Configure the universal forwarder

Before a forwarder can forward data, it must have a configuration. A configuration:

- Tells the forwarder what data to send.
- Tells it where to send the data.

Because the universal forwarder does not have Splunk Web, you must give the forwarder a configuration either during the installation (on Windows systems only) or later, as a separate step. To perform post-installation configuration, you can:

- Use the **CLI**. The CLI lets you do nearly all configuration in a small number of steps, but does not give you full access to the feature set of the forwarder.
- Create or modify configuration files on the forwarder directly.
- Use a deployment server. The deployment server can ease distribution of configurations, but does not make a forwarder forward data by itself. You must use the deployment server to deliver configurations to the forwarders so that they collect the data you want and send it to the place you want.

About configuring the universal forwarder with configuration files

Configuration files are text files that the universal forwarder reads when it starts up or when you reload a configuration. Forwarders must read configuration files to know where to get and send data. These files give you full access to the forwarder feature set, but editing configuration files can be difficult or mistake-prone at times. See "About configuration files" and "Configuration file precedence" in the Splunk Enterprise *Admin* manual, for details on how configuration files work.

Key configuration files are:

- 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.

You make changes to configuration files by editing them with a text editor. You can use any editor that you want as long as it can write files in ASCII/UTF-8 format.

The forwarder works with configurations for forwarding data in `outputs.conf` in `$SPLUNK_HOME/etc/system/local/`). See Configure forwarding with outputs.conf.

> The universal forwarder has a SplunkUniversalForwarder app, which includes preconfigured settings that let the forwarder run in a streamlined mode. Do not edit any configuration files within that app unless you receive specific instructions.

Best practices for deploying configuration updates across universal forwarders

You can use the following methods to deploy configuration updates across your set of universal forwarders:

- Edit or copy the configuration files for each universal forwarder manually (This is only useful for small deployments.)
- Use the Splunk **deployment server** to push configured apps to your set of universal forwarders.

- Use your own deployment tools (puppet or Chef on *nix or System Center Configuration Manager on Windows) to push configuration changes.

Configure the universal forwarder from the CLI

The CLI lets you configure most forwarding parameters without having to edit configuration files. It does not give you full access to all forwarding parameters, and you must edit configuration files in those cases.

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/`). See Configure forwarding with outputs.conf, for information on `outputs.conf`.

Examples for using the CLI to configure a universal forwarder

Following are example procedures on how to configure a universal forwarder to connect to a receiving indexer.

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.

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
```

Uninstall the universal forwarder

Prerequisites to uninstalling 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
`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.

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.)

Start the universal forwarder

After you install the universal forwarder, you must start it before it can forward data. If you make changes to the forwarder configuration using either files or the CLI, you must start (or restart) the forwarder in most cases.

Commands for starting the universal forwarder

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

Run the following commands to start the universal forwarder at any time. If this is the first time the forwarder has started, and you have not included parameters to avoid prompts or automatically accept the license agreement, the forwarder performs the following:

- Prompts you to accept the license agreement. You must read and accept it to continue.
- Prompts you to create an administrator password. The password you create must meet eligibility requirements.

- 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`

- 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`

- 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`

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.

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*.

To learn how to start or restart the universal forwarder, see Start the universal forwarder.

- Run the following commands to stop the universal forwarder.

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