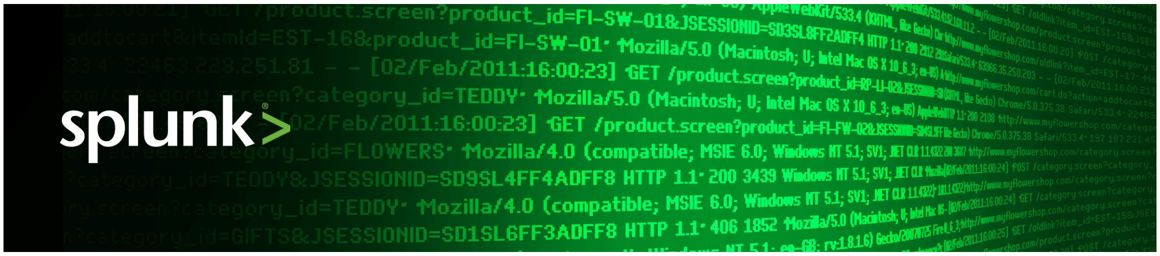

Splunk® Enterprise Installation Manual 6.5.0

Install on Windows using the command line

Generated: 11/09/2016 1:15 pm

Install on Windows using the command line

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

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

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

When to install from the command line

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

- You want to install Splunk Enterprise, but do not want it to start right away.
- You want to automate installation of Splunk Enterprise with a script.
- You want to install Splunk Enterprise on a system that you will clone later.
- You want to use a deployment tool such as Group Policy or System Center Configuration Manager.
- You want to install Splunk Enterprise on a system that runs a version of Windows Server Core.

Install using PowerShell

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

Upgrading?

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

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

Before you install

Choose the Windows user Splunk Enterprise should run as

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

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

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

Disable or limit antivirus software if able

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

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

Install Splunk Enterprise from the command line

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

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

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

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

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

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

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

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

Supported flags

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

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

Flag	Purpose	Default
`AGREETOLICENSE=Yes|No`	Use this flag to agree to the EULA. This flag must be set to `Yes` for a silent installation.	`No`
`INSTALLDIR="<directory_path>"`	Use this flag to specify directory to install. Splunk's installation directory is referred to as `$SPLUNK_HOME` or `%SPLUNK_HOME%` throughout this documentation set.	`C:\Program Files\Splunk`
`SPLUNKD_PORT=<port number>`	Use this flag to specify alternate ports for `splunkd` and `splunkweb` to use. If you specify a port and that port is not available, Splunk automatically selects the next available port.	`8089`
`WEB_PORT=<port number>`	Use this flag to specify alternate ports for `splunkd` and `splunkweb` to use.	`8000`

	If you specify a port and that port is not available, Splunk will automatically select the next available port.	

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

`REGISTRYCHECK_U=1/0`
`REGISTRYCHECK_BASELINE_U=1/0`
	Use these flags to specify whether or not Splunk should
	index events from
	capture a baseline snapshot of
	the Windows Registry user hive (`HKEY_CURRENT_USER`).
	Note: You can set both of these at the same time.
		`0` (off)

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

	Use these flags to specify which	`0` (off)

WMICHECK_CPUTIME=1/0
WMICHECK_LOCALDISK=1/0
WMICHECK_FREEDISK=1/0
WMICHECK_MEMORY=1/0
	popular WMI-based performance metrics Splunk should index:
	CPU usage
	Local disk usage
	Free disk space
	Memory statistics
	Note: If you need this instance of Splunk to monitor remote Windows data, then you must also specify the LOGON_USERNAME and LOGON_PASSWORD installation flags. Splunk cannot collect any remote data that it does not have explicit access to. Additionally, the user you specify requires specific rights, administrative privileges, and additional permissions, which you must configure before installation. Read "Choose the Windows user Splunk should run as" in this manual for additional information about the required credentials.
	There are many more WMI-based metrics that Splunk can index. Review "Monitor WMI Data" in the Getting Data In Manual for specific information.	

LOGON_USERNAME="<domain\username>"
LOGON_PASSWORD="<pass>"
	Use these flags to provide domain\username and password information for the user that Splunk will run as. The splunkd and splunkweb services are configured with these credentials. For the LOGON_USERNAME flag, you must specify the domain with the username in the format "domain\username."
	These flags are mandatory if you want this Splunk Enterprise installation to monitor any remote data. Review "Choose the Windows user Splunk
		none

	should run as" in this manual for additional information about which credentials to use.	
`SPLUNK_APP="<SplunkApp>"`	Use this flag to specify an included Splunk application configuration to enable for this installation of Splunk. Currently supported options for `<SplunkApp>` are: `SplunkLightForwarder` and `SplunkForwarder`. These specify that this instance of Splunk will function as a light forwarder or heavy forwarder, respectively. Refer to the "About forwarding and receiving" topic in the *Forwarding Data* manual for more information. If you specify either the Splunk forwarder or light forwarder here, you must also specify FORWARD_SERVER="<server:port>". To install Splunk Enterprise with no applications at all, omit this flag. **Note:** The full version of Splunk does not enable the universal forwarder. The universal forwarder is a separate downloadable executable, with its own installation flags.	none
`FORWARD_SERVER="<server:port>"`	Use this flag only when you also use the `SPLUNK_APP` flag to enable either the Splunk heavy or light forwarder. Specify the server and port of the Splunk server to which this forwarder will send data.	none
`DEPLOYMENT_SERVER="<host:port>"`	Use this flag to specify a deployment server for pushing configuration updates. Enter the deployment server name (hostname or IP address) and port.	none
`LAUNCHSPLUNK=0/1`	Use this flag to specify whether or not Splunk should start up automatically on	`1` (on)

	system boot. **Note:** If you enable the Splunk Forwarder by using the `SPLUNK_APP` flag, the installer configures Splunk to start automatically, and ignores this flag.	
`INSTALL_SHORTCUT=0/1`	Use this flag to specify whether or not the installer should create a shortcut to Splunk on the desktop and in the Start Menu.	`1` (on)

Silent installation

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

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

Examples

The following are some examples of using different flags.

Silently install Splunk Enterprise to run as the Local System user

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

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

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

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

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

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

Avoid Internet Explorer (IE) Enhanced Security pop-ups

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

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

What's next?

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

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