Abstract

This document explains the different methods in installing the Splunk Universal Forwarder

Splunk Universal Forwarder Installation Guide

Contents

[**Introduction** 2](#_Toc34857319)

[**Splunk Universal Forwarder Installation on Windows** 2](#_Toc34857320)

[Splunk UF Manual Installation on Windows OS 2](#_Toc34857321)

[Splunk UF Script based Installation on Windows OS (supports only for windows 2012 and above servers) 2](#_Toc34857322)

[Splunk UF Installation on Windows using SCCM 3](#_Toc34857323)

[For upgrading Splunk UF using SCCM: 3](#_Toc34857324)

[For fresh Splunk agent installation using SCCM: 3](#_Toc34857325)

[Splunk Client - Deployment Server Troubleshoot 3](#_Toc34857326)

[Splunk UF Manual Upgrade on Windows: 3](#_Toc34857327)

[Splunk UF Script based Upgrade on Windows 4](#_Toc34857328)

[**Splunk Universal Forwarder Installation on Linux OS** 4](#_Toc34857329)

[Splunk UF Manual Installation on Linux OS 4](#_Toc34857330)

[Splunk UF Script based Installation on Linux/Unix/Ubuntu/SunOS 5](#_Toc34857331)

[Splunk UF Script based Upgrade on Linux/Unix/Ubuntu/SunOS 5](#_Toc34857332)

[Linux – Manual - Upgrade Splunk Universal Forwarder: 6](#_Toc34857333)

# **Introduction**

Splunk infrastructure is distributed deployment that requires centralized mechanism of configuring the various element of the system. The purpose of this document describe steps of how to download, install Splunk Universal Forwarder(or Splunk UF agent).

# **Splunk Universal Forwarder Installation on Windows**

## Splunk UF Manual Installation on Windows OS

This sections details the manual installation instruction for the Splunk UF on a Windows Operating System.

1. Ensure no existing Splunk or Splunk universal forwarder is installed. If installed already please see II section .
2. Delete any Splunk directories if present i.e. c:\program files\splunkuniversalforwarder
3. Follow link below to locate and download the appropriate Splunk Universal Forwarder package.
   1. Windows 2008 Servers

[Splunk Client Package for 2008 64 bit](https://download.splunk.com/products/universalforwarder/releases/6.3.14/windows/splunkforwarder-6.3.14-35a0c0a79a86-x64-release.msi)

* 1. Windows 2008 R2 servers

[Splunk Client Package for 2008 R2](https://download.splunk.com/products/universalforwarder/releases/7.2.9/windows/splunkforwarder-7.2.9-2dc56eaf3546-x64-release.msi)

* 1. Windows 2012,2012R2,2016,2019

[Splunk client package for 2012,R2,2016 & 2019](https://download.splunk.com/products/universalforwarder/releases/8.2.3/windows/splunkforwarder-8.2.3-cd0848707637-x64-release.msi)

* 1. Windows Server 2022

Splunk client package for 2022

1. Open and Run the command prompt as an administrator and execute the command below:

msiexec.exe /i splunkforwarder-<...>-x64-release.msi DEPLOYMENT\_SERVER=":8089" AGREETOLICENSE=yes SPLUNKUSER=admin SPLUNKPASSWORD='' /quiet

1. Proceed to the Control Panel > Programs > Programs and Features. Check if the Splunk UF has been installed. This should take no more than 3 minutes.
2. Proceed to the Local Services and Start the Splunk Forwarder Service if not running.

## Splunk UF Script based Installation on Windows OS (supports only for windows 2012 and above servers)

Copy and paste the following into the command line of your entity.

This script must be run by user with administrator privileges, and it should also have the following dependencies available on the entity.

* PowerShell
* Internet access

$env:SPLUNK\_DEPLOYMENT\_URL="" ; $env:SPLUNK\_HOME="C:\Program Files\SplunkUniversalForwarder" ; $web=New-Object Net.WebClient; $path=Convert-Path .; [System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true}; [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12 ; $files="xyz \_install\_uf.ps1","xyz \_install\_uf\_script.ps1"; **Foreach**($file **in** $files) { $web.DownloadFile("https://:8000/static/app/splunk\_uf\_agent/windows\_scripts/$file",$path+"\$file")}; [System.Net.ServicePointManager]::ServerCertificateValidationCallback = $null; **if** ($?) {.\xyz \_install\_uf.ps1}

## Splunk UF Installation on Windows using SCCM

Follow link below to locate and download the appropriate Splunk Universal Forwarder package.

* Windows 2008 Servers
  + [Splunk Client Package for 2008 64 bit](http://splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=windows&version=6.3.14&product=universalforwarder&filename=splunkforwarder-6.3.14-35a0c0a79a86-x64-release.msi&wget=true)
* Windows 2008 R2 servers
  + [Splunk Client Package for 2008 R2](http://splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=windows&version=7.2.9.1&product=universalforwarder&filename=splunkforwarder-7.2.9.1-605df3f0dfdd-x64-release.msi&wget=true)
* Windows 2012,2012R2,2016,2019
  + [Splunk client package for 2012,R2,2016 & 2019](https://download.splunk.com/products/universalforwarder/releases/8.2.3/windows/splunkforwarder-8.2.3-cd0848707637-x64-release.msi)

### For upgrading Splunk UF using SCCM:

**msiexec.exe /i splunkuniversalforwarder-<...>-x64-release.msi DEPLOYMENT\_SERVER=":8089" AGREETOLICENSE=Yes SPLUNKUSER=admin SPLUNKPASSWORD='' /quiet**

### For fresh Splunk agent installation using SCCM:

**msiexec.exe /i splunkuniversalforwarder-<...>-x64-release.msi DEPLOYMENT\_SERVER=":8089" AGREETOLICENSE=Yes SPLUNKUSER=admin SPLUNKPASSWORD='' /quiet**

## Splunk Client - Deployment Server Troubleshoot

This Section details the manual instructions for existing Splunk UF if the server is not Phoning Home to Splunk deployment server.

1. Ensure existing Splunk or Splunk universal forwarder is installed. Use control panel > Programs, if not present, please follow the installation instructions on this doc.
2. Go to c:\program files\splunkuniversalforwarder\etc\system\local\
3. Copy the below deploymentclient.conf to **c:\program files\splunkuniversalforwarder\etc\system\local\**

1. Proceed to the Local Services and Restart the Splunk Forwarder Service.

## Splunk UF Manual Upgrade on Windows:

You can upgrade a single forwarder by running the command line installer. To upgrade a group of forwarders, load the command line installer into a deployment tool such as Group Policy or System Center Configuration Manager.

You cannot make configuration changes during an upgrade. The installer ignores any command line flags that you specify except for the AGREETOLICENSE flag.

1. Download the new MSI file from the Splunk universal forwarder download page.
   1. Windows 2008 Servers

[Splunk Client Package for 2008 64 bit](http://splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=windows&version=6.3.14&product=universalforwarder&filename=splunkforwarder-6.3.14-35a0c0a79a86-x64-release.msi&wget=true)

* 1. Windows 2008 R2 servers

[Splunk Client Package for 2008 R2](http://splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=windows&version=7.2.9.1&product=universalforwarder&filename=splunkforwarder-7.2.9.1-605df3f0dfdd-x64-release.msi&wget=true)

* 1. Windows 2012,2012R2,2016,2019

[Splunk client package for 2012,R2,2016 & 2019](http://splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=windows&version=7.3.4&product=universalforwarder&filename=splunkforwarder-7.3.4-13e97039fb65-x64-release.msi&wget=true)

1. Run msiexec.exe to Install the universal forwarder from the command line.
   1. For 32-bit platforms, use splunkforwarder-<...>-x86-release.msi.

**msiexec.exe /i splunkforwarder-<...>-x64-release.msi DEPLOYMENT\_SERVER=":8089" AGREETOLICENSE=Yes SPLUNKUSER=admin SPLUNKPASSWORD='' /quiet**

* 1. For 64-bit platforms, use splunkforwarder-<...>-x64-release.msi.

**msiexec.exe /i splunkforwarder-<...>-x64-release.msi DEPLOYMENT\_SERVER=":8089" AGREETOLICENSE=Yes SPLUNKUSER=admin SPLUNKPASSWORD='' /quiet**

The value of <...> varies according to the particular release, for example, splunkforwarder-6.3.0-aa7d4b1ccb80-x64-release.msi.

1. Wait for the upgrade to complete. The forwarder starts automatically when you complete the installation.

The installer puts a log of upgrade changes in the %TEMP% directory. It also reports any errors in the Application Event Log

## Splunk UF Script based Upgrade on Windows

Copy and paste the following into the command line of your entity.

This script must be run by user with administrator privileges, and it should also have the following dependencies available on the entity.

* PowerShell
* Internet access

$env:SPLUNK\_DEPLOYMENT\_URL="";$env:SPLUNK\_HOME="C:\Program Files\SplunkUniversalForwarder" ; $web=New-Object Net.WebClient; $path=Convert-Path .; [System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true}; [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12 ; $files="upgrade\_splunk\_uf.ps1","upgrade\_splunk\_uf\_script.ps1"; **Foreach**($file **in** $files) { $web.DownloadFile("https://:8000/static/app/splunk\_uf\_agent/windows\_scripts/$file",$path+"\$file")}; [System.Net.ServicePointManager]::ServerCertificateValidationCallback = $null; **if** ($?) {.\upgrade\_splunk\_uf\_script.ps1}

# **Splunk Universal Forwarder Installation on Linux OS**

## Splunk UF Manual Installation on Linux OS

1. Follow the link below and download the file "**splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86\_64.rpm**".

[*Splunk Linux Package*](https://download.splunk.com/products/universalforwarder/releases/8.2.3/linux/splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86_64.rpm)

1. Distribute the **"splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86\_64.rpm"** to the required system/s.
2. Install the Splunk UF by running the following command as root.

***rpm -i splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86\_64.rpm***

1. Set the initial configuration options by executing the commands below.

***/opt/splunkforwarder/bin/splunk start --accept-license --answer-yes --no-prompt --seed-passwd***

***/opt/splunkforwarder/bin/splunk set deploy-poll:8089 -auth admin:***

1. Modify the permissions on generic logs listed below so Splunk can read them.

***cd /var/log  
chmod +r messages secure auth audit/audit.log cron maillog boot.log yum.log sudo.log***

6. Restart Splunk service  
 ***/opt/splunkforwarder/bin/splunk restart***

## Splunk UF Script based Installation on Linux/Unix/Ubuntu/SunOS

Follow the instructions to install an agent on your Linux machine.

1. Supported OS type: Centos, Debian, Fedora, RedHat Enterprise Linux, Solaris, Ubuntu.
2. This script must be run by user with **root** privileges, and it should also have the following dependencies available on the entity:

* wget (CSWwget for Solaris)
* apt-get(Debian, Ubuntu)
* yum(Redhat, CentOS, Fedora)
* pkgutil(Solaris)
* bash
* Internet access

1. Copy and paste the following into the command line of your entity

**export** INSTALL\_LOCATION=/opt/ && AUTHENTICATED\_INSTALL=Yes && wget --no-check-certificate https://:8000/static/app/splunk\_uf\_agent/unix\_agent/ \_install\_uf.sh && bash \_install\_uf**.**sh --force-**continue** && rm -f \_install\_uf**.**sh && rm -f splunkforwarder-7**.**3**.**4-13e97039fb65-Linux-x86\_64**.**tgz

## Splunk UF Script based Upgrade on Linux/Unix/Ubuntu/SunOS

Follow the instructions to install an agent on your Linux machine.

1. Supported OS type: Centos, Debian, Fedora, RedHat Enterprise Linux, Solaris, Ubuntu.
2. This script must be run by user with **root** privileges, and it should also have the following dependencies available on the entity:

* wget (CSWwget for Solaris)
* apt-get(Debian, Ubuntu)
* yum(Redhat, CentOS, Fedora)
* pkgutil(Solaris)
* bash
* Internet access

1. Copy and paste the following into the command line of your entity

**export** INSTALL\_LOCATION=/opt/ && AUTHENTICATED\_INSTALL=Yes && wget --no-check-certificate https://:8000/static/app/splunk\_uf\_agent/unix\_agent/ \_install\_uf.sh && bash \_install\_uf**.**sh --force-**continue** && rm -f \_install\_uf**.**sh && rm -f splunkforwarder-7**.**3**.**4-13e97039fb65-Linux-x86\_64**.**tgz

## Linux – Manual - Upgrade Splunk Universal Forwarder:

1. Follow the link below and download the file " **splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86\_64.rpm**".

[*Splunk Linux Package*](https://download.splunk.com/products/universalforwarder/releases/8.2.3/linux/splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86_64.rpm)

1. Distribute the " **splunkforwarder-8.2.3-cd0848707637-linux-2.6-x86\_64.rpm**" to the required system/s.
2. Stop the forwarder.

***$SPLUNK\_HOME/bin/splunk stop***

1. Install the universal forwarder package directly over the existing deployment.

***rpm -U <splunk\_package\_name>.rpm***

1. Start the forwarder again.

***/opt/splunkforwarder/bin/splunk start --accept-license --answer-yes --no-prompt --seed-passwd***

***/opt/splunkforwarder/bin/splunk set deploy-poll:8089 -auth admin:***