```

This installs Splunk in the default directory, `/opt/splunk/`

To install Splunk in a different directory:

```
pkg_add -v -p /usr/splunk splunk_package_name-5.4-intel.tgz
```

#### Tarball install

To install Splunk on a FreeBSD system, expand the tarball into an appropriate directory. The default install directory is `/opt/splunk`.

When installing with the tarball:

- Splunk does not create the `splunk` user automatically. If you want Splunk 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.

#### After you install

To ensure that Splunk functions properly on FreeBSD, you must:

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
```

A restart of the OS is required for the changes to effect.

#### What gets installed

To see the list of Splunk packages:

```
pkg_info -L splunk
```

To list all packages:

```
pkg_info
```

#### Start Splunk

Splunk can run as any user on the local system. If you run Splunk as a non-root user, make sure that Splunk has the appropriate permissions to read the inputs that you specify. Refer to the instructions for running Splunk as a non-root user for more information.

To start Splunk from the command line interface, run the following command:

```
`${SPLUNK_HOME}/bin/splunk start
```

By convention, this document uses:

- ``${SPLUNK_HOME}` to identify the path to your Splunk installation.
- ``${SPLUNK_HOME}/bin/`` to indicate the location of the command line interface.

#### Startup options

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

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

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

For more information, refer to Splunk startup options

If this is an upgrade to 3.2 or later, you have the option of reviewing changes to be made to your configuration files during migration. Refer to the upgrade instructions for more details.

#### Launch Splunk Web and log in

After you start Splunk and accept the license agreement,

1. In a browser window, access Splunk Web at `http://<hostname>:port.`

- `hostname` is the host machine.
- `port` is the port you specified during the installation (the default port is 8000).

2. If you are running Splunk with a Free license, Splunk Web launches without prompting you for login information. If you are running Splunk with an Enterprise license, Splunk Web prompts you for login information (default, username `admin` and password `changeme`) before it launches.

### Manage your license

If you are performing a new installation of Splunk or switching from one license type to another, you must update your license.

### Uninstall Splunk

Use your local package management commands to uninstall Splunk. 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.

To uninstall Splunk from the default location:

```
pkg_delete splunk
```

To uninstall Splunk from a different location:

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

## Linux installation

### Linux installation

This topic will guide you through installing or upgrading Splunk on the Linux platform.

**Note:** If you are upgrading, review the upgrade documentation later in this manual and check the migration documentation for any migration considerations before proceeding.

### Install Splunk

The Linux build comes in three forms: RPM, DEB, and tarball.

#### RedHat RPM install

To upgrade an existing Splunk installation using the RPM:

```
rpm -U splunk_package_name.rpm
```

To install the Splunk RPM from scratch, in the default directory `/opt/splunk`:

```
rpm -i splunk_package_name.rpm
```

To install Splunk in a different directory, use the `--prefix` flag:

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

To upgrade an existing Splunk installation that was done in a different directory, use the `--prefix` flag:

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

If you want to automate your RPM install with kickstart, add the following to your kickstart file:

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

**Note:** The second line is optional for the kickstart file. Read more about [Configuring Splunk to start at boot time](#).

To verify the RPM package signature, refer to our [PGP public key](#).

#### Debian DEB install

To install the Splunk DEB package:

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

**Note:** You can only install the Splunk DEB package in the default location, `/opt/splunk`.

**Important:** There is an issue with the Splunk 3.3 Debian package resulting in errors when you try to start Splunk. To work around this issue, once you've run the installer, edit `/var/lib/dpkg/info/splunk.postinst` and modify line 13 by adding a `/` before `opt` (`SPLUNK_HOME="/opt/$PRODUCT"`). Then run the script: `sh /var/lib/dpkg/info/splunk.postinst`. This completes the installation and you can then start Splunk.

This issue was resolved in Splunk 3.3.1.

#### Tarball install

To install Splunk on a Linux system, expand the tarball into an appropriate directory. The default install directory is `/opt/splunk`.

When installing with the tarball:

- Splunk does not create the `splunk` user automatically. If you want Splunk 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.

## What gets installed

Splunk package status:

```
dpkg --status splunk
```

List all packages:

```
dpkg --list
```

## Start Splunk

Splunk can run as any user on the local system. If you run Splunk as a non-root user, make sure that Splunk has the appropriate permissions to read the inputs that you specify. Refer to the instructions for running Splunk as a non-root user for more information.

To start Splunk from the command line interface, run the following command:

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

By convention, this document uses:

- `$SPLUNK_HOME` to identify the path to your Splunk installation.
- `$SPLUNK_HOME/bin/` to indicate the location of the command line interface.

## Startup options

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

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

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

For more information, refer to Splunk startup options

If this is an upgrade to 3.2 or later, you have the option of reviewing changes to be made to your configuration files during migration. Refer to the upgrade instructions for more details.

## Launch Splunk Web and log in

After you start Splunk and accept the license agreement,

1. In a browser window, access Splunk Web at `http://<hostname>:port`.

- `hostname` is the host machine.
- `port` is the port you specified during the installation (the default port is 8000).

2. If you are running Splunk with a Free license, Splunk Web launches without prompting you for login information. If you are running Splunk with an Enterprise license, Splunk Web prompts you for login information (default, username `admin` and password `changeme`) before it launches.

### Manage your license

If you are performing a new installation of Splunk or switching from one license type to another, you must update your license.

### Uninstall Splunk

Use your local package management commands to uninstall Splunk. 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.

If you can't use package management commands, follow the instructions for manually uninstalling Splunk components.

#### RedHat Linux

To uninstall from RedHat Linux

```
rpm -e splunk_product_name
```

#### Debian Linux

To uninstall from Debian Linux:

```
dpkg -r splunk
```

To purge (delete everything, including configuration files):

```
dpkg -P splunk
```

## Mac OS installation

### Mac OS installation

This topic provides detailed instructions for installing Splunk on Mac OS.

**Note:** If you are upgrading, review the upgrade documentation later in this manual and check the migration documentation for any migration considerations before proceeding.

**Important:** Users of LDAP on Mac OSX Leopard should back up `ldap.conf` before upgrading via DMG to 3.4. If you are using LDAP authentication and are upgrading from any version of Splunk to version 3.4, the Leopard DMG manager will delete your existing `ldap.conf` and replace it with the newer `ldap.conf.default`. If you've made changes to `ldap.conf`, make a backup copy of this

file before upgrading to 3.4 and then reinstate it after you have upgraded.

## Install Splunk

The Mac OS build comes in two forms: a DMG package and a tarball. Below are instructions for the:

- Graphical (basic) and command line installs using the DMG file.
- Tarball install.

### Graphical install

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 Splunk 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.

- 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**.

Your installation will begin. It may take a few minutes.

7. When your install completes, click **Finish**.

## Command line install

### 1. To mount the dmg:

```
hdiid splunk_package_name.dmg
```

### 2. To Install

- To the root volume:

```
installer -pkg splunk.pkg -target /
```

- To a different disk or partition:

```
installer -pkg splunk.pkg -target /Volumes/Disk
```

`-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, use the graphical installer as described above.

## Tarball install

To install Splunk on a Mac OS, expand the tarball into an appropriate directory. The default install directory is `/Applications/splunk`.

When installing with the tarball:

- Splunk does not create the `splunk` user automatically. If you want Splunk 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.

## Start Splunk

Splunk can run as any user on the local system. If you run Splunk as a non-root user, make sure that Splunk has the appropriate permissions to read the inputs that you specify. Refer to the instructions for running Splunk as a non-root user for more information.

To start Splunk from the command line interface, run the following command:

```
`${SPLUNK_HOME}/bin/splunk start
```

By convention, this document uses:

- ``${SPLUNK_HOME}` to identify the path to your Splunk installation.
- ``${SPLUNK_HOME}/bin/` to indicate the location of the command line interface.`

## Startup options

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

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

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

For more information, refer to Splunk startup options

If this is an upgrade to 3.2 or later, you have the option of reviewing changes to be made to your configuration files during migration. Refer to the upgrade instructions for more details.

## Launch Splunk Web and log in

After you start Splunk and accept the license agreement,

1. In a browser window, access Splunk Web at `http://<hostname>:port`.

- `hostname` is the host machine.
- `port` is the port you specified during the installation (the default port is 8000).

2. Login to Splunk with username `admin` and password `changeme`.

## Manage your license

If you are performing a new installation of Splunk or switching from one license type to another, you must update your license.

## Uninstall Splunk

Use your local package management commands to uninstall Splunk. 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.

If you can't use package management commands, follow the instructions for manually uninstalling Splunk components.

# Solaris installation

## Solaris installation

This topic provides instructions for installing Splunk on Solaris systems.

**Note:** If you are upgrading, review the upgrade documentation later in this manual and check the

migration documentation for any migration considerations before proceeding.

### **Install Splunk**

The Solaris build comes in two forms: a PKG file and a tarball.

#### **Native install**

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

1. To install Splunk using a PKG file:

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

A list of the available packages displays.

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

3. Next, the installer prompts you to specify a base installation directory.

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

#### **Native upgrade**

To upgrade an existing Splunk installation using a PKG file, use the same exact command line as you would for a fresh install.

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

You will be prompted to overwrite any changed files, answer yes to every one.

To run the upgrade silently (and not have to answer yes for every file overwrite), type:

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

#### **Tarball install**

To install Splunk on a Solaris system, expand the tarball into an appropriate directory. By default, Splunk installs into `/opt/splunk/`.

When installing with the tarball:

- Splunk does not create the `splunk` user automatically. If you want Splunk 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.

## What gets installed

### Splunk package info:

```
pkginfo -l splunk
```

### List all packages:

```
pkginfo
```

## Start Splunk

Splunk can run as any user on the local system. If you run Splunk as a non-root user, make sure that Splunk has the appropriate permissions to read the inputs that you specify. For more information, refer to the instructions on running Splunk as a non-root user.

**Note:** If you are installing on Solaris 10, refer to this page for additional information about configuring user privileges.

To start Splunk from the command line interface, run the following command:

```
`${SPLUNK_HOME}/bin/splunk start
```

By convention, this document uses:

- ``${SPLUNK_HOME}` to identify the path to your Splunk installation.
- ``${SPLUNK_HOME}/bin/`` to indicate the location of the command line interface.

## Startup options

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

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

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

For more information, refer to Splunk startup options

If this is an upgrade to 3.2 or later, you have the option of reviewing changes to be made to your configuration files during migration. Refer to the upgrade instructions for more details.

## Launch Splunk Web and log in

After you start Splunk and accept the license agreement,

1. In a browser window, access Splunk Web at `http://mysplunkhost:port`, where:

- `mysplunkhost` is the host machine.

- `port` is the port you specified during the installation (8000).

2. If you are running Splunk with a Free license, Splunk Web launches without prompting you for login information. If you are running Splunk with an Enterprise license, Splunk Web prompts you for login information (default, username `admin` and password `changeme`) before it launches.

### Manage your license

If you are performing a new installation of Splunk or switching from one license type to another, you must update your license.

### Uninstall Splunk

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

```
pkgrm splunk
```

If you can't use package management commands, follow the instructions for manually uninstalling Splunk components.

## Windows installation

### Windows installation

**Important:** By default, starting with version 3.4 of Splunk, Splunk for Windows is installed with the Splunk Desktop application configuration pre-enabled. You can change this by either specifying another application using the `SPLUNK_APP` flag when installing via the commandline, or by disabling the SplunkDesktop application after you have completed the installation process.

**Note:** The Splunk desktop application is not enabled by default if you are upgrading to from an earlier version. It is only enabled by default if you are installing Splunk for the first time.

If you are upgrading Splunk for Windows from version 3.2.x to 3.3.x or later, please review the the Windows migration instructions before proceeding to the upgrade instructions.

You can choose to install Splunk for Windows either via the GUI installer as described in this topic, or via the commandline.

**Important:** Running the 32-bit version of Splunk for Windows on a 64-bit platform is not recommended. If you can run 64-bit Splunk on 64-bit hardware, we strongly recommend it. The performance is greatly improved over the 32-bit version.

Before you proceed, be sure to review this important information about running Splunk on Windows.

You can also watch this video walkthrough of the Windows installation.

#### Choosing the user Splunk should run as

When you run the Splunk Windows installer, you are given the option to select a user Splunk will run as.

If you install as the Local System user, Splunk will have access to all or nearly all of your local machines' important information. However, the Local System user has no privileges on other Windows machines by design. If you intend to read Event Logs or performance counters from other machines via WMI, or read network shares for log files, you will need a domain account. That account must be a local Administrator or equivalent, and should have rights to the external data you want to Splunk. Please consult your Windows domain administrator for an account if you are unsure of what credentials to give Splunk.

Minimum permissions required for the two Splunk services:

#### Required user rights for the splunkd service:

- Full control over Splunk's installation directory
- Read access to any flat-files
- Permission to log on as a service
- Permission to log on as a batch job
- Replace a process-level token
- Permission to act as part of the operating system
- Permission to bypass traverse checking

#### Required user rights for the splunkweb service:

- Full control over Splunk's installation directory
- Permission to log on as a service

**Note:** These are the rights that `splunkd` and `splunkweb` specifically invoke. Other rights or permissions may be required depending on your usage and what data you want to access. Additionally, many user right assignments and other group policy restrictions can prevent Splunk from running. If you have issues, consider using a tool such as Sysinternals to troubleshoot your environment, or reverting to running the `splunkd` service as an administrator or equivalent account.

**Important:** If you must change the user Splunk runs as after you have installed, you must ensure that the user you create has the necessary permissions, and also ensure that that user has Full Control permissions to the `%SPLUNK_HOME%\var` directory.

#### Install Splunk via the GUI installer

The Windows installer is an MSI file.

1. To start the installer, double-click the `splunk.msi` file.

The Welcome panel is displayed.

2. To begin the installation, click **Next**.

**Note:** On each panel, you can click **Next** to continue, **Back** to go back a step, or **Cancel** to close the installer.

The licensing panel is displayed.

3. Read the licensing agreement and select "I accept the terms in the license agreement". Click **Next** to continue installing.

The **Customer Information** panel is displayed.

4. Enter the requested details and click **Next**.

The **Destination Folder** panel is displayed.

**Note:** Splunk is installed by default into the `\Program Files\Splunk`.

5. Click **Change...** to specify a different location to install Splunk, or click **Next** to accept the default value.

The **Logon Information** panel is displayed.

Splunk installs and runs two Windows services, `splunkd` and `splunkweb`. These services will be installed and run as the user you specify on this panel. You can choose to run Splunk with Local System credentials, or provide a specific account. That account should have local administrator privileges, plus appropriate domain permissions if you are collecting data from other machines.

The user Splunk runs as must have permissions to:

- Run as a service.
- Read whatever files you are configuring it to monitor.
- Collect performance or other WMI data.
- Write to Splunk's directory.

**Note:** If you install as the Local System user, some network resources may not be available to the Splunk application. Additionally, WMI remote authentication will not work; this user has null credentials and Windows servers normally disallow such connections. Only local data collection with WMI will be available. Contact your systems administrator for advice if you are unsure what user to specify.

6. Select a user type and click **Next**.

If you specified the local system user, proceed to step 8. Otherwise, the **Logon Information: specify a username and password** panel is displayed.

7. Specify a username and password to install and run Splunk and click **Next**.

**Note:** To use an existing user, you can enter or browse for the username and domain details. Splunk recommends using the **Browse...** button to ensure that you select a valid user. If you cannot browse for the user because that user doesn't exist in your security context, or you mistype the username, your installation will fail. Splunk cannot start without a valid username and password; browsing confirms the user is correct.

**Important:** You cannot change the user Splunk runs as or the directory into which Splunk is installed during an upgrade. Also, changing the user Splunk runs as through the Windows Service Control Panel is not supported; Splunk will stop functioning. Make sure you define and select the user account to correctly reflect the access you want Splunk to have.

The Configure Splunk Data Sources panel is displayed.

8. Check or uncheck boxes to tell Splunk what data you want monitored and indexed:

- Select which Windows event logs you want indexed
- Choose which local registry hives to monitor, and whether or not Splunk should establish a baseline snapshot for them when it starts next. Refer to the documentation about Windows registry inputs for information.
- Choose to enable WMI collection of local system data. Refer to the documentation about WMI inputs for more information.

**Important:** If you choose to enable baseline snapshots of your local registry hives, you may notice this process taking a long time, especially if you have installed Splunk with the default desktop application configuration enabled. The reason for this is that this configuration throttles the process so that it will not overwhelm your system. For more information about baseline snapshots and monitoring the Windows registry, refer to [Get a baseline snapshot](#).

The pre-installation summary panel is displayed.

9. Click **Install** to proceed.

The installer runs and displays the **Installation Complete** panel. You may see a number of warnings in a command prompt dialog box; you can safely ignore these.

10. Check the boxes to **Start Splunk** and **Start Splunk Web** now. Click **Finish**.

The installation completes, Splunk starts, and Splunk Web launches in a supported browser.

**Note:** The first time you access Splunk Web after installation, login with the default username `admin` and password `changeme`.

#### Launch Splunk in a Web browser

To access Splunk Web after you start Splunk on your machine, you can either:

- Click the Splunk icon in **Start>Programs>Splunk**

or

- Open a Web browser and navigate to `http://localhost:8000`.

Log in using the default credentials: username: `admin` and password: `changeme`. Be sure to change the admin password as soon as possible and make a note of what you changed it to.

Now that you're ready to use Splunk, refer to the User Manual and begin with the Splunk Tutorial.

#### Change the Splunk Web or splunkd service ports

If you want the Splunk Web service or the splunkd service to use a different port, you can change the defaults.

- To change the splunk web service port:

From the `%SPLUNK_HOME%\bin\` directory: `splunk set web-port ####`

- To change the splunkd port:

From the `%SPLUNK_HOME%\bin\` directory: `splunk set splunkd-port ####`

#### Avoid 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

#### Install or upgrade license

If you are performing a new installation of Splunk or switching from one license type to another, you must update your license.

#### Uninstall Splunk

To uninstall Splunk, use the **Add or Remove Programs** option in the **Control Panel**.

## Windows installation via the commandline

#### Windows installation via the commandline

**Important:** By default, starting with version 3.4 of Splunk, Splunk for Windows is installed with the Splunk Desktop application configuration pre-enabled. You can change this by either specifying another application using the `SPLUNK_APP` flag when installing via the commandline as described in this topic, or by disabling the SplunkDesktop application after you have completed the installation process.

If you are upgrading Splunk for Windows from version 3.2.x to 3.3.x or later, please review the the Windows migration instructions before proceeding to the upgrade instructions.

You can install Splunk for Windows using the MSI on the commandline by typing the following:

```
msiexec.exe /i Splunk.msi
```

This section lists the available flags for doing this, as well as provides a few examples of doing this in various configurations.

You can specify

- which Windows event logs to index or not
- which Windows registry hive to monitor
- which WMI information to pull
- the user Splunk runs as (be sure the user you specify has the appropriate permissions to access the content you want Splunk to index)
- an included application configuration for Splunk to enable (such as the Splunk light forwarder)
- whether or not Splunk should start up automatically when the installation is completed

**Important:** If you are enabling the Splunk forwarder, Splunk will start automatically; this cannot be overridden.

**Note:** The first time you access Splunk Web after installation, log in with the default username `admin` and password `changeme`.

#### Supported flags

The following is a list of the flags you can use when installing Splunk for Windows via the commandline.

**Note:** To run the installation silently, add `/quiet` to the end of your string.

Use this flag to specify directory to install. Default is `c:\program files\splunk`.

- `INSTALLDIR=<directory_path>`

Use these flags to specify whether or not Splunk should index a particular Windows event log. All three are set to 1 (on) by default.

- `WINEVENTLOGAPPCHECK=1/0`
- `WINEVENTLOGSECHECK=1/0`
- `WINEVENTLOGSYSCHECK=1/0`

Use these flags to specify whether or not Splunk should index the Windows registry USER hive. By default these are set to 0 (off).

- `REGISTRYCHECK_U=1/0`

- REGISTRYCHECK\_BASELINE\_U=1/0

Use these flags to specify whether or not Splunk should index the Windows registry LocalMachine hive. By default, these are set to 0 (off).

- REGISTRYCHECK\_LM=1/0
- REGISTRYCHECK\_BASELINE\_LM=1/0

Use these flags to specify which WMI performance information to index. These are set to 0 (off) by default.

- WMICHECK\_DISK=1/0
- WMICHECK\_MEMORY=1/0
- WMICHECK\_SPLUNKD=1/0

Use this flag to specify a user Splunk should run as. Supported values are: 1 for the LocalSystem user and 2 for a different user. The default value is 1.

- RBG\_LOGON\_INFO\_USER\_CONTEXT=1/2

Use these flags to provide username, password, and group membership information for the user specified in RBG\_LOGON\_INFO\_USER\_CONTEXT

- IS\_NET\_API\_LOGON\_USERNAME="<username>"
- IS\_NET\_API\_LOGON\_PASSWORD="<pass>"

Use this flag to specify an included Splunk application configuration to enable for this installation of Splunk. Currently supported options for <SplunkApp> are: SplunkLightForwarder, SplunkForwarder, SplunkDesktop. Refer to the documentation about the Splunk forwarder, light forwarder, and desktop configurations for more information. If you specify either the Splunk forwarder or light forwarder here, you must also specify FORWARD\_SERVER="<server:port>"

- SPLUNK\_APP=<SplunkApp>

**Note:** By default, Splunk enables the Splunk desktop application configuration when you install on Windows. You can change this by either specifying another application using the `SPLUNK_APP` flag, or by disabling the SplunkDesktop application after you have completed the installation process. To install Splunk with no applications at all, specify this flag but leave the value empty ( `SPLUNK_APP=""` ).

Use this flag *only* when you are also using `SPLUNK_APP` to enable either the Splunk forwarder or light forwarder. Specify the server and port of the Splunk server to which this forwarder will send data.

- FORWARD\_SERVER="<server:port>"

Use this flag to specify whether or not Splunk should start up automatically when the installation completes. The default value is 1 (on).

- LAUNCHSPLUNK=0/1

**Important:** If you are enabling the Splunk forwarder, Splunk will start automatically; this cannot be overridden.

**Install Splunk to run as LocalSystem:**

```
msiexec.exe /i Splunk.msi RBG_LOGON_INFO_USER_CONTEXT=1
```

**Install Splunk to run as another user in the system or domain:**

**Note:** If you pick this option, you **MUST** provide a username and password.

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder" RBG_LOGON_INFO_USER_CONTEXT=2 IS_NET_API
```

**Specify the username and the group/domain the user belongs to:**

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder" RBG_LOGON_INFO_USER_CONTEXT=2 IS_NET_API
```

**Enable SplunkForwarder, disable 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>" WINEVENT
```

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

**Launch Splunk in a Web browser**

To access Splunk Web after you start Splunk on your machine, you can either:

- Click the Splunk icon in **Start>Programs>Splunk**

or

- Open a Web browser and navigate to `http://localhost:8000`.

Log in using the default credentials: username: `admin` and password: `changeme`. Be sure to change the admin password as soon as possible and make a note of what you changed it to.

Now that you're ready to use Splunk, refer to the User Manual and begin with the Splunk Tutorial.

**Avoid 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

**Install or upgrade license**

If you are performing a new installation of Splunk or switching from one license type to another, you must update your license.

## Uninstall Splunk

To uninstall Splunk, use the **Add or Remove Programs** option in the **Control Panel**.

You can also use `msiexec` from the commandline.

## Startup options

### Startup options

This topic discusses options for starting Splunk and Splunk server processes after a new installation.

By convention, this document uses:

- `$SPLUNK_HOME` to identify the path to your Splunk installation.
- `$SPLUNK_HOME/bin/` to indicate the location of the command line interface.

### Add Splunk to your shell path

Before you continue, you may want to set a `SPLUNK_HOME` environment variable and add `$SPLUNK_HOME/bin` to your shell's path. The example below works for bash users who accepted the default installation location. Use the correct syntax and path for your own installation.

```
# export SPLUNK_HOME=/opt/splunk
# export PATH=$SPLUNK_HOME/bin:$PATH
```

### Start Splunk

To start Splunk, use the command line interface:

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

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

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

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

The startup sequence displays:

```
Checking prerequisites...
Checking http port [8000]: open
Checking mgmt port [8089]: open
```

```
Verifying configuration. This may take a while...
Finished verifying configuration.
Checking index directory...
Verifying databases...
Verified databases: _audit, _blocksignature, _internal, _thefishbucket, history, main, sampled
Checking index files
All index checks passed.
All preliminary checks passed.
Starting splunkd...
Starting splunkweb...
Splunk Server started.
The Splunk web interface is at http://<hostname>:8000
If you get stuck, we're here to help. Feel free to email us at 'support@splunk.com'.
```

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

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

### Start and disable individual processes

You can start and stop individual Splunk processes by adding the process as an object to the `start` command. The objects include:

- `splunkd`, the Splunk server daemon.
- `splunkweb`, Splunk's Web interface process.
- `watchdog`, a keep-alive process that restarts `splunkd` if it shuts down. When it notices the `splunkd` pid no longer exists, it will try up to three times to restart `splunkd`. This option does not work on Windows. Instead, set recovery options in the Service Management console.

For example, to start only `splunkd`:

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

To disable `splunkweb`:

```
$SPLUNK_HOME/bin/splunk disable webserver
```

Or to start Splunk watchdog:

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

To shutdown watchdog, use the following command:

```
$SPLUNK_HOME/bin/splunk stop watchdog
```

For more information about `start`, refer to the CLI help page:

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

### Open Splunk in a Web browser

After Splunk starts, it displays the URL for Splunk Web at the end of its startup summary:

```
The Splunk web interface is at http://<hostname>:<port>
```

Note that `<hostname>` is specific to the machine on which you've installed Splunk and `<port>` is the HTTP port you defined at installation. The HTTP port defaults to 8000 if not otherwise specified.

To access Splunk Web, open a Web browser to this URL. Refer to the System Requirements for the list of supported Web browsers for your operating system.

To begin using Splunk, refer to the User Manual and Splunk Tutorial.

## License management

### License management

All Splunk servers require a license; Splunk provides two types of licenses, a Free license and an Enterprise license. Splunk ships with a Free license.

The first time you download Splunk, you are asked to register. Your registration authorizes you to receive the Free license, which allows a maximum indexing volume of 500 MB/day. The Free license is not a trial license and does not expire.

The Enterprise license enables higher data indexing volume and the following additional features:

- Multiple user accounts and access controls.
- Distributed search and data routing.
- Deployment management.

**Important:** Beginning with 3.4.2, users running Splunk with the Free license can set their instance to receive data from a forwarder. In earlier versions of Splunk, users needed an Enterprise license to change this distributed setting.

To evaluate Enterprise features before purchasing, you can request a 30-day trial Enterprise license.

**Important:** You cannot use the same Enterprise license on multiple servers. Each instance of Splunk (including forwarders) must have its own unique license, whether a Free license or an Enterprise license. The only exception to this is the 1 MB/day forward-only license that can be installed on multiple forwarding instances. For more information, read [About Splunk licenses](#).

#### Access your license

All Splunk servers have a license located in `$SPLUNK_HOME/etc/`, whether it is a Free license (`splunk-free.license`) or an Enterprise license (`splunk.license`).

#### Example of a Splunk license

```
user@company.com;EQ/GQXW/J7u9VLJShPsW4m8yi+5a+geRrof4Bep70j32xsBpq
JI+tM5pdntRf14auply366BAjTMnfTB6JyzJOZLplyBQijk02fQjgKjak10o14N5G6Wr
09ufnSe3iOXVAay24hzFfgDkaijOnkoGOPJqnHaVzaWC9dxIuKUvDpt3UcKtKdv0Gka
Q4EZxAvZKAFImvOF4PmDoNaMiBgLLkWibGhezFTTDh10PLl9kyeVThGzAyN23J512pVM
3xqNIg3pFcd2aJf31xspt1HRdSwofkfnuCVpzildy3qMbae4g85KpCfND+aJ6z2LoUu3
RQ4OV4SpXMXEZ4PgSGZ6dwA==
```

#### Where is your new license?

When you request a new license, you should receive the license in an email from Splunk. You can also access that new license in your `splunk.com` My Orders page. To install a new license (or change and update your existing license), replace your existing license with the new license.

You can install and update your licenses from Splunk Web's **Admin > License & Usage** page or with the CLI.

**Note:** These instructions are for Splunk 3.0 and later, for earlier versions, see 2.2.3 instructions.

#### Install via Splunk Web

To install or update your license using Splunk Web:

1. Start Splunk and open Splunk Web in a supported browser.
2. On the upper righthand corner of any of the dashboards, click **Admin**.
3. Click **License & Usage**.

The **Admin > License & Usage** page displays your license level, peak usage and license violations.

4. Click **Change License**.

The **License & Usage: Change License** page opens and displays your existing license key or `splunk.license` file.

5. Copy your new license key and paste (overwrite) the existing license.

6. Click **Save**.

7. Restart your Splunk server to apply your new license.

**Note:** You can restart your server from Splunk Web. On the **Admin > Server: Control Server** page, click **Restart Now**.

#### Install via CLI

To install or update your license using the CLI:

1. Create a new file named `splunk.license`.

2. Copy your new license key and paste it into `splunk.license`.

3. Move your license file, `splunk.license`, into the `$SPLUNK_HOME/etc/` directory:

```
mv splunk.license $SPLUNK_HOME/etc/
```

**Note:** If a `splunk.license` file already exists in this directory, `mv` will overwrite it without prompting for confirmation of the action. This does not overwrite the Free license, `splunk-free.license`. However, by default Splunk ignore the Free license file if `splunk.license` exists.

4. Restart your Splunk server to apply your new license:

```
$SPLUNK_HOME/bin/splunk restart
```

#### First login after applying new trial or Enterprise license

To log in for the first time after applying an Enterprise license (converting from free), use the default username "admin" with the password "changeme". If you later clean (reset) your user data, your username/password is reset to this default.

#### License violations

Violations occur when you exceed the maximum indexing volume allowed for your license. If you exceed your licensed daily volume on any one calendar day, you will get a violation warning. The message persists for 14 days. If you have more than 7 violations in a rolling 30-day period, search will be disabled. Search capabilities return when you have less than 7 violations in the previous 30 days or when you apply a new license with a larger volume limit.

**Note:** During a license violation period, Splunk does not stop indexing your data. Splunk only blocks access while you exceed your license.

If you have other issues with your license, refer to the Admin Manual for troubleshooting tips.

## Install Splunk Enterprise Manager

### Install Splunk Enterprise Manager

Get stats on your Splunk!

Splunk Enterprise Manager provides visibility into the connectivity of Splunk forwarders to one or more indexers, the availability of Splunk forwarders and indexers, the data volumes passed by forwarders and the data volumes consumed by indexers. You can get it by going to:

[http://www.splunkbase.com/apps/All/Operations/Server\\_Management/app:Splunk+Enterprise+Manager](http://www.splunkbase.com/apps/All/Operations/Server_Management/app:Splunk+Enterprise+Manager).

Install from the Splunk Admin-->Applications page in Splunk Web following the instructions in "Installing Splunk Applications" in the Admin Guide.

By default, the dashboard that Enterprise Manager adds to Splunk is only viewable by the "admin" user, but you can change this in `prefs.conf` using the information in "Configure application directories" in the Admin Guide.

# Splunk forwarder, light forwarder, and other configurations

## Enable the Splunk forwarder or light forwarder

### Enable the Splunk forwarder or light forwarder

As of version 3.4, the Splunk forwarder and light forwarder (formerly referred to as the lightweight forwarder) are now packaged as applications that you can enable via Splunk Web or the CLI.

**Important:** If you are configuring forwarding and receiving, your receiving Splunk instance must be running the same (or later) version of Splunk as your forwarders. Also, you cannot use data balancing in conjunction with the light forwarder because the data is not parsed before being sent--events may be split into parts before reaching the receiver, resulting in partial events.

### What's different about the Splunk light forwarder?

The Splunk light forwarder can monitor local log files and directories, collect Windows event logs and use scripted inputs (including local WMI and registry data sources on Windows). To cut down on overhead, however, many other features are disabled.

Specifically, the Splunk light forwarder:

- Disables event signing and checking if the disk is full  
(`/$SPLUNK_HOME/etc/apps/SplunkLightForwarder/default/default-mode.conf`)
- Limits internal data inputs to `splunkd` and metrics logs only, and makes sure these are forwarded  
(`/$SPLUNK_HOME/etc/apps/SplunkLightForwarder/default/inputs.conf`)
- Disables most local indexing  
(`/$SPLUNK_HOME/etc/apps/SplunkLightForwarder/default/indexes.conf`)
- Does not parse data. Therefore, install applications that include `inputs.conf` on both the light forwarder and the receiving instance.
- Disables the Splunk Web interface  
(`/$SPLUNK_HOME/etc/apps/SplunkLightForwarder/default/web.conf`)
- Limits throughput to 256KBps on monitor, exec, and Windows event log inputs  
(`/etc/apps/SplunkLightForwarder/default/limits.conf` and the configurations under `/etc/apps/SplunkLightForwarder/config/input/*`)
- Disables the following modules in  
(`/$SPLUNK_HOME/etc/apps/SplunkLightForwarder/default/setup.conf`):

```
[modules]
distributedDeployment = disabled
distributedSearch = disabled
input/FIFO = disabled
input/UDP = disabled
input/tcp = disabled
input/syslogFIFO = disabled
input/syslogUDP = disabled
```

These modules are the deployment server (not the deployment client), distributed search, and from named pipes / FIFOs, and direct input from network ports.

For a detailed view of the exact configuration, look at the `setup.conf` file for the SplunkLightForwarder application in

`$SPLUNK_HOME/etc/apps/SplunkLightForwarder/default`, where `$SPLUNK_HOME` is the directory into which you installed Splunk.

#### Change the configuration

To alter the configuration of Splunk light forwarder (to add back in a specific input type, for example), edit the `setup.conf` for the SplunkLightForwarder application. To change the bandwidth limit, create a new `limits.conf` in a local directory (do not change the one in default) with a new `[thruput]` stanza for your desired limit.

#### What's different about the Splunk forwarder?

The Splunk forwarder disables the following modules in

(`$SPLUNK_HOME/etc/apps/SplunkForwarder/default/setup.conf`):

```
[modules]
distributedDeployment = disabled
distributedSearch = disabled
input/FIFO = disabled
```

These modules are the deployment server (not the deployment client), distributed search, and input from named pipes / FIFOs.

All other functions and modules remain enabled.

For a detailed view of the exact configuration, you can look at the `setup.conf` file for the SplunkForwarder application in `$SPLUNK_HOME/etc/apps/SplunkForwarder/default`, where `SPLUNK_HOME` is the directory into which you installed Splunk.

#### Read this before you enable Splunk forwarder or light forwarder

Splunk Web is turned off in the light forwarder to reduce the footprint of Splunk on the forwarding host. Therefore, if you want to use Splunk Web to configure your forwarding Splunk instance, do this **before** you enable the forwarder application. After you enable the forwarder application, you can only configure your forwarder via the Splunk CLI.

You must configure a receiver before setting up forwarding. This way, the Splunk receiving host is prepared for the forwarded data. Then, configure your forwarder(s). Follow these general steps to deploy Splunk forwarders and light forwarders effectively.

First, enable a Splunk server to receive data:

1. Decide which machine to use as a receiver.

2. Configure it to receive data using these instructions.

**Note:** Your receiving Splunk instance must be running the same version of Splunk as your forwarders, or a later version.

Then, on the forwarding Splunk instance:

1. Install Splunk on the machine that will be forwarding data.
2. Enable data forwarding by pointing your forwarder at the receiver using these instructions. You have the option of enabling local indexing at this time, which means that any data that is forwarded is also indexed locally. This applies to any pre-existing data on the forwarder as well.
3. Use Splunk Web or the CLI to add inputs as described here. Data from these inputs will be sent via the forwarder to the receiver as soon as you do this (and indexed locally if you've configured this).
4. Then, use Splunk Web or the CLI to enable Splunk forwarder or light forwarder.

After you configure a Splunk instance to forward data, add any additional settings, such as routing, cloning, filtering or data balancing. Configuration changes are done on the forwarder side, on the host that is reading the data input.

If, once you've enabled the Splunk forwarder or light forwarder, you want to disable it, you must do it via the CLI as described below.

**Important:** You MUST provide this forwarder/light forwarder with the hostname and port of the Splunk server to which it will send data, using the information in this topic. You must also use the same information to set the Splunk server that will be receiving the data as a receiver.

#### Licensing for Splunk forwarder and light forwarder

When you enable either the Splunk forwarder or light forwarder, you must manually switch licenses as appropriate.

#### Enable via Splunk Web

To enable Splunk forwarder or light forwarder via Splunk Web:

1. Log into Splunk Web.
2. Navigate to the Admin section, and click **Applications**.

The **Applications:View/Manage Applications** page is displayed.

3. Find the Splunk application you want to enable for this system and click **Enable**.

The application is enabled.

**Note:** Remember, if you enable Splunk forwarder or light forwarder, Splunk Web will subsequently be unreachable.

#### Enable via CLI

To enable Splunk forwarder or light forwarder via the CLI:

```
./splunk enable app [SplunkForwarder|SplunkLightForwarder] -auth <username>:<password>
```

**Note:** If you are running Splunk with a free license, you do not have to provide a username and password.

#### Disable via CLI

To disable Splunk forwarder or light forwarder via the CLI:

```
./splunk disable app [SplunkForwarder|SplunkLightForwarder] -auth <username>:<password>
```

**Note:** If you are running Splunk with a free license, you do not have to provide a username and password.

## Commandline installation for Splunk forwarder or light forwarder on Windows

### Commandline installation for Splunk forwarder or light forwarder on Windows

This procedure gives some examples of how to install Splunk with the Splunk forwarder or light forwarder application pre-enabled via the commandline on Windows. You can do this silently (so that you can script it) or interactively. **All the flags for installing Splunk for Windows via the commandline are described in this Windows installation topic.**

**Note:** By default, Splunk enables the Splunk desktop application configuration when you install on Windows. You can change this by either specifying another application using the `SPLUNK_APP` flag, or by via Splunk Web disabling the Splunk desktop application after you have completed the installation process.

**Important:** You MUST provide the forwarder/light forwarder with the hostname and port of the Splunk server to which it will send data, using the information in this topic. You must also use the same information to set the Splunk server that will be receiving the data as a receiver.

**Note:** If you are enabling a Splunk light forwarder, Splunk will start automatically when the installation process is completed. If you want Splunk to not start automatically, add

```
LAUNCHSPLUNK=0
```

to your installation string.

**Important:** If you are enabling the Splunk forwarder, Splunk will start automatically; this cannot be overridden.

#### Silent commandline install of Splunk light forwarder

This example installs Splunk via the MSI with the Splunk light forwarder application configuration enabled:

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkLightForwarder" FORWARD_SERVER="<server:port>" /quiet
```

where "<server:port>" are the server and port of the Splunk server to which this light forwarder will send data.

#### Commandline install of Splunk forwarder as the LocalSystem user

This example installs Splunk via the MSI to run as the LocalSystem user with the Splunk forwarder application configuration enabled:

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder" FORWARD_SERVER="<server:port>" RBG_LOGO=
```

where "<server:port>" are the server and port of the Splunk server to which this forwarder will send data.

## Enable Splunk desktop configuration

#### Enable Splunk desktop configuration

Starting with version 3.4 of Splunk, you can enable a lighter configuration of Splunk designed especially for desktop machines like Windows and Mac laptops. Splunk desktop is not a Splunk forwarder, but rather a scaled-back Splunk for use on non-production-level hardware. Use the Splunk desktop configuration for your own personal Splunk installation, or when you're trying out Splunk on your laptop for the first time.

#### What's different about Splunk desktop?

This configuration scales back the indexing throughput and disables the file system change monitor. This keeps Splunk from using a lot of memory and processing power on systems you use for other purposes (like laptops).

To alter the configuration of Splunk desktop (to add back in a specific input type, for example), you can edit the `setup.conf` for the SplunkDesktop application in `$SPLUNK_HOME/etc/apps/SplunkDesktop/default`, where `SPLUNK_HOME` is the directory into which you installed Splunk.

**Note:** Splunk desktop is configured by default when you install Splunk on Windows. You can disable it and run Splunk in its standard configuration by following the instructions below.

**Note:** The Splunk desktop configuration disables deployment server functionality, but supports running as a deployment client. To run the Splunk deployment server, you must disable the desktop configuration app.

#### Enable via Splunk Web

To enable Splunk desktop via Splunk Web:

1. Log into Splunk Web.
2. Navigate to the Admin section, and click **Applications**.

The **Applications:View/Manage Applications** page is displayed.

3. Find SplunkDesktop and click **Enable**.
4. Restart Splunk server from **Server > Control screen**.

The application is enabled.

#### Disable via Splunk Web

When you disable Splunk desktop, Splunk reverts to a standard deployment. This means that all limits on indexing and throughput are removed, and Splunk will use more memory and processing power.

1. Log into Splunk Web.
2. Navigate to the Admin section, and click **Applications**.

The **Applications:View/Manage Applications** page is displayed.

3. Find SplunkDesktop and click **Disable**.
4. Restart Splunk server from **Server > Control screen**.

The application is disabled.

#### Enable via CLI

To enable Splunk desktop via the CLI:

```
./splunk enable app SplunkDesktop -auth <username>:<password>  
./splunk restart
```

## Disable via CLI

To disable Splunk desktop via the CLI:

```
./splunk disable app SplunkDesktop -auth <username>:<password>  
./splunk restart
```

## Enable the Splunk light forwarder via the deployment server

### Enable the Splunk light forwarder via the deployment server

Splunk 3.4 introduces the Splunk light forwarder application. Enabling this application on your Splunk deployment client configures it to be a Splunk light forwarder. This application is installed with Splunk 3.4 and later by default, but is not enabled by default.

Once you've installed Splunk on your deployment clients, you can use the Splunk deployment server to enable the Splunk light forwarder application.

To do this, you must first have set up a deployment server and clients. Then, deploy the `$/SPLUNK_HOME/etc/modules/distributedDeployment/classes/EnableLightForwarder` server class using the standard deployment instructions. This restarts Splunk on the deployment client, and enables the light forwarder.

You can configure the deployment client to monitor the files and directories you're interested in either before or after you enable the light forwarder. Refer to these recommendations before proceeding.

**Note:** You cannot use "round-robin" forwarding in conjunction with the light forwarder because the data is not parsed before being sent--events may be split into parts before reaching the receiver, resulting in partial events.

# Advanced Installation Topics

## Configure Splunk before startup

### Configure Splunk before startup

This topic discusses optional configurations you may want to include in your Splunk work environment.

#### To start at boot time

Splunk provides a utility that updates your system boot configuration so that Splunk starts when the system boots up. This utility creates a suitable `init` script (or makes a similar configuration change, depending on your OS).

As root, run:

```
$SPLUNK_HOME/bin/splunk enable boot-start
```

If you don't start Splunk as root, you can pass in the `-user` parameter to specify which user to start Splunk as. For example, if Splunk runs as the user `bob`, then as root you would run:

```
$SPLUNK_HOME/bin/splunk enable boot-start -user bob
```

If you want to stop Splunk from running at system startup time, run:

```
$SPLUNK_HOME/bin/splunk disable boot-start
```

More information is available in `$SPLUNK_HOME/etc/init.d/README` and if you type `help boot-start` from the command line.

#### To bind to an IP

In Splunk 2.1 and all later versions, you can force Splunk to bind its ports to a specified IP address. To make this a temporary change, set the environment variable `SPLUNK_BINDIP=<ipaddress>` before starting Splunk.

If you want this to be a permanent change in your working environment, modify `$SPLUNK_HOME/etc/splunk-launch.conf` to include the `SPLUNK_BINDIP` attribute and `<ipaddress>` value. For example, to bind Splunk ports to `127.0.0.1`, `splunk-launch.conf` should read:

```
# Modify the following line to suit the location of your Splunk install.
# If unset, Splunk will use the parent of the directory this configuration
# file was found in
#
# SPLUNK_HOME=/opt/splunk
SPLUNK_BINDIP=127.0.0.1
```

This will affect the binding address of all ports opened by splunk and splunkweb, including the http server, and network inputs.

**Note:** You can also use `splunk-launch.conf` to define `$SPLUNK_HOME` and `$SPLUNK_DB`.

## Run Splunk as non-root user

### Run Splunk as non-root user

Splunk can run as any user on the local system. If you run Splunk as a non-root user, make sure Splunk has the appropriate permissions to:

- Read the files and directories it is configured to watch. Some log files and directories may require root or superuser access to be indexed.
- Write to Splunk's directory and execute any scripts configured to work with your alerts or scripted input.
- Bind to the network ports it is listening on (ports below 1024 are reserved ports that only root can bind to).

**Note:** Because ports below 1024 are reserved for root access only, Splunk will only be able to listen on port 514 (the default listening port for syslog) if it is running 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.

### Instructions

To run Splunk as a non-root user, you need to first install Splunk as `root`. Then, **before you start Splunk for the first time**, change the ownership of the `splunk` directory to the desired user. The following are instructions to install Splunk and run it as a non-root user, `splunk`.

1. Create the user and group, `splunk`.

### For Linux, Solaris, and FreeBSD:

```
useradd splunk
groupadd splunk
```

### For Mac OS:

You can use the **System Preferences > Accounts** panel to add users and groups.

2. As `root` and using one of the packages (not a tarball), run the installation.

**Important:** Do not start Splunk yet.

3. Use the `chown` command to change the ownership of the `splunk` directory and everything under it to the desired user.

```
chown -R splunk $SPLUNK_HOME/
```

**Note:** `$SPLUNK_HOME` refers to installation directory of Splunk.

#### 4. Start Splunk.

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

Also, if you want to start Splunk 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
```

This example command assumes:

- If Splunk is installed in an alternate location, update the path in the command accordingly.
- Your system may not have `sudo` installed. If this is the case, you can use `su`.
- If you are installing using a tarball and want Splunk to run as a particular user (such as `splunk`), you must create that user manually.
- The `splunk` user will need access to `/dev/urandom` to generate the certs for the product.

#### Solaris 10 privileges

When installing 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
```

## Disable update checker

#### Disable update checker

Splunk Web is configured to check for new versions of itself and display a banner. If you are running Splunk on a LAN that is not connected to the rest of the Web, modify `web.conf` to disable this feature.

**Note:** The default `web.conf` is located in `$SPLUNK_HOME/etc/system/default/`. DO NOT edit this file. Instead, copy `web.conf` into `$SPLUNK_HOME/etc/system/local/`; then, edit the copy. For more information about configuration files, refer to this Admin manual topic.

To disable update checker, add the following to `$SPLUNK_HOME/etc/system/local/web.conf`:

```
[settings]
updateCheckerBaseUrl = 0
```

# Configure SELinux

## Configure SELinux

If you have SELinux active on your system, you must add Splunk to the list of authenticated applications that can run in your SELinux environment.

To configure SELinux to allow Splunk to run, you need to run the `chcon` command on the Splunk `lib` directory, where `$SPLUNK_HOME` is the path to your Splunk installation:

```
chcon -c -v -R -u system_u -r object_r -t lib_t $SPLUNK_HOME/lib 2>&1 > /dev/null
```

After you configure SELinux to allow Splunk to run, you can disable the check from occurring each time you start Splunk. To disable the SELinux check, add this line to

`$SPLUNK_HOME/etc/splunk-launch.conf`:

```
SPLUNK_IGNORE_SELINUX=1
```

**Important:** Depending on the SELinux distribution, if you turn off the check before configuring SELinux, Splunk may not function properly.

## Uninstall Splunk manually

### Uninstall Splunk manually

This topic discusses how to remove installed components of Splunk if you can't use package management commands.

**Note:** These will not remove any `init` scripts that have been created.

#### 1. Stop Splunk.

```
$SPLUNK_HOME/bin/splunk stop
```

#### 2. Find and `kill` any lingering processes that contain "splunk" in its 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 installation directory, `$SPLUNK_HOME`.

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

#### 3. Remove any Splunk datastore or indexes outside the top-level directory, if they exist.

```
rm -rf /opt/splunkdata
```

4. Delete the `splunk` user and group, if they exist.

**For Linux, Solaris, and FreeBSD:**

```
userdel splunk  
groupdel splunk
```

**For Mac OS:** You can use the **System Preferences > Accounts** panel to manage users and groups.

# Upgrade Instructions

## Upgrade and migrate to 3.3 and later

### Upgrade and migrate to 3.3 and later

You can upgrade and migrate directly to Splunk 3.3 and later from versions 3.0 and later. If you are currently running a version of Splunk that is older than 3.0, refer to this documentation for options.

When you upgrade to 3.3 or later, your configuration files will be updated and changed. You can run the migration preview utility to see what will be changed before you actually upgrade and migrate. When you do this, a file containing the changes that the script proposes to make is written to `$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>`

**Important:** Before you perform the upgrade, we strongly recommend that you review these migration considerations and back up all of your files, including Splunk configurations, data and binaries. Splunk does not provide a means of downgrading to previous versions; if you need to revert to an older Splunk release, just reinstall it.

1. Execute the `$SPLUNK_HOME/bin/splunk stop` command.
2. To upgrade and migrate from version 3.0 and later, install the Splunk package over your existing Splunk deployment.

If you are using a TAR file, expand it into the same directory as your existing Splunk instance. This overwrites and replaces matching files but does not remove unique files.

If you are using a package manager, such as an RPM:

```
rpm -U splunk_package_name.rpm
```

3. Execute the `$SPLUNK_HOME/bin/splunk start` command.

The following output is displayed:

```
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]
```

4. You're given the choice of running the migration preview script to see what changes will be made to your existing configuration files, or proceeding with the migration and upgrade right away.

5. If you choose to view the expected changes, the script provides a list.

6. Once you've reviewed these changes and are ready to proceed with migration and upgrade, run `$(SPLUNK_HOME)/bin/splunk start` again.

**Note:** You can complete Steps 3 to 5 in one line:

To accept the license and view the expected changes (answer 'n') before continuing the upgrade:

```
$(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
```

**Important:** After upgrading, Splunk may start reading some files incorrectly as binaries. You can override this behavior in `props.conf` by adding `NO_BINARY_CHECK = true` to a source stanza.

## Upgrade Splunk on Windows

### Upgrade Splunk on Windows

**Important:** Before you upgrade:

- Review these migration considerations.
- Back up your files, including Splunk configurations, data and binaries.
- Stop Splunk either using the Windows Start menu option or by executing the `$(SPLUNK_HOME)/bin/splunk stop` command.
- Be aware that you cannot change the user Splunk runs as during an upgrade. Do not change the user from the Windows Service Control panel; Splunk will stop working. If you must change the user, you must uninstall and reinstall Splunk.

1. Download the new MSI file from the Splunk download page.

2. Double-click the MSI file.

The Welcome panel is displayed. Follow the onscreen instructions to upgrade Splunk.

For information about each panel, refer to the installation instructions.

When you reach the **Install** step, you have the option to preview changes that will be made for this upgrade.

3. Preview your upgrade and migration if desired.

When you upgrade, your configuration files are updated and changed to support the new functionality. You can run the migration preview utility to see what will be changed before you actually upgrade and migrate. When you do this, a file containing the changes that the script proposes to make is written to `$(SPLUNK_HOME)/var/log/splunk/migration.log.<timestamp>`

The following text is displayed:

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]
```

**Important:** If you are upgrading to 3.3.2 or later and you have made manual changes to the `$SPLUNK_HOME/etc/system/local/inputs.conf` file, make a backup copy of this file to compare the full migration changes, including any changes to Windows-specific type data inputs, after the process is complete. Some global settings (like "host = foohost") may not be preserved. See the Known issues for version 3.3.2 for details.

4. You're given the choice of running the migration preview script to see what changes will be made to your existing configuration files, or proceeding with the migration and upgrade right away.

5. If you choose to view the expected changes (select **N**), the script provides a list.

You can scroll up to review the changes or look at them in `$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>`. At the end of the list, you will see an error message, which you can ignore.

6. Press **Enter** to return to step 3 and finish your upgrade by typing **Y**.

#### Start Splunk

On Windows, Splunk is installed by default into `\Program Files\Splunk`

You can start and stop the following Splunk processes via the Windows Services Manager:

- Server daemon: `splunkd`
- Web interface: `splunkweb`

You can also start, stop, and restart both processes at once by going to `\Program Files\Splunk\bin` and typing

```
# splunk.exe [start|stop|restart]
```

**Note:** If you do not select **Start Splunk Services** now, they will be set to manual startup and therefore will not start after a reboot. You must start them from the Windows Service Manager MMC, and optionally configure `auto-start` if you want them to start automatically at boot time.

**Important:** After upgrading, Splunk may start reading some files incorrectly as binaries. You can override this behavior in `props.conf` by adding `NO_BINARY_CHECK = true` to a source stanza.

## Migration considerations

### Migration considerations

This topic discusses various issues and considerations you should review before upgrading to Splunk 3.3.

You should also review the Known Issues for additional information before you upgrade.

### Stop Splunk and back up all of your files

Before you perform the upgrade, stop Splunk and back up all of your files, including configurations, data and binaries. Splunk does not provide a means of downgrading to previous versions; if you need to revert to an older Splunk release, just reinstall it.

### Users of LDAP on MacOSX Leopard should back up `ldap.conf` before upgrading via DMG to 3.4

If you are using LDAP authentication and are upgrading from any version of Splunk to version 3.4, the Leopard DMG manager will delete your existing `ldap.conf` and replace it with the newer `ldap.conf.default`. If you've made changes to `ldap.conf`, make a backup copy of this file before upgrading to 3.4 and then reinstate it after you have upgraded.

### Bundles configuration directory structure changed and renamed

Starting with version 3.3, Splunk's custom bundle directory structure and terminology have both changed. Bundles are now referred to as applications, and a new directory structure is in place. The existing directory structure and nomenclature will be supported in 3.3, but a switch to the new structure will be enforced in a future release. For detailed information about the new applications directory structure, refer to the documentation about configuration files.

Splunk provides a script for migrating your existing bundles directories to the new structure. Refer to these instructions for more information

### Scripts in `/splunk/bin` may not be saved

- If you have configured an alert to call a script, that script resides in `$SPLUNK_HOME/bin/scripts`. Make a backup of these scripts and reinstate them after the upgrade.

- If you are using a Splunk-provided archiving script (`compressedExport.sh` or `flatfileExport.sh`), these scripts may be removed or overwritten upon upgrade. Make a backup of these scripts and reinstate them after the upgrade.

#### Saved searches and search operators

Be aware of the following regarding saved searches:

- If the search contains fixed scheduling, and actually takes longer to run than the interval allows, the search will not work.
- If your search contains `foo=bar` and you have an indexed field configured from previous versions as `foo::bar`, your search will fail if `bar` isn't anywhere in the raw data of an event. Make saved searches that fail for this reason work by either:
  - ◆ adding or changing `INDEXED = True` or `INDEXED_VALUE = False` in the stanza for `foo` in `fields.conf`.
  - ◆ changing your search in the search bar by replacing `foo=bar` with `foo::bar`.
- Metadata commands like `| admin` or `| metaevents` are not supported, and will generate a warning.
- Some field names for Windows-specific deployments have been changed. Splunk provides a script for migrating your saved searches, refer to these instructions for more information.

#### Saved searches and `prefs.conf` references to "query" in context of the "admin" command no longer supported

If you have a saved search containing the `admin` command which also contains a reference to the `query` field, you must recreate your search so that it does not use `query`. The `admin` command now uses `search` instead of `query`.

#### Affected search examples:

```
| admin mysavedsearches | rename query AS term stanza as name
| admin mysavedsearches | top query
```

#### Unaffected search examples:

```
| admin mysavedsearches | rename stanza as name
| admin mysavedsearches | stats count(name)
```

#### Changes to `indexes.conf`

If you have made changes to the default values in `indexes.conf`, the configuration will not migrate. Make a backup of your changes and re-add them post-upgrade.

### Must upgrade all instances of Splunk in a distributed environment

As mentioned in the Known Issues, you must upgrade all members of your distributed cluster to the same version.

### Instances of Splunk deployment server must match clients

As mentioned in the Known Issues, if you are running Splunk's deployment server, you must upgrade the deployment server and all its clients to the same version. Splunk recommends that you upgrade your Splunk deployment server first, before you migrate your other Splunk instances.

If you are unable to migrate all clients at one time, you can set up two deployment servers, one for your new 3.3.x clients, and one for your 3.1.x clients. This way, you can move each client over to communicate with the 3.3.x deployment server as you are able to upgrade it.

## Migrate your 32-bit Splunk Windows installation to 64-bit

### Migrate your 32-bit Splunk Windows installation to 64-bit

- Please review these general splunk migration considerations.

If you've already deployed a 32-bit Splunk for Windows **on 64-bit hardware** in anticipation of 64-bit support, this topic walks you through what you must do to migrate your installation in place to the 64-bit version of Splunk available starting with version 3.4.2.

1. Before you begin, you must upgrade your existing 32-bit Splunk installation to the 32-bit release of 3.4.2 using the information in "Upgrade Splunk on Windows".
2. Once you are running the 32-bit release of Splunk 3.4.2 (on Windows 64-bit hardware), stop the Splunk services (`splunkd` and `splunkweb`). You can use the commandline or the Windows Services Manager:

You can start and stop the following Splunk processes via the Windows Services Manager:

- Server daemon: `splunkd`
- Web interface: `splunkweb`

You can also start, stop, and restart both processes at once by going to `C:\Program Files (x86)\Splunk\bin` and typing

```
# splunk.exe [start|stop|restart]
```

**Note:** On 64-bit versions of Windows, the default value of `$SPLUNK_HOME` for the 32-bit version of Splunk is `C:\Program Files (x86)\Splunk`.

3. Make a copy of the `$SPLUNK_HOME\var\` and `$SPLUNK_HOME\etc\` directories.

This will include your indexes (by default, your main Splunk index is located in `$SPLUNK_HOME\var\lib\splunk\`) and any configuration files you've changed in `$SPLUNK_HOME\etc\local` and `$SPLUNK_HOME\etc\apps`.

**4. Uninstall the 32-bit version of Splunk 3.4.2 using the **Add or Remove Programs** option in the **Control Panel**.**

**Important:** You must perform this step before installing the 64-bit version of Splunk.

**5. Install the 64-bit version of Splunk 3.4.2 using the instructions in "Windows installation".**

**6. Start up Splunk and verify everything is working, and then stop the Splunk services (`splunkd` and `splunkweb`) again.**

**7. Copy the following files and directories from the copy of `$SPLUNK_HOME\etc\` that you set aside (indexes and configuration files) back into the same locations in the new installation.**

`$SPLUNK_HOME\etc\myinstall\splunkd.xml`

`$SPLUNK_HOME\etc\system\local`

`$SPLUNK_HOME\etc\apps`

`$SPLUNK_HOME\etc\auth`

`$SPLUNK_HOME\etc\modules`

`$SPLUNK_HOME\etc\openldap`

`$SPLUNK_HOME\etc\splunk.license`

`$SPLUNK_HOME\etc\splunk-launch.conf`

`$SPLUNK_HOME\etc\passwd`

Keep in mind that for the 32-bit version of Splunk, the default value of `$SPLUNK_HOME` was `C:\Program Files (x86)\Splunk` and the 64-bit version of Splunk will be in `C:\Program Files\Splunk`.

**8. In your new 64-bit installation of Splunk, rename the `$SPLUNK_HOME\var\` directory to something else (like `$SPLUNK_HOME\var.delete\`) and then copy over the `$SPLUNK_HOME\var\` directory you saved from the 32-bit version of Splunk.**

You can later delete the `var.delete` directory.

**9. Restart Splunk, and check your configurations.**

# Migrate your Windows saved searches to 3.3.x and later

## Migrate your Windows saved searches to 3.3.x and later

Use the information in this topic if you are upgrading from a version of Splunk for Windows that is older than 3.3.

Some Splunk terminology for Windows-specific field names has changed or been added starting in version 3.3. These changes were made to better reflect commonly-used Windows terminology. As a result, you must migrate any existing saved searches you created in 3.2.x to use the new terminology. Splunk provides a script for you to do this.

The script backs up any saved searches that appear to contain the deprecated terms, and converts them to use the new terminology.

- You have the option of seeing a preview of what the script will change when you run it.
- If you are deploying to multiple servers, perhaps using automation of some kind, you can also skip the 5 second pause Splunk introduces by default to let you read the informational text that is displayed when you run the script by hand.

## Run the migration script

To run the migration script without seeing a preview and with the 5 second pause, from `$SPLUNK_HOME`, run:

```
./splunk migrate win-searches
```

## Optional parameters:

- To see a preview of the changes Splunk will make, use `-dry-run true` (the default is `false`).
- To skip the 5 second pause, use `-no-wait true` (the default is `false`).

## What has changed

The following field names are new:

- `Category`
- `EventType`
- `Message`

The following field names have changed:

- `evtlog_category` -> `CategoryString`
- `evtlog_id` -> `EventCode`
- `evtlog_severity` -> `Type`

- `evtlog_account` -> User
- `evtlog_domain` -> ComputerName
- `evtlog_sid` -> Sid
- `evtlog_sid_type` -> SidType

## Migrate bundles to new application directory structure

### Migrate bundles to new application directory structure

The information in this topic applies to you if you are upgrading to the current version of Splunk from a version of Splunk that is older than 3.3.

Starting with version 3.3, Splunk's custom bundle directory structure and terminology have both changed. The existing directory structure and nomenclature will be supported in 3.3, but a switch to the new structure will be enforced in a future release. For detailed information about the new applications directory structure, refer to the documentation about configuration files.

Splunk provides a script for migrating your existing bundles directories to the new structure. This script is not run automatically, and can be run on a per-bundle/application basis. You must restart Splunk after you run the script, each time you run it.

### Things to consider

- You must restart Splunk for changes to take effect.
- Some custom bundles may not work after migration; in particular, bundles that contain conf files or scripts that refer to hard-coded paths might break, since migration moves files around. Consider using relative paths for flexibility.

### Run the migration script

To run the script and migrate all your bundles to the new application directory structure, from `$SPLUNK_HOME`, run:

```
./splunk migrate bundle [-name value]
```

To migrate a single bundle to the new structure, add `-name [name of the bundle]`. For example:

```
./splunk migrate bundle -name local
```

```
./splunk migrate bundle -name code
```

```
./splunk migrate bundle
```

# Help

## Getting Help

### Getting Help

The most in-depth documentation for Splunk is within the set of manuals you're currently reviewing. However, you can also get help within Splunk Web and the command line interface.

### Accessing help in Splunk Web

Click **Help** in Splunk Web to launch a set of help pages.

### Accessing help in the command line (CLI)

From the command line on your Splunk Server host, type:

```
$SPLUNK_HOME/bin/splunk help
```

### How can I learn more about Splunk's advanced features?

The best way to explore advanced features is to take the tutorial

You can also explore the command line interface using its inline help. To get started, type:

```
$SPLUNK_HOME/bin/splunk help
```

### I lost my Splunk.com password. What do I do?

Use the recover password feature of the site to have your username and/or password emailed to the address on record.

### How do I report problems?

Submit your issue with on our online case submission form or email us at [support@splunk.com](mailto:support@splunk.com).

### **How can I make suggestions?**

You can always send an email to our support team at [support@splunk.com](mailto:support@splunk.com). Also check out our Live Roadmap where you can vote on upcoming features.

### **I have some questions that aren't answered here. Where can I get help?**

Start with our [Documentation](#).

For help from experienced Splunkers, come to our [Wiki](#) and check out what other people have done with their Splunk deployments.

For help -- yes, it's free! -- from the Splunk Support team, submit an online support case (you must be a registered user and log in to use this service). You can also use our IRC support channel. The channel name is #splunk on the EFnet IRC ([irc.efnet.org](http://irc.efnet.org)) network.

Splunk customers with an enterprise license have additional premium support options. For full information on our support offerings, [click here](#).

# Reference

## File Manifest

### File Manifest

A complete inventory of the files and permissions that ship with your Splunk installation can be found in the root directory of your Splunk installation. The file will end with `-manifest`.

## PGP Public Key

### PGP Public Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.1 (GNU/Linux)
mQGIBeBE21QRBADEMonUxCV2kQ2oxsJTjYXrYCWCTH5/OnmhK51T2TQaE9QUTs+w
nM3sVInQqwRwBDH2qsHggqjJS0PIE867n+lVuk0gSVzS5S01YzQjnSrisvyN452MF
2PgetHq8Lb884cPJnxR6xoFTHqOQueKEOXCovz1eVrjrjfpnmWKA/+5X8wCg/CJ7
pT7OXHFN4XOseVQabetEbWcEAIUaazF2i2x9QDJ+6twTAlX2oqAquqtBzJX5qaHn
OyRdBUE2g4ndiE3QAKybuq5f0UM7GXqdllihVUBatqafySfj1TBaMVzd4ttrDRpq
Wya4ppPMIWcnFG2CXf4+HuyTPgj2cry2oMBm2LMfGhxcqM5mpoyHqUiCn7591Ra/
J2/FA/0c2UAUh/eSiOn89I6FhFOict5RptRpxMoEM1Di15zJ7EXY+xBVF9rutqHR
5OI9kdHibYTwf4qjOOPOA7237N1by9GiXY/8s+rDWmSNKZB+xAaLy17cDhYMv7CP
qFTutvE8BxTsF0MgRuzIHfJQE2quuxKJFs9lkSFGuZhvRuwRcrQgS21tIFdhbGxh
Y2UgPHJ1bGVhc2VAc3BsdW5rLmNvbT6IXgQTEQIAHGUcrsTbVAIbAwYLCQgHAWID
FQIDAxYCAQIEaQIXgAAKCRApYLH9ZT+xEhsPAKDimP8sdCr2ecPm8mre/8TK3Bha
pQCg3/xEickiRKKlpKnySUNLR/ZBh3m5Ag0ERsTbbRAIAIdfWiOBeCj8BqrcTXxm
6MMvdEkjdJCr4xmwaQpYmS4JKK/hJFfpyS8XUgHjBz/7zfr8Ipr2CU59Fy4vb5oU
HeOecK9ag5JFdG2i/VWH/vEJAMCKbN/6aWwhHt992PUZC7EHQ5ufRdxGGap8SPZT
iIKY0OrX6Km6usoVWMTYKNm/v7my8dJ2F46YJ7wIBF7arG/voM0glCbn7pCwCatg
jOhgjdPXRJUEzZP3AfLIc3t5iq5n5FYLGaOpT70IroM5AkgbVLfj+cjKaGD5UZW7
S00akWhTbVHSCDJoZAGJrvJs5DHcEnCjVy9AJxTNMs9GOWaixfyQ7jgMNWKHJp+
EyMAAwYH/RLNK0HHVSBYPwnS2t5sXedIGAgm0fTHhVUCWQxN3knDIRMdkqDTnDKd
qcqYfEsEljazI2kx1Z1WdUGmvU+Zb8FCH90ej8O6jdFLKJaq50/I/oY0+/+DRBZJG
3oKu/CK2NH2VnK1KLzAYnd2wZQAEja401CBV0hgutVf/ZxzDUAr/XqPHY5+EYg96
4Xz0PdZiZiKOhJ5g4QjhhOL3jQwcBuyFbJADw8+Tsk8RJqZvhfuwPouVU+8F2vLJK
iF2HbKOUJvdH5GfFuk6o5V8nnir7xSrVj4abfP4xA6RVum3HtWoD7t//75gLcW77
kXDR8pmmnddm5VXnAuk+GTPGACj98+eISQQYEQIACQUCRsTbbQIbDAAKCRApYLH9
ZT+xEiVuAJ9INUCilkgXSnu9p27zxTZh1kL04QCg6YfWldq/MWPCwalPgiHrVJng
p4s=
=Mz6T
-----END PGP PUBLIC KEY BLOCK-----
```

### Installing the key

Copy and paste the key into a file. Install the key using:

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