Splunk® Universal Forwarder Forwarder Manual 9.0.2

Generated: 11/07/2022 9:17 pm

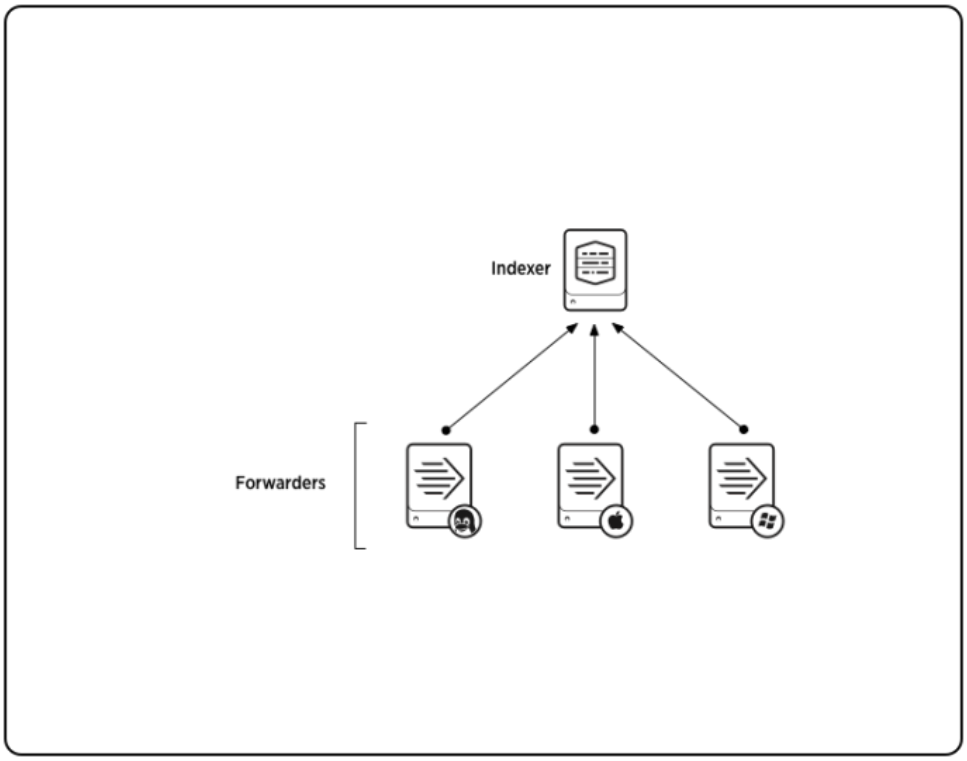
Table of Contents

About the universal forwarder

About the universal forwarder

Universal forwarders stream data from your machine to a data receiver. This receiver is usually a Splunk index where you store your Splunk data. Universal forwarder streaming lets you monitor data in real time.

The universal forwarder also ensures the that your data is correctly formatted before sending it to Splunk. You can also manipulate your data before it reaches the indexes or manually add the data. See the following example diagram:



This is the most common configuration for the universal forwarder. See Deploy the Universal Forwarder to create this configuration. See Advanced Universal Forwarder Configurations for examples of more advanced forwarder configurations.

Benefits of the Universal Forwarder

Universal forwarders are highly scalable. Universal Forwarders use significantly less hardware resources than other Splunk products. You can install thousands of them without impacting network performance and cost. The universal forwarder does not have a user interface, which helps minimize resource use.

Forwarders provide the following capabilities:

- metadata tagging, including source, source type, and host.
- configurable buffering
- data compression
- SSL security
- Use of any available network ports

Deploy the universal forwarder

Universal forwarder prerequisites

See the following Universal Forwarder prerequisites sections:

- Decide if you want to use the Splunk deployment server
- Computer Hardware Prerequisites
- Compatible Operating System

Decide if you want to use the Splunk deployment server

If you want to personalize how data is sent to the indexer, you must edit the universal forwarder's configuration files. The deployment server lets you edit multiple universal forwarders at once by manually editing a single file. See deployment server and forwarder management in the *Updating Splunk Enterprise Instances* manual.

Computer Hardware Prerequisites

The universal forwarder has the following minimum processing, RAM, and disk space requirements:

Processing	1.5Ghz
RAM	512MB
Free Disk Space	5GB

Compatible Operating Systems

For compatible operating systems, see Supported Operating Systems in the Splunk Enterprise installation manual.

Deploy the universal forwarder

1. Make sure you have the necessary Universal Forwarder prerequisites.
2. Install the Universal Forwarder:
    - For Windows, see Install a Windows universal forwarder.
    - For *nix, see Install a *nix universal forwarder.
3. To send data to Splunk Enterprise, enable a Splunk Enterprise indexer receiver. See Enable a receiver.
4. To send data to Splunk Cloud, see Install and configure the Splunk Cloud Platform universal forwarder credentials package. This gives you permissions to use the Splunk Cloud indexer.
5. Optionally Configure the universal forwarder using configuration files to further modify how data is sent to the indexer.
6. Start or restart the universal forwarder. See Start or stop the universal forwarder.

Install the universal forwarder

Install a Windows universal forwarder

If you are a Windows user, you can either install the Universal Forwarder using an installer or the command line. The **installer** is recommended for **larger deployments**, and the **command line** is recommended for **smaller deployments:**

- Install from an installer
- Install from the command line

Install a Windows universal forwarder from an installer

See the following steps to install a Windows universal forwarder from an installer:

1. Download the universal forwarder from splunk.com. Double-click the MSI file to start the installation.
2. The first screen of the installer should pop-up. Select the **Check this box to accept the License Agreement** check box and the check box for either Splunk Enterprise or Splunk Cloud.
3. To change any of the default installation settings, click the "Customize Options" button. See the following steps. Otherwise, click **Next**.
    1. (Optional) In the **Destination Folder** dialog box, click **Change** to specify a different installation directory.
    2. On the **Certificate Information** page, click **Next** as a best practice. Do not specify any parameters.
    3. As a best practice, run the Universal Forwarder as the Local System user and click **Next**. See "Install as a low-privilege user" for information about securing your system when installing as a local user.
    4. (Optional) Select one or more Windows inputs from the list and click **Next**.
4. Create a username and password for your Universal Forwarder administrator account. Check **Generate random password** to let Splunk generate a password for you.
5. Do at least one of the following two steps:
    - In the **Deployment Server** pane, enter a host name or IP address and management port for the deployment server that you want the universal forwarder to connect to and click **Next**.
    - In the **Receiving Indexer** pane, enter a host name or IP address and the receiving port for the receiving indexer that you want the universal forwarder to send data to and click **Next**.
6. Click **Install** to proceed with the installation. The installer runs and displays the **Installation Completed** dialog box. The universal forwarder automatically starts.
7. From Windows Control Panel, confirm that the `SplunkForwarder` service runs.

Install a Windows universal forwarder from the command line

You can install the universal forwarder on a Windows machine from a command prompt or a PowerShell window.

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

Install the universal forwarder with installation flags

Review the supported command line flags table to determine the flags you need to accomplish your command line installation task. From a command prompt or PowerShell window, run the `msiexec.exe` installer program with the appropriate flags, using the following syntax:

msiexec.exe /i splunkuniversalforwarder.msi [<flag>=<value>]...[<flagN>=<value>] Follow the prompts on screen to complete the installation. Panes for flags that you have specified in the command line will not appear.

Install the universal forwarder silently

If your Windows machine has User Account Control (UAC) enabled, you must run a silent installation as a Windows administrator user.

Review the supported command line flags table to determine the flags you need to accomplish the command-line installation task. From a command prompt or PowerShell window, run `msiexec.exe` with the appropriate flags and add `AGREETOLICENSE=yes /quiet` to the end of the command string, as follows:

msiexec.exe /i splunkuniversalforwarder.msi [<flag>=<value>]...[<flagN>=<value>] AGREETOLICENSE=yes /quiet

The installation completes silently and the universal forwarder starts if there is no error during installation.

Install the universal forwarder in low-privilege mode

When you install the universal forwarder in low privilege mode, the Windows user that you specify during installation does not need to have administrative level privileges to run the forwarder software on the Windows machine.

There are some caveats to running the forwarder in low-privilege mode:

- The Windows user that you use to install the forwarder must have local administrator privileges to perform the installation.
- You do not have administrative access to any resources on either the host or the domain when you run the universal forwarder in low-privilege mode.
- You might need to add the domain user to additional domain groups in order to access remote resources. Additionally, you might need to add the user to local groups to access local resources that only privileged users would have access to.
- You cannot collect Windows Management Instrumentation (WMI) data as a non-admin user.

1. Review the supported command line flags table to determine the flags you need to accomplish the command-line installation task.
2. From a command prompt or PowerShell window, run `msiexec.exe` with the appropriate flags and add `LOGON_USERNAME = <username> LOGON_PASSWORD = <password> SET_ADMIN_USER = 0` to the end of the command string.

   ```
   msiexec.exe /i splunkuniversalforwarder.msi [<flag>=<value>]...[<flagN>=<value>]
   LOGON_USERNAME=<username> LOGON_PASSWORD=<password> SET_ADMIN_USER=0
   ```
3. (Optional) If you want to perform a silent installation, append `AGREETOLICENSE=yes /quiet` to the end of the command line string.

   ```
   msiexec.exe /i splunkuniversalforwarder.msi [<flag>=<value>]...[<flagN>=<value>]
   LOGON_USERNAME=<username> LOGON_PASSWORD=<password> SET_ADMIN_USER=0 AGREETOLICENSE=yes /quiet
   ```
4. You can optionally install windows as an MSA/gMSA user. To create the installation user: `LOGON_USERNAME=domain\msa$ is the install user, with {domain name}\{msa account name}$ format.` Please note that the last $ is required by Windows.
5. Follow the prompts on screen to complete the installation. Installer configuration panes for flags that you have specified in the command line do not appear.

The forwarder installs and runs in "low-privilege" mode.

Install the universal forwarder and enable verbose logging during installation

For more information on the `msiexec` logging command, see To set logging level on MS TechNet.

1. Review the supported command line flags table to determine the flags you need to accomplish your command-line installation task.
2. From a command prompt or PowerShell window, run the `msiexec.exe` installer program with the appropriate flags, using the following syntax:

   ```
   msiexec.exe /i splunkuniversalforwarder.msi [<flag>=<value>]...[<flagN>=<value>] /L*v logfile.txt
   ```
3. Follow the prompts on screen to complete the installation. Installer configuration panes for flags that you have specified in the command line do not appear.

Examples

Install the universal forwarder silently, agree to the license, and set the forwarder admin credentials to "SplunkAdmin/Ch@ng3d!"

You should always create a password for the Splunk `admin` user. If you do not, then the universal forwarder can start with no defined users, which means that you cannot log in or make changes to the initial forwarder configuration.

```
msiexec.exe /i splunkforwarder_x64.msi AGREETOLICENSE=yes SPLUNKUSERNAME=SplunkAdmin
SPLUNKPASSWORD=Ch@ng3d! /quiet
```

Install the universal forwarder to run as the Local System user and request configuration from deploymentserver1

You might do this for new deployments of the forwarder.

```
msiexec.exe /i splunkuniversalforwarder_x86.msi DEPLOYMENT_SERVER="deploymentserver1:8089"
AGREETOLICENSE=Yes /quiet
```

Install the universal forwarder to run as a domain user, but do not launch it immediately

You might do this when preparing a sample host for cloning.

```
msiexec.exe /i splunkuniversalforwarder_x86.msi LOGON_USERNAME="AD\splunk" LOGON_PASSWORD="splunk123"
DEPLOYMENT_SERVER="deploymentserver1:8089" LAUNCHSPLUNK=0 AGREETOLICENSE=Yes /quiet
```

Install the universal forwarder, enable indexing of the Windows security and system event logs, and run the installer in silent mode

You might do this to collect just the Security and System event logs through a silent installation.

```
msiexec.exe /i splunkuniversalforwarder_x86.msi RECEIVING_INDEXER="indexer1:9997" WINEVENTLOG_SEC_ENABLE=1
WINEVENTLOG_SYS_ENABLE=1 AGREETOLICENSE=Yes /quiet
```

Install the universal forwarder in low-privilege mode and enable verbose installation logging to a log file

You might do this when you need to run the forwarder as a user who does not have administrative privileges on the local server.

```
msiexec.exe /i splunkuniversalforwarder_x64.msi /l*v install_splunkforwarder-6.1-201357-x64-release.msi.log
LOGON_USERNAME=adtest1\lowpriv-testuser LOGON_PASSWORD=win1@splunk
AGREETOLICENSE=Yes SET_ADMIN_USER=0 /quiet
```

Supported commandline flags

Command-line flags let you configure your forwarder at installation time. Using command-line flags, you can specify a number of settings, including:

- The user the universal forwarder runs as. (When you specify this flag, confirm the user you specify has the appropriate permissions to access the content you want to forward.)
- Whether or not the forwarder runs in "low-privilege" mode - as a user who does not have local administrative access.
- The receiving Splunk instance that the universal forwarder will send data to.
- A deployment server for updating the configuration.
- The Windows event logs to index.
- Whether the universal forwarder should start automatically when the installation is completed.

The installer for the full version of Splunk Enterprise has its own set of installation flags. For information on the full Splunk installer, see Install on Windows in the Splunk Enterprise *Installation Manual*.

The following list shows the flags available and provide a few examples of various configurations.

Flag	Purpose	Default
`AGREETOLICENSE=Yes|No`	Agrees to the license. You must set this flag to `Yes` to perform a silent installation. The flag does not work when you click the MSI to start installation.	`No`
`INSTALLDIR="<directory_path>"`	Specifies the installation directory. Do not install the universal forwarder over an existing installation of full Splunk Enterprise.	`C:\Program Files\Splunk UniversalForwarder`

`LOGON_USERNAME="<domain\username>"`
 	
`LOGON_PASSWORD="<pass>"`
	Provide domain\username and password information for the user to run the `SplunkForwarder` service. Specify the domain with the username in the format: `domain\username`. If you don't include these flags, the universal forwarder installs as the Local System user.	n/a

`RECEIVING_INDEXER="<host:port>"`	(Optional) Specify the receiving indexer to which the universal forwarder will forward data. Enter the name (host name or IP address) and **receiving port** of the receiver. This flag accepts only a single receiver. To specify multiple receivers (to implement load balancing), configure this setting through the CLI or `outputs.conf`. If you do not specify this flag and also do not specify DEPLOYMENT_SERVER, the universal forwarder cannot determine which indexer to forward to.	
n/a`DEPLOYMENT_SERVER="<host:port>"`	Specify a **deployment server** for pushing configuration updates to the universal forwarder. Enter the deployment server name (hostname or IP address) and port.	

Note: If you do not specify this flag and also do not specify `RECEIVING_INDEXER`, the universal forwarder cannot determine which indexer to forward to.

n/a`LAUNCHSPLUNK=1|0`Specify whether the universal forwarder should start when the installation finishes.1 (yes)`SERVICESTARTTYPE=auto|manual`Specify whether the universal forwarder should start when the system reboots.

By setting LAUNCHSPLUNK to 0 and SERVICESTARTTYPE to auto, you will cause the universal forwarder to not start forwarding until the next system boot. This is useful when you want to clone a system image.

auto`MONITOR_PATH="<directory_path>"`Specify a file or directory to monitor.n/a

`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`

Enable these Windows event logs.

application

security

system

forwarders

setup

You can specify more than one of these flags in a command.

0 (no)`PERFMON=<input_type>,<input_type>,...`Enable Performance Monitor inputs. `<input_type>` can be any of these:

`cpu memory network diskspace`

n/a`ENABLEADMON=1|0`Enable Active Directory monitoring for a remote deployment.0 (not enabled)

`CERTFILE=<c:\path\to\certfile.pem>`

`ROOTCACERTFILE=<c:\path\to\rootcacertfile.pem>`

`CERTPASSWORD=<password>`

Supply SSL certificates:

Path to the cert file that contains the public/private key pair.

Path to the file that contains the Root CA cert for verifying CERTFILE is legitimate (optional).

Password for private key of CERTFILE (optional).

> You must set RECEIVING_INDEXER for these flags to have any effect.

n/aCLONEPREP=1|0Delete any instance-specific data in preparation for creating a clone of a machine. This runs the `splunk clone-prep-clear-config` CLI command, which removes machine-specific information from configuration files after the instance runs for the first time.0 (do not prepare the instance for cloning.)SET_ADMIN_USER=1|0Specify if the user you specify is an administrator. If you set this flag to 0, the universal forwarder runs in "low-privilege" mode as a user without administrator privileges on the local machine. This mode is available for customers that cannot run programs as an administrator on servers.

You must set both the `LOGON_USERNAME` and `LOGON_PASSWORD` flags when you set this flag.

1 (Install the universal forwarder as a user with administrative privileges. The universal forwarder runs in normal mode and not "low-privilege" mode.)SPLUNKUSERNAME=<username>Create a username for the Splunk administrator user. If you specify a quiet installation with the `/quiet` flag, and do not specify this setting, then the software uses the default value of admin, but you must still specify a password with the `SPLUNKPASSWORD` or `GENRANDOMPASSWORD` flags for the installation to add the credentials successfully.N/ASPLUNKPASSWORD=<password>Create a password for the Splunk administrator user. The password must meet eligibility requirements and be in plaintext. If you specify a quiet installation with the `/quiet` flag and do not specify this flag or the `SPLUNKUSERNAME` flag, then the universal forwarder installs without a user. and you must create one by editing the `user-seed.conf` configuration file.N/AMINPASSWORDLEN=<positive integer>When using the `SPLUNKPASSWORD` flag to set a password, you can also set password eligibility requirements for password creation and modification. The `MINPASSWORDLEN` flag specifies the minimum length that a password must be to meet these eligibility requirements going forward. It cannot be set to 0 or a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.> 1MINPASSWORDDIGITLEN=<integer>When using the `SPLUNKPASSWORD` flag to set a password, you can also set password eligibility requirements for password creation and modification. The `MINPASSWORDDIGITLEN` flag specifies the minimum number of numeral (0 through 9) characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.0MINPASSWORDLOWERCASELEN=<integer>When using the `SPLUNKPASSWORD` flag to set a password, you can also set password eligibility requirements for password creation and modification. The `MINPASSWORDLOWERCASELEN` flag specifies the minimum number of lowercase ('a' through 'z') characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.0MINPASSWORDUPPERCASELEN=<integer>When using the `SPLUNKPASSWORD` flag to set a password, you can also set password eligibility requirements for password creation and modification. The `MINPASSWORDUPPERCASELEN` flag specifies the minimum number of uppercase ('A' through 'Z') characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.0MINPASSWORDSPECIALCHARLEN=<integer>When using the `SPLUNKPASSWORD` flag to set a password, you can also set password eligibility requirements for password creation and modification. The `MINPASSWORDSPECIALCHARLEN` flag specifies the minimum number of special characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. The ':' (colon) character cannot be used as a special character. Any new password you create and any existing password you change must meet the new requirements after you set this flag.0GENRANDOMPASSWORD=1|0Generate a random password for the `admin` user and write the password to the installation log file. The installer writes the credentials to `%TEMP%\splunk.log`. After the installation completes, you can use the `findstr` utility to search that file for the word "PASSWORD". After you get the credentials, delete the installation log file, as retaining the file represents a significant security risk.1

Install a *nix universal forwarder

This topic describes how to install the universal forwarder software on a *nix host, such as Linux, Solaris, or Mac OS X. It assumes that you plan to install directly onto the host, rather than use a deployment tool. This type of deployment best suits these needs:

- Small deployments.
- Proof-of-concept test deployments.
- System image or virtual machine for eventual cloning.

The universal forwarder installation packages are available for download from splunk.com.

On *nix operating systems, the installation comes as a tar file or an installation package (.rpm, .deb, .pkg, etc.)

A tar file contains only the files needed to install and run the universal forwarder and can be installed wherever you have permissions. Installation packages contain logic that checks for software dependencies and install in a predetermined place, depending on your operating system.

To install the universal forwarder on a *nix host, follow the directions later in this topic for your specific OS.

- Install on Linux
- Install on Solaris
- Install on Mac OS X
- Install on FreeBSD
- Install on AIX

Default installation location

The universal forwarder installs by default in the `/opt/splunkforwarder` directory. The default installation directory for Splunk Enterprise is `/opt/splunk`.

About installing with tar files

When you install the universal forwarder using a tar file:

- Some non-GNU versions of `tar` might not have the `-C` argument available. In this case, to install in a specific directory, either `cd` to the directory where you want to install the forwarder or place the tar file in that directory before you run the `tar` command.
- The universal forwarder does not create the `splunk` user on the machine. If you want the forwarder to run as a specific user, you must create the user manually before you install.
- Confirm that the disk partition has enough space to hold the uncompressed volume of the data you plan to index.

Do not install the universal forwarder over an existing installation of full Splunk Enterprise.

Install the universal forwarder on Linux

About the least-privileged user

Running the universal forwarder as a root user is not a security best practice. However, a user running the forwarder as a basic non-root user cannot fully manage the forwarder or add-ons. To resolve this issue, the universal forwarder installer creates "least privileged" users with capabilities specific to running the universal forwarder.

If Splunk is unable to install a least privileged user, it will install as a non-root user. To learn more about how to add, enable, disable, and troubleshoot least privileged users, see Secure you *nix universal forwarder with a least privileged user.

For the universal forwarder to create a least privileged user at installation, your system must meet the following criteria:

- One or more Universal Forwarders; least privileged mode does not run on other systems or applications.
- `systemd` version 219 or greater.
- Linux x86_64, ARM, ARM64

1. Login as ROOT to the machine that you want to install the Splunk Universal Forwarder.
2. Create the Splunk user and group.
   ```
   useradd -m splunk
   groupadd splunk
   ```
3. Install the Splunk software, as described in the installation instructions for your platform in Installation instructions. Create the `$SPLUNK_HOME` directory wherever desired.
   ```
   export SPLUNK_HOME="/opt/splunkforwarder"
   mkdir $SPLUNK_HOME
   ```
4. Make sure the `splunkforwarder` package is present in `$SPLUNK_HOME`:

For a tar package:	`tar xvzf splunkforwarder_package_name.tgz`
For an rpm package:	♦ If necessary, change permissions on the file: `chmod 644 splunkforwarder_package_name.rpm` ♦ Install the Splunk Enterprise RPM in the default directory `/opt/splunk`: `rpm -i splunkforwarder_package_name.rpm`
For a .deb package:	`dpkg -i splunkforwarder_package_name.deb`

5. Run the `chown` command to change the ownership of the splunk directory and everything under it to the user that you want to run the software.
   ```
   chown -R splunk:splunk $SPLUNK_HOME
   ```
   If you change users, you must run this command again

   .

   If the `chown` binary on your system does not support changing group ownership of files, you can use the `chgrp` command instead. See the Man pages on your system for additional information on changing group ownership.
6. Switch to the least privileged (non-root) user and run
   ```
   sudo SPLUNK_HOME/bin/splunk start
   ```
   Or

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

Install the universal forwarder on Solaris

The universal forwarder is available for Solaris as a tar file or a PKG file.

If you plan to install a universal forwarder on a Sun SPARC system that runs Solaris, confirm that you have patch level SUNW_1.22.7 or later of the C library (libc.so.1). If you do not, the universal forwarder cannot run because it needs this version of the library.

Install from a tar file

Use the `tar` command to install the forwarder.

- To install into the folder `/opt/splunkforwarder`:

1. Uncompress the tar file. `uncompress splunkforwarder-<version-os-arch>.tar.Z`

2. Extract the tar file. `tar xvf splunkforwarder-<version-os-arch>.tar -C /opt`

- To install into the current working directory under the `splunkforwarder` folder:

1. Uncompress the tar file. `uncompress splunkforwarder-<version-os-arch>.tar.Z`
2. Extract the tar file. `tar xvf splunkforwarder-<version-os-arch>.tar`

For post-installation configuration and credential creation, see After you install: Start and configure the universal forwarder.

Install the universal forwarder on Mac OS X

The universal forwarder is available for Mac OS X as a tar file or a DMG package.

Install the universal forwarder from the Finder

1. Navigate to the folder or directory where the installer is located.
2. Double-click the DMG file.
   A Finder window that contains the `splunkforwarder.pkg` opens.
3. Double-click the `Install Splunk Universal Forwarder` icon to start the installer.
4. The **Introduction** panel lists version and copyright information. Click **Continue**.
5. The **License** panel lists shows the software license agreement. Click **Continue**.
6. You will be asked to agree to the terms of the software license agreement. Click **Agree**.
7. In the **Installation Type** panel, click **Install**. This installs the universal forwarder in the default directory `/Applications/SplunkForwarder`.
8. You are prompted to type the password that you use to login to your computer.
9. When the installation finishes, a popup informs you that an initialization must be performed. Click **OK**.
10. A terminal window appears and you are prompted to specify a userid and password to use with the universal forwarder.

    The password must be at least 8 characters in length. The cursor will not advance as you type. Make note of the userid and password. You will use these credentials to authenticate when using CLI commands on the forwarder.
11. A popup appears asking what you would like to do. Click **Start Splunk**.
12. Close the **Install Splunk Forwarder** window.

    The installer places a shortcut on the Desktop so that you can start or stop the universal forwarder from your Desktop any time.

Install from a tar file

Use the `tar` command to install the forwarder.

- To install the forwarder into the folder `/Applications/splunkforwarder`, run:

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

- To install the forwarder into the current working directory under the `splunkforwarder` folder, run:

```
tar xvzf splunkforwarder.tgz
```

For post-installation configuration and credential creation, see After you install: Start and configure the universal forwarder.

Install the universal forwarder on FreeBSD

The universal forwarder is available for FreeBSD as a .txz file package.

Prerequisites

FreeBSD best practices maintain a small root filesystem. Verify that the root filesystem has sufficient free space for the universal forwarder installation.

The package installs the forwarder in the default directory, `/opt/splunkforwarder`. If `/opt` does not exist, you might receive an error message.

Basic FreeBSD installation

1. Download the FreeBSD package file from splunk.com (login required.)
2. Install the universal forwarder on FreeBSD using the `pkg` command:
   `pkg install splunkforwarder-<version>-freebsd-<version>-amd64.txz`
3. Start the universal forwarder service and create a local user and password. For post-installation configuration and credential creation, see After you install: Start and configure the universal forwarder.

Requirements after installing the forwarder on FreeBSD

These instructions ensure that the forwarder functions properly on FreeBSD. If your host has less than 2 GB of memory, reduce the `kern.maxdsiz` and `kern.dfldsiz` values accordingly.

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

Install the universal forwarder on AIX

The universal forwarder is available for AIX as a tar file. The default installation directory is `/opt/splunkforwarder`.

Do not use the AIX version of `tar` to unarchive the file. Use the GNU version instead. This version comes with the AIX Toolbox for Linux Applications package that comes with a base AIX installation. If your AIX does not come with this package installed, you can download it from IBM. See IBM AIX Toolbox download information.

1. Confirm that the user that the universal forwarder runs as has permission to read the `/dev/random` and `/dev/urandom` devices.
2. Expand the tar file into an appropriate directory:
   `tar xvzf splunkforwarder-<...>.tgz`

Enable the universal forwarder to automatically start at boot time

The AIX version of the universal forwarder does not register itself to auto-start on reboot. You can register it by running the following command from the `$SPLUNK_HOME/bin` directory at a prompt:

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

This command invokes the following system commands to register the forwarder in the System Resource Controller (SRC):

```
mkssys -G splunk -s splunkd -p <path to splunkd> -u <splunk user> -a _internal_exec_splunkd -S -n 2 -f 9
```

When you enable automatic boot start, the SRC handles the run state of the forwarder. This means that you must use a different command to start and stop the forwarder manually:

- `/usr/bin/startsrc -s splunkd` to start the forwarder.
- `/usr/bin/stopsrc -s splunkd` to stop the forwarder.

If you attempt to start and stop the forwarder using the `./splunk [start|stop]` method from the `$SPLUNK_HOME` directory, the SRC catches the attempt and the forwarder displays the following message:

```
Splunk boot-start is enabled. Please use /usr/bin/[startsrc|stopsrc] -s splunkd to [start|stop] Splunk.
```

To prevent this message from occurring and restore the ability to start and stop the forwarder from the `$SPLUNK_HOME` directory, disable boot start:

```
./splunk disable boot-start
```

- For more information on the `mkssys` command line arguments, see Mkssys command on the IBM pSeries and AIX Information Center website.
- For more information on the SRC, see System resource controller on the IBM Knowledge Center website.

Secure your Linux universal forwarder with a least-privileged user

Installing a Splunk universal forwarder on Linux automatically creates a least-privileged user. This is a non-root user with permissions specific to the successful operation of the universal forwarder features and add-ons.

To install the universal forwarder with a least-privileged user, see Install a *nix universal forwarder.

Least-privileged users are created when you install or update any Linux installation packaging format, including, .deb, .rpm, and .tgz. formats.

The least-privileged user possesses `AmbientCapabilities` that lets the user operate universal forwarder features and common add-ons without permission issues. These capabilities are:

Capability	Desc	Use
`CAP_DAC_READ_SEARCH`	Bypass file read permission checks and directory read and execute permission checks;	Collects data from files outside of `$SPLUNK_HOME`
`CAP_NET_ADMIN`	Perform various network-related operations: • perform interface configuration • administer IP firewall, masquerading, and accounting	Used by the Stream Forwarder

Capability	Desc	Use
	• modify routing tables • bind to any address for transparent proxying • set type-of-service (TOS) • clear driver statistics • set promiscuous mode • enable multicasting	
CAP_NET_RAW	• Use RAW and PACKET sockets • bind to any address for transparent proxying	Used by the Stream forwarder

Disable, enable, or change least-privileged user

The least-privileged user is enabled automatically during installation or upgrade. You can manually enable or disable it. To disable it, stop Splunk and run:

```
[sudo] $SPLUNK_HOME/bin/splunk disable boot-start
```

This command removed the unit file as well as the startup file. This will remove unit files from both locations:

```
/usr/lib/systemd/system
/etc/systemd/system
```

To enable or overwrite an existing least-privileged user configuration, run:

```
[sudo] $SPLUNK_HOME/bin/splunk enable boot-start
```

This command will grant least-privilege capabilities by default, and the unit file is created in the user level directory.

To change users, you must run this command again.

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

Troubleshooting

Manually enable a least privilege user

If you encounter an error during installation that prevents the creation of a least-privileged user, you can use the following command to manually create or recreate the default least privileged user:

```
[sudo] $SPLUNK_HOME/bin/splunk enable boot-start -systemd-managed 1 -user <username> -group <groupname>
```

This creates a unit file with the following permissions:

```
######## Added for least privilege mode #########
NoNewPrivileges=yes
AmbientCapabilities=CAP_DAC_READ_SEARCH CAP_NET_ADMIN CAP_NET_RAW
#################################################
```

Editing unit files

Splunk software potentially creates two unit files in two locations when you Install the least privileged user on a Linux machine. If you have error messages, you may have to check and edit both files. To locate both files run the following command:

```
./splunk display boot-start
```

Error messages

Error message	Description
Cannot create file /usr/lib/systemd/system/SplunkForwarder.service: permission denied.	You must create the unit file manually or the current user does not have permission to create the unit file.
Failed to auto-set default user. Please create the unit file manually.	The system cannot find a valid Linux user.
Failed to create splunk unit file. Please create the unit file manually	Usually a system error, for example, the system cannot create the folder, create the startup file, or reload systemd.

Reference

About the unit files created for the least privileged user

Splunk software potentially creates two unit files in different locations when you Install the least-privileged user on a Linux machine.

- If the first unit file is created successfully at installation, no further unit files are created.
- If the first file fails during installation, another file is created on the user level in the local folder.
- If you use the `[sudo] $SPLUNK_HOME/bin/splunk enable boot-start` command after a least privileged user is created, a new file is created locally. This either creates a new file in the local directory or overwrites any local file that exists.
- The local file takes precedence over the system file.

To see your unit files and their location in your environment, you can run `Splunk display boot-start`.

/usr/lib/systemd/system	where services are provided by installed packages	This is automatically created during installation, and can be overwritten during upgrade or by running `[sudo] $SPLUNK_HOME/bin/splunk enable boot-start`
/etc/systemd/system	where system-wide user services are placed by the system administrator	Created when running `splunk enable boot-start -systemd-managed 1`

Reference unit file template

This is an example of a unit file template. You can use it to manually create a unit file.

```
#This unit file replaces the traditional start-up script for systemd
#configurations, and is used when enabling boot-start for Splunk on
#systemd-based Linux distributions.

[Unit]
Description=Systemd service file for Splunk, generated by 'splunk enable boot-start'
After=network.target

[Service]

######## Added for least privilege mode #########
NoNewPrivileges=yes
AmbientCapabilities=CAP_DAC_READ_SEARCH CAP_NET_ADMIN CAP_NET_RAW
#################################################

Type=simple
Restart=always
ExecStart=/opt/splunk/bin/splunk _internal_launch_under_systemd
KillMode=mixed
```

```
KillSignal=SIGINT
TimeoutStopSec=360
LimitNOFILE=65536
SuccessExitStatus=51 52
RestartPreventExitStatus=51
RestartForceExitStatus=52
User=splunk
Group=splunk
Delegate=true
CPUShares=1024
MemoryLimit=<value>
PermissionsStartOnly=true
ExecStartPost=/bin/bash -c "chown -R splunker:splunker /sys/fs/cgroup/cpu/system.slice/%n"
ExecStartPost=/bin/bash -c "chown -R splunker:splunker /sys/fs/cgroup/memory/system.slice/%n"

[Install]
WantedBy=multi-user.target
```

Enable a receiver for Splunk Enterprise

A receiver is a Splunk software instance that is configured to listen on a specific port for incoming communications from a forwarder. Usually, the receiver is an indexer or a cluster of indexers.

For Splunk Enterprise forwarder and indexer compatibility see Compatibility between forwarders and Splunk Enterprise indexers in the *Splunk Products Version Compatibility Matrix* manual.

Sometimes the receiver is another forwarder, which is called an intermediate forwarder. To learn more about how intermediate forwarders work, see Configure an intermediate forwarder.

A Splunk Cloud receiving port is configured and enabled by default. Instead, you need credentials to access it. See Install and configure The Splunk Cloud universal forwarder credentials package.

Configure a receiver using Splunk Web

Use Splunk Web to configure a receiver:

1. Log into Splunk Web as a user with the admin role.
2. In Splunk Web, go to **Settings > Forwarding and receiving**.
3. Select "Configure receiving."
4. Verify if there are existing receiver ports open. You cannot create a duplicate receiver port. The conventional receiver port configured on indexers is port `9997`.
5. Optionally select "New Receiving Port."
6. Add a port number and save.

Splunk Web is only available with Splunk Enterprise, not the universal forwarder.

Configure a receiver using the command line

Use the command line interface (CLI) to configure a receiver:

1. Open a shell prompt
2. Change the path to $SPLUNK_HOME/bin
3. Type: `splunk enable listen <port> -auth <username>:<password>.`
4. Restart Splunk software for the changes to take effect.

*nix example	Windows example
`./splunk enable listen 9997 -auth admin:password`	`splunk enable listen 9997 -auth admin:password`

Configure a receiver using a configuration file

Configure a receiver using the `inputs.conf` file:

1. Open a shell prompt
2. Change the path to `$SPLUNK_HOME/etc/system/local`.
3. Edit the `inputs.conf` file.
4. Create a `[splunktcp]` stanza and define the receiving port. Example:

```
[splunktcp://9997]
disabled = 0
```

5. Save the file.
6. Restart Splunk software for the changes to take effect.

Install and configure the Splunk Cloud Platform universal forwarder credentials package

To enable your forwarders to send data to the Splunk Cloud Platform, download the universal forwarder credentials file.

You can:

- Install the forwarder credentials on individual forwarders.
- Install the forwarder credentials on many forwarders using a deployment server.

Install the forwarder credentials on individual forwarders in *nix

1. From your Splunk Cloud Platform instance, go to **Apps > Universal Forwarder**.
2. Click **Download Universal Forwarder Credentials**.
3. Note the location where the credentials file `splunkclouduf.spl` has been downloaded.
4. Copy the file to a temporary directory, this is usually your "/tmp" folder.
5. Install the `splunkclouduf.spl` app by entering the following in command line: `$SPLUNK_HOME/bin/splunk install app /tmp/splunkclouduf.spl`.
6. When you are prompted for a user name and password, enter the user name and password for the Universal Forwarder. The following message displays if the installation is successful: `App '/tmp/splunkclouduf.spl' installed`.
7. Restart the forwarder to enable the changes by entering the following command: `./splunk restart`.

Install the forwarder credentials on many forwarders using a deployment server in *nix

1. From your Splunk Cloud Platform instance, go to **Apps > Universal Forwarder**.
2. Click **Download Universal Forwarder Credentials**.
3. Note the location where the credentials file was downloaded. The credentials file is named `splunkclouduf.spl`.
4. Copy the file to your system's temporary (/tmp) folder.
5. (optional) Use file management tools to move the `splunkclouduf.spl` file to the `$SPLUNK_HOME/etc/deployment-apps/` directory on the deployment server.
6. In a shell or command prompt, unpack the credentials package by running the following command: `tar xvf splunkclouduf.spl`

.
7. Navigate to the `/bin` subdirectory of the deployment server.
8. Install the credentials package by running the following command:
   `splunk install app <full path to splunkclouduf.spl> -auth <username>:<password>`
   where `<full path to splunkclouduf.spl>` is the path to the directory where the `splunkclouduf.spl` file is located and `<username>:<password>` are the username and password of an existing admin account on the deployment server.
9. Restart the deployment server by running the following command:
   `/splunk restart`
   .

Install the forwarder credentials on individual forwarders in Windows

1. From your Splunk Cloud Platform instance, go to **Apps > Universal Forwarder**.
2. Click **Download Universal Forwarder Credentials**.
3. Note the location where the credentials file was downloaded. The credentials file is named `%HOMEPATH%\Downloads`.
4. Copy the file to your system's temporary (\tmp) folder.
5. Install the `splunkclouduf.spl` app by entering the following command: `%SPLUNK_HOME%\bin\splunk.exe install app %HOMEPATH%\Downloads\splunkclouduf.spl`.
6. When you are prompted for a username and password, enter the username and password for the Universal Forwarder. The following message displays if the installation is successful:
   `App %HOMEPATH%\Downloads\splunkclouduf.spl installed`.
   1. Restart the forwarder to enable the changes by entering the following command. `.\splunk.exe restart`.

Install the forwarder credentials on many forwarders using a deployment server in Windows

1. From your Splunk Cloud Platform instance, go to **Apps > Universal Forwarder**.
2. Click **Download Universal Forwarder Credentials**.
3. Note the location where the credentials file `splunkclouduf.spl` was downloaded.
4. Copy the file to your system's temporary (\tmp) folder.
5. (optional) Use file management tools to move the `splunkclouduf.spl` file to the `$SPLUNK_HOME\etc\deployment-apps\` directory on the deployment server.
6. In a shell or command prompt, unpack the credentials package by running the following command:
   `tar xvf splunkclouduf.spl`
   .
7. Navigate to the `\bin` subdirectory of the deployment server.
8. Install the credentials package by running the following command:
   `splunk install app <full path to splunkclouduf.spl> -auth <username>:<password>`
   where `<full path to splunkclouduf.spl>` is the path to the directory where the `splunkclouduf.spl` file is located and `<username>:<password>` are the username and password of an existing admin account on the deployment server.
9. Restart the deployment server by running the following command:
   `\splunk restart`

.

Configure the universal forwarder using configuration files

Optionally edit the Universal forwarder configuration files to further modify how your machine data is streamed to your indexers. See the following steps:

1. Find the configuration files.

2. Edit the configuration files.
3. Restart the universal forwarder.

Find the configuration files

Navigate to `outputs.conf` in `$SPLUNK_HOME/etc/system/local/` to locate your Universal Forwarder configuration files.

Key configuration files:

- inputs.conf controls how the forwarder collects data.
- outputs.conf controls how the forwarder sends data to an indexer or other forwarder.
- server.conf for connection and performance tuning.
- deploymentclient.conf for connecting to a deployment server.

Edit the configuration files

You can edit them however you normally edit files, such as through a text editor or the command line, or you can use the Splunk Deployment Server.

When you make configuration changes with the CLI, the universal forwarder writes the configuration files. This prevents typos and other mistakes that can occur when you edit configuration files directly.

The forwarder writes configurations for forwarding data to `outputs.conf` in `$SPLUNK_HOME/etc/system/local/`).

Edit the configuration files through the command line

You can choose to edit the configuration files through the command line. For more details on using the CLI in general, see Administer Splunk Enterprise with the CLI in the Splunk Enterprise *Admin Manual*.

The general syntax for a CLI command is:

```
./splunk <command> [<object>] [[-<parameter>] <value>]...
```

See the following examples of using the command line to edit configuration files:

Configure the universal forwarder to connect to a receiving indexer

From a shell or command prompt on the forwarder, run the command:

```
./splunk add forward-server <host name or ip address>:<listening port>
```

For example, to connect to the receiving indexer with the hostname `idx.mycompany.com` and that host listens on port 9997 for forwarders, type in:

```
./splunk add forward-server idx1.mycompany.com:9997
```

Configure the universal forwarder to connect to a deployment server

From a shell or command prompt on the forwarder, run the command:

```
./splunk set deploy-poll <host name or ip address>:<management port>
```

For example, if you want to connect to the deployment server with the hostname `ds1.mycompany.com` on the default management port of 8089, type in:

```
./splunk set deploy-poll ds1.mycompany.com:8089
```

Configure a data input on the forwarder

The Splunk Enterprise *Getting Data In* manual has information on what data a universal forwarder can collect.

1. Determine what data you want to collect.

2. From a shell or command prompt on the forwarder, run the command that enables that data input. For example, to monitor the `/var/log` directory on the host with the universal forwarder installed, type in:

```
./splunk add monitor /var/log
```

The forwarder asks you to authenticate and begins monitoring the specified directory immediately after you log in.

Configure your forwarder protocol level in Splunk Cloud Platform version 9.0.2208 or later

For Splunk Cloud Platform version 9.0.2208 and later, if you configure the universal forwarder to use the old protocol, a warning message is generated. To avoid warning messages, you can set negotiateProtocolLevel to a value that is larger than 0, or set negotiateNewProtocol=true to use the new Splunk-to-Splunk protocol. For more information, please check negotiateProtocolLevel and negotiateNewProtocol in outputs.conf.

Start or stop the universal forwarder

After you install the universal forwarder, you must start it. Also, if you make changes to the universal forwarder, you must start or restart it:

- Restart the universal forwarder
- Start the universal forwarder
- Stop the universal forwarder

Restart the universal forwarder

Some configuration changes might require that you restart the forwarder.

To restart the universal forwarder, use the same CLI `restart` command that you use to restart a full Splunk Enterprise instance:

- **On Windows:** Go to `%SPLUNK_HOME%\bin` and run this command:

```
splunk restart
```

- **On *nix systems:** From a shell prompt on the host, go to `$SPLUNK_HOME/bin`, and run this command:

```
./splunk restart
```

Start the universal forwarder

See the following steps to start the universal forwarder:

1. Set up environment variables on your machine, which are necessary to run these commands. It is possible these variables have automatically been set up. See Change default values in the *Admin Manual*.
2. Run the following commands to start the universal forwarder at any time. If this is your first time starting the forwarder, you may be asked to review and accept a license agreement and create a username and password:
    - ♦ If you want to start the universal forwarder, run this command.

Unix	Windows
`cd $SPLUNK_HOME/bin` `./splunk start`	`cd %SPLUNK_HOME%\bin` `.\splunk start`

1. ♦ If you want to accept the license agreement without reviewing it when you start the forwarder for the first time, run this command.

Unix	Windows
`cd $SPLUNK_HOME/bin` `./splunk start --accept-license`	`cd %SPLUNK_HOME%\bin` `.\splunk start --accept-license`

1. ♦ If you want to restart the forwarder after you make a configuration change, run this command. When you do, the forwarder first stops itself, then starts itself again.

Unix	Windows
`cd $SPLUNK_HOME/bin` `./splunk restart`	`cd %SPLUNK_HOME%\bin` `.\splunk restart`

Additionally, you can configure the universal forwarder to start at boot time. See Configure Splunk Enterprise to start at boot time for the procedure.

The universal forwarder prompts for administrator credentials the first time you start it

When you start the forwarder for the first time under most conditions, it prompts you to create credentials for the Splunk administrator user. The following text appears:

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

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username:
```

1. Type in the name you want to use for the administrator user. This is the user that you log into the universal forwarder with, not the user that you use to log into your machine or onto splunk.com. You can press Enter to use the default username of `admin`.
   The following text appears:

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

2. Type in the password that you want to assign to the user. The password must meet the requirements that the prompt displays.

See Create a secure administrator password in *Securing Splunk* for additional information about creating a secure password.

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

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

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

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

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

Stop the universal forwarder

You must stop the universal forwarder if you do not want it to forward data any more, or as part of a restart sequence when you make a configuration change that requires a restart.

The following commands use environment variables that might not be automatically set on your host. The environment variables represent where the universal forwarder has been installed on the host. To learn how to set these environment variables, see Change default values in the *Admin Manual*.

- Run the following commands to stop the universal forwarder.

Unix	Windows
`cd $SPLUNK_HOME/bin` `./splunk stop`	`cd %SPLUNK_HOME%\bin` `.\splunk stop`

Upgrade or uninstall the universal forwarder

Upgrade the universal forwarder

See the following instructions to upgrade the Windows universal forwarder or the *nix universal forwarder:

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

If you are planning to upgrade the universal forwarder to version 9.0, see About upgrading to 9.0 READ THIS FIRST in the "Installation Manual" first.

As of version 9.0, the configuration change tracker is enabled by default. To track your indexer configuration logs using this functionality, either upgrade your indexers to 9.0 or enable index(_configtracker) for your indexers.

Upgrade the Windows universal forwarder

When you upgrade a universal forwarder, the installer updates the software without changing its configuration. You must make any necessary configuration changes after you complete the upgrade. A deployment server can assist in the configuration update process.

There are several forwarder upgrade scenarios:

- You can upgrade a single forwarder with the GUI installer
- You can upgrade a single forwarder with the command line installer
- You can perform a remote upgrade of a group of forwarders (good for deployments of any size)

As best practice when upgrading a Windows universal forwarder on Splunk Cloud Platform, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud Platform environment.

When you upgrade on Windows, make sure to stop Splunk. If Splunk is running during upgrade, the upgrade fails with error "ERROR: In order to migrate, Splunkd must not be running." "

Confirm that an upgrade is necessary

Begin by checking the forwarder compatibility. To determine if you need to upgrade your forwarder version to remain in support or use specific features, see the appropriate topic for your deployment:

- Splunk Cloud Platform: Supported forwarder versions in the *Splunk Cloud Platform Service Description*.
- Splunk Enterprise: Compatibility between forwarders and Splunk Enterprise indexers in the *Splunk Products Version Compatibility Matrix*.

If your forwarders are on the same major release of Splunk software as the indexers, they are compatible. However, you might need an upgrade to a different minor release due to a technical issue in a specific feature. Before upgrading forwarders, review the Known Issues and Fixed Issues.

You must perform any platform architecture changes manually

You cannot upgrade a 32-bit version of the universal forwarder with a 64-bit universal forwarder installer. To upgrade from 32-bit to 64-bit, follow these instructions:

1. Stop splunkd if it is running.
2. Back up your configurations, including any apps or add-ons (in `%SPLUNK_HOME%\etc\apps`). Also back up the checkpoint files located in `%SPLUNK_HOME%\var\lib\splunk\modinputs`.
3. Uninstall the existing 32-bit forwarder, as described in Uninstall the universal forwarder.
4. Install the 64-bit forwarder, as described in Install the universal forwarder from an installer.
5. Restore apps, configurations and checkpoints by copying them to the appropriate directories:

   `%SPLUNK_HOME%\etc\system\local` for configuration files.
   `%SPLUNK_HOME%\etc\apps` for apps and add-ons.
   `%SPLUNK_HOME%\var\lib\splunk\modinputs` for checkpoint files.

Back your files up

Before you perform an upgrade, back up configuration files. See Back up configuration information in the Splunk Enterprise *Admin* manual.

There is no means of downgrading to a previous version. If you need to revert to an older forwarder release, uninstall the current version and reinstall the older release.

Upgrade a single forwarder using the GUI installer

You can upgrade a single forwarder with the GUI installer. The installer stops the forwarder as part of the upgrade process.

1. Stop splunkd if it is running.
2. Download the new MSI file from the universal forwarder download page.
3. Double-click the MSI file. The installer displays the "Accept license agreement" panel.
4. Accept the license agreement and click "Install." The installer upgrades the forwarder, retains the existing configuration, and starts automatically when you complete the installation.

The installer puts a log of upgrade changes in the `%TEMP%` directory (This is usually the `C:\TEMP` directory but can be different based on your Windows machine configuration.) It also reports any errors in the Application Event Log.

Upgrade a single forwarder using the command line

You can upgrade a single forwarder by running the command line installer.

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

1. Stop splunkd if it is running.
2. Download the new MSI file from the Splunk universal forwarder download page.
3. Run `msiexec.exe` to Install the universal forwarder from the command line.
   - For 32-bit platforms, use `splunkuniversalforwarder-<...>-x86-release.msi`.

     ```
     msiexec.exe /i splunkuniversalforwarder-<...>-x86-release.msi [AGREETOLICENSE=Yes /quiet]
     ```
   - For 64-bit platforms, use `splunkuniversalforwarder-<...>-x64-release.msi`.

```
msiexec.exe /i splunkuniversalforwarder-<...>-x64-release.msi [AGREETOLICENSE=Yes /quiet]
```

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

4. 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.

Perform a remote upgrade of one or more forwarders

You can use a deployment tool such as Group Policy or System Center Configuration Manager to distribute the forwarder software among a group of forwarders in your environment. You might want to test the upgrade locally on one machine before performing a remote upgrade across all your forwarders.

The Splunk Enterprise deployment server cannot distribute the universal forwarder, only its apps and configurations. Do not attempt to use deployment server to distribute universal forwarders.

1. Download the new MSI file from the Splunk universal forwarder download page.
2. Load the MSI into your deployment tool. In the tool, specify the command line as follows.

```
msiexec.exe /i splunkuniversalforwarder-<...>.msi AGREETOLICENSE=Yes /quiet
```

3. Start the deployment with your deployment tool.
4. Use the deployment monitor to verify that the universal forwarders function properly.

Upgrade the *nix universal forwarder

You have several scenarios for upgrading a *nix universal forwarder:

- Upgrade a single forwarder manually.
- Perform a remote upgrade of a group of forwarders. (Use this option for deployments of any size)

As best practice when upgrading a *nix universal forwarder on Splunk Cloud Platform, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud Platform environment.

Confirm that an upgrade is necessary

Begin by checking the forwarder compatibility. To determine if you need to upgrade your forwarder version to remain in support or use specific features, see the appropriate topic for your deployment:

- Splunk Cloud Platform: Supported forwarder versions in the *Splunk Cloud Platform Service Description*
- Splunk Enterprise: Compatibility between forwarders and Splunk Enterprise indexers in the *Splunk Products Version Compatibility Matrix*.

If your forwarders are on the same major release of Splunk software as the indexers, they are compatible. However, you might need an upgrade to a different minor release due to a technical issue in a specific feature. Before upgrading forwarders, review the Known Issues and Fixed Issues.

Back your files up

Before you perform the upgrade, back up your configuration files. See Back up configuration information in the Splunk Enterprise *Admin Manual*.

If you need to revert to an older forwarder release, uninstall the upgrade and reinstall the older release.

Confirm that you do not have scripts in place to auto-start forwarders. If you do, disable such scripts for now. You can re-enable them later, after the upgrade.

How upgrading works

After you perform the installation of the new forwarder, you must restart it for any changes to take effect. You can run the migration preview utility at that time to see what will change before the files are updated. If you choose to view the changes before proceeding, the forwarder writes the proposed changes to `$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>`

Upgrade a single forwarder

There are several packages that you can use to upgrade a universal forwarder. Tar files and pre-built package such as an .rpm, .deb, or .dmg file are available depending on the operating system.

If you use a .tar file to upgrade a forwarder, expand it into the same directory with the same ownership as the existing universal forwarder instance. This overwrites and replaces matching files but does not remove unique files.

If you use an RPM file, use the RPM package manager (`rpm -U <splunk_package_name>.rpm`) from a shell prompt to perform the upgrade.

If you use a .dmg file (on MacOS), double-click it and follow the instructions. After the installation starts, specify the same installation directory as your existing installation.

On hosts that run AIX, do not use the AIX version of `tar` to unarchive a tar file during an upgrade. Use the GNU version of `tar` instead. This version comes with the AIX Toolbox for Linux Applications package that comes with a base AIX installation. If your AIX does not come with this package installed, you can download it from IBM. See IBM AIX Toolbox download information.

1. Stop the forwarder.

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

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

As best practice when upgrading a *nix universal forwarder on Splunk Cloud Platform, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud Platform environment.

3. Start the forwarder again.

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

The forwarder displays the following:

```
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. Choose whether you want to run the migration preview script to see what changes will be made to your existing configuration files, or proceed with the migration and upgrade right away. If you choose to view the expected changes, the script provides a list of those changes.

5. Once you have reviewed these changes and are ready to proceed with migration and upgrade, run `$SPLUNK_HOME/bin/splunk start` again.

You can complete the last three steps 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
```

- For Linux upgrade you must use sudo to upgrade as the root user.

```
sudo $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
```

Perform a remote upgrade

To perform a remote upgrade, first perform an upgrade on a test machine. Then, create a script to automate the upgrade on remote machines. You can use the following script, but you might need to modify the script to meet the needs of an upgrade.

1. Upgrade the universal forwarder on a test machine, as described in Install a nix universal forwarder.

2. Create a script wrapper for the upgrade commands.

3. Run the script on representative target machines to verify that it works with all required shells.

4. Execute the script against the desired set of hosts.

```
#!/bin/sh

# This script provides an example of how to deploy the universal forwarder
# to many remote hosts via ssh and common Unix commands.
#
# Note that this script will only work unattended if you have SSH host keys
# setup & unlocked.
# To learn more about this subject, do a web search for "openssh key management".
```

```
# ----------- Adjust the variables below -----------

# Populate this file with a list of hosts that this script should install to,
# with one host per line.  You may use hostnames or IP addresses, as
# applicable.  You can also specify a user to login as, for example, "foo@host".
#
# Example file contents:
# server1
# server2.foo.lan
# you@server3
# 10.2.3.4

HOSTS_FILE="/path/to/splunk.install.list"

# This is the path to the tar file that you wish to push out.  You may
# wish to make this a symlink to a versioned tar file, so as to minimize
# updates to this script in the future.

SPLUNK_FILE="/path/to/splunk-latest.tar.gz"

# This is where the tar file will be stored on the remote host during
# installation.  The file will be removed after installation.  You normally will
# not need to set this variable, as $NEW_PARENT will be used by default.
#
# SCRATCH_DIR="/home/your_dir/temp"

# The location in which to unpack the new tar file on the destination
# host.  This can be the same parent dir as for your existing
# installation (if any).  This directory will be created at runtime, if it does
# not exist.

NEW_PARENT="/opt"

# After installation, the forwarder will become a deployment client of this
# host.  Specify the host and management (not web) port of the deployment server
# that will be managing these forwarder instances.  If you do not wish to use
# a deployment server, you may leave this unset.
#
# DEPLOY_SERV="splunkDeployMaster:8089"

# A directory on the current host in which the output of each installation
# attempt will be logged.  This directory need not exist, but the user running
# the script must be able to create it.  The output will be stored as
# $LOG_DIR/<[user@]destination host>.  If installation on a host fails, a
# corresponding file will also be created, as
# $LOG_DIR/<[user@]destination host>.failed.

LOG_DIR="/tmp/splunkua.install"

# For conversion from normal Splunk Enterprise installs to the universal forwarder:
# After installation, records of progress in indexing files (monitor)
# and filesystem change events (fschange) can be imported from an existing
# Splunk Enterprise (non-forwarder) installation.  Specify the path to that installation here.
# If there is no prior Splunk Enterprise instance, you may leave this variable empty ("").
#
# NOTE: THIS SCRIPT WILL STOP THE SPLUNK ENTERPRISE INSTANCE SPECIFIED HERE.
#
# OLD_SPLUNK="/opt/splunk"

# If you use a non-standard SSH port on the remote hosts, you must set this.
# SSH_PORT=1234
```

```
# You must remove this line, or the script will refuse to run.  This is to
# ensure that all of the above has been read and set. :)

UNCONFIGURED=1

# ----------- End of user adjustable settings -----------


# helpers.

faillog() {
  echo "$1" >&2
}

fail() {
  faillog "ERROR: $@"
  exit 1
}

# error checks.

test "$UNCONFIGURED" -eq 1 && \
  fail "This script has not been configured.  Please see the notes in the script."
test -z "$HOSTS_FILE" && \
  fail "No hosts configured!  Please populate HOSTS_FILE."
test -z "$NEW_PARENT" && \
  fail "No installation destination provided!  Please set NEW_PARENT."
test -z "$SPLUNK_FILE" && \
  fail "No splunk package path provided!  Please populate SPLUNK_FILE."
if [ ! -d "$LOG_DIR" ]; then
  mkdir -p "$LOG_DIR" || fail "Cannot create log dir at \"$LOG_DIR\"!"
fi

# some setup.

if [ -z "$SCRATCH_DIR" ]; then
  SCRATCH_DIR="$NEW_PARENT"
fi
if [ -n "$SSH_PORT" ]; then
  SSH_PORT_ARG="-p${SSH_PORT}"
  SCP_PORT_ARG="-P${SSH_PORT}"
fi

NEW_INSTANCE="$NEW_PARENT/splunkforwarder" # this would need to be edited for non-UA...
DEST_FILE="${SCRATCH_DIR}/splunk.tar.gz"

#
#
# create script to run remotely.
#
#

REMOTE_SCRIPT="
  fail() {
    echo ERROR: \"\$@\" >&2
    test -f \"$DEST_FILE\" && rm -f \"$DEST_FILE\"
    exit 1
  }
"

###   try untarring tar file.
```

```
REMOTE_SCRIPT="$REMOTE_SCRIPT
  (cd \"$NEW_PARENT\" && tar -zxf \"$DEST_FILE\") || fail \"could not untar /$DEST_FILE to $NEW_PARENT.\"
"

###   setup seed file to migrate input records from old instance, and stop old instance.
if [ -n "$OLD_SPLUNK" ]; then
  REMOTE_SCRIPT="$REMOTE_SCRIPT
    echo \"$OLD_SPLUNK\" > \"$NEW_INSTANCE/old_splunk.seed\" || fail \"could not create seed file.\"
    \"$OLD_SPLUNK/bin/splunk\" stop || fail \"could not stop existing splunk.\"
  "
fi

###   setup deployment client if requested.
if [ -n "$DEPLOY_SERV" ]; then
  REMOTE_SCRIPT="$REMOTE_SCRIPT
    \"$NEW_INSTANCE/bin/splunk\" set deploy-poll \"$DEPLOY_SERV\" --accept-license --answer-yes \
      --auto-ports --no-prompt || fail \"could not setup deployment client\"
  "
fi

###   start new instance.
REMOTE_SCRIPT="$REMOTE_SCRIPT
  \"$NEW_INSTANCE/bin/splunk\" start --accept-license --answer-yes --auto-ports --no-prompt || \
    fail \"could not start new splunk instance!\"
"

###   remove downloaded file.
REMOTE_SCRIPT="$REMOTE_SCRIPT
  rm -f "$DEST_FILE" || fail \"could not delete downloaded file $DEST_FILE!\"
"

#
#
# end of remote script.
#
#

exec 5>&1 # save stdout.
exec 6>&2 # save stderr.

echo "In 5 seconds, will copy install file and run the following script on each"
echo "remote host:"
echo
echo "====================="
echo "$REMOTE_SCRIPT"
echo "====================="
echo
echo "Press Ctrl-C to cancel..."
test -z "$MORE_FASTER" && sleep 5
echo "Starting."

# main loop.  install on each host.

for DST in `cat "$HOSTS_FILE"`; do
  if [ -z "$DST" ]; then
    continue;
  fi

  LOG="$LOG_DIR/$DST"
  FAILLOG="${LOG}.failed"
  echo "Installing on host $DST, logging to $LOG."
```

```
  # redirect stdout/stderr to logfile.
  exec 1> "$LOG"
  exec 2> "$LOG"

  if ! ssh $SSH_PORT_ARG "$DST" \
      "if [ ! -d \"$NEW_PARENT\" ]; then mkdir -p \"$NEW_PARENT\"; fi"; then
    touch "$FAILLOG"
    # restore stdout/stderr.
    exec 1>&5
    exec 2>&6
    continue
  fi

  # copy tar file to remote host.
  if ! scp $SCP_PORT_ARG "$SPLUNK_FILE" "${DST}:${DEST_FILE}"; then
    touch "$FAILLOG"
    # restore stdout/stderr.
    exec 1>&5
    exec 2>&6
    continue
  fi

  # run script on remote host and log appropriately.
  if ! ssh $SSH_PORT_ARG "$DST" "$REMOTE_SCRIPT"; then
    touch "$FAILLOG" # remote script failed.
  else
    test -e "$FAILLOG" && rm -f "$FAILLOG" # cleanup any past attempt log.
  fi

  # restore stdout/stderr.
  exec 1>&5
  exec 2>&6

  if [ -e "$FAILLOG" ]; then
    echo "    FAILED  "
  else
    echo "      SUCCEEDED"
  fi
done

FAIL_COUNT=`ls "${LOG_DIR}" | grep -c '\.failed$'`
if [ "$FAIL_COUNT" -gt 0 ]; then
  echo "There were $FAIL_COUNT remote installation failures."
  echo "  ( see ${LOG_DIR}/*.failed )"
else
  echo
  echo "Done."
fi

# Voila.
```

Uninstall the universal forwarder

Before you uninstall the forwarder, stop it and remove it from any system start-up scripts first. Run these commands from a shell or command prompt or Terminal or PowerShell window.

1. If you configured the universal forwarder to start on boot, remove it from your boot scripts before you uninstall.

Unix	Windows

Unix	Windows
`cd $SPLUNK_HOME` `./splunk disable boot-start`	`cd %SPLUNK_HOME%` `.\splunk disable boot-start`

2. Stop the forwarder.

Unix	Windows
`./splunk stop`	`.\splunk stop`

Uninstall the universal forwarder with your package management utilities

Use your local package management commands to uninstall the universal forwarder. Files that were not originally installed by the package will be retained. These include configuration and index files within the installation directory.

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

RedHat Linux

- Run the following command to uninstall the forwarder.

```
rpm -e splunk_product_name
```

Debian Linux

1. Run the following command to uninstall the forwarder.

```
dpkg -r splunkforwarder
```

2. (Optional) Run the following command to purge all universal forwarder files, including configuration files.

```
dpkg -P splunkforwarder
```

FreeBSD

1. Run the following command to uninstall the forwarder.

```
pkg_delete splunkforwarder
```

2. (Optional) Run the following command to uninstall the forwarder from a different location.

```
pkg_delete -p <location> splunkforwarder
```

Solaris

- Run the following command to uninstall the forwarder.

```
pkgrm splunkforwarder
```

Uninstall the universal forwarder on *nix systems manually

If you are not able to use package management commands, or you run HP-UX, use these instructions to uninstall the software manually.

1. Stop the forwarder.

   ```
   $SPLUNK_HOME/bin/splunk stop
   ```
2. Find any lingering processes that contain "splunk" in their name and use the `kill` to end them.

Linux and Solaris	FreeBSD and Mac OS X
`kill -9 `ps -ef | grep splunk | grep -v grep | awk '{print $2;}'``	`kill -9 `ps ax | grep splunk | grep -v grep | awk '{print $1;}'``

3. Remove the universal forwarder installation directory, `$SPLUNK_HOME`.

   ```
   rm -rf /opt/splunkforwarder
   ```
4. (Optional) On Mac OS X, use the Finder to remove the installation directory by dragging the folder into the Trash.
5. (Optional) Delete any `splunk` users and groups that you created, if they exist.

Linux, Solaris, and FreeBSD	Mac OS X
`userdel splunk` `groupdel splunk`	Use the **System Preferences > Accounts** control panel to manage users and groups.

Note: Where the service is configured to run on *nix under systemd, use the following commands:

```
systemctl stop splunkforwarder

systemctl disable splunkforwarder
```

Uninstall the Windows universal forwarder

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

1. Stop the `SplunkForwarder` service. You have several options:
   Use a PowerShell or command prompt to stop the forwarder.
   ```
   cd  %SPLUNK_HOME%\bin
   .\splunk stop
   ```

   Use a PowerShell or command prompt to stop the `SplunkForwarder` service.

   `NET STOP SplunkForwarder` Use the Services MMC snap-in (**Start > Administrative Tools > Services**) to stop the `SplunkForwarder` service.
2. Open the Control Panel and use the **Add or Remove Programs** application to start the uninstallation process. On Windows 7, 8, 10, Server 2008, and Server 2012, that option is available under **Programs and Features.**
3. Follow the installer prompts to remove the forwarder from the Windows host.

Uninstall the Windows universal forwarder from the command line

You can also use the Services MMC snap-in (**Start > Administrative Tools > Services**) to stop the `SplunkForwarder` service.

1. Use a PowerShell window or command prompt to stop the `SplunkForwarder` service.

   ```
   cd  %SPLUNK_HOME%\bin
   .\splunk stop
   ```
2. Run the Microsoft Installer to perform the uninstallation.
   ```
   msiexec /x splunkuniversalforwarder-<...>-x86-release.msi
   ```

The installer has one supported flag that you can use during uninstallation.

Flag	Description	Default
`REMOVE_FROM_GROUPS=1|0`	Specifies whether or not to take away rights and administrative group membership from the user you installed the forwarder as. This flag is available only when you uninstall the universal forwarder. If you set this flag to 1, the installer takes away group membership and elevated rights from the user you installed the forwarder as. If you set this flag to 0, the installer does not take away group membership and elevated rights from the user	1 (Take away elevated rights and group membership on uninstall.)

Forward data

Forward data with the logd input

logd input is a modular input that collects log data. Using the logd modular input, the forwarder pushes Unified Logging data to your Splunk platform deployment. logd input is supported on macOS 10.15, 11, or 12.

Before you begin

Before you run logd input for the first time, decide how much, if any, historical data you want to ingest on the first run. By default, the input ingests all available historical data stored by logd, which can be days, weeks, or even months of data. To limit this, use the logd-starttime configuration parameter described in this task to specify the earliest time for records to be read.

In order to read logd files, you must run Splunk with Admin privileges.

Best practices for configuring logd input

Here's a few best practices to keep in mind when configuring your logd input

- Start with a simple configuration before you build something more complex.
- For more information on configurations, see the spec file splunkforwarder/etc/apps/logd_input/README/inputs.conf.spec.

Define your stanzas

1. On your forwarder, navigate to `splunkforwarder/etc/apps/logd_input/default/`.
2. Copy the `inputs.conf` file.
3. Navigate to `splunkforwarder/etc/apps/logd_input/local/`.
4. Paste the copy of the `inputs.conf` file.
5. Open the `inputs.conf` file with a text editor.
6. Define the `logd` stanza by configuring data retrieval and data formatting parameters. For a full list of parameters, see the Parameters table. The number of stanzas determines the number of input instances that are run. For example, if you define five unique stanzas on a forwarder, the logd input returns five unique reports.
7. Save your changes.
8. Restart your forwarder.
9. (Optional) Use a deployment server to push the changes to your settings to other forwarders in your Splunk platform deployment. For more information, see Use forwarder management to manage apps topic in the *Updating Splunk Enterprise Instances* manual.

Reference: parameter definitions

The following table describes each parameter that you can set in your logd input stanza.

Parameter	Description
`logd-show = <string>`	Shows contents of the system log datastore.

Parameter	Description
`logd-backtrace = <string>`	Backtraces the system log datastore.
`logd-debug = <string>`	Debug logs for the system log datastore.
`logd-info = <string>`	Shows information about the system log datastore.
`logd-loss = <string>`	Shows data loss for the system log datastore.
`logd-signpost = <string>`	Shows data loss for the system log datastore.
`logd-predicate = <string>`	Filters messages using the provided predicate based on NSPredicate. Only a single predicate is supported..
`logd-process = <string>`	The process on which to operate. You can pass this option more than once to operate on multiple processes. This attribute is only supported for macOS 11, it is not supported for macOS 10.
`logd-source = <string>`	Include symbol names and source line numbers for messages, if available.
`logd-include-fields = <string>`	A comma-separated list of fields to include in a query.
`logd-exclude-fields = <string>`	A comma-separated list of fields to exclude from a query.
`logd-interval = <string>`	Query frequency interval in seconds.
`logd-starttime = <string>`	Date and time from when the first query should first pull data, in the format: "YYYY-MM-DD HH:mm:SS"

Configuration examples

Example of two logd inputs on one forwarder

```
[logd://bigsur]

logd-predicate = (subsystem == "com.apple.locationd.Position") && ((senderImagePath ENDSWITH "locationd")
OR (senderImagePath ENDSWITH "IOHDCPFamily"))
logd-backtrace = no
logd-debug = no
logd-info = true
logd-loss = no
logd-signpost = yes
logd-exclude-fields = bootUUID,formatString

[logd://bigsur_2]

logd-backtrace = no
logd-debug = yes
logd-info = no
logd-loss = yes
logd-signpost = false
logd-include-fields = bootUUID,formatString
```

Example of two universal forwarder instances with two stanzas on each instance

The example shows the same stanza in different universal forwarders.

- Instance one:

```
[logd://bigsur]

logd-info = true
logd-source = yes
logd-exclude-fields = bootUUID,formatString

[logd://bigsur_2]

logd-backtrace = no
logd-debug = yes
logd-include-fields = bootUUID,formatString
```

- Instance two:

```
[logd://catalina]

logd-predicate = category IN { "GeneralCLX", "calendarinterval" }
logd-backtrace = no
logd-debug = yes
logd-info = no
logd-loss = yes
logd-signpost = false
logd-source = yes


[logd://bigsur_2]

logd-backtrace = no
logd-debug = yes
logd-include-fields = bootUUID,formatString
```

Troubleshoot the logd input

Note that the input is subject to all forwarder data transformation and routing rules. For example, if the eventMessage field contains timestamps, by default the pipeline retrieves that timestamp and uses it instead of the timestamp you explicitly specified. To disable this behavior, see Tune timestamp recognition for better indexing performance.

I can't see my logd data

If you cannot see your data, try the following steps:

- Check to make sure that logd is enabled. By default logd is disabled. You must define a stanza to enable it.
- Make sure that the logd reading utility is running. Use the command: `ps aux | grep "log show"`.
- Verify that your parameters are correctly configured. To do this, run a shell command that runs the mod-input against a specific stanza so that you can see the output to stdout.

```
$SPLUNK_HOME/bin/splunk cmd splunkd print-modinput-config logd logd://z | $SPLUNK_HOME/bin/splunkd
logd-modinput
```

Timestamps are incorrect

The universal forwarder does not parse events before passing them on to the indexer, if you timestamps are incorrection, make sure the props.conf and transforms.conf settings are properly configured on your indexer. See the Managing Indexers and Clusters of Indexers manual for more information about configuring indexers.

The ingested data is not what I expected

If you do not see the data you expect, or you see data that you do not expect, check which switches were added for the journalctl utilities.

Run `ps aux | grep "log show"` and verify that the result is what you configured in the stanza.

Note that you may need to run this command more than once to capture the results while input instances are running, as this command executes only periodically and does not run continuously

I see data duplicates

If you have multiple stanzas running, make sure the stanza attributes do not overlap.

How the logd reader works

The settings you define in a logd stanza create filters for your data.

If you enable and configure without parameters, the logd input ingests the full content of the logd persistent storage, starting with the oldest entry. logd configuration supports both prescriptive and restrictive declaration of record definitions using "logd-include-fields" and "logd-exclude-fields" parameters. If one or more `FIELD=VALUE` match arguments are passed, the output is retrieved and formatted accordingly.

Once logd input runs, it starts saving (writing to disk) the timestamp of the last record sent into Splunk platform. This ensures data continuity when the forwarder is restarted.

1. When a forwarder starts, it looks for the checkpoint with a previously saved timestamp. The discovered checkpoint is the starting point for resumed data collection.

2. If a checkpoint is not located, the input uses the logd-starttime value instead.

3. If the input finds neither the checkpoint nor the logd-startime parameter, the input attempts to retrieve all available historical data from the persistent logd storage.

This feature does not support "log stream" ingestion mode.

Configure an intermediate forwarder

Intermediate forwarding is where a forwarder receives data from one or more forwarders and then sends that data on to another indexer. This kind of setup is useful when, for example, you have many hosts in different geographical regions and you want to send data from those forwarders to a central host in that region before forwarding the data to an indexer. All forwarder types can act as an intermediate forwarder.

Configure intermediate forwarding

Set up the intermediate forwarding tier

1. Install the forwarder on your intermediate host.
2. See Configure the forwarder to configure the intermediate forwarder to send data to a receiving indexer if you are using Splunk Enterprise. For Splunk Cloud, see Install and configure the Splunk Cloud Platform universal

forwarder credentials package to set up credentials.
    1. If you install the forwarder on Windows, you can specify the receiving indexer during the installation process.
3. Configure the intermediate forwarder to receive data. See Configure a receiver using a configuration file.
4. (Optional) Configure any local data inputs on the intermediate forwarder. See Configure local data inputs.
5. Restart the forwarder services.

You can repeat these steps to add more forwarders to the intermediate tier.

Configure forwarders to use the intermediate forwarding tier

1. Install the universal forwarder.
2. Configure the forwarder to send data to the intermediate forwarder. In this scenario, the intermediate forwarder acts as the receiver.
3. Configure local data inputs on the forwarder.
4. Restart the forwarder services.

Test the configuration

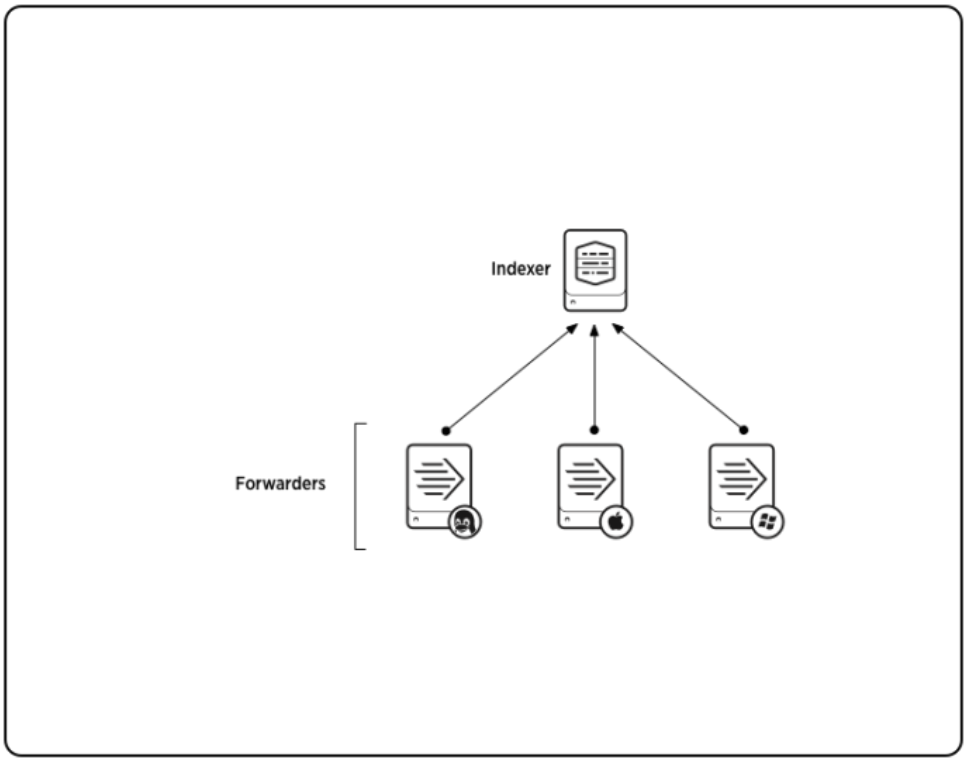
1. In Splunk Web, log into your Splunk deployment.
2. Open the Search and Reporting app.
3. Run a search that contains a reference to one of the hosts that you configured to send data to the intermediate forwarder

```
host=<name or ip address of forwarder> index=_internal
```

   If you do not see events, then the host has not been configured properly. See Troubleshoot the universal forwarder for possible fixes.

Consolidate data from multiple hosts

One of the most common forwarding use cases is to consolidate data that originates across numerous machines. Forwarders located on the machines send the data to a central Splunk deployment. This diagram illustrates a common scenario, where universal forwarders residing on machines running diverse operating systems send data to a single Splunk instance, which indexes and provides search capabilities across all the data.



The diagram illustrates a small deployment. In practice, the number of universal forwarders in a data consolidation use case could number into the thousands.

1. Determine the data and machines you need to access.

2. Install a Splunk instance on a host.

This instance functions as the **receiver**. Data goes there to be indexed and searched.

3. Using the CLI, enter this command from `$SPLUNK_HOME/bin/`:

```
./splunk enable listen <port> -auth <username>:<password>
```

- `<port>` is the network port you want the receiver to listen on.

4. Install universal forwarders on each machine that will generate data.

5. Configure inputs for each forwarder.

To learn what Splunk software can index and how to configure inputs, see What data can I index? in *Getting Data In*.

6. Configure each universal forwarder to send data to the receiver. For Windows forwarders, you can do this at installation time or through the CLI after installation. For *nix forwarders, you must do this through the CLI.

```
./splunk add forward-server <host>:<port> -auth <username>:<password>
```

- `<host>:<port>` are the host and receiver port number of the receiver. For example, `splunk_indexer.acme.com:9997`.

Alternatively, if you have many forwarders, you can use an `outputs.conf` file to specify the receiver. For example:

```
[tcpout:my_indexers]
server= splunk_indexer.acme.com:9997
```

You can create this file once and distribute copies of it to each forwarder.

How to forward data to Splunk Cloud Platform

To forward data to your Splunk Cloud Platform instance, you perform the following procedures:

1. Download and install the universal forwarder software.
2. Download the Splunk universal forwarder credentials package.
3. Install the Splunk universal forwarder credentials package on the universal forwarder machine. See Install and configure the Splunk Cloud Platform universal forwarder credentials package.
4. To manage forwarders using Splunk Web, configure the universal forwarder to act as a deployment client.
5. Configure inputs to collect data from the host that the universal forwarder is on. For an overview, see Configure the universal forwarder. For detailed examples of using the CLI to add inputs, see the individual data topics in *Getting Data In*.

For details on installing Splunk Cloud Platform, see the platform-specific installation instructions in the Splunk Cloud Platform *Admin Manual* for the type of data you want to forward.

- Get Windows Data into Splunk Cloud Platform
- Get *nix data into Splunk Cloud Platform
- Forward data from files and directories to Splunk Cloud Platform

Advanced configuration

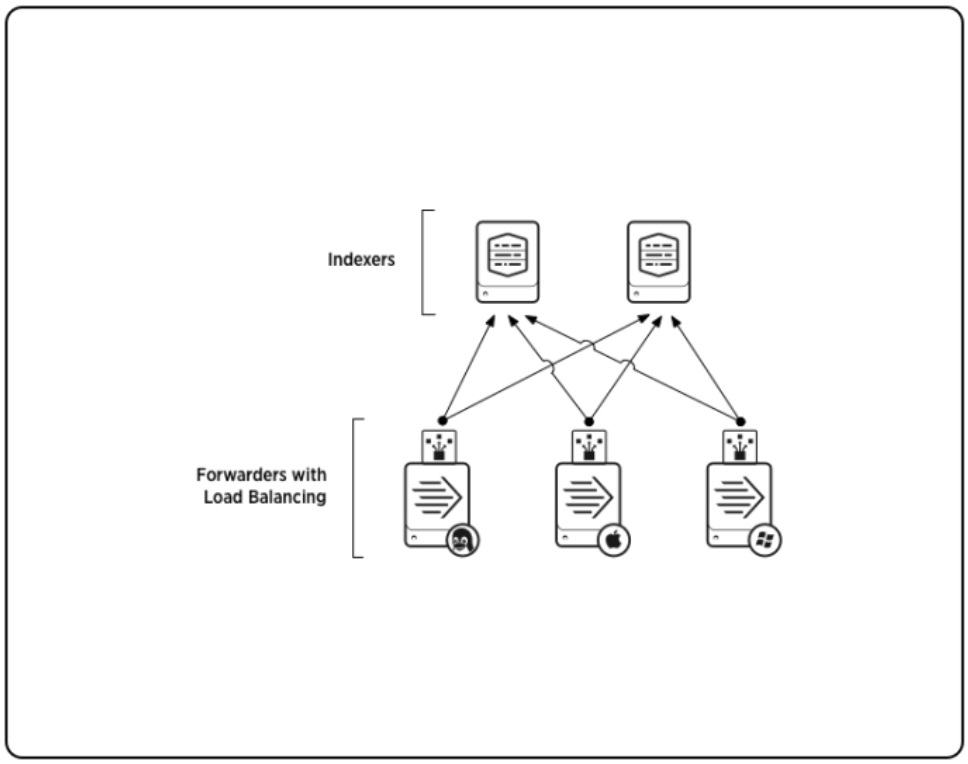
Advanced configurations for the universal forwarder

See the following Universal Forwarder advanced setup examples:

Load balancing

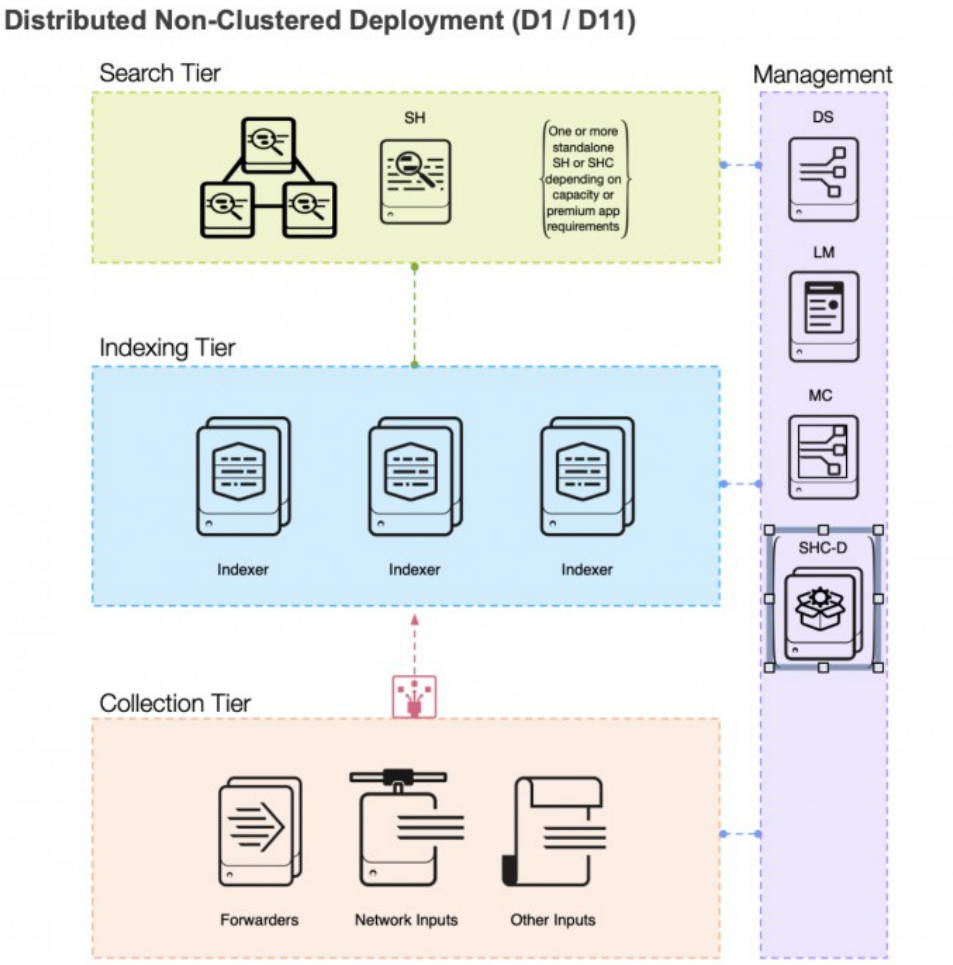
During **load balancing**, a forwarder distributes data across several receiving instances. Each receiver gets a portion of the total data, and together the receivers hold all the data. If a host goes down, the forwarder sends data to the next available receiver. Forwarders perform load balancing automatically. See Set up load balancing in the *Forwarding Data* manual.

The forwarder routes data to different indexers on a specified time or volume interval that you can specify. For example, if you have a load-balanced group that consists of indexer A, B, and C, at a specified interval, the forwarder switches the data stream to another indexer in the group at random. The forwarder might switch from indexer B to indexer A to indexer C, and so on. If one indexer is down, the forwarder immediately switches to another.



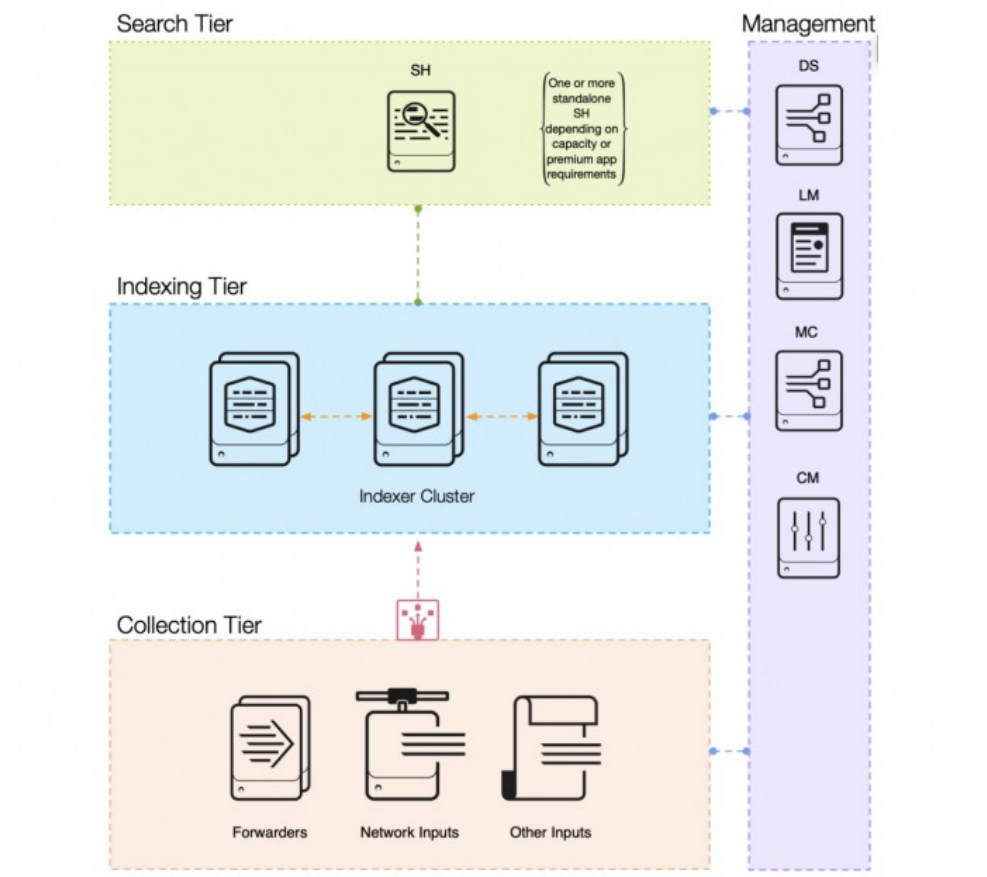
Distributed deployment

In a distributed deployment, the indexing logic and the data search logic are separated. It has both an indexer getting data from several inputs, and a search head, which searches across all the data found in this indexer. This is a great option if your daily data volume exceeds the capacity of a single-server deployment, or you want highly available data ingest. See Scale your deployment with Splunk Enterprise components in the *Distributed Deployment Manual*.



Distributed clustered deployment

This setup includes **Indexer clustering** with an appropriately configured data replication policy. In addition to being distributed, you combine multiple indexers to form an indexer cluster. This configuration keeps multiple copies of your data, increasing protection from data loss and availability of data. See Scale your deployment with Splunk Enterprise components in the *Distributed Deployment Manual*.



For more examples of advanced configurations, see https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf for detailed information on advanced Universal Forwarder setups.

Control forwarder access

You can configure Splunk Enterprise to allow communication from authorized forwarders through the use of tokens. A token is a unique key that is generated and enabled on the indexer, and configured on the forwarder. A forwarder attempting to send data to an indexer without the correct token value will be rejected. Forwarder access control is independent of Secure Sockets Layer (SSL,) and can be used in environments that do not have SSL enabled between Splunk platform instances.

Prerequisites to configuring forwarder access control

The token creation process requires command line access to the management port of the Splunk platform indexers and an administrative level Splunk Enterprise account to create and enable tokens. To access the REST API, use the `curl` command. There's no integrated support for `curl` on the Windows Operating System (OS.) You can use a Linux system to configure and manage tokens, or find a supported Windows OS tool.

Forwarder access controls are not available for Splunk Cloud.

Once a token is generated, it must be enabled on the Splunk platform indexers and configured in the outputs.conf on the forwarders that connect to the indexer. For forwarder configuration management options, see Best practices for deploying configuration updates across universal forwarders in the *Updating Splunk Enterprise Instances* manual.

Token management

The token is created on the receiver. The receiver can be a heavy forwarder, or an indexer.

Generate a token

Before you can configure token-based authentication, you must generate a token to use:

1. From a command or shell prompt, use the REST API to connect to a Splunk Enterprise indexer to create the token:

   ```
   curl -v -k -u <user>:<password>
   https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken -d "name=<token_name>"
   ```

   In this command:

- `user` and `password` are the administrative credentials you'll use to log into the Splunk platform indexer.
- `host` is the host name or IP address of the indexer.
- `management_port` is the TCP management port on the indexer (default: 8089.)
- `token_name` is the friendly name that you want to assign the token.

- The REST command response is returned to the command line and includes the token value. Copy the token value into a password management vault or other repository for later use in configuring the forwarders.
- The token must be enabled on the indexer before it can be used for forwarder authentication.

For example, to create a token named "my_token" on the host `idx1.mycompany.com` using the Splunk admin user and password:

```
curl -v -k -u admin:changeme https://idx1.mycompany.com:8089/services/data/inputs/tcp/splunktcptoken -d
"name=my_token"
```

The REST response includes the token value:

```
<s:key name = "token">808F7BD7-1444-4910-B8F5-87B83D694E18</s:key>
```

Enable a token

A token can be enabled using the REST API, or by modifying the inputs.conf of the receiving indexer.

To use the REST API to enable a token, from a command or shell prompt, run:

```
curl -v -k  -X "POST" -u <user>:<password>
https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken/<token_name>/enable
```

Optionally, use the inputs.conf to enable a token:

1. Edit `inputs.conf` on the indexer and add the stanza:

   ```
   [splunktcptoken://<token_name>]
   disabled = 0
   token = <token_value>
   ```
2. Restart Splunk Enterprise services.

Disable a token

To disable a token using the REST API, use the following command:

```
curl -v -k  -X "POST" -u <username>:<password>
https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken/<token_name>/disable
```

Delete a token

To remove a token using the REST API, use the following command:

```
curl -v -k -X "DELETE" -u <username>:<password>
https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken/<token_name>
```

List tokens

To receive a list of configured tokens using the REST API, use the following command:

```
curl -v -k -u <user>:<password> https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken
```

Configure the forwarder with a token

Add the token value to the forwarder's outputs.conf under the `[tcpout]` stanza to configure authentication with an indexer.

1. Edit the outputs.conf for the forwarder and add the `token` value under the `[tcpout]` stanza:

   ```
   [tcpout]
   ```

```
server=idx1.mycompany.com:9997
token = <token_value>
...
```

2. Restart the forwarder services.

Confirm that the forwarder and indexer can communicate using the tokens

When you configure a forwarder with a token, the communication process with the indexer becomes:

- The forwarder connects to the indexer.
- The indexer requests authentication.
- The forwarder provides the token to the indexer.
- The indexer compares the token it received with the token it has.
- If the tokens match, the indexer accepts the TCP connection and sets up the data stream. If the tokens do not match, the indexer rejects the connection and logs an entry in the `splunkd.log`.

A forwarder without the correct token value for an indexer cannot forward data to that indexer.

Common error messages

A forwarder that does not have the correct token generates this event in `splunkd.log`:

```
ERROR TcpInputProc - Exception: Token sent by forwarder does not match configured tokens
src=127.0.0.1:58798! for data received from src=127.0.0.1:58798
```

A forwarder that does not submit a token to an indexer with a token enabled generates this event in `splunkd.log`:

```
ERROR TcpInputProc - Invalid S2S token=Token not sent by forwarder for data received from
src=127.0.0.1:58796
```

Troubleshoot the universal forwarder

Troubleshoot the universal forwarder

See common Splunk Universal Forwarder errors and how to fix them. For more troubleshooting information, see https://community.splunk.com/t5/Community/ct-p/en-us/.

Warning appears in the universal forwarder when you run an SPL command

When you run an SPL command in the universal forwarder, the following messages may appear:

- Warning: Attempting to revert the SPLUNK_HOME ownership
- Warning: Executing "chown -R splunk /opt/splunkforwarder".

These warning do not affect functionality and can be ignored.

Splunk isn't receiving data from the universal forwarder

1. In the indexer user interface, go to **forwarding and receiving**, or go to inputs.conf.
2. Identify or select a port in **Received Data** to listen to. Make sure it is the same port set in outputs.conf for the forwarder to send data to. See Configure the universal forwarder using configuration files. Usually, the port 9997 splunktcp is preferred.
3. Check that the destination host for your indexers, including the IP address and hostname, is correct in outputs.conf.
4. After configuring your change, restart your Universal Forwarder. See Start or stop the Universal Forwarder.

Splunk is only receiving "\x00\" data

1. Go to your indexer user interface.
2. Ensure you are receiving data from **Forwarding and receiving** in indexer settings, and not **Data inputs -> TCP/UDP**.

Ingestion lagging

The most common cause of ingestion lagging is that you are taking in too much data from one sourcetype, which is blocking data from other sourcetypes. You can solve this by shortening your data ingestion intervals using the universal forwarder user interface, or inputs.conf.

Release Notes

Known issues

This topic lists known issues that are specific to the universal forwarder. For information on fixed issues, see Fixed issues.

Universal forwarder issues

Date filed	Issue number	Description
2022-10-27	SPL-232147	Debian package failed to start on armv8 agent `re-pkg-arm64` Workaround: Make the following changes to /etc/systemd/system/SplunkForwarder.service - modify all ExecStartPost= with ExecStartPost=- allowing it to fail if the directory is not found. For instance change, ExecStartPost=/bin/bash to ExecStartPost=-/bin/bash

2022-07-30	SPL-227653, SPL-231927	UF throws erroneous WARN for KVSTORE SSL misconfiguration on startup - server.conf//sslVerifyServerCert or "Starting migrate-kvstore."
		
		Workaround:
		It's safe to ignore the warning or you can disable the kvstore explicitly with server.conf:
		`[kvstore]`
		`disabled = true`

2022-06-23	SPL-226019	Warning appears in the universal forwarder whenever any spl command is run: Warning: Attempting to revert the SPLUNK_HOME ownership Warning: Executing "chown -R splunk /opt/splunkforwarder". This warning is expected and will not affect functionality.
2022-06-06	SPL-225379	Ownership of files mentioned in manifest file is splunk:splunk instead of root:root after enabling boot start as root user for initd Workaround: whenever changing UF user, pls manually chown SPLUNK_HOME to the new user, including first time install/upgrade, or manually enable boot-start
2022-05-16	SPL-224264, SPL-224265	Splunk UF not starting on Debian 11 (x86_64 and arm64)
2022-05-13	SPL-224167	Splunk UF for CentOS-7 (ARM64) is not available Workaround: UF for CentOS7 ARM 64 will be available in the 9.0.1 maintenance release.
2020-11-09	SPL-197140	UF failed to start on Solaris 11.3 with error: "symbol in6addr_any: referenced symbol not found" Workaround: 1. Do not upgrade past Splunk 8.0.5 on Solaris 11.3 OR 2. Upgrade to Solaris 11.4

Date filed	Issue number	Description

Fixed issues

The following issues were fixed in releases of the universal forwarder.

9.0.2

Version 9.0.2 was released on November 2, 2022. It delivers relevant fixes described in the November 2, 2022 quarterly security update on the Splunk Product Security page. This release also fixes the following universal forwarder issues:

Universal forwarder issues

Date resolved	Issue number	Description
2022-09-21	SPL-222917, SPL-230428	Crash in indexer discovery service on search head
2022-09-09	SPL-229853, SPL-229208	PowerShell Modular input stopped working after UF 9.0 upgrade

9.0.1

Version 9.0.1 was released on August 16, 2022. It delivers relevant fixes described in the August 16, 2022 quarterly security patch on the Splunk Product Security page.

9.0.0.1

Version 9.0.0.1 was released on July 20, 2022. This release introduces no changes to universal forwarder functionality. This release is provided only for version parity with Splunk Enterprise 9.0.0.1, which fixes the one issue described in Splunk Enterprise 9.0.0.1 fixed issues.

9.0.0

Version 9.0.0 was released on June 14, 2022. This release fixes no new universal forwarder issues.

Third-party software

Some of the components included in the universal forwarder are licensed under free or open source licenses. We wish to thank the contributors to those projects. See the Splunk Enterprise third-party software notices.

Plan your universal forwarder deployment

Compatibility between forwarders and Splunk Enterprise indexers

The following table shows which versions of forwarder and indexer are compatible. A best practice is to use indexers with versions that are the same or higher than forwarder versions.

Determine forwarder-indexer compatibility

The following are the supported forwarder versions for Splunk Enterprise. This information is applicable to universal and heavy forwarders that are communicating directly to indexers and cluster peers, and includes forwarders deployed in an intermediate forwarding tier. If the forwarder version you want to use is not in this table, then there is no support for it. See Product Supported Version Timelines on splunk.com and Splunk Support Programs. As a best practice, forwarders should communicate with indexers that are the same or higher version.

This table applies to Splunk Enterprise only. Splunk Cloud Platform forwarder compatibility information is provided in Supported Forwarder Versions in the *Splunk Cloud Platform Service Description* manual.

- **E - Events**. This version of forwarder can send event data to the corresponding version of indexer.
- **H - HTTPOUT**. This version of forwarder can send event data from Splunk instance to Splunk instance (S2S) over Hypertext Transfer Protocol Secure (HTTPS).
- **M - Metrics**. This version of forwarder can send both event data and metrics data to the corresponding version of indexer.
- **S - SSL change required**. This version of forwarder can send event data to this version of indexer only if you change the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) version and cipher suite on the forwarder.
- An empty cell indicates that Splunk does not support sending any type of data from this version of forwarder to the corresponding version of indexer.

Forwarder version	Splunk Enterprise indexer version		
	8.1.x	8.2.x	9.0.x
7.x (P3 support only)	E, M	E, M	E, M
8.0.x (P3 support only)	E, M	E, M	E, M
8.1.x	E, M	E, H, M	E, H, M
8.2.x	E, M	E, H, M	E, H, M
9.0.x	E, M	E, H, M	E, H, M

For app-specific compatibility restrictions, see the app documentation on Splunkbase.