Splunk® Universal Forwarder Forwarder Manual 8.0.4

Generated: 6/23/2020 8:42 am

Table of Contents

Table of Contents

Introducing the universal forwarder

The universal forwarder

About the universal forwarder

The **universal forwarder** collects data from a data source or another forwarder and sends it to a forwarder or a Splunk deployment. With a universal forwarder, you can send data to Splunk Enterprise, Splunk Light, or Splunk Cloud. It also replaces the Splunk Enterprise light forwarder. The universal forwarder is available as a separate installation package.

The universal forwarder offers advantages over using a **heavy** or **light forwarder**. The most notable benefit is that it uses significantly fewer hardware resources than other Splunk software products. It can, for example, coexist on a host that runs a Splunk Enterprise instance. It also is more scalable than the other Splunk products, as you can install thousands of universal forwarders with little impact on network and host performance.

Another benefit is its availability for installation on many diverse computing platforms and architectures. You can install it on more platforms than you can Splunk Enterprise.

The universal forwarder includes only the essential components that it needs to forward data to other Splunk platform instances. While it does not have a Web interface, you can still configure, manage, and scale it by editing configuration files or by using the Forwarder Management or Monitoring Console interfaces in Splunk Web.

This manual discusses the universal forwarder

This manual discusses the universal forwarder and how to plan, download, install, and configure it. There are two other types of forwarders. To learn about heavy and light forwarders and how they forward data, see About forwarding and receiving data in the *Forwarding Data Manual*.

To achieve higher performance and a lighter resource footprint, the universal forwarder has a subset of the functionality provided by a full Splunk platform deployment, specifically:

- Cannot search or index data.
- Cannot send alerts.
- Does not **parse** incoming data, except in certain cases, such as structured data or some forms of Windows data.
- Cannot send data to `syslog` servers as it has no syslog pipeline.
- Does not include a version of Python.

How the universal forwarder compares to the light forwarder

The **light forwarder** is a full Splunk Enterprise instance with certain features that have been disabled to achieve a smaller resource footprint. The universal forwarder differs from the light forwarder in the following ways:

- It puts less load on the host CPU, uses less memory, and has a smaller disk space footprint.
- It cannot be converted to function as a heavy forwarder or other Splunk Enterprise role.
- It does not have Splunk Web, which means that you cannot perform any configuration with that user interface.

The light forwarder was deprecated in Splunk Enterprise version 6.0, which means that support for it can be removed in a future version of Splunk Enterprise. When you install the universal forwarder, you can migrate from an existing light forwarder that runs version 4.0 or later. See Migrate a Windows light forwarder or Migrate a *nix light forwarder for details.

Information on Windows third-party binaries that ship with the universal forwarder

For information on third-party Windows binaries provided with the Windows version of the universal forwarder, see Information on Windows third-party binaries distributed with Splunk Enterprise in the Splunk Enterprise *Installation Manual*.

For information about running the universal forwarder in Windows Safe Mode, see Splunk Enterprise Architecture and Processes also in the *Installation* Manual.

About forwarding and receiving data

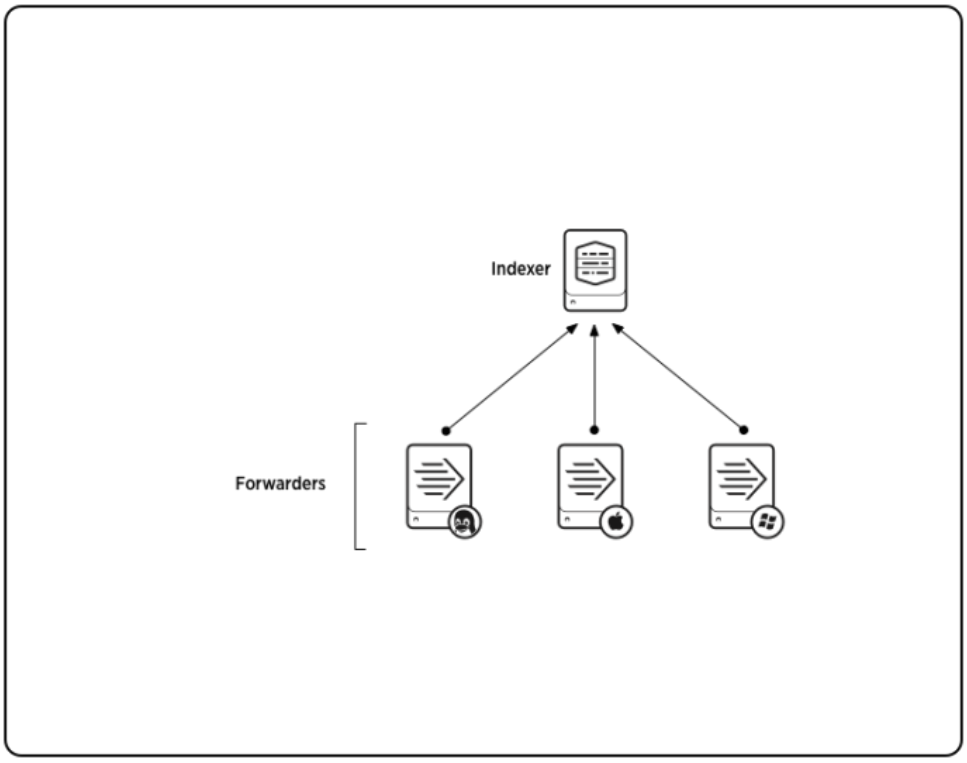
You can forward data to Splunk Enterprise, Splunk Light, and Splunk Cloud deployments as well as to systems that don't run the Splunk platform.

A Splunk instance that **receives** data from one or more forwarders is called a **receiver**. The receiver is usually a Splunk **indexer**, but can also be another forwarder.

The *Forwarding Data Manual* has more information about forwarding and receiving data with heavy and light forwarders.

Sample forwarding layout

This diagram shows three universal forwarders sending data to a single receiver (an indexer), which then indexes the data and makes it available for searching. This layout is basic, but you can define many forwarding combinations based on your specific environment and network topology.



Forwarders represent a much more robust solution for data forwarding than raw network feeds, with their capabilities for:

- Tagging of metadata (source, source type, and host)
- Configurable buffering
- Data compression
- SSL security
- Use of any available network ports

Use the universal forwarder to perform functions like **data consolidation** and **load balancing**.

Plan your universal forwarder deployment

Universal forwarder system requirements

The system requirements for a universal forwarder are different than those for a heavy or light forwarder. To learn about system requirements for heavy and light forwarders, see System requirements in the Splunk Enterprise *Installation Manual*.

Platform and hardware requirements

For details about the platforms where you can install the universal forwarder, see Supported Operating Systems in the Splunk Enterprise *Installation Manual*.

The hardware requirements for universal forwarders appear in the following table:

Recommended	Dual-core 1.5GHz+ processor, 1GB+ RAM
Minimum	1.0Ghz processor, 512MB RAM, 5GB of free disk space

Licensing requirements

The universal forwarder ships with its own license. See Types of Splunk software licenses in the *Admin Manual* for details.

Other requirements

Sun SPARC systems

Before you 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`). The universal forwarder needs this version of the library to run on Solaris for SPARC architecture.

User rights

To perform the installation of the universal forwarder, you must have administrator or equivalent rights.

To use the forwarder, you do not need elevated privileges, but the user that the forwarder runs as must have read access to the resources that you want to monitor and forward.

Forwarders and Splunk Enterprise indexer clusters

When you use forwarders to send data to peer nodes in a Splunk Enterprise indexer cluster, there are installation requirements that diverge from the specifications shown in this topic. To learn more about forwarders and clusters, see Use forwarders to get data into the indexer in *Managing Indexers and Clusters of Indexers*.

Splunk Enterprise/universal forwarder version compatibility

Many versions of universal forwarder and indexer are compatible with one another. See Compatibility between forwarders and indexers in the *Forwarding Data Manual* for details on the versions of forwarder that work with a specific version of indexer.

Example forwarder deployment topologies

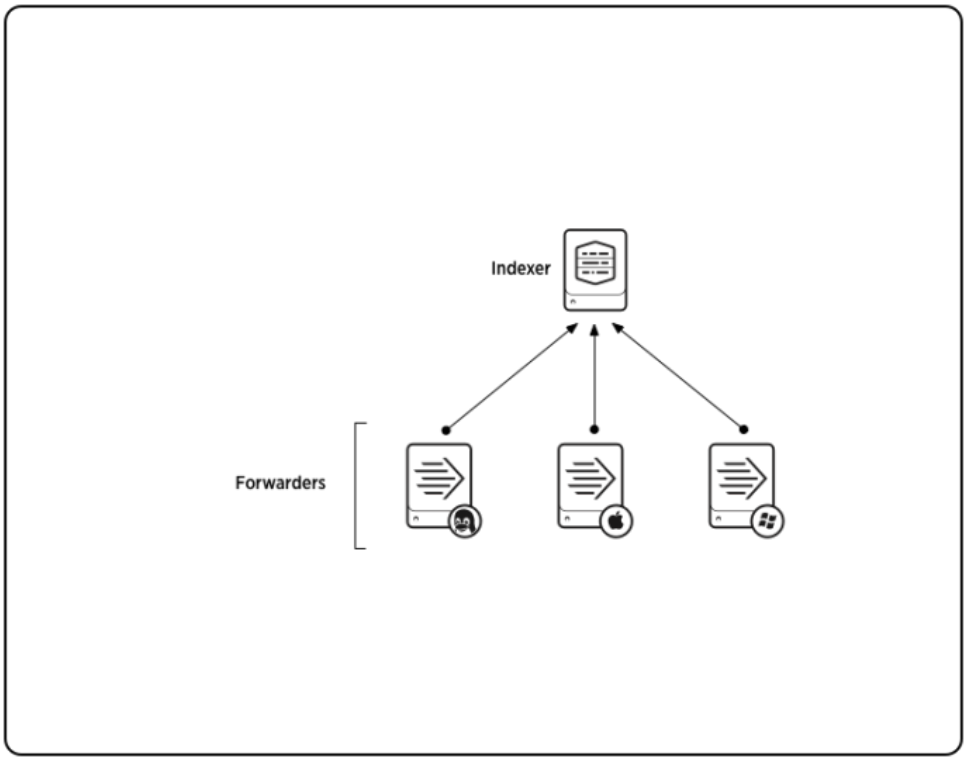
You can deploy universal forwarders in a wide variety of scenarios. This topic provides an overview of some of the most useful types of topologies that you can create with universal forwarders.

Data consolidation topology

Data consolidation is one of the most common topologies, with multiple forwarders sending data to a single Splunk deployment. The scenario involves universal forwarders that send unparsed data from hosts to a central Splunk deployment for consolidation and indexing.

For more information on data consolidation, see Consolidate data from multiple hosts.

In the following diagram, three universal forwarders send data to a single indexer:

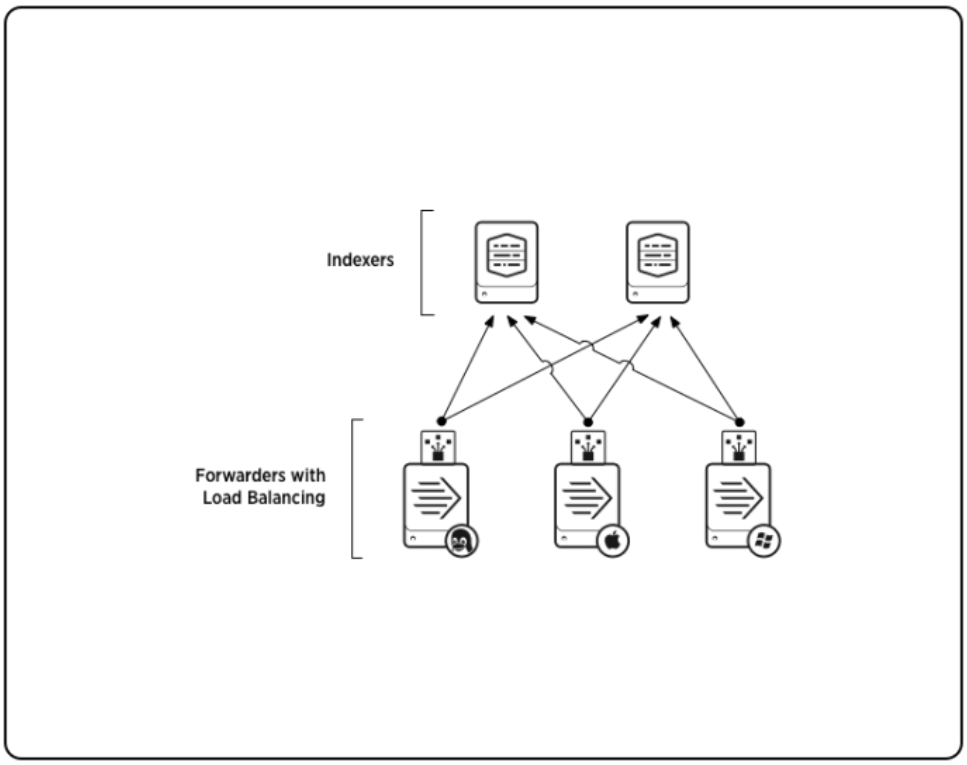


Load balancing topology for Splunk Enterprise

Load balancing simplifies the process of distributing data across several indexers to handle considerations such as high data volume, horizontal scaling for enhanced search performance, and fault tolerance. In load balancing, the forwarder routes data sequentially to different indexers at specified intervals.

For more information on how to configure load balancing, see Configure load balancing.

In the following diagram, three universal forwarders are each performing load balancing between two indexers:

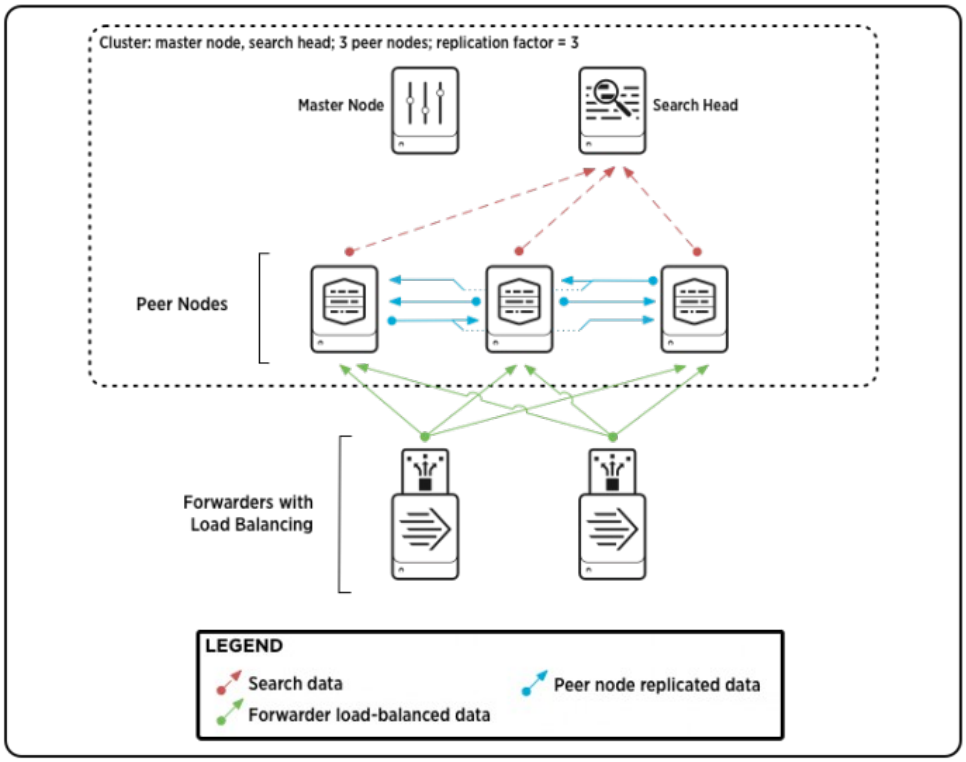


Forwarders and indexer clusters for Splunk Enterprise

You can use universal forwarders to send data to peer nodes in an indexer cluster. It is recommended that you use forwarders in a load-balanced configuration for that purpose.

To learn more about universal forwarders and indexer clusters, see Use forwarders to get your data in *Managing Indexers and Clusters of Indexers*. To learn more about indexer clusters in general, see About indexer clusters and index replication, also in that manual.

This diagram shows two load-balanced forwarders sending data to a Splunk Enterprise indexer cluster:



Intermediate forwarding

To handle some advanced use cases, you might want to insert an intermediate forwarder between a group of forwarders and the indexer. Universal forwarders can also act as intermediate forwarders.

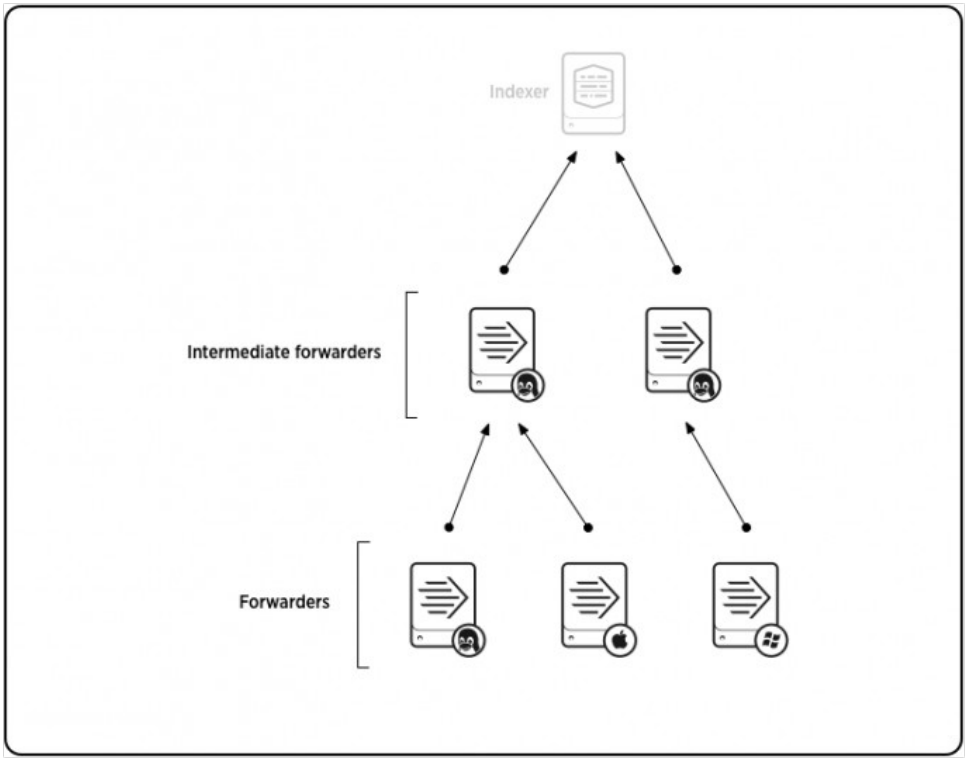
In this type of scenario, the originating forwarders send data to a consolidating forwarder, which then forwards the data on to an indexer, usually after indexing it locally. This forwarder can also route and filter data, if it is a heavy forwarder.

Typical use cases are situations where you want to reduce or limit network bandwidth usage on specific network segments (for example, if you have multiple data centers around the world and want to limit bandwidth in a certain region) or if you have some need to limit access to the indexer machine; for instance, for security reasons.

You can also use intermediate forwarding when you need an intermediate index (either for "store-and-forward" requirements or to enable localized searching) but this requires a heavy forwarder.

To enable intermediate forwarding, see Configure an intermediate forwarder.

The following diagram shows a simple intermediate forwarding layout:



Minimize open ports for Splunk Cloud

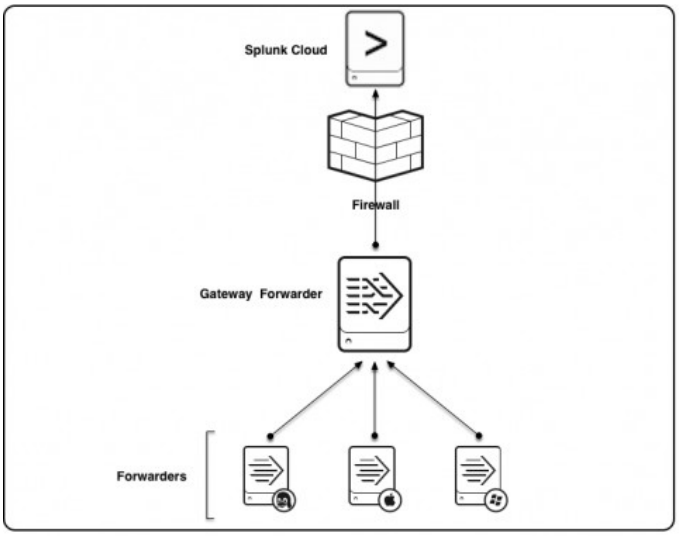
For security, you can minimize the number of open firewall ports required to send data from your network to Splunk Cloud by configuring a **gateway forwarder**. In this approach, all your forwarders send data to a single gateway forwarder, which then sends data to Splunk Cloud. This approach also simplifies the administration of certificates and provides a single location where apps are installed.

You can also use a gateway forwarder to configure a single point for anonymizing data that is exiting your corporate environment. Configure a **heavy forwarder** as the gateway forwarder and specify the transforms required to hide sensitive information. For details about anonymizing data, see Anonymize Data in the Splunk Enterprise *Getting Data In* manual. If you do not need to anonymize or transform outbound data, configure a universal forwarder as your gateway forwarder.

To configure a universal forwarder instance as a gateway forwarder, perform the following steps.

1. On the gateway forwarder, run the following command to enable listening: `/opt/splunkforwarder/bin/splunk enable listen <port> -auth <username>:<password>`
2. Restart the gateway forwarder.
3. To configure another forwarder to send data to the gateway forwarder, run the following command: `/opt/splunkforwarder/bin/splunk add forward-server <host name or ip address>:<listening port>`
4. Restart the forwarder.

The following figure shows a basic gateway forwarder configuration that opens a single firewall port to direct data from three internal forwarders to Splunk Cloud.



Routing and filtering

Universal forwarders cannot route, filter, or transform data because they do not have the frameworks necessary to perform those actions. However, you can configure a universal forwarder to send data to an intermediate forwarding tier that consists of heavy forwarders, which can route data based on criteria such as source, source type, or patterns in the events themselves.

For more information on routing and filtering, see Route and filter data in the Splunk Enterprise *Forwarding Data Manual*.

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 table shows the versions of forwarder and indexer that can be used together. As a best practice, forwarders should communicate with indexers that are the same or higher version. 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.

If you are looking for the Splunk Cloud forwarder compatibility list, see Supported Forwarder Versions in the *Splunk Cloud Service Description* manual.

- **E - Events**. This version of forwarder can send event data to the corresponding version of indexer.
- **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	Indexer version	
	7.0.x-7.3.x	8.x
6.0.x-6.2.x (Unsupported)	E, S	
6.3.x-6.6.x (Limited support)	E	
7.x	E, M	E, M
8.x	E	E, M

The table provides version 6.x compatibility for universal forwarders only. Version 6.x forwarders are compatible with higher versions of indexer, but Splunk will not provide support for version 6.0.x - 6.2.x forwarders. Version 6.3.x - 6.6.x universal forwarders have limited support through June 4, 2021.

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

Forward data to Splunk Light

How to forward data to Splunk Light

To forward data to your Splunk Light on-premises instance, you perform the following procedures.

1. Configure Splunk Light to receive data from the universal forwarder.
2. Download and install the universal forwarder software.
3. Configure the universal forwarder to send data to the Splunk Light instance.
4. 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 details, see the platform-specific installation instructions in the Splunk Light "Getting Started Manual" for the operating system from which you want to forward data.

- Forward data to Splunk Light from Microsoft Windows
- Forward data to Splunk Light from Linux
- Forward data to Splunk Light from Mac OS X

How to forward data to Splunk Light Cloud

To forward data to your Splunk Light cloud service 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.
4. 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 details, see the platform-specific installation instructions in the *Splunk Light Cloud Service* manual for the operating system from which you want to forward data.

- Forward data to Splunk Light cloud service from Microsoft Windows
- Forward data to Splunk Light cloud service from Linux
- Forward data to Splunk Light cloud service from Mac OS X

Forward data to Splunk Cloud

How to forward data to Splunk Cloud

To forward data to your Splunk Cloud 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 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, see the platform-specific installation instructions in the Splunk Cloud *User Manual* for the type of data you want to forward.

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

Install and configure the Splunk Cloud universal forwarder credentials package

To enable your forwarders to send data to Splunk Cloud, download the universal forwarder credentials file. This file contains a custom certificate for your Splunk Cloud deployment.

Download the forwarder credentials

1. In your Splunk Cloud deployment, navigate to the Splunk Cloud Home page.
2. Click **Universal Forwarder**.
3. On the Splunk Cloud Home page, click **Download Universal Forwarder Credentials** to download the `splunkclouduf.spl` file.
4. When prompted, click **Save File** and click **OK**. By default, the `splunkclouduf.spl` file downloads to the `Downloads` directory. If you download to a different location, make note of that location.

Install the file onto your forwarders using one of the two installation options described in this topic. Apply these credentials to forwarders of any type that you need to connect to your Splunk Cloud instance.

Install the forwarder credentials on individual forwarders

1. Move the `splunkclouduf.spl` file to the `$SPLUNK_HOME/etc/apps/` directory of your forwarder.
2. Open a command prompt window and run the following command `tar xvf splunkclouduf.spl`.
3. Navigate to the `/bin` subdirectory of your deployment server.
4. In the command prompt window, run 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 forwarder.
5. Restart your forwarder: `/splunk restart`.

Install the forwarder credentials on a deployment server

1. Move the `splunkclouduf.spl` file to the `$SPLUNK_HOME/etc/deployment-apps/` directory of your deployment server.
2. Open a command prompt window, and run the command `tar xvf splunkclouduf.spl`.
3. Navigate to the `/bin` subdirectory of your deployment server.
4. In the command prompt window, run the 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 universal forwarder.
5. Restart your deployment server: `/splunk restart`.

Forward data to Splunk Enterprise

How to forward data to Splunk Enterprise

The most common way to use the universal forwarder is to send data to a Splunk Enterprise indexer or indexer cluster.

You can also forward data to Splunk Enterprise from heavy and light forwarders. See Enable forwarding on a Splunk Enterprise instance in the Splunk Enterprise *Forwarding Data Manual* for details.

1. Configure receiving on a Splunk Enterprise instance or cluster.
2. Download and install the universal forwarder.
3. Start the universal forwarder and accept the license agreement. Some installers do this for you.
4. (Optional) Change the credentials on the universal forwarder from their defaults.
5. Configure the universal forwarder to send data to the Splunk Enterprise instance.
6. (Optional) Configure the universal forwarder to act as a deployment client.
7. Configure the universal forwarder to collect data from the host it is on.

After you set up forwarding, you can perform these advanced, optional steps for increased security and data reliability.

- Configure the forwarder to send data between multiple indexers. See Configure load balancing.
- Configure a forwarder to send data to an indexer that is behind a proxy server. See Configure a forwarder to use a SOCKS proxy.
- Configure an intermediate forwarding tier, where forwarders send data to other forwarders that then send data to receiving indexers. See Configure an intermediate forwarder.
- Configure an indexer to acknowledge data that it has received before it accepts more. See Protect against the loss of in-flight data.
- Control how forwarders access indexers with tokens. See Control forwarder access.

Configure receiving on Splunk Enterprise

You must configure a Splunk Enterprise indexer to receive data before you can send data to it. If you do not do this, data does not go anywhere.

See Enable a receiver to configure a Splunk Enterprise indexer to receive data.

Download and install the universal forwarder

If you have not downloaded the universal forwarder, do so now.

You must select the correct type of forwarder for your operating system. Splunk provides a universal forwarder for many operating systems. See the following topics for specific installation instructions:

- Install a nix universal forwarder for installation on *nix operating systems.
- Install a Windows universal forwarder from an installer for installation on various Windows operating systems.

Start the universal forwarder

Before the universal forwarder can accept configurations and forward data, it must be started.

The Windows and Mac OS X universal forwarder installation packages let you view and accept the license agreement and start the universal forwarder automatically. For other installation packages, you must start the universal forwarder and accept the license agreement from the command line.

See Start the universal forwarder to learn how to start the universal forwarder, whether it is the first time or after you have made configuration changes.

Configure the universal forwarder to send data to the Splunk Enterprise indexer

Before the universal forwarder can send data to Splunk Enterprise, you must configure it with the Splunk Command Line Interface (CLI).

This procedure details a basic configuration. For additional configuration options, see Configure the universal forwarder.

1. From a command or shell prompt on the universal forwarder, go to the `$SPLUNK_HOME/bin` directory.

Unix	Windows
`cd $SPLUNK_HOME/bin`	`cd %SPLUNK_HOME%\bin`

2. Specify the host name or ip address of the Splunk Enterprise receiver.

Unix	Windows
`./splunk add forward-server <host>:<port>`	`.\splunk add forward-server <host>:<port>`

   The `host` is the name or IP address of the Splunk Enterprise host that should receive the data.
   The `port` is the TCP port that you configured in Enable a receiver in this manual.
   The instance confirms your credentials before adding the forwarding host.

   Example:

```
./splunk add forward-server splunkaday-linux:9997
Added forwarding to: splunkaday-linux:9997.
```

Configure the universal forwarder as a deployment client

When you configure the universal forwarder as a deployment client, you can control configuration of the universal forwarder from a central place. You can use Splunk Web to configure things such as what configurations a forwarder gets, what add-ons it receives, and what data it collects.

Before you can deploy configurations to a universal forwarder with a deployment server, you must configure it to connect to the deployment server. Every Splunk Enterprise indexer can be a deployment server, and the deployment server automatically activates when a universal forwarder connects to the indexer management port. The forwarder then becomes a **deployment client**.

1. From a command or shell prompt on the universal forwarder, go to the `$SPLUNK_HOME/bin` directory.

Unix	Windows
`cd $SPLUNK_HOME/bin`	`cd %SPLUNK_HOME%\bin`

2. Specify the host name or IP address of the deployment server.

Unix	Windows
`./splunk set deploy-poll <host>:<port>`	`.\splunk set deploy-poll <host>:<port>`

`host` is the name or IP address of the deployment server.
`port` is the management port of the deployment server. It defaults to `8089`.

Configure the universal forwarder to send data to Splunk Enterprise

You can collect data on the universal forwarder using several methods.

Define inputs on the universal forwarder with the CLI

You can use the CLI to define inputs on the universal forwarder. After you define the inputs, the universal forwarder collects data based on those definitions as long as it has access to the data that you want to monitor.

For example, to define a Windows event log input on a Windows version of the universal forwarder:

```
.\splunk enable eventlog System
```

To define a file monitor input against the /var/log/messages file on a *nix host:

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

For more examples of using the CLI to add inputs, see the data ingestion topics in the Splunk Enterprise *Getting Data In* manual.

Define inputs on the universal forwarder with configuration files

If the input you want to configure does not have a CLI argument for it, you can configure inputs with configuration files.

1. Using a command or shell prompt, navigate to the universal forwarder configuration directory.

Unix	Windows
`cd $SPLUNK_HOME/etc/system/local`	`cd %SPLUNK_HOME%\etc\system\local`

2. Create an inputs.conf file in this directory.
3. Edit the file by adding stanzas to `inputs.conf`.
   For example, to add the Windows Security, Application, and System event logs to a monitoring stanza on the universal forwarder.

```
# Windows platform specific input processor.
[WinEventLog://Application]
disabled = 0

[WinEventLog://Security]
disabled = 0

[WinEventLog://System]
disabled = 0
```

   To monitor Apache log files:

```
[monitor:///apache/*.log]
disabled = 0
```

For more examples of using configuration files to define inputs, see Monitor files and directories with inputs.conf in *Getting Data In*.

Install an add-on into the universal forwarder

1. Stop the universal forwarder.

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

2. Download the add-on from Splunkbase, if you have not already.
3. Install the add-on into the universal forwarder.

Unix	Windows
`tar xvzf /path/to/add-on.tgz -C $SPLUNK_HOME/etc/apps`	No Windows equivalent of `tar`, use WinZip or another archive utility to unarchive the application into the %SPLUNK_HOME%\etc\apps folder

4. (Optional) Configure the add-on on the forwarder by editing configuration files or running scripts included with the add-on.
5. Restart the universal forwarder.

Enable a receiver

The receiver is a Splunk software instance that is configured to listen on a specific port for incoming communications from a forwarder. The receiver is typically an indexer, but can be another forwarder if you are using intermediate forwarding. An intermediate forwarder must be configured for both receiving and forwarding.

Updating configurations directly on Splunk software instances is only appropriate for single-instance deployments. To manage Splunk Enterprise configurations at scale, see About deployment server and forwarder management in the *Updating Splunk Enterprise Instances* manual.

Configure a receiver using Splunk Web

Use Splunk Web to configure a receiver for splunk-to-splunk (S2S) communication:

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 on indexers is port `9997`.
5. 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 for S2S communication:

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 an `inputs.conf` file for S2S communication:

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 the universal forwarder software

Before you install a universal forwarder, you must get the correct version for your operating system. You can download the universal forwarder for Windows and different versions of *nix.

To find out which operating systems the universal forwarder supports, see the system requirements page in the Installation manual. Then proceed to the universal forwarder download page and download the correct forwarder for your operating system and application.

After you download the forwarder installation package, follow the installation topic that matches your installation requirements most closely. During or immediately after the installation, you also perform configuration. Each installation topic contains one or more use cases that cover specific scenarios from installation through configuration and deployment.

Install the universal forwarder on Windows

You have several options for installing the universal forwarder on Windows. Choose the one that best fits your application.

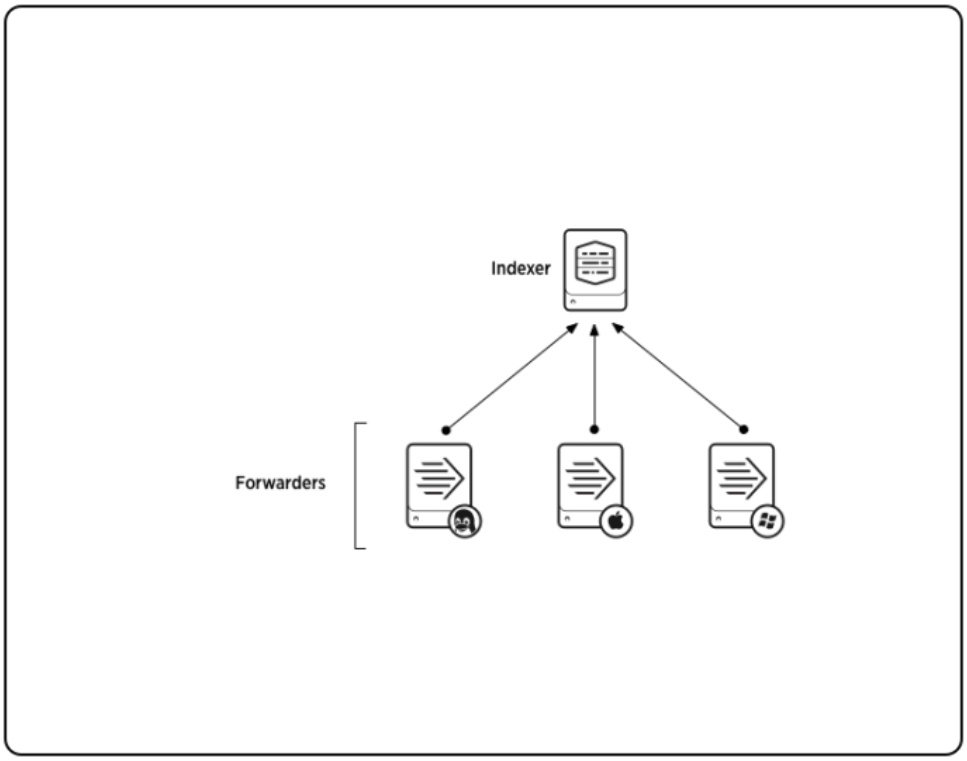
- Install a Windows universal forwarder from an installer. This is the most common method, where you use a MSI package to install the software.
- Install a Windows universal forwarder from the command line. This method lets you perform more configuration than the installer method.
- Install a Windows universal forwarder remotely with a static configuration. Use this method if you want to install the universal forwarder on a system image that you can clone to multiple hosts.

Install the universal forwarder on *nix

- Install a *nix universal forwarder. This is the most common method, where you use a tar file or other package to install on a *nix host.
- Install a *nix universal forwarder remotely with a static configuration. Use this method when you want to install the universal forwarder on a system image that you can clone to multiple hosts.

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.

Install the universal forwarder software

Install a Windows universal forwarder from an installer

You can install the universal forwarder on a Windows host with the Windows universal forwarder installer package. This method of installation is best for the following:

- Small deployments.
- Proof-of-concept test deployments.
- System images or virtual machines for eventual cloning.

You can install the universal forwarder in other ways as well.

- You can install from the command line, using the `msiexec` installer. The command-line installation provides more configuration options for data inputs and other settings. Install from the command line if you do not want the forwarder to run immediately after installation. See Install a Windows universal forwarder from the command line.
- You can install from a ZIP file. This method of installation has some limitations. See Install a Windows universal forwarder from a ZIP file.

Prerequisites to installing the universal forwarder on Windows

Before you install the Windows universal forwarder, read the following prerequisites.

Determine if you will forward data to Splunk Enterprise or to Splunk Cloud

Installation procedures differ depending on the destination Splunk platform. See the following topics for installation instructions:

- Install the universal forwarder for use with on-premises Splunk instances. This method is the most common and following the procedures results in an installation that works with an on-premises instance of Splunk Enterprise.
- Install the universal forwarder for use with Splunk Cloud. Use this method if you want to connect the forwarder to a Splunk Cloud deployment.

Choose the Windows user that the universal forwarder should run as

When you install the universal forwarder, you can select the Windows user that the forwarder uses to get data. You have two choices.

- **Local System**. If you specify the **Local System** user during the installation process, the universal forwarder collects any kind of data that is available on the local host. It cannot collect data from other hosts.

- **Domain account**. This option installs the forwarder as the Windows user you specify. The forwarder has the permissions that have been assigned to that user, and collects data that the user has read access to. It does not collect data from resources that the Windows user does not have access to. If you need to collect data from those resources, you must give the Windows user access to those resources.

Install the forwarder as a **Domain account** to do any of the following:

- Read Event Logs remotely

- Collect performance counters remotely
- Read network shares for log files
- Access the Active Directory schema, using Active Directory monitoring

Choose and configure the user that the universal forwarder should run as before installing the forwarder for remote Windows data collection. If you do not, installation can fail.

If you install as a domain user, specify a user that has access to the data you want to monitor. See Choose the Windows user Splunk should run as in the Splunk Enterprise *Installation Manual* for concepts and procedures on the user requirements that must be in place before you collect remote Windows data.

If you install as a domain user, you can choose whether or not the user has administrative privileges on the local machine. If you choose not to give the user administrative privileges, the universal forwarder enables "low-privilege" mode. See Install the universal forwarder in low-privilege mode.

Configure your Windows environment for remote data collection

If your monitoring needs require that you install the universal forwarder to collect remote Windows data, then configure your Windows environment for the proper installation of the forwarder.

The configuration process includes adding or editing Active Directory security groups and granting the Windows universal forwarder user access to those groups. It can also include creating and updating Group Policy Objects (GPOs) to provide further security and access for the user.

For step-by-step instructions on how to modify your Windows network, domain, or Active Directory forest, see Prepare your Windows network for a Splunk Enterprise installation as a network or domain user in the Splunk Enterprise *Installation Manual.*

1. Create and configure security groups with the user you want the universal forwarder to run as.
2. (Optional) Configure the universal forwarder account as a managed service account.
3. Create and configure Group Policy objects (GPOs) for security policy and user rights assignment.
4. Assign appropriate user rights to the GPO.
5. Deploy the GPOs with the updated settings to the appropriate objects.

Have credentials for the Splunk administrator user ready

When you install the universal forwarder, you must create credentials for the Splunk administrator user. The installer does not create credentials for the user. Think of a username and password and be ready to supply them when you perform the installation. If you do not supply at least a password during a silent installation, the universal forwarder can install without any users defined, which prevents login. You must then create a user-seed.conf file to fix the problem and restart the forwarder.

Install the universal forwarder for use with on-premises Splunk Enterprise instances

The Windows universal forwarder installer installs and configures the universal forwarder to send data to an on-premises Splunk Enterprise instance. It offers you the option of migrating your checkpoint settings from an existing forwarder.

Do not install or run the 32-bit version of the Splunk universal forwarder for Windows on a 64-bit Windows system or an unsupported version of Windows. Do not install the universal forwarder over an existing installation of full Splunk Enterprise.

Universal forwarder installation options

When you install the universal forwarder on Windows, you can install with the default settings or customize installation options prior to installing.

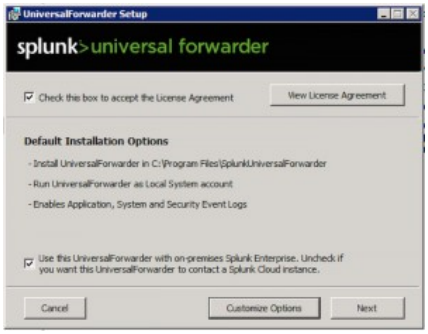
If you choose not to customize options, the installer does the following:

- Installs the universal forwarder in `\Program Files\SplunkUniversalForwarder` on the system drive (the drive that booted your Windows host.)
- Installs the universal forwarder with the default management port of TCP/8089.
- Configures the universal forwarder to run as the Local System user.
- Prompts you to create a Splunk administrator password. You must complete this step before installation can continue.
- Enables the Application, System, and Security Windows Event Log data inputs.

To understand the ramifications of the Windows user that the universal forwarder runs as, see Choose the user Splunk Enterprise should run as in the *Installation Manual*.

Install the forwarder with the default options

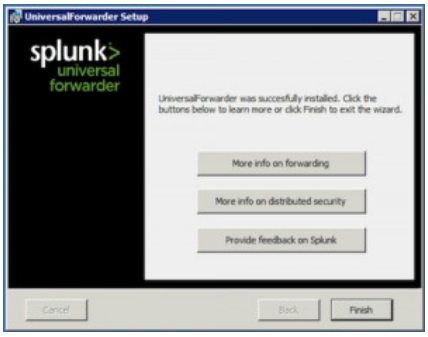
1. Download the universal forwarder from splunk.com.
2. Double-click the MSI file to start the installation.
3. (Optional) To view the license agreement, click the "View License Agreement" button.



4. Select the **Check this box to accept the License Agreement** check box.
5. To change any of the default installation settings, click the "Customize Options" button and see Customize options. Otherwise, click **Install** to install the software with the defaults.

   Perform at least one of the following two steps, or the universal forwarder cannot send data anywhere.

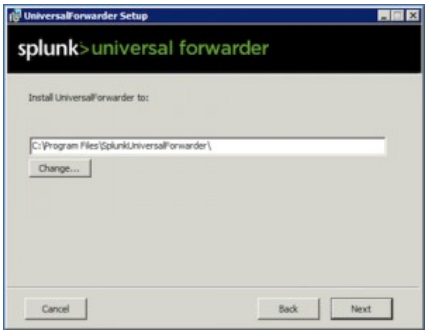
6. (Optional) In the **Deployment Server** pane, enter a host name or IP address and management port for the deployment server that you want the universal forwarder to connect to and click **Next**.
7. (Optional) In the **Receiving Indexer** pane, enter a host name or IP address and the receiving port for the receiving indexer that you want the universal forwarder to send data to and click **Next**.
8. Click **Install** to proceed. The installer runs and displays the **Installation Completed** dialog. The universal forwarder starts automatically.



9. From the Control Panel, confirm that the `SplunkForwarder` service runs.

Customize Options

If you chose "Customize options" in the **Universal forwarder setup** dialog box, the installer presents you with the following options.



The installer puts the universal forwarder into the `C:\Program Files\SplunkUniversalForwarder` directory by default.

1. (Optional) Click **Change** to specify a different installation directory.

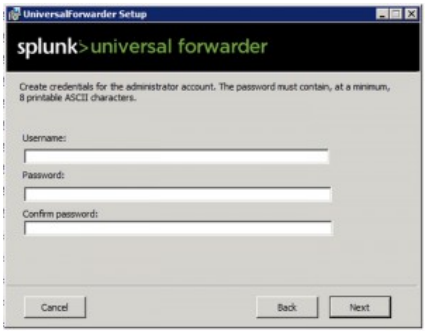
2. (Optional) Select an SSL certificate to verify the identity of this machine. Depending on your certificate requirements, you might need to specify a password and a Root Certificate Authority (CA) certificate to verify the identity of the certificate. If not, these fields can be left blank.

3. Select the **Local System** or **Domain Account** check box and click **Next**. If you specify **Local System**, the installer displays the **Enable Windows Inputs** dialog box. If you specify **Domain account**, the installer displays a second dialog box where you enter domain and user information.

4. If you selected "Domain account", the installer displays a dialog box for user name and password credentials. Enter the user name and password into the **User name** and **Password** fields. Specify the user name in `domain\username` format only, or the installation can fail.
5. Enter the password again in the **Confirm password** field.
6. To add the domain user you specified to the local Administrators group, select the "Add user as local administrator" check box and click **Next**. The installer adds the domain user you specified to the local Administrators group. If you do not select the "Add user as local administrator" check box, the universal forwarder installs in "low-privilege" mode. See "Run the universal forwarder in low-privilege mode" later in this topic for additional information and caveats.

7. (Optional) Select one or more Windows inputs from the list and click **Next**.

   You can enable inputs later, by editing `inputs.conf` within the universal forwarder directory. See "Considerations for enabling data inputs in the installer" later in this topic about what happens when you enable inputs in this dialog.



8. Create credentials for the Splunk administrator user, then click **Next**.

   You must complete this action, as installation of the universal forwarder cannot proceed without it. If you do not specify a username, the universal forwarder installer creates the `admin` user during the installation process.

9. (Optional) Enter the hostname or IP address and management port for your deployment server and click **Next**.

   Perform at least one of the next two steps. While both are optional, the forwarder does nothing if you perform neither step because it does not have a configuration.

10. (Optional) Enter the hostname or IP address and **receiving port** of the receiving indexer (receiver) and click **Next**.
11. Click **Install** to proceed with the installation.

Install the universal forwarder for use with Splunk Cloud

An installation of the universal forwarder for Splunk Cloud is similar to an installation for on-premises versions of Splunk Enterprise.

1. Download the universal forwarder from splunk.com.
2. Double-click the MSI file to start the installation:
3. Check the **Check this box to accept the License Agreement** checkbox.
4. Uncheck the **Use this UniversalForwarder with on-premises Splunk Enterprise...** checkbox.
5. To change any of the default installation settings, click the **Customize Options** button and proceed to the Customize options for a cloud install procedure. Otherwise, click **Next**.

   Note: Perform at least one of the following two steps, or the universal forwarder cannot send data anywhere.

6. (Optional) 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**.
7. (Optional) 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**.
8. Click **Install**. The installer runs and displays the **Installation Completed** dialog. The universal forwarder automatically starts.

Customize options for a Splunk Cloud installation

Follow these instructions if you need to perform a detailed configuration of the universal forwarder for use with Splunk Cloud.

1. (Optional) In the **Destination Folder** dialog box, click **Change** to specify a different installation directory.
2. In the **Certificate Information** dialog box, click **Next.** Do not specify any parameters.
3. Specify whether you want the universal forwarder to run as the Local System user or a domain user and click **Next**. If you specified **Local System**, the installer skips the second screen and takes you directly to the "Enable Windows Inputs" dialog box.
4. If you specified **Domain account**, the installer displays a second dialog box, where you enter domain and user information. Enter the user name and password into the **User name** and **Password** fields. Specify the user name in `domain\username` format, or the installation can fail.
5. Enter the password again in the **Confirm password** field.
6. To add the domain user you specified to the local Administrators group, select the "Add user as local administrator" check box and click **Next**. The installer adds the domain user you specified to the local Administrators group. If you do not select the "Add user as local administrator" check box, the universal forwarder installs in "low-privilege" mode. See "Run the universal forwarder in low-privilege mode" later in this topic for additional information and caveats.
7. (Optional) Select one or more Windows inputs from the list and click **Next**.
8. If you have an on-premises deployment server and you want to use it, fill in the appropriate information and click **Next.** Otherwise, do not specify any parameters here.
9. Click **Next.** Do not specify any parameters here.
10. Click **Install** to proceed with the installation. The installer runs and displays the **Installation Completed** dialog box. The universal forwarder automatically starts.
11. From Windows Control Panel, confirm that the `SplunkForwarder` service runs.

Install the universal forwarder in "low-privilege" mode

When you specify a domain user during an installation and do not give that user local administrator rights, the forwarder installs and runs in "low-privilege" mode.

There are some caveats to doing this:

- 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.

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. To install the software with a GUI installer, see Install a Windows universal forwarder with the installer.

When to install from the command line?

Here are some scenarios where installing from the command line is useful:

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

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

Prerequisites for installing the universal forwarder on Windows

Choose the Windows user the universal forwarder should run as

When you install the universal forwarder, you can select the user it should run as. By default, the forwarder installs as the Local System user. To specify a domain account to run the forwarder as, specify the `LOGON_USERNAME` and `LOGON_PASSWORD` flags in the installation command.

You can also install the forwarder as a user who is not an administrator on the local machine. Use the `SET_ADMIN_USER` installation flag to install the forwarder in "low privilege" mode.

If you install the forwarder as the Local System user, the forwarder can collect any kind of data that is available on the local machine. It cannot collect data from other machines. This is by design.

You must give the universal forwarder a user account if you intend to do any of the following:

- Read Event Logs remotely
- Collect performance counters remotely

- Read network shares for log files
- Enumerate the Active Directory schema, using Active Directory monitoring

See Choose the Windows user Splunk should run as in the Splunk Enterprise *Installation Manual* for concepts and procedures on the user requirements for collecting remote Windows data.

Configure your Windows environment prior to installation

The following steps are high-level. For step-by-step instructions, see Prepare your Windows network for a Splunk Enterprise installation as a network or domain user in the Splunk Enterprise *Installation Manual*.

1. Create a security group for the user that you want to run the universal forwarder as.
2. Add the user you want the universal forwarder to run as to this group.
3. (Optional) Set up the universal forwarder user as a managed service account.
4. Use the Group Policy Management Console to create and configure Group Policy or Local Security Policy objects for user rights assignments.
5. Use the Group Policy Management Console to assign appropriate security rights to the universal forwarder user.
6. If you use Active Directory, deploy the Group Policy objects with the updated settings.

Have credentials for the Splunk admin user ready

When you install the universal forwarder, you must create credentials for the Splunk administrator user. The installer does not create credentials for the user. Think of a user name and password and be ready to supply them when you perform the installation. If you do not supply at least a password during a silent installation, the universal forwarder can install without any users defined, which prevents login. You must then create a user-seed.conf file to fix the problem and restart the forwarder.

See Create secure administrator credentials in *Securing Splunk* for more information on how to create credentials for the Splunk administrator account.

Install the universal forwarder

You can install the forwarder with flags to prevent the installer from asking some questions, or you can specify the `/quiet` argument and set the `AGREETOLICENSE` flag for a completely silent installation.

For examples on how to install the universal forwarder from the command line, see "Examples" below.

Install the universal forwarder with installation flags

This method of installation acts like the method that is explained in Install the Windows universal forwarder from an installer, but does not ask some questions during the installation process, depending on the installation flags that you specify.

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>]
   ```
3. 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.

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 `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. 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.

Supported command line 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	n/a

Flag	Purpose	Default
	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.	
`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:	n/a

Flag	Purpose	Default
	`cpu memory network diskspace`	
`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/a

`CLONEPREP=1|0`	Delete 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|0`	Specify 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/A
`SPLUNKPASSWORD=<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	N/A

Flag	Purpose	Default
	the universal forwarder installs without a user. and you must create one by editing the `user-seed.conf` configuration file.	
`MINPASSWORDLEN=<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.	`> 1`
`MINPASSWORDDIGITLEN=<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.	`0`
`MINPASSWORDLOWERCASELEN=<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.	`0`
`MINPASSWORDUPPERCASELEN=<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.	`0`
`MINPASSWORDSPECIALCHARLEN=<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	`0`

Flag	Purpose	Default
	password you change must meet the new requirements after you set this flag.	
`GENRANDOMPASSWORD=1|0`	Generate 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.	0

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
```

Install a Windows universal forwarder from a ZIP file

You can install the universal forwarder from a ZIP file that Splunk provides. To install with a GUI interface, see Install a Windows universal forwarder from an installer. To install with the installer from the command line, see Install a Windows universal forwarder from the command line.

When to install from a ZIP file

This installation method is useful when you want to do the following:

- Install more than one universal forwarder on a Windows machine

Limitations to installing the universal forwarder on Windows from a ZIP file

There are several caveats that exist to installing the Windows universal forwarder from a ZIP file.

- Splunk supports this method of installation on specific versions of Windows Server only. See the prerequisites later in this topic for the supported versions. It is not available on other versions of Windows Server, or on workstation-class versions of Windows (such as 7, 8, 8.1, or 10.)
- These instructions apply only to versions 6.5.0 and later of the universal forwarder ZIP file. They do not apply to ZIP files for earlier versions that might appear on the download page.
- The ZIP file is not publicly available. You must contact Support to get the file.
- The process of both installation and uninstallation is almost completely manual. For example, you must place the files in the installation directory, register driver files, edit configuration files, and start and stop services manually. Also, you cannot uninstall the program through the Control Panel.
- You must create the Splunk `admin` account prior to starting the forwarder.
- You cannot cross-grade an installation of a ZIP file with an MSI file, or vice versa. You must use an updated ZIP file to upgrade.
- You must install the forwarder with a user that is a local administrator on the installation machine.
- If you install the forwarder to run as a user other than the Local System user, that user must also be a local administrator.
- You cannot enable "low privilege" mode with this installation method.
- Only one forwarder on a machine can monitor any of the network monitor, Registry monitor, or MonitorNoHandle inputs at a time. This means that, for example, if you have two forwarders on a machine and one monitors the Registry, the other cannot.
    - If you install three forwarders on a machine, each can monitor one of these inputs simultaneously, as long as not more than one does.

Prerequisites to installing the universal forwarder on Windows

Before you install the Windows universal forwarder from a ZIP file, confirm that you have all of the following:

- An account with administrative privileges on the Windows machine that you want to install the forwarder.
- A Windows universal forwarder ZIP file.
- A Windows machine that runs 64-bit Windows Server 2008 R2 or Server 2012 R2.

Get the ZIP file from Splunk Support

The Windows universal forwarder ZIP file is not available for download on the Splunk website. To get the file, you must contact your Support representative who can provide a download link.

Choose the Windows user that the universal forwarder should run as

After you install the universal forwarder, you can configure it to run as the Local System user or as another Windows user that you specify by editing the user in the Services control panel.

The **Local System** user lets the universal forwarder collect any kind of data that is available on the local machine. It cannot collect data from other machines.

A **Domain account** lets the forwarder run as the Windows user you specify. The forwarder has the permissions that have been assigned to that user, and collects data from resources across the domain or forest that the user has read access to. It does not collect data from resources that the Windows user does not have access to. If you need to collect data from those resources, you must give the Windows user access to those resources.

Install the forwarder as a **Domain account** to do any of the following:

- Read Event Logs remotely
- Collect performance counters remotely
- Read network shares for log files
- Access the Active Directory schema, using Active Directory monitoring

You must determine and configure the user that the universal forwarder should run as before installing the forwarder for remote Windows data collection.

If you install as a domain user, specify a user that has access to the data you want to monitor. See Choose the Windows user Splunk should run as in the Splunk Enterprise *Installation Manual* for concepts and procedures on the user requirements that must be in place before you collect remote Windows data.

Configure your Windows environment for remote data collection

If your monitoring needs require that you install the universal forwarder to collect remote Windows data, then configure your Windows environment for the proper installation of the forwarder.

The configuration process includes adding or editing Active Directory security groups and granting the Windows universal forwarder user access to those groups. It can also include creating and updating Group Policy Objects (GPOs) to provide further security and access for the user.

For step-by-step instructions on how to modify your Windows network, domain, or Active Directory forest, see Prepare your Windows network for a Splunk Enterprise installation as a network or domain user in the Splunk Enterprise *Installation Manual*.

1. Create and configure security groups with the user you want the universal forwarder to run as.
2. (Optional) Configure the universal forwarder account as a managed service account.
3. Create and configure Group Policy objects (GPOs) for security policy and user rights assignment.
4. Assign appropriate user rights to the GPO.
5. Deploy the GPOs with the updated settings to the appropriate objects.

Install the universal forwarder

This procedure assumes that no other forwarder has been installed on the Windows machine. If there are other forwarders that are present, see "Install additional forwarders" later in this topic.

Begin installing the forwarder

1. Contact your Splunk Support representative to get the universal forward ZIP download link.
2. Download the link to the machine that is to run the forwarder.
3. Unpack the archive to a directory of your choosing.
4. Open a PowerShell window or command prompt.
5. Change to the `bin` directory where you unpacked the universal forwarder ZIP file.

Register Splunk monitoring input drivers

This part of the procedure is only required if you want to use the Registry monitor, the Network monitor, or the `MonitorNoHandle` file monitoring input. These inputs have separate drivers that must be registered before they can be used with the universal forwarder instance. If you do not want to use these inputs, then proceed to the next section.

If you need to register Splunk monitoring drivers, confirm that you specify the commands exactly as shown. Errors in command syntax can severely damage your Windows installation. If you do not feel comfortable with the driver registration steps in this procedure, then install the universal forwarder with the installer.

- (Optional) Register the Splunk monitoring drivers that you need for the universal forwarder. The command line is as follows.

  ```
  rundll32 SETUPAPI.dll,InstallHinfSection DefaultInstall 132 <full path to driver .inf file>
  ```
  In this command, `<full path to driver .inf file>` is the path to the .inf file for the Splunk monitoring driver that you want to register. You must always specify the full path to confirm that the utility operates on the correct file.

  There are several drivers that are available for registering:

  - `Splunkdrv.inf`, which handles the Registry Monitor input driver.
  - `Splknetdrv.inf` which handles the Network Monitor input driver.
  - `SplunkMonitorNoHandleDrv.inf`, which handles the `MonitorNoHandle` driver.

  All of these drivers are in the `%SPLUNK_HOME%\bin` directory.
- (Optional) If you receive an error message that says "`Installation failed.`", then confirm that you have specified the correct path to the file and try the operation again.

Create the Splunk "admin" account and password with user-seed.conf

Before starting the forwarder for the first time, you must create the Splunk `admin` account by editing `user-seed.conf`. If you do not, the universal forwarder starts with no defined users, which means you cannot log into it and make changes.

See Create a secure administrator password in *Securing Splunk* for more information on how to create a secure password for the admin account.

1. Open a PowerShell window or command prompt, if one is not already open.
2. In the directory where you unpacked the universal forwarder files, change to the `/etc/system/local` directory. For example, if you unpacked the files to `C:\Program Files\UF`, change to the `C:\Program Files\UF\etc\system\local` directory.
3. Use a text editor like Notepad to create a file `user-seed.conf` for editing.

4. In this file, add the following block of text:

```
[user_info]
USERNAME = admin
PASSWORD = <new password>
```

5. Substitute `<new password>` with a password of your choosing. The password must meet eligibility requirements (currently, it must be at least 8 characters in length.)
6. Save the `user-seed.conf` file and close it.

Complete the universal forwarder installation

1. Enable the universal forwarder to start at boot time.

   ```
   .\splunk enable boot-start
   ```
   The universal forwarder responds with the following.

   ```
   This appears to be your first time running this version of Splunk.
   Installing service SplunkForwarder
   Service installed
   Windows services installed.
   Windows services are configured to run at boot.
   ```
2. (Optional) If you want the forwarder to run as a different user, complete the procedure shown in Correct the user selected during Windows installation in the *Installation Manual*.
3. Start the universal forwarder.

   ```
   .\splunk start
   ```

Install additional forwarders

After you have installed the first forwarder, you can install additional forwarders by changing the service name for the new instances.

Any forwarders that you previously installed on the machine should be running when you perform this installation. This forces the forwarder that you are installing to prompt you to choose a different network management port when it starts. Each universal forwarder must use its own network management port.

If a forwarder that is already on the system uses a monitoring input that requires a driver, then this instance cannot monitor the same type of input. For example, if a forwarder already monitors the Registry, then subsequent instances cannot monitor the Registry. This is the same for the Network monitoring or `MonitorNoHandle` inputs.

Begin the universal forwarder installation

1. Confirm that any existing universal forwarders on the machine are running.
2. Contact your Splunk Support representative to get the universal forward ZIP download link.
3. Download the link to the machine that is to run the forwarder.
4. Unpack the archive to the installation directory.

   If you already have a universal forwarder installed on the machine, do not unpack the ZIP file into the same directory.
5. Open a PowerShell window.
6. Change to the `etc` directory where you unpacked the universal forwarder ZIP file.
7. (Optional) Register any Splunk monitoring input drivers that you need for this installation, as specified in "Register Splunk monitoring input drivers" earlier in this topic.

Change name of universal forwarder services in splunk-launch.conf

1. Use Notepad or another text editor to edit the `splunk-launch.conf` file.
2. In the `splunk-launch.conf` file, change the `SPLUNK_SERVER_NAME` and `SPLUNK_WEB_NAME` values to a new name that does not conflict with the existing service names.

```
# Splunkd service name
SPLUNK_SERVER_NAME=SplunkForwarder2

# Splunkweb service name
SPLUNK_WEB_NAME=splunkweb2
```

3. Save the file and exit the text editor.

Complete the universal forwarder installation

1. Change to the `bin` directory.
2. Enable the universal forwarder to start at boot time, as you did previously.

```
.\splunk enable boot-start
```

   The universal forwarder responds with the following.

```
This appears to be your first time running this version of Splunk.
Installing service SplunkForwarder
Service installed
Windows services installed.
Windows services are configured to run at boot.
```

3. (Optional) If you want the forwarder to run as a different user, complete the procedure shown in Correct the user selected during Windows installation in the *Installation Manual*.
4. Start the universal forwarder.

```
.\splunk start
```

5. When the forwarder warns you that the management port is in use and prompts you to change it, enter `y`.
6. Specify a new management port number.

Install a Windows universal forwarder remotely with a static configuration

You can install a universal forwarder remotely onto a Windows host with a static configuration.

There are several scenarios where you would install a universal forwarder with a static configuration:

- You don't need to change the configuration later.
- You will make any post-installation changes with a non-Splunk deployment tool such as System Center Configuration Manager, Altris, or BigFix/Tivoli.

For this type of installation, install the universal forwarder from the command line. Specify all configuration options and use silent mode (`/quiet`). See Install a Windows universal forwarder from the command line for instructions and a list of installation flags that the installer supports.

Install the universal forwarder with a static configuration

After you download the universal forwarder and plan your installation, install the forwarder:

1. Install and configure the universal forwarder on a test machine, using the command line interface and the flags you want.
2. Test and tune the installation.
3. Load the universal forwarder MSI file into your software deployment tool.
4. Specify the tested flags with your deployment tool.
5. Execute installation with your deployment tool.

Required installation flags

When you install a universal forwarder with a static configuration, specify the `/quiet` flag and a minimum of the following flags:

- `AGREETOLICENSE=Yes`
- `SPLUNKPASSWORD=<password for 'admin' user that you create>`
- `RECEIVING_INDEXER="<server:port>"`

If you do not plan to install an add-on into the forwarder, you also must include at least one data input flag, such as `WINEVENTLOG_APP_ENABLE=1`. See Install a Windows universal forwarder from the command line for a list of all available command line flags.

Example of remote installation with a static configuration

Install as the local system user, set the Splunk admin password to "Ch@ng3d!", get events from the Security event log channel, and forward those events to an indexer

This example sets the universal forwarder to run as the Local System user, get events from the Windows Security and System event logs, send data to `indexer1`, and launch automatically:

```
msiexec.exe /i splunkuniversalforwarder_x86.msi RECEIVING_INDEXER="indexer1:9997" SPLUNKPASSWORD=Ch@ng3d!
WINEVENTLOG_SEC_ENABLE=1 WINEVENTLOG_SYS_ENABLE=1 AGREETOLICENSE=Yes /quiet
```

Install with a secure configuration by specifying certificate files and authority

This example installs a secure configuration and specifies an SSL certificate:

```
msiexec.exe /i splunkuniversalforwarder.msi CERTFILE=<c:\path\to\certfile.pem>
ROOTCACERTFILE=<c:\path\to\rootcacertfile.pem> CERTPASSWORD=<password> SPLUNKPASSWORD=MyNewPassword
RECEIVING_INDEXER="indexer1:9997" WINEVENTLOG_SEC_ENABLE=1 AGREETOLICENSE=yes
```

For more information, see the list of supported command line flags.

Test the deployment

A Splunk best practice is to install a universal forwarder on one host and confirm that it works before installing forwarders on additional hosts.

1. After installing the forwarder, ensure that it gets the desired data and sends it to the indexer.
2. After you confirm that the forwarder works the way you want, continue installation of the forwarder software on the remaining hosts.

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.) Choose the package type that suits your needs and you are comfortable with.

In general, 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
- Install on HP-UX

After you install: Start and configure the universal forwarder

After you complete the installation of the universal forwarder, you must configure it before it can do anything.

You can configure the forwarder from the command line or by using configuration files. If you want to configure from the command line, the forwarder must be running.

1. Start the universal forwarder and accept the license agreement. See Start the universal forwarder.
2. Configure the universal forwarder, either from the command line or with a configuration file. See Configure the universal forwarder or Configure forwarding with outputs.conf.
3. Restart the forwarder to enable the configuration changes that you made.

Install the universal forwarder on Linux

The universal forwarder is available for Linux as a tar file, an RPM package, and a DEB package.

Install from a tar file

Use the `tar` command to install the forwarder.

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

```
tar xvzf splunkforwarder-<?>-Linux-x86_64.tgz -C /opt
```

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

```
tar xvzf splunkforwarder-<?>-Linux-x86_64.tgz
```

Install from a RedHat Package Manager (RPM) package

Use the `rpm` command to install the forwarder.

- To install the forwarder RPM package into the default directory `/opt/splunkforwarder`:

```
rpm -i splunkforwarder-<?>-linux-2.6-x86_64.rpm
```

Install from a Debian package management (DEB) file

Use the `dpkg` command to install the forwarder DEB package.

- To install the forwarder DEB package in the default directory `/opt/splunkforwarder`:

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

The DEB package only supports installation into: `/opt/splunkforwarder`

Install the universal forwarder on Solaris

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

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`

Install from a Solaris PKG file

The PKG installation includes a request file that asks you a few questions before installation starts.

1. Uncompress the PKG file. `uncompress splunkforwarder-<version-os-arch>.pkg.Z`
2. Run the installer. `pkgadd -d ./splunkforwarder-<version-os-arch>.pkg`

3. The installer displays a list of available packages. Select the default (all packages) or select only the packages you want.
4. Specify an installation directory. Enter a path and directory to install the forwarder into, or leave it blank to install to the default directory `/opt/splunkforwarder`.

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.

   If you're installing on OSX 10.15, right-click the `Install Splunk Universal Forwarder` icon and click Open. When prompted again, click Open.
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
```

Install the universal forwarder on FreeBSD

The universal forwarder is available for FreeBSD as a tar file.

Prerequisites for installing the universal forwarder on FreeBSD

For FreeBSD 8, only, the universal forwarder requires compatibility packages. To install the compatibility package:

1. Install the port: `portsnap fetch update cd /usr/ports/misc/compat7x/ && make install clean`
2. Add the package: `pkg_add -r compat7x-amd64`

Basic FreeBSD installation

FreeBSD best practices maintain a small root filesystem. You might want to create a symbolic link to another filesystem and install Splunk there, rather than attempting to install in `/opt`.

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

1. Confirm that the `/opt/splunkforwarder` directories exist.
2. If the directories do not exist, create them or link to another file system from there.
3. Install the universal forwarder on FreeBSD using the intel installer:
   `pkg_add splunkforwarder-intel.tgz`

To install the forwarder in a different directory:

```
pkg_add -v -p /usr/splunk splunkforwarder-intel.tgz
```

Install from a tar file

Expand the universal forwarder tar file into an appropriate directory using the `tar` command. The default install directory is `splunkforwarder` in the current working directory.

```
tar xvzf splunkforwarder.tgz
```

To install into `/opt/splunkforwarder`, execute:

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

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 FreeBSD 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 automatic starting of the universal forwarder 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.

Install the universal forwarder on HP-UX

The universal forwarder is available for HP/UX as a tar file. The default install directory is `/opt/splunkforwarder`.

The version of `tar` that comes with HP-UX does not successfully extract the universal forwarder tar file. Either use the GNU version of `tar` or unpack the tar file on another platform.

- Use the GNU version `tar` to expand the file into an appropriate directory:
  `tar xvzf splunkforwarder-<...>.tgz`

Considerations for installing the universal forwarder

When you perform an installation of the universal forwarder, note the following caveats:

Installation of the universal forwarder as a non-root user

The instructions for installing a universal forwarder for a non-root user are the same as installation of Splunk Enterprise as a non-root user. The only difference will be the default destination folder. See Run Splunk Enterprise as a different or non-root user in the *Installation Manual*.

Installation with tar files

When you install the universal forwarder with 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. 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.

Sun SPARC systems that run Solaris require a minimum patch level to install a universal forwarder

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.

Default installation location

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

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

Do not install the universal forwarder over an existing installation of full Splunk Enterprise. This is particularly vital if you plan to migrate from a light forwarder as described in "Migrate a nix light forwarder".

Install a *nix universal forwarder remotely with a static configuration

You can use scripts or management tools such as `yum` or `puppet` to install many *nix universal forwarders remotely.

For information on how to install and configure a single universal forwarder on *nix operating systems, see Install a nix universal forwarder.

Install a *nix universal forwarder with a static configuration

1. Download the universal forwarder software for your platform.

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

3. Test and tune the configuration.

4. Create a script wrapper for the installation and configuration commands.

5. Run the script on representative target hosts to verify that it works with all required command shells.

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

Create and execute the universal forwarder installation wrapper script

After you validate your installation and configuration process by testing a fully configured universal forwarder, incorporate the process into a script.

Script requirements

Place the installation package or tar file in a network location accessible by the target machines. You can either set this up so that the script pushes the file over to each target host, or you can place the file in a generally accessible location, such as an NFS mount.

The script is responsible for reporting errors.

Sample script

The following is a sample script you can use as a starting point. It is only an example of the type of script you could create for your deployment. The comments in the script provide some guidance on how to modify it for your needs. You might need to modify it further, beyond what has been indicated by the comments.

The script has been designed to:

- Deploy the forwarder tar file to a list of hosts specified in a file that the `HOST_FILE` variable points to. You need to provide this file in the format specified in the script comments.
- Specifies the location on each destination host where the tar file will get unpacked.
- Specifies a Splunk Enterprise instance to serve as a **deployment server** that can subsequently manage and update the forwarders. This is an optional configuration step.
- Starts the forwarder executable on each host.

The script contains many comments. Study it carefully before modifying it for your environment.

```
#!/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.
```

Execute the script

After executing the script, check any log files that it generates for errors. The sample script in this topic saves logs to `/tmp/splunkua.install/<destination hostname>`.

Install universal forwarders in virtual and containerized environments

Make a universal forwarder part of a host image

You can deploy a universal forwarder as part of a host image or virtual machine. This is particularly useful if you have a large number of universal forwarders to deploy. If you have just a few, you might find it simpler to install them manually, as described for Windows and nix hosts.

Steps to deployment

Once you have downloaded the universal forwarder and have planned your deployment, perform these steps:

1. Install the universal forwarder on a test machine.

2. Perform any post-installation configuration.

3. Test and tune the deployment.

4. Install the universal forwarder with the tested configuration onto a source machine.

5. Stop the universal forwarder.

6. Run this CLI command on the forwarder:

```
./splunk clone-prep-clear-config
```

This clears instance-specific information, such as the server name and GUID, from the forwarder. This information will then be configured on each cloned forwarder at initial start-up.

7. Prepare your image or virtual machine, as necessary, for cloning.

8. On *nix systems, set the splunkd daemon to start on boot using cron or your scheduling system of choice. On Windows, set the service to `Automatic` but do not start it.

9. Distribute the system image or virtual machine clones to machines across your environment and start them.

10. Confirm that forwarders have connected to the indexers you specified during forwarder setup.

Referenced procedures

Steps in the above deployment procedure reference these subtopics.

Install the universal forwarder

Install the universal forwarder using the procedure specific to your operating system:

- **To install on a *nix host,** see Install a nix universal forwarder.

- **For a Windows host,** you can use the installer or the command line interface. To install with an installer, see Install a Windows universal forwarder from an installer. For information on the command line interface, see Install a Windows universal forwarder from the command line.

If you do not want the universal forwarder to start on a Windows host after installation, install from the command line . Using the proper command line flags, you can configure the universal forwarder so that it does not start on the source machine when installed but does start automatically on the clones, once they're activated.

At the time of installation, you can also configure the universal forwarder. See Configure the universal forwarder.

Perform additional configuration

You can update your universal forwarder's configuration, post-installation, by directly editing its configuration files, such as `inputs.conf` and `outputs.conf`. See Configure the universal forwarder.

For information on distributing configuration changes across multiple universal forwarders, see "About deployment server" in the *Updating Splunk Enterprise Instances* manual.

Test the deployment

Test your configured universal forwarder on a single machine, to make sure it functions correctly, before deploying the universal forwarder across your environment. When testing the deployment, ask these questions:

1. Do the data inputs that you configured in the forwarder collect the data you want?

If they don't:

- Check the inputs.conf on the forwarder and confirm that the input stanzas are correct. For example, if you want to configure monitoring a file, confirm that the inputs.conf on the forwarder references that file.
- Confirm that the stanza that references the file is not disabled (look for 'disabled = 1' in the stanza.)

2. Does the forwarder send the data you expect to the place you expect it?

If it doesn't:

- Confirm that the outputs.conf on the forwarder has been correctly configured. The outputs.conf file should reference a receiving indexer that the forwarder can access over the network via a host name or IP address and port that you specify.
- Confirm that no firewall blocks network traffic on the ports you specify on both the forwarder and receiver.
- Confirm that the ports you specify on the forwarder and receiver are the same, as they must be for forwarding to occur. For example, if you specify port 9997 as the receiving port on the indexer, you must specify this same port as the target in the outputs.conf configuration on the forwarder.
- Use the Search page on the receiving indexer to confirm that you see events that you configured on the forwarder.

Deploy and run a universal forwarder inside a Docker container

If you are a first-time Splunk user, Splunk's Docker containers for Splunk Enterprise and universal forwarder helps you quickly deploy and gain hands-on experience with the Splunk software, while still allowing for complex deployments in the future.

Containerized Splunk software provides the following flexibility and scalability to your Splunk environment:

- Deployment of Splunk Enterprise and universal forwarder that can be run on your laptop or desktop, or pushed to a large orchestrator
- Support for multiple Splunk Enterprise topologies including standalone server and distributed multi-node deployments
- Automatic installation of all upcoming versions of Splunk Enterprise and universal forwarder (beginning with version 7.2)
    - Defaults to the latest official Splunk Enterprise/universal forwarder release
    - Previously released versions can be installed and upgraded to the most current version of Splunk Enterprise/universal forwarder. However, Splunk versions prior to 7.2 are not supported.

Splunk's official repository containing Dockerfiles for building Splunk Enterprise and Universal Forwarder images using containerization technology can be found on GitHub: https://github.com/splunk/docker-splunk

Containerized Splunk software prerequisites

At the current time, Splunk software container images only support the Docker runtime engine and requires the following system prerequisites:

- Linux-based operating system (Debian, CentOS, etc.)
- Chipset
    - splunk/splunk image supports x86-64 chipsets
    - splunk/universalforwarder image supports both x86-64 and s390x chipsets
- Kernel version > 4.0
- Docker engine
    - Docker Enterprise Engine 17.06.2 or later
    - Docker Community Engine 17.06.2 or later
- overlay2 Docker daemon storage driver

For more details, please see the official supported architectures and platforms for containerized Splunk environments as well as hardware and capacity recommendations.

Deploy Splunk universal forwarder Docker containers

You deploy Splunk universal forwarder inside a Docker container by downloading and launching the required universal forwarder Docker image. The image is an executable package that includes everything you need to run Splunk universal forwarder. A container is a runtime instance of an image.

1. From a shell prompt, run the following command to download the required universal forwarder image to your local Docker image library.

   ```
   docker pull splunk/universalforwarder:latest
   ```
2. Run the downloaded Docker image.

   ```
   docker run -d -p 9997:9997 -e "SPLUNK_START_ARGS=--accept-license" -e "SPLUNK_PASSWORD=<password>"
   --name uf splunk/universalforwarder:latest
   ```
   Where `<password>` is the new password you want to set for the universal forwarder instance. For information on password requirements, see Configure a Splunk password policy in Authentication.conf in *Securing Splunk Enterprise*.

`-p 9997:9997` exposes the default port of the universal forwarder inside the container to the outside world by mapping it to a port on the local host. In this case, the outside port is also 9997. If port 9997 is occupied by another service on the host, you can use the `-p` parameter to map the application port to another available port on the host, for example, `-p 9998:9997`.

Accept the license agreement with `SPLUNK_START_ARGS=--accept-license`. This must be explicitly accepted on every splunk/universalforwarder container, otherwise the universal forwarder will not start.

3. The output of the `docker run` command is a hash of numbers and letters that represents the container ID of your new universal forwarder deployment. Run the following command with the container ID to display the status of the container.

```
docker ps -a -f id=<container_id>
```

4. When the status of the container becomes healthy, it means the container is already up and running.

Administer Splunk universal forwarder Docker containers

You can use the following Docker commands to manage containers.

- To see a list of example commands and environment variables for running a forwarder in a container, run:

```
docker run -it splunk/universalforwarder help
```

- To see a list of your running containers, run:

```
docker ps
```

- To stop your forwarder container, run:

```
docker container stop <container_id>
```

- To restart a stopped container, run:

```
docker container start <container_id>
```

- To access a running forwarder container to perform administrative tasks, such as modifying configuration files, run:

```
docker exec -it <container_id> bash
```

To learn more about Splunk Enterprise and Docker commands, see the documentation on GitHub for Splunk-Docker.

Start and stop the universal forwarder

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

The procedure for configuring the universal forwarder to start when the machine starts is the same as for Splunk Enterprise, with the universal forwarder installation directory being the only difference. 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.

Create credentials for the administrator account.
Characters do not appear on the screen when you type the password.

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 then 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`

Configure the universal forwarder

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
```

Configure forwarding with outputs.conf

The outputs.conf file defines how forwarders send data to receivers. You can specify some output configurations at installation time (Windows universal forwarders only) or the CLI, but most advanced configuration settings require that you edit `outputs.conf`.

The topics that describe various forwarding topologies, such as load balancing and intermediate forwarding, provide detailed examples on configuring `outputs.conf` to support those topologies.

Although `outputs.conf` is a required file for configuring forwarders, it addresses only the outputs from the forwarder, where you want the forwarder to send the data it collects. To specify the data that you want to collect from the forwarder, you must separately configure the inputs, as you would for any Splunk instance. See Add data and configure inputs in *Getting Data In*.

Edit outputs.conf to configure forwarding

This procedure details the steps you must take to edit the default `outputs.conf` which is in `$SPLUNK_HOME/etc/system/local`. You might have to edit the file in other places, as sections in this topic explain. For an example of what an `outputs.conf` file looks like, see "Examples of outputs.conf" later in this topic.

1. On the host that forwards that data that you want to collect, open a shell or command prompt or PowerShell window.
2. Go to the configuration directory for the forwarder.

Unix	Windows
`cd $SPLUNK_HOME/etc/system/local`	`cd %SPLUNK_HOME%\etc\system\local`

3. Open `outputs.conf` for editing with a text editor.

Unix	Windows
`vi outputs.conf`	`notepad outputs.conf`

4. Edit outputs.conf. Add a minimum of at least one forwarding target group or a single receiving host.
5. Save the `outputs.conf` file and close it.
6. Restart the universal forwarder to complete your changes.

Unix	Windows

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

Types of outputs.conf files

A single forwarder can have multiple `outputs.conf` files. For example, one can be located in an apps directory and another in `$SPLUNK_HOME/etc/system/local`. No matter how many `outputs.conf` files the forwarder has and where they reside, the forwarder combines all their settings, using the rules of configuration file precedence. The forwarder contains both default and custom `outputs.conf` files.

Default versions of outputs.conf

The universal forwarder ships with these default versions of `outputs.conf`:

- One in `$SPLUNK_HOME/etc/system/default`.
- Another in `$SPLUNK_HOME/etc/apps/SplunkUniversalForwarder/default`.

The default version in the `SplunkUniversalForwarder` app has precedence over the version under `/etc/system/default`.

Do not edit default versions of any configuration files. See About configuration files.

Custom versions of outputs.conf

When you configure forwarding behavior, those changes get saved in custom versions of `outputs.conf`. There are several ways you can specify forwarding behavior:

- While installing the forwarder (on the Windows universal forwarder only.)
- By running CLI commands.
- By directly editing an `outputs.conf` file.

The forwarder automatically creates or edits custom versions of `outputs.conf` in response to the first three methods. The locations of those versions vary, depending on the type of forwarder and other factors.

- If you use the CLI to make changes to universal forwarder output behavior, the CLI creates or edits a copy of `outputs.conf` in `$SPLUNK_HOME/etc/system/local`.
- The Windows installation process writes configuration changes to an `outputs.conf` file located in the `MSICreated` app.

In addition to any `outputs.conf` files that you create and edit indirectly (for example, through the CLI), you can also create or edit an `outputs.conf` file directly with a text editor. You should work with a single copy of the file, which you place in `$SPLUNK_HOME/etc/system/local/`. If a copy of the file already exists in that directory, because of configuration changes made through the CLI, edit that copy. For purposes of distribution and management simplicity, you can combine settings from all non-default versions into a single custom `outputs.conf` file.

The universal forwarder must be restarted after you make changes to `outputs.conf`.

For information on `outputs.conf`, see the outputs.conf spec file.

Configuration levels for outputs.conf

There are two types of output processors for forwarding data: `tcpout` and `syslog`. The universal forwarder only has the `tcpout` processor, which uses the `[tcpout]` header in `outputs.conf`.

You can configure the `tcpout` processor at three levels of stanzas:

- **Global.** (Optional) At the global level, you specify any attributes that you want to apply globally, as well as certain attributes only configurable at the system-wide level for the output processor.
- **Target group.** A target group defines settings for one or more receiving indexers. There can be multiple target groups per output processor. Most configuration settings can be specified at the target group level.
- **Single server.** (Optional) You can specify configuration values for single servers (receivers) within a target group.

Configurations at the more specific levels take precedence over the global level. For example, if you specify `compressed=true` for a target group, the forwarder sends the hosts in that target group compressed data, even if you set the `compressed` attribute to "false" for the global level.

Outputs.conf global stanza

The global stanza in `outputs.conf` lets you set any attributes that you want to apply globally. While this stanza is optional, there are several attributes that you can set only at the global level, including `defaultGroup`.

The `[tcpout]` header specifies the global stanza for the `tcpout` processor. Following is an example of a global tcpout stanza.

```
[tcpout]
defaultGroup=indexer1
compressed=true
```

This global stanza includes two attribute/value pairs:

- **defaultGroup=indexer1** This tells the forwarder to send all data to the "indexer1" target group. See "Default target groups".
- **compressed=true** This tells the forwarder to compress the data before it forwards the data to receiving indexers in the target groups. If you set `compressed` to "false", the forwarder sends raw data.

Set default target groups in outputs.conf

The `defaultGroup` attribute lets you set default groups for automatic forwarding at the global level, in your `[tcpout]` stanza.

The defaultGroup specifies one or more target groups that you define later in `tcpout:<target_group>` stanzas. The forwarder sends all events to the specified groups.

```
[tcpout]
defaultGroup= <target_group1>, <target_group2>, ...
```

If you do not want to forward data automatically, do not set the `defaultGroup` attribute.

Outputs.conf target group stanza

The target group identifies a set of receivers. It also specifies how the forwarder sends data to those receivers. You can define multiple target groups.

Here is the basic pattern for the target group stanza.

```
[tcpout:<target_group>]
server=<receiving_server1>, <receiving_server2>, ...
<attribute1> = <val1>
<attribute2> = <val2>
...
```

You can specify a receiving server in a target group by using the format `<ipaddress_or_hostname>:<port>`, where `<port>` is the receiving host **receiving port**. For example, `myhost.splunk.com:9997`. When you specify multiple receivers, the forwarder load balances among them.

A target group stanza name cannot have spaces or colons in it. Splunk software ignores target groups whose stanza names contain spaces or colons in them.

See Define typical deployment topologies later in this topic for information on how to use the target group stanza to define several deployment topologies.

Outputs.conf single-host stanza

You can define a specific configuration for an individual receiving indexer. However, the receiver must also be a member of a target group.

When you define an attribute at the single-host level, it takes precedence over any definition at the target group or global level.

Here is the syntax for defining a single-host stanza:

```
[tcpout-server://<ipaddress_or_hostname>:<port>]
<attribute1> = <val1>
<attribute2> = <val2>
...
```

Examples of outputs.conf

The following `outputs.conf` example contains three stanzas for sending data to Splunk receivers.

- Global settings. In this example, there is one setting, to specify a `defaultGroup`.
- Settings for a single target group consisting of two receivers. Here, we specify a load-balanced target group consisting of two receivers.
- Settings for one receiver within the target group. In this stanza, you can specify any settings specific to the `mysplunk_indexer1` receiver.

```
[tcpout]
defaultGroup=my_indexers
```

```
[tcpout:my_indexers]
server=mysplunk_indexer1:9997, mysplunk_indexer2:9996

[tcpout-server://mysplunk_indexer1:9997]
```

Define typical forwarder deployment topologies

You can configure a forwarder to support several typical deployment topologies. See the other topics in the "Forward data" chapter for information on how to configure forwarders for other topologies.

Configure load balancing on a universal forwarder with outputs.conf

When you specify a target group with multiple receivers in `outputs.conf` on a forwarder, the forwarder performs **load balancing** between the receivers.

In the example that follows, the target group consists of three receivers. The forwarder balances load between the three receivers you specify. If one receiver goes down, the forwarder automatically switches to the next available receiver.

```
[tcpout:my_LB_indexers]
server=10.10.10.1:9997,10.10.10.2:9996,10.10.10.3:9995
```

Note: While 9997 is the standard network port for receiving data from forwarders, you can specify any network port above 1024 to receive data.

Configure data cloning on a universal forwarder with outputs.conf

When you specify multiple target groups with a separate stanza for each group in `outputs.conf`, the forwarder performs **data cloning** between the groups. In data cloning, the forwarder sends copies of all its events to the receivers in two or more target groups. Data cloning usually results in similar, but not necessarily exact, copies of data on the receiving indexers. An example of how to configure data cloning follows.

```
[tcpout]
defaultGroup=indexer1,indexer2

[tcpout:indexer1]
server=10.1.1.197:9997

[tcpout:indexer2]
server=10.1.1.200:9997
```

The forwarder sends duplicate data streams to the servers specified in both the `indexer1` and `indexer2` target groups.

Configure data cloning with load balancing on a universal forwarder

You can combine load balancing with data cloning. For example:

```
[tcpout]
defaultGroup=cloned_group1,cloned_group2

[tcpout:cloned_group1]
server=10.10.10.1:9997, 10.10.10.2:9997, 10.10.10.3:9997
```

```
[tcpout:cloned_group2]
server=10.1.1.197:9997, 10.1.1.198:9997, 10.1.1.199:9997, 10.1.1.200:9997
```

The forwarder sends full data streams to both the `cloned_group1` and `cloned_group2` groups. The forwarders load-balance the data within each group, rotating among receivers every 30 seconds (the default frequency).

Common attributes for outputs.conf

The `outputs.conf` file provides a large number of configuration options that offer considerable control and flexibility in forwarding. Of the attributes available, several are of particular interest:

Attribute	Default	Where configured	Value
`defaultGroup`	n/a	global stanza	A comma-separated list of one or more target groups. Forwarder sends all events to all specified target groups.
`server`	n/a	target group stanza	Required. Specifies the hosts that function as receivers for the forwarder. This must be set to a value using the format `<ipaddress_or_servername>:<port>`, where `<port>` is the receiving server's receiving port.
`disabled`	false	any stanza level	Specifies whether the stanza is disabled. If set to "true", it is equivalent to the stanza not being there.
`sendCookedData`	true	global or target group stanza	Specifies whether data is cooked before forwarding.
`compressed`	false	global or target group stanza	Specifies whether the forwarder sends compressed data.
`ssl....`	n/a	any stanza level	Set of attributes for configuring SSL. See "About securing data from forwarders" in the *Securing Splunk Enterprise* manual for information on how to use these attributes.
`useACK`	false	global or target group stanza	Specifies whether the forwarder waits for indexer acknowledgment confirming that the data has been written to the file system.
`dnsResolutionInterval`	300	global or target group stanza	Specifies base time interval in seconds at which indexer DNS names will be resolved to IP address.
`autoLBVolume`	0	global or target group stanza	Specifies, in bytes, how much data a forwarder that has been configured for load balancing sends to an indexer before it selects another indexer.

The `outputs.conf.spec` file, which you can find here, along with several examples, provides details for these and all other configuration options. In addition, most of these settings are discussed in topics that deal with specific forwarding scenarios.

DNS resolution interval

The `dnsResolutionInterval` attribute specifies the base time interval (in seconds) at which receiver DNS names will be resolved to IP addresses. The forwarder uses this value to compute the run-time interval as follows:

```
run-time interval = dnsResolutionInterval + (number of receivers in server attribute - 1) * 30
```

The run-time interval increases by 30 seconds for each additional receiver that you specify in the `server` attribute (each additional receiver across which the forwarder load-balances.) The `dnsResolutionInterval` attribute defaults to 300 seconds.

For example, if you leave the attribute at the default setting of 300 seconds and the forwarder is load-balancing across 20 indexers, DNS resolution will occur every 14 1/2 minutes:

```
(300 + ((20 - 1) * 30)) = 870 seconds = 14.5 minutes
```

If you change `dnsResolutionInterval` to 600 seconds, and keep the number of load-balanced indexers at 20, DNS resolution will occur every 19 1/2 minutes:

```
(600 + ((20 - 1) * 30)) = 1170 seconds = 19.5 minutes
```

Supported CLI commands

The universal forwarder supports a subset of objects for use in CLI commands. Certain objects valid in full Splunk Enterprise, like `index` (as in `add index`), are not applicable in the context of the universal forwarder.

Commands act upon objects. If you type an invalid command/object combination, the universal forwarder returns an error message.

Valid CLI objects

The universal forwarder supports all CLI commands for these objects:

```
add
app
config
datastore-dir
default-hostname
deploy-client
deploy-poll
eventlog
exec
forward-server
monitor
oneshot
perfmon
registry
servername
splunkd-port
tcp
udp
user
wmi
```

Note: A few commands, such as `start` and `stop` can be run without an object. A command with no object is also valid for the universal forwarder.

Introduction to CLI syntax

The general syntax for a CLI command is:

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

As described above, the *object* determines whether a command is valid in the universal forwarder. For example, the above list includes the `monitor` object. Therefore, the `add monitor` and `edit monitor` command/object combinations are both valid. For more information on the `monitor` object, see "Use the CLI to monitor files and directories" in *Getting Data In*.

For more details on using the CLI in general, see Administer Splunk Enterprise with the CLI in the Splunk Enterprise *Admin Manual*. In particular, the topic "CLI admin commands" provides details on CLI syntax, including a list of all commands supported by full Splunk Enterprise and the objects they can act upon.

Upgrade the universal forwarder

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)

Prerequisites to upgrading a universal forwarder

Confirm that you understand or have all of the following prior to upgrading a forwarder.

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: Compatibility between forwarders and Splunk Enterprise indexers.

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. 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`.
2. Uninstall the existing 32-bit forwarder, as described in Uninstall the universal forwarder.
3. Install the 64-bit forwarder, as described in Install the universal forwarder from an installer.
4. 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. Download the new MSI file from the universal forwarder download page.
2. Double-click the MSI file. The installer displays the "Accept license agreement" panel.
3. 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. To upgrade a group of forwarders, load the command line installer into a deployment tool such as Group Policy or System Center Configuration Manager, as described in Perform a remote upgrade.

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

1. Download the new MSI file from the Splunk universal forwarder download page.
2. 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`.
3. 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.

See Upgrade using the command line, for details on the command line syntax to use in the deployment tool.

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)

Prerequisites to upgrading a *nix universal forwarder

Read this section before performing an upgrade. Also, see How to upgrade Splunk Enterprise for up-to-date information and potential issues you might encounter when you upgrade Splunk Enterprise.

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: Compatibility between forwarders and Splunk Enterprise indexers.

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.

Make sure no other processes can start the forwarder automatically

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.

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
```

- 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 sample script that is in the Install a nix universal forwarder remotely with a static configuration topic, 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 Upgrade a single forwarder.

2. Create a script wrapper for the upgrade commands, as described in Install a nix universal forwarder remotely with a static configuration.

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.

Upgrade a universal forwarder to a heavy forwarder

The universal forwarder is the recommended method to gather data from hosts and send it to your Splunk deployment. However, there might be times where you need the routing and filtering capabilities that a heavy forwarder can provide. In such a case, you can upgrade a universal forwarder to a heavy forwarder.

Because the universal forwarder and the heavy forwarder install in separate directories by default, you can install the heavy forwarder on the same host as the universal forwarder and move the universal forwarder data to the heavy forwarder.

A heavy forwarder requires a larger amount of disk space than a universal forwarder does. It also uses more network and memory resources than a universal forwarder does (though you can configure the instance to use less.)

Splunk Enterprise also requires a separate license after the 60-day trial license expires.

Upgrade a universal forwarder to a heavy forwarder

1. Stop the universal forwarder on the host that you want to upgrade to a heavy forwarder.
2. Download Splunk Enterprise onto the host.
3. Install Splunk Enterprise on the host.
4. Copy the fishbucket and persistent databases from the universal forwarder to the same directory on the heavy forwarder.
5. Copy `inputs.conf` and `outputs.conf` from the universal forwarder to the heavy forwarder.
6. (Optional) Copy any add-ons you have installed from the universal forwarder to the heavy forwarder.
7. Edit `props.conf` and `transforms.conf` on the heavy forwarder, or use a deployment server to send configurations to the forwarder.
8. Restart the heavy forwarder.
9. Confirm that the heavy forwarder sends data to the indexer.
10. Uninstall the universal forwarder.

Uninstall the universal forwarder

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.)

Perform advanced configuration

Configure load balancing for Splunk Enterprise

With **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. To access the full set of forwarded data, you need to set up distributed searching across all the receivers. See About distributed search in *Distributed Search*.

Load balancing enables horizontal scaling for improved performance. In addition, its automatic switchover capability ensures resiliency in the face of machine outages. If a host goes down, the forwarder sends data to the next available receiver.

Load balancing can also be of use when you get data from network devices like routers. To handle syslog and other data generated across TCP port 514, a single universal forwarder can monitor port 514 and distribute the incoming data across several indexers.

Note: Do not use an external load balancer to implement load balancing between forwarders and receivers. This practice does not generate the results you would expect. Use the load balancing capability that comes with the forwarder.

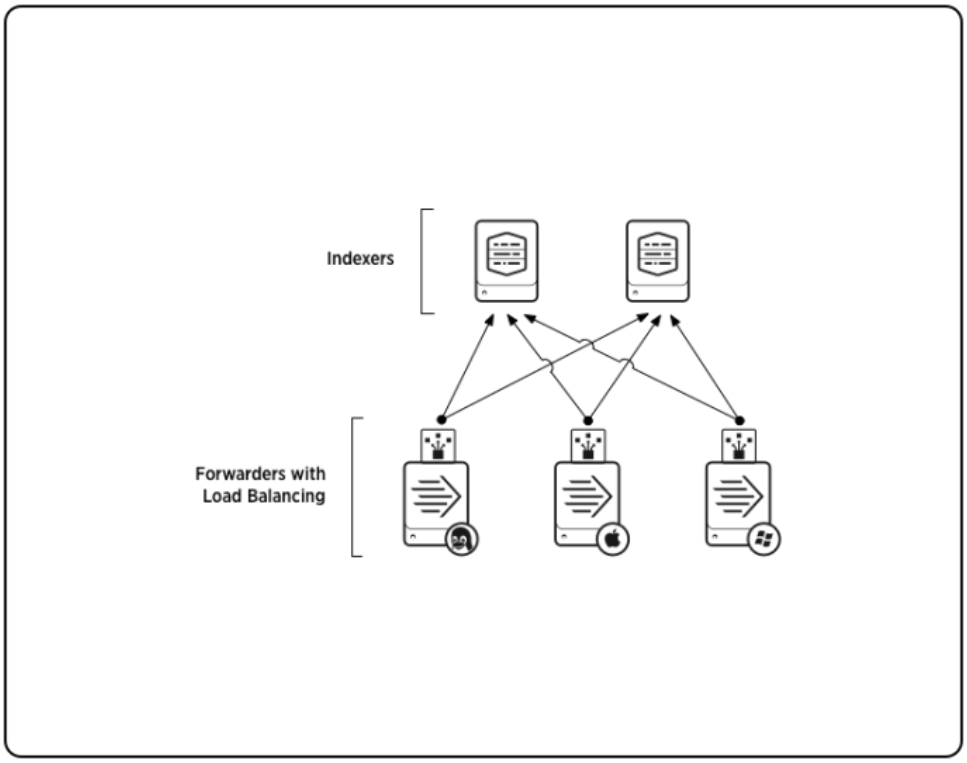
How load balancing works

Forwarders perform automatic load balancing. 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.

There is a data stream for each of the inputs that the forwarder monitors. The forwarder determines if it is safe for a data stream to switch to another indexer. Then, at the specified interval, it switches the data stream to the newly selected indexer. If it cannot switch the data stream to the new indexer safely, it keeps the connection to the previous indexer open and continues to send the data stream until it has been safely sent.

Universal forwarders cannot switch indexers when they monitor TCP network streams of data unless the forwarder encounters an end-of-file (EOF) or the receiving indexer goes down. At that point, the forwarder switches to the next indexer in the list. Because the universal forwarder does not parse data and identify event boundaries before forwarding the data to the indexer (unlike a heavy forwarder), it does not know when it is safe to switch to the next indexer unless it receives an EOF.

The following diagram shows a typical load-balancing scenario, in which three forwarders are sending load-balanced data across a set of two receiving indexers:



Options for configuring receiving targets for load balancing

Specify static or DNS lists for receiving indexers

When you configure a set of target receivers for load balancing, you can choose either DNS or static lists.

DNS lists provide greater flexibility and allow for simplified scaling, particularly for large deployments. Through DNS, you can change the set of receivers without needing to re-edit each forwarder `outputs.conf` file.

Static lists let you specify a different port for each receiver. This is useful if you need to perform load balancing across multiple receivers that run on a single host, as each receiver can listen on a separate network port.

Choose a load balancing method

You can choose how you want the forwarders to load balance between the indexers in a load balancing list.

- **By time**. The default method for load balancing is how frequently the forwarders change indexers in the load balanced list. The `autoLBFrequency` setting in outputs.conf controls how often forwarders switch between indexers. The default frequency is every 30 seconds, but you can set it higher or lower.

- **By volume**. Another option is to set how much data a forwarder sends to an indexer before it switches between indexers in a load-balanced list. The `autoLBVolume` setting in `outputs.conf` controls the amount of data that a forwarder sends to a receiving indexer before it changes to another one. By default, this setting is not active (0 bytes.) If you set it to anything other than 0, then the forwarder will change indexers based on the amount of data that it has sent.

If you enable both settings, then the forwarder chooses an indexer based on the following logic:

- If the forwarder has sent more than `autoLBVolume` bytes of data to a forwarder, it changes indexers regardless of whether or not `autoLBFrequency` have passed since the last change to a receiving indexer.
- If the forwarder has not sent more than `autoLBVolume` bytes of data before `autoLBFrequency` seconds have elapsed, then it changes indexers after that time has passed.

Specify a static list target

1. On a forwarder that you want to set a static list target, edit `$SPLUNK_HOME/etc/system/local/outputs.conf`. You might have to create this file beforehand.
2. In the `outputs.conf` file, specify each of the receivers in the target group `[tcpout]` stanza.
3. Save the `outputs.conf` file.
4. Restart the forwarder. The forwarder sends data to the static list targets.

Examples of a static load-balancing configuration file

In the following example, the target group consists of three receivers, specified by IP address and receiving port number. The universal forwarder balances load between the three receivers. If one receiver goes down, the forwarder switches to another one on the list.

```
[tcpout: my_LB_indexers]
server=10.10.10.1:9997,10.10.10.2:9996,10.10.10.3:9995
```

In the following example, the target group consists of four receivers, specified by IP address and receiving port number. The universal forwarder has been configured to send a specific amount of data (in this case, 1MB) to a receiver before it switches to another receiver in the list.

```
[tcpout: my_LB_indexers]
server=10.10.10.1:9997,10.10.10.2:9996,10.10.10.3:9995,10.10.10.4:9994
autoLBVolume=1048576
```

In the following example, the target group consists of three receivers. one with a DNS hostname and two with IP addresses. The universal forwarder has been configured to send data to one indexer for 3 minutes (180 seconds) before switching to another receiver.

```
[tcpout:My_LB_Indexers]
server=192.168.1.15:9997,192.168.1.179:9997,server1.mktg.example.com:9997
autoLBFrequency=180
```

Specify a DNS list target

1. On a forwarder that you want to set a DNS list target, edit `$SPLUNK_HOME/etc/system/local/outputs.conf`. You might have to create this file beforehand.
2. In the `outputs.conf` file, specify a single host in the target group `[tcpout]` stanza.
3. Save the `outputs.conf` file.
4. Restart the forwarder. The forwarder sends data to the DNS list targets.

5. On your DNS server, create a DNS A record for each host IP address, referencing the server name you specified in `outputs.conf`..
   ```
   splunkreceiver.mycompany.com   A   10.10.10.1
   splunkreceiver.mycompany.com   A   10.10.10.2
   splunkreceiver.mycompany.com   A   10.10.10.3
   ```
6. Reload the updated configuration on your DNS server. It might take a while for DNS changes to take effect, depending on the size of your network topology.

Examples of a DNS-based load-balancing configuration file

In the following example, the forwarder has been configured to send data to what appears to be a single host. The changes you made in DNS now have this hostname refer to three different IP addresses.

```
[tcpout:my_LB_indexers]
server=splunkreceiver.mycompany.com:9997
```

The forwarder uses the DNS list to load balance, sending data in intervals, switching among the receivers specified. If a receiver is not available, the forwarder skips it and sends data to another one on the list.

If you have a topology with many forwarders, the DNS list method lets you update the set of receivers by making changes on the DNS server, without having to edit `outputs.conf`.

Configure universal forwarder load balancing for horizontal scaling

When you configure load balancing for horizontal scaling, you should first determine your needs, particularly your horizontal scaling and whether or not you need failover. This helps you develop a topology based on those needs, which can include multiple forwarders as well as receivers and a search head to search across the receivers.

Set up DNS-based load balancing

This procedure assumes a topology of three universal forwarders and three receivers and uses a DNS list to designate the receivers. The receivers must all listen the same port.

1. Install a set of three Splunk Enterprise instances as receivers.
2. Configure receiving on the receivers. Specify the same receiving port. For example:
   ```
   ./splunk enable listen 9997 -auth <username>:<password>
   ```
3. Install a set of universal forwarders, as described in Install the universal forwarder software.
4. On your DNS server, set up a DNS list with an A record for each receiver IP address.
   ```
   splunkreceiver.mycompany.com   A   10.10.10.1
   splunkreceiver.mycompany.com   A   10.10.10.2
   splunkreceiver.mycompany.com   A   10.10.10.3
   ```
5. Reload the updated configuration on your DNS server. It might take a while for DNS changes to take effect, depending on the size of your network topology.
6. Create an `outputs.conf` file for all the forwarders to use. This example specifies the DNS server name used in the DNS list and the port the receivers are listening on.
   ```
   [tcpout]
   defaultGroup=my_LB_indexers

   [tcpout:my_LB_indexers]
   disabled=false
   autoLBFrequency=40
   server=splunkreceiver.mycompany.com:9997
   ```

This `outputs.conf` file uses the `autoLBFrequency` attribute to set a load-balance frequency of 40 seconds. Every 40 seconds, the forwarders switch to another receiver. The default frequency is 30 seconds.
7. Distribute the `outputs.conf` file to all the forwarders. You can use the **deployment server** to handle the distribution.

Specify load balancing from the CLI

You can also use the CLI to specify load balancing. You do this when you start forwarding activity to a set of receivers.

```
./splunk add forward-server <host>:<port> -method autobalance
```

where `<host>:<port>` is the host and receiver port of the receiver.

This example creates a load-balanced group of four receivers:

```
./splunk add forward-server indexer1:9997 -method autobalance
./splunk add forward-server indexer2:9997 -method autobalance
./splunk add forward-server indexer3:9997 -method autobalance
./splunk add forward-server indexer4:9997 -method autobalance
```

Configure improved load balancing with props.conf

You can improve how the universal forwarder distributes data during load balancing by using the `props.conf` configuration file. In the file, you specify settings to enable use of a special processor called `ChunkedLBProcessor` that distributes data more evenly amongst the indexers in a load-balanced target group. This configuration can be enabled for any source type. The processor and these settings are available on universal forwarders that are version 6.5.0 and later only.

This feature works with any kind of load balancing setup. It controls how the forwarders package and send the data to the receivers.

1. Set up your forwarders and receivers for load balancing, as described earlier in this topic.
2. On the forwarders where you want to improve data distribution, edit `$SPLUNK_HOME/etc/system/local/props.conf`. You might have to create this file beforehand.
3. In the `props.conf` file, add a stanza for the source type where you want to improve data distribution. You do not need to perform this step if the source type stanza already exists.
4. In the stanza, set the `EVENT_BREAKER_ENABLE` setting to `true`.
5. (Optional) Add and configure the `EVENT_BREAKER` setting to a regular expression that represents the event boundary. The forwarder uses this expression to determine when it is okay to change between receivers in a load balancing configuration.
6. Save the `props.conf` file and close it.
7. Restart the universal forwarder.

Props.conf settings to improve distribution of data in load balancing

The settings for using the `ChunkedLBProcessor` processor on the universal forwarder are as follows.

Attribute	Description	Default
`EVENT_BREAKER_ENABLE`	Enables the use of the `ChunkedLBProcessor` data processor, which improves distribution of data from universal forwarders to receiving indexers for a given source type. A value of true tells the forwarder to use the `ChunkedLBProcessor` processor for the source type. A value of false	`false`

Attribute	Description	Default
	tells the forwarder to send data to the receiver through standard load balancing methods.	
EVENT_BREAKER	A regular expression that specifies the event boundary for the universal forwarder to use to determine when it can send events to the indexer. The regular expression must contain a capturing group (a pair of parentheses that defines an identified sub-component of the match.) This setting is similar to the LINE_BREAKER setting for heavy forwarders and indexers, except that the forwarder does not discard the contents of the capturing group when it encounters a match. The forwarder looks for the EVENT_BREAKER regular expression pattern match in the data stream and uses the match to identify the event boundaries. When it finds a match, the forwarder considers the first capturing group to be the end of the previous event and the end of the capturing group to be the beginning of the next event. The forwarder can then change the receiving indexer based on these event boundaries. This setting works best with multiline events.	\r\n (the standard event breaking string)

Troubleshoot line merging problems for forwarded custom source types at the indexer

When you configure these settings on the forwarder in conjunction with a custom source type, it is possible that events could be merged incorrectly on the indexer. If this happens, you can configure `props.conf` on the indexer with the `SHOULD_LINEMERGE` setting for the affected source type. If the source type mainly generates single line events, set `SHOULD_LINEMERGE` to `false` for the source type on the indexer.

For example, if you have a custom source type `json_logs` and you notice that the events for the source type appear to be merged incorrectly when you search the source type on your indexers, edit the source type on the indexer to prevent this behavior.

1. On the indexer, open `$SPLUNK_HOME/etc/system/local/props.conf` for editing.
2. In the file, locate the `json_logs` stanza. If this stanza does not exist, create it.
3. Add the `SHOULD_LINEMERGE=false` entry to the stanza.

```
[json_logs]
SHOULD_LINEMERGE=false
```

4. Save the `props.conf` file and close it.
5. (Optional) Add the stanza to `props.conf` on all other indexers.
6. Restart Splunk Enterprise on the indexers.

Example of ChunkedLBProcessor usage

The following example turns on the processor and uses the standard event boundary to determine when to send events.

```
[mysourcetype]
EVENT_BREAKER_ENABLE=true
```

The following example uses the processor to break up events for a source type that generates multiline Java event logs.

```
[mysourcetype2]
```

```
EVENT_BREAKER_ENABLE=true
EVENT_BREAKER=([\r\n]+)(\d\d\d\d-\d\d-\d\d \d\d?:\d\d:\d\d)
```

Configure a forwarder to use a SOCKS proxy

You can configure a forwarder with a Socket Secure version 5 (SOCKS5) proxy server as a target with the intent of forwarding data to an indexer beyond the proxy server.

By default, a Splunk forwarder requires a direct network connection to any receiving indexers. If a firewall blocks connectivity between the forwarder and the indexer, the forwarder cannot send data to the indexer.

You can configure a forwarder to use a SOCKS5 proxy host to send data to an indexer by specifying attributes in a stanza in the `outputs.conf` configuration file on the forwarder. After you configure and restart the forwarder, it connects to the SOCKS5 proxy host, and optionally authenticates to the server on demand if you provide credentials. The proxy host establishes a connection to the indexer and the forwarder begins sending data through the proxy connection.

Any type of Splunk forwarder can send data through a SOCKS5 proxy host.

This implementation of the SOCKS5 client complies with the Internet Engineering Task Force (IETF) Request for Comments (RFC) Memo #1928. See "Network Working Group: Request for Comments: 1928" (http://www.ietf.org/rfc/rfc1928.txt) on the IETF website.

Security considerations

When you use the SOCKS5 proxy feature on a universal forwarder, note the following security considerations:

- SOCKS5 proxy support only exists between the forwarder and the indexer inclusive. There is no support for the usage of SOCKS with any other Splunk features, apps, or add-ons.
- The SOCKS5 protocol sends authentication credentials in clear text. Due to this implementation, these credentials are vulnerable to a man-in-the-middle attacker. This means that an attacker can secretly relay and possibly change communication between the SOCKS client and the SOCKS proxy host. This is a caveat of the SOCKS protocol, not the implementation of this feature in Splunk software.
- For the most secure results, use the SOCKS attributes only on forwarders which are inside networks that a SOCKS proxy host protects. Deploying a forwarder in an unprotected environment can result in the interception of SOCKS credentials by a third party, even though the forwarder has SOCKS proxy support enabled.

Configure a SOCKS5 proxy connection with configuration files

To configure a SOCKS5 proxy connection, edit stanzas in `outputs.conf` and specify certain attributes to enable the proxy. For a list of valid proxy attributes, see Proxy configuration values. You cannot configure proxy servers in Splunk Web.

1. Open `$SPLUNK_HOME/etc/system/local/outputs.conf` for editing.

2. Define forwarding servers or output groups in `outputs.conf` by creating `[tcpout]` or `[tcpout-server]` stanzas.

3. In the stanza for connections that should have SOCKS5 proxy support, add attributes for SOCKS that fit your proxy configuration. Specify at least the `socksServer` attribute to enable proxy support.

4. Save the file and close it.

5. Restart the forwarder.

6. On the receiving indexer, user the Search and Reporting app to confirm that the indexer received the data.

Proxy configuration values

Use the following attributes to configure SOCKS5 on the forwarder:

Attribute	Description	Default
`socksServer`	Specify the host name or IP address and port of the SOCKS5 proxy it should connect to for forwarding data. Specify one of `host:port` or `IP address:port`. Specify both the host name or the IP address and the port. You must specify this attribute to enable SOCKS5 support.	N/A
`socksUsername`	(Optional) Specifies the username to authenticate to the SOCKS5 proxy host if it demands authentication during the connection phase.	N/A
`socksPassword`	(Optional) Specifies the password when authenticating into a SOCKS5 proxy host that demands authentication during the connection phase. The forwarder obfuscates this password when it loads the configuration that is associated with the stanza.	N/A
`socksResolveDNS`	(Optional) Specify whether or not the forwarder should use DNS to resolve the host names of indexers in the output group before passing that information on to the SOCKS5 proxy host. When you set this attribute to `true`, the forwarder sends the name of the indexers to the SOCKS5 proxy host as is, and the SOCKS5 proxy host must then resolve the indexer host names through DNS. Set to `true` if, for example, the forwarder and the proxy server are on different networks served by different DNS servers. When you set it to `false`, the forwarder attempts to resolve the indexer host names through DNS itself, and if it is successful, sends the resolved IP addresses of the indexers to the SOCKS5 proxy host. This attribute only applies if you specify host names for indexers in the `[tcpout]` or `[tcpout-server]` stanzas. If you specify IP addresses, DNS resolution does not happen.	`false`

Examples of SOCKS5 support

Here are some examples of `outputs.conf` stanzas with SOCKS5 proxy support enabled:

This example establishes a connection to a SOCKS5 proxy host that forwards the data to indexers beyond the host:

```
[tcpout]
defaultGroup = proxy_indexers

[tcpout:proxy_indexers]
server = indexer1.slapstick.com:9997, indexer2.slapstick.com:9997
socksServer = prx.slapstick.com:1080
```

This example uses credentials to authenticate into the proxy host before attempting to send data, and tells the proxy host to resolve DNS to determine the indexers to connect for sending data:

```
[tcpout]
defaultGroup = socksCredentials

[tcpout:socksCredentials]
server = indexer3.slapstick.com:9997
socksServer = prx.slapstick.com:1081
socksUsername = proxysrv
socksPassword = letmein
socksResolveDNS = true
```

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 immediate forwarder.

Configure intermediate forwarding

Set up the intermediate forwarding tier

1. Install the universal forwarder. If you install the universal forwarder on Windows, you can specify the receiving indexer that the forwarder should send data to during the installation process.

2. Configure the forwarder to send data to the receiving indexer.

3. Edit `inputs.conf` to configure the forwarder to receive data.

4. (Optional) Edit `inputs.conf` to configure any local data inputs on the forwarder.

5. Restart the forwarder.

You can repeat these steps to add more forwarders to the 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 case, the intermediate forwarder is the receiver.

3. Configure local data inputs on the forwarder.

4. Restart the forwarder.

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.

Configure a forwarder to handle multiple pipeline sets

You can configure a forwarder to use multiple processing pipelines to increase forwarding throughput for machines that forward a large amount of data and have more than one core available.

Forwarding pipelines

The universal forwarder can be configured to handle multiple pipeline sets. A pipeline set is an instance of the event processing section of the data pipeline. A universal forwarder with multiple pipeline sets can process multiple events at once, thus increasing forwarder throughput and getting events to indexers faster. The feature that both indexers and forwarders use to handle multiple streams is called **index parallelization**.

Other than the fact that the forwarders can send more than one stream of data at a time, forwarders with parallelization enabled look just like other forwarders to indexers. As well, indexers process data streams from forwarders with parallelization enabled in the same way that they process forwarders with one data stream.

While it is possible to increase the number of pipelines by any number, you should not increase it to more than two unless you receive instruction to do so by Splunk Professional Services.

When you enable multiple pipeline sets on a forwarder, any throughput-related settings apply to each pipeline set on the forwarder, rather than to the forwarder itself. For example, if you have two pipeline sets enabled on a forwarder, the maximum network throughput default of 256KBps (2 Mbps) is for each pipeline, for a total of 512KBps (4Mbps) for the forwarder.

For more information about how forwarders use parallelization to process more data, see Forwarders and multiple pipeline sets in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

Configure a universal forwarder to use multiple pipeline sets

1. At a command or shell prompt on the universal forwarder, change to the local configuration directory:

Unix	Windows
`cd $SPLUNK_HOME/etc/system/local`	`cd %SPLUNK_HOME%\etc\system\local`

2. Create the file `server.conf` in this directory.

3. Open the `server.conf` file for editing.

4. Add the following stanza to enable parallelization:

```
[general]
parallelIngestionPipelines = 2
```

5. Save the file and close it.

6. Restart the universal forwarder.

Configure forwarding to Splunk Enterprise indexer clusters

If you have Splunk Enterprise, you can send data from universal forwarders to indexers that participate in an indexer cluster.

Use forwarders with indexer clusters for the following reasons:

- **To ensure that all incoming data gets indexed.** By activating the forwarder's optional **indexer acknowledgment** feature, you can ensure that all incoming data gets indexed and stored on the cluster. See How indexer acknowledgment works in *Managing Indexers and Clusters of Indexers*.
- **To handle potential node failure.** With **load-balanced** forwarders, if one peer in the group goes down, the forwarder continues to send its data to the remaining peers in the group. See How load balancing works in *Managing Indexers and Clusters of Indexers*.
- **To simplify the process of connecting data sources and peer nodes.** By enabling indexer discovery on your forwarders, the forwarders automatically load balance across all available peer nodes, including any that are later added to the cluster. See Advantages of the indexer discovery method in *Managing Indexers and Clusters of Indexers*.

Configure forwarders to interact with indexer clusters

To use forwarders to get data into clusters, you must perform two types of configuration:

- Connect forwarders to peer nodes.
- Configure the forwarders' data inputs.

Before you continue, you must be familiar with forwarders and how to use them to get data into Splunk Enterprise. For an introduction to forwarders, see About forwarding and receiving.

Connect forwarders to peer nodes

There are two ways to connect forwarders to peer nodes:

- **Use the indexer discovery feature.** With **indexer discovery**, each forwarder queries the master node for a list of all peer nodes in the cluster. It then uses load balancing to forward data to the set of peer nodes. In the case of a multisite cluster, a forwarder can optionally query the master for a list of all peers on a single site. For the procedure on using index discovery, see Use indexer discovery to connect forwarders to peer nodes.
- **Connect forwarders directly to peer nodes.** This is the traditional method for establishing forwarder/indexer connectivity. You specify the peer nodes directly on the forwarders as **receivers.** See Connect forwarders directly to peer nodes in *Managing Indexers and Clusters of Indexers*.

Advantages of the indexer discovery method

Indexer discovery has advantages over the traditional method:

- When new peer nodes join the cluster, you do not need to reconfigure and restart your forwarders to connect to the new peers. The forwarder automatically gets the updated list of peers from the master. It uses load balancing to forward to all peers in the list.
- You can add new forwarders without needing to determine the current set of cluster peers. You just configure indexer discovery on the new forwarders.
- You can use **weighted load balancing** when forwarding data across the set of peers. With indexer discovery, the master can track the amount of total disk space on each peer and communicate that information to the forwarders. The forwarders then adjust the amount of data they send to each peer, based on the disk capacity.

Configure the data inputs to each forwarder

After you specify the connection between the forwarders and the receiving peers using the method you prefer, you must specify the data inputs to each forwarder, so that the forwarder has data to send to the cluster. You usually do this by editing `inputs.conf` on each forwarder.

Read the *Getting Data In* manual, starting with What Splunk can index for detailed information on configuring data inputs. The Use forwarders topic in that manual provides an introduction to specifying data inputs on forwarders.

How indexer acknowledgment works

To ensure end-to-end data fidelity, you must explicitly enable indexer acknowledgment on each forwarder sending data to the cluster.

In brief, indexer acknowledgment works like this: The forwarder sends data continuously to the receiving peer, in blocks of approximately 64kB. The forwarder maintains a copy of each block in memory until it gets an acknowledgment from the peer. While waiting, it continues to send more data blocks.

If all goes well, the receiving peer:

- Receives the block of data, parses and indexes it, and writes the data (raw data and index data) to the file system.
- Streams copies of the raw data to each of its target peers.
- Sends an acknowledgment back to the forwarder.

The acknowledgment assures the forwarder that the data was successfully written to the cluster. Upon receiving the acknowledgment, the forwarder releases the block from memory.

If the forwarder does not receive the acknowledgment, that means there was a failure along the way. Either the receiving peer went down or that peer was unable to contact its set of target peers. The forwarder then automatically resends the block of data. If the forwarder uses load-balancing, it sends the block to another receiving node in the load-balanced group. If the forwarder is not set up for load-balancing, it attempts to resend data to the same node as before.

For more information on how indexer acknowledgment works, see Protect against loss of in-flight data in this manual.

How load balancing works

In load balancing, the forwarder distributes incoming data across several receiving peer nodes. Each node gets a portion of the total data, and together the receiving nodes get all the data.

Splunk forwarders perform automatic load balancing. The forwarder routes data to different nodes based on a specified time interval. For example, assume you have a load-balanced group consisting of three peer nodes: A, B, and C. At the interval specified by the `autoLBFrequency` attribute in `outputs.conf` (30 seconds by default), the forwarder switches the data stream to another node in the group, selected at random. So, every 30 seconds, the forwarder might switch from node B to node A to node C, and so on. If one node is down, the forwarder immediately switches to another.

To expand on this, each of the inputs on the forwarder has its own data stream. At the specified interval, the forwarder switches the data stream to the newly selected node, if it is safe to do so. If it cannot safely switch the data stream to the new node, it keeps the connection to the previous node open and continues to send the data stream to that node until it has been safely sent.

Load balancing, in conjunction with indexer acknowledgment, is of key importance in a clustered deployment because it helps ensure that you don't lose any data in case of a node failure. If a forwarder does not receive indexer acknowledgment from the node it sends data to, it resends the data to the next available node in the load-balanced group.

Forwarders that use the indexer discovery feature always use load balancing to send data to the set of peer nodes. You can enable weighted load balancing, which means that the forwarder distributes data based on the amount of disk capacity on each peer. For example, a peer with a 400GB disk receives twice the data of a peer with a 200GB disk. See Use weighted load balancing in *Managing Indexers and Clusters of Indexers*.

For further information on:

- Load balancing with indexer discovery, see Use indexer discovery to connect forwarders to peer nodes in *Managing Indexers and Clusters of Indexers*.
- load balancing without indexer discovery, see Configure load balancing.
- how load balancing works with indexer acknowledgment, see Protect against loss of in-flight data.

Control forwarder access

If you have Splunk Enterprise, you can control how forwarders connect to receiving indexers with tokens. When you assign a token to a receiving indexer, any forwarders that connect to it must provide that token before they can forward data to it. Forwarder access control is different than a Secure Sockets Layer configuration and can be used in environments that do not have SSL enabled between Splunk instances.

Prerequisites to configuring forwarder access control

You must use the REST API to create, configure, and delete tokens. The commands in this topic use the `curl` command-line tool.

While this tool is available on most *nix systems, you must download a separate executable on Windows systems as there is no native default. You can get it at the cURL website.

You must reference tokens with configuration files.

Forwarder-indexer communication

When you configure tokens on the universal forwarder and indexer, the following communication happens when a forwarder connects to send data:

- 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 connection and sets up the data stream.
- If the tokens do not match, the indexer rejects the connection and logs an entry in `splunkd.log`.

Generate a token

Before you can configure token-based forwarding, you must generate at least one token to use.

1. From a command or shell prompt on the indexer where you want to generate the token, 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=<name>"
```

In this command:

- `user` and `password` are the credentials you use to log into the Splunk Enterprise indexer.
- `host` is the host name or IP address of the indexer.
- `management_port` is the TCP management port on the indexer.
- `name` is the friendly name that you want to assign the token.

For example, to create a token called `my_token` on the `idx1.mycompany.com` instance with the standard user and password for the `admin` user:

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

The host responds with:

```
token=808F7BD7-1444-4910-B8F5-87B83D694E18
```

This is the Globally Unique Identifier (GUID).

Enable a token

1. From a command or shell prompt, run:

```
curl -v -k  -X "POST" -u <user>:<password>
https://idx1.mycompany.com:8089/services/data/inputs/tcp/splunktcptoken/tok1/enable
```

Disable a token

1. From command or shell prompt, run:

```
curl -v -k  -X "POST" -u <username>:<password>
https://idx1.mycompany.com/services/data/inputs/tcp/splunktcptoken/my_token/disable
```

Delete a token

To change a token, issue the following command:

```
curl -v -k -X "DELETE" -u <username>:<password>
https://idx1.mycompany.com:8089/services/data/inputs/tcp/splunktcptoken/my_token
```

Configure the indexer with the token

Before you can control forwarders with tokens, set up the indexer with the token you generated. Edit inputs.conf on the forwarder to specify a special stanza along with the token that you generated.

1. Configure the indexer as a receiving indexer.

2. From a shell or command prompt on the indexer, edit `inputs.conf`:

```
vi $SPLUNK_HOME/etc/system/local/inputs.conf
```

3. In this file, add the following stanza:

```
[splunktcptoken://my_token]
disabled = 0
token = 808F7BD7-1444-4910-B8F5-87B83D694E18
```

4. Save `inputs.conf` and close it.

5. Restart the indexer.

Configure the forwarder with the token

Configure forwarders with the new token. You can specify tokens in `tcpout` and load balancing groups. See Configure forwarding with outputs.conf.

1. From a shell or command prompt on the forwarder, edit `outputs.conf`:

```
vi $SPLUNK_HOME/etc/system/local/outputs.conf
```

2. Add the following stanza:

```
[tcpout]
server=idx1.mycompany.com:9997
token = 08F7BD7-1444-4910-B8F5-87B83D694E18
...
```

3. Save the file and close it.

4. Restart the universal forwarder.

Confirm that the forwarder and indexer can communicate with the tokens

On the indexer, review `splunkd.log` for information about forwarder attempts to communicate with an indexer that has tokens enabled.

A forwarder that does not have the correct token generates this output:

```
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 that has an enabled token generates this output:

```
ERROR TcpInputProc - Exception: Token not sent by forwarder src=127.0.0.1:58796! for data received from
src=127.0.0.1:58796
```

In either case, the indexer terminates the connection to the forwarder.

A forwarder that does not submit the right token to an indexer that asks for one does not generate an error. It does not forward data to that indexer.

Protect against loss of in-flight data

To guard against loss of data when **forwarding** to an **indexer**, you can use the **indexer acknowledgment** capability. With indexer acknowledgment, the **forwarder** will resend any data not acknowledged as "received" by the indexer.

You enable indexer acknowledgment on the forwarder in `outputs.conf`. By default, the feature is not active.

Indexer acknowledgment and indexer clusters

When you use forwarders to send data to peer nodes in an indexer cluster, it is a best practice to enable indexer acknowledgment. To learn more about forwarders and indexer clusters, including indexer acknowledgement and indexer clusters, see Use forwarders to get your data in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

How indexer acknowledgment works in normal operation

The forwarder sends data continuously to the indexer, in blocks of approximately 64kB. The forwarder maintains a copy of each block in memory, in its wait queue, until it gets an acknowledgment from the indexer. While waiting, it continues to send more data blocks.

During normal operation, the indexer:

- Receives a block of data.
- Parses the data.
- Writes the data to the file system as events (raw data and index data).
- Sends an acknowledgment to the forwarder.

The acknowledgment tells the forwarder that the indexer received the data and successfully wrote it to the file system. Upon receiving the acknowledgment, the forwarder releases the block from memory.

If the wait queue is of sufficient size, it does not fill up while waiting for acknowledgments to arrive. It can, however, fill up quickly if network or hardware conditions prevent acknowledgments from getting back to the forwarder. See Indexer acknowledgment and forwarded data throughput for issues and ways to address them.

Note: To accommodate the data availability requirements of indexer clusters, the process of acknowledgement works somewhat differently with indexer clusters. To learn more about indexer acknowledgement and indexer clusters, see Use forwarders to get your data in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

How indexer acknowledgment works when a failure occurs

When there is a failure in the round-trip process, the forwarder does not receive an acknowledgment. At this point it attempts to resend the block of data.

Reasons for lack of indexer acknowledgment

These are the reasons that a forwarder might not receive acknowledgment:

- Indexer goes down after receiving the data, possibly due to a hardware failure.
- Indexer is unable to write to the file system, possibly because the disk is full.
- Network goes down while acknowledgment is en route to the forwarder.

How the forwarder handles lack of indexer acknowledgments

After the forwarder sends a data block, it maintains a copy of the data in its wait queue until it receives an acknowledgment. Meanwhile, it continues to send additional blocks. If the forwarder doesn't get acknowledgment for a block within 300 seconds (by default), it closes the connection.

If the forwarder is in an **auto-load-balancing** configuration, it then opens a connection to the next indexer in the group (if one is available) and sends the data to it. If the forwarder is not set up for auto-load balancing, it attempts to open a connection to the same indexer as before and resend the data.

The forwarder maintains the data block in the wait queue until acknowledgment is received. After the wait queue fills up, the forwarder stops sending additional blocks until it receives an acknowledgment for one of the blocks, at which point it can free up space in the queue.

You can change the wait time by setting the `readTimeout` attribute in `outputs.conf`.

Other reasons the forwarder might close a connection to the indexer

There are three conditions that can cause the forwarder to close the network connection:

- *Read timeout.* The forwarder doesn't receive acknowledgment within 300 (default) seconds. This is the condition described above.
- *Write timeout.* The forwarder is not able to finish a network write within 300 (default) seconds. The value is configurable in `outputs.conf` by setting `writeTimeout`.
- *Read/write failure.* This condition usually happens because the indexer has crashed or the network has failed.

In all these cases, the forwarder attempts to open a connection to the next indexer in the load-balanced group, or to the same indexer again if load-balancing is not enabled.

How lack of indexer acknowledgment can cause the duplication of indexed data

It is possible for the indexer to index the same data block twice. This can happen if there is a network problem that prevents an acknowledgment from reaching the forwarder. For instance, assume the indexer receives a data block, parses it, and writes it to the file system. It then generates the acknowledgment. However, on the round-trip to the forwarder, the network goes down, so the forwarder never receives the acknowledgment. When the network comes back up, the forwarder then resends the data block, which the indexer parses and writes as if it were new data.

To deal with such a possibility, every time the forwarder resends a data block, it writes an event to its `splunkd.log` noting

that it's a possible duplicate. The admin is responsible for using the log information to track down the duplicate data on the indexer.

Here's an example of a duplicate warning:

```
10-18-2010 17:32:36.941 WARN  TcpOutputProc - Possible duplication of events with
channel=source::/home/jkerai/splunk/current-install/etc/apps/sample_app
/logs/maillog.1|host::MrT|sendmail|, streamId=5941229245963076846, offset=131072
subOffset=219 on host=10.1.42.2:9992
```

Enable indexer acknowledgment

Configure indexer acknowledgment on the forwarder by setting the `useACK` attribute to `true` in `outputs.conf`

You can set `useACK` either globally or by target group, at the `[tcpout]` or `[tcpout:<target_group>]` stanza levels. You cannot set it for individual receiving indexers at the `[tcpout-server: ...]` stanza level.

For more information, see the outputs.conf spec file.

```
[tcpout:<target_group>]
server=<server1>, <server2>, ...
useACK=true
```

Identify data duplication when indexer acknowledgement is enabled

When `useACK` is enabled in the `outputs.conf` on forwarders, and there is either a network issue, indexer saturation (for example, pipeline blocks) or a replication problem, your Splunk platform deployment's indexers cannot respond to your deployment's forwarders acknowledgement. Based on your deployment environment, use the `_event_status::resent` field to create a search that can validate data duplication. For example:

Example 1

1. Run the following search in order to identify events that have been resent by forwarders:

   ```
   index=<prod-index> sourcetype=<prod-sourcetype> _event_status::resent
   ```

2. Run the following Splunk search to verify the resent events are really duplicates.

   ```
   index=<prod_index> sourcetype=<prod_sourcetype> NOT _event_status="*" earliest=<earliestTime>
   latest=<latestTime> [ search index=<prod_index> sourcetype=<prod_sourcetype> _event_status::resent
   earliest=<earliestTime> latest=<latestTime> | fields _time, source, sourcetype, host, _raw ]
   ```

It is a best practice to minimize the search time range as much as possible to avoid potential search performance issues caused by too much data.

Example 2

1. Run the following search in order to identify events that have been resent by forwarders:

   ```
   index=<prod-index> sourcetype=<prod-sourcetype> _event_status::resent
   ```

2. If events contain a unique field, use that unique field to confirm duplicates. For example:

```
index=<prod_index> sourcetype=<prod_sourcetype> NOT _event_status="*" earliest=<earliestTime>
latest=<latestTime> [ search index=<prod_index> sourcetype=<prod_sourcetype> _event_status::resent
earliest=<earliestTime> latest=<latestTime> | fields sourcetype, <uniqueFieldName>]
```

Resent events are not always duplicate events. To clean up duplicates, pipe your search to the `| delete` search command. Verify that the data is really a duplicate before deleting.

Indexer acknowledgment and forwarded data throughput

The forwarder uses a wait queue to manage the indexer acknowledgment process. This queue has a default maximum size of 21MB, which is generally sufficient. In rare cases, you might need to manually adjust the wait queue size.

If you want more information about the wait queue, read this section. It describes how the wait queue functions as well as how to configure it.

How the wait queue size is configured

You do not set the wait queue size directly. Instead, you set the size of the in-memory output queue, and the wait queue sets to three times the output queue size. To configure the output queue size, use the `maxQueueSize` attribute in `outputs.conf`.

The default for the `maxQueueSize` attribute is `auto`. This is the recommended setting. It optimizes the queue sizes, based on whether indexer acknowledgment is active:

- When `useACK=true`, the output queue size is 7MB and the wait queue size is 21MB.
- When `useACK=false`, the output queue size is 500KB.

You can set `maxQueueSize` to specific values if necessary. See the outputs.conf spec file for further details on `maxQueueSize`.

Note: When you turn on indexer acknowledgment, the increase in queue size takes effect only after you restart the forwarder.

Why the wait queue matters

If you enable indexer acknowledgment, the forwarder uses a wait queue to manage the acknowledgment process. Because the forwarder sends data blocks continuously and does not wait for acknowledgment before sending the next block, its wait queue maintains many blocks, each waiting for its acknowledgment. The forwarder continues to send blocks until its wait queue is full, at which point forwarding stops. The forwarder then waits until it receives an acknowledgment, which lets it release a block from its queue and thus resume forwarding.

A wait queue can fill up when something is wrong with the network or indexer. It can also fill up even when the indexer functions normally. This is because the indexer only sends the acknowledgment after it has written the data to the file system. Any delay in writing to the file system slows the pace of acknowledgment, which can lead to a full wait queue.

There are a few reasons that a normal functioning indexer might delay writing data to the file system (and thus delay sending acknowledgments):

- The indexer is very busy. For example, at the time the data arrives, the indexer might be dealing with multiple search requests or with data coming from a large number of forwarders.
- The indexer receives too little data.

For efficiency, an indexer only writes to the file system periodically -- either when a write queue fills up or after a timeout of a few seconds. If a write queue is slow to fill up, the indexer waits until the timeout to write. If data comes from only a few forwarders, the indexer can end up in the timeout condition, even if each of those forwarders sends a normal quantity of data. Since write queues exist on a per-hot-bucket basis, the condition occurs when a particular bucket gets only a small amount of data. Usually this means that a particular index gets only a small amount of data.

To ensure that throughput does not degrade because of a stalled forwarder, retain the default setting of `maxQueueSize=auto`. In rare cases, you might need to increase the wait queue size so that the forwarder has sufficient space to maintain all blocks in memory while waiting for acknowledgments to arrive. On the other hand, if you have many forwarders feeding a single indexer and a moderate number of data sources per forwarder, you might be able to conserve a few megabytes of memory by using a smaller size.

When the receiver is a forwarder

You can also use indexer acknowledgment when the data transmission occurs via an intermediate forwarder; that is, where an originating forwarder sends the data to an intermediate forwarder, which then forwards it to the indexer. For this scenario, if you want to use indexer acknowledgment, it is recommended that you enable it along all segments of the data transmission. That way, you can ensure that the data gets delivered along the entire path from originating forwarder to indexer.

Assume you have an originating forwarder that sends data to an intermediate forwarder, which in turn forwards that data to an indexer. To enable indexer acknowledgment along the entire line of transmission, you must enable it twice: first for the segment between originating forwarder and intermediate forwarder, and again for the segment between intermediate forwarder and indexer.

If you enable both segments of the transmission, the intermediate forwarder waits until it receives acknowledgment from the indexer and then it sends acknowledgment back to the originating forwarder.

However, if you enable just one of the segments, you only get indexer acknowledgment over that part of the transmission. For example, say indexer acknowledgment is enabled for the segment from originating forwarder to intermediate forwarder but not for the segment from intermediate forwarder to indexer. In this case, the intermediate forwarder sends acknowledgment back to the originating forwarder as soon as it sends the data on to the indexer. It then relies on TCP to safely deliver the data to the indexer. Because indexer acknowledgment is not enabled for this second segment, the intermediate forwarder cannot verify delivery of the data to the indexer. This second case has limited value and is not recommended.

Migrate from Splunk light forwarders

Migrate from a light forwarder

The universal forwarder provides the functionality of the **light forwarder** but in a smaller resource footprint with better performance. You can migrate your existing light forwarder installations to universal forwarders. Splunk provides tools that ease the migration process and ensure that the new universal forwarder does not send an indexer any data already sent by the old light forwarder.

You can migrate from light forwarders of version 4.0 or later of Splunk Enterprise.

How to migrate a forwarder

Migration is available as an option during the universal forwarder installation process. See Migrate a Windows light forwarder or Migrate a nix light forwarder for migration instructions. After you complete the migration and confirm that the universal forwarder is active, uninstall the old light forwarder.

What migration does

Migration copies checkpoint data, including the fishbucket directory, from the old forwarder to the new universal forwarder. This prevents the universal forwarder from resending data that the previous forwarder had already sent to an indexer. This in turn avoids unnecessary re-indexing, ensuring that you maintain your statistics and keep your license usage under control.

What migration does not do

Migration does not copy any configuration files, such as `inputs.conf` or `outputs.conf`. This is because it would not be possible to conclusively determine where all existing versions of configuration files reside on the old forwarder. Therefore, you still need to configure your data inputs and outputs, either during installation or later. If you choose to configure later, you can copy over the necessary configuration files manually or you can use the deployment server to push them out to all your universal forwarders. See Configure the universal forwarder for information on configuration files.

If the data inputs for the universal forwarder differ from the old forwarder, you can still migrate. The universal forwarder ignores migrated checkpoint data that pertains to any unconfigured inputs. If you decide to add those inputs later, the universal forwarder uses the migrated checkpoints to determine where in the data stream to start forwarding.

Migration also does not copy over any apps from the light forwarder. If you have any apps that you want to migrate to the universal forwarder, you must do so manually.

Migrate a Windows light forwarder

If you want to replace an existing light forwarder with a universal forwarder, you need to first migrate its checkpoint data to the new forwarder. Checkpoint data is internal data that the forwarder compiles to keep track of what data it has already forwarded to an indexer. By migrating the checkpoint data, you prevent the new universal forwarder from forwarding any data already sent by the old light forwarder. This ensures that the same data does not get indexed twice.

You can migrate checkpoint data from an existing Windows light forwarder (version 4.0 or later) to the universal forwarder. For an overview of migration, see Migrate from a light forwarder.

If you want to migrate, do so during the installation process. You cannot migrate after an installation.

You must install the universal forwarder in a different directory from the existing light forwarder. Since the default install directory for the universal forwarder is `C:\Program Files\SplunkUniversalForwarder` and the default install directory for full Splunk Enterprise (including the light forwarder) is `C:\Program Files\Splunk`, you'll be safe if you just stick with the defaults.

You perform a Windows installation with either the installer GUI or the command line:

- If you use the installer GUI, one of the screens will prompt you to migrate. See Install a Windows universal forwarder from an installer for a walkthrough of the GUI installation procedure.
- If you install using the command line, the flag `MIGRATESPLUNK=1` specifies migration. See Deploy a Windows universal forwarder from the command line for a list of supported flags and how to use them to configure your installation.

What the installer does when you migrate a light forwarder

Whichever installation method you use, the Windows installer performs the following actions:

- Searches for an existing heavy or light forwarder on the machine.
- Determines whether the forwarder is eligible for migration (must be at version 4.0 or above).
- If it finds an eligible forwarder, the GUI offers you the option of migrating. (The command line installer looks to see whether the `MIGRATESPLUNK=1` flag exists.)
- If you specify migration (or the `MIGRATESPLUNK=1` flag exists), the installer shuts down any running services for the existing forwarder. It also sets the startup type of the services to manual, so that they don't start up again upon reboot.
- Migrates the checkpoint files to the universal forwarder.
- Completes installation and configuration of the universal forwarder.

Perform additional configuration after the migration completes

At the end of this process, you might want to perform additional configuration on the universal forwarder. Since the migration process only copies checkpoint files, you should check or manually copy over the old forwarder `inputs.conf` configuration file.

Once the universal forwarder is up and running (and after you have ensured that migration worked correctly), you can uninstall the old forwarder.

Migrate a *nix light forwarder

If you want to replace an existing light forwarder with a universal forwarder, you need to first migrate its checkpoint data to the new forwarder. Checkpoint data is internal data that the forwarder compiles to keep track of what data it has already forwarded to an indexer. By migrating the checkpoint data, you prevent the new universal forwarder from forwarding any data already sent by the old light forwarder. This ensures that the same data does not get indexed twice.

You can migrate checkpoint data from an existing *nix light forwarder (version 4.0 or later) to the universal forwarder. For an overview of migration, see Migrate from a light forwarder.

Install the universal forwarder into a different directory from the existing light forwarder.

You must migrate a light forwarder the first time you start the universal forwarder. It is not possible to migrate later.

1. Stop the existing forwarder:

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

2. Complete the basic installation of the universal forwarder. Do not start the universal forwarder yet.

3. In the universal forwarder installation directory, create a file named `old_splunk.seed`. For example, if you installed the UF into `/opt/splunkforwarder`, create `/opt/splunkforwarder/old_splunk.seed`.

4. Edit this file so that it contains a single line that references the path of the old forwarder installationdirectory. For example, if the old forwarder was located in `/opt/splunk` add the line:

```
/opt/splunk
```
.

5. Save the file and close it.

6. Start the universal forwarder:

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

The universal forwarder migrates the checkpoint files from the forwarder specified in the `$SPLUNK_HOME/old_splunk.seed` file. Migration only occurs the first time you run the `start` command. You can leave the `old_splunk.seed` in place, The forwarder examines the file only the first time you start the forwarder after you install it.

7. Perform additional configuration of the universal forwarder, as described in Install a nix universal forwarder. Because the migration process only copies checkpoint files, review or copy over the old forwarder `inputs.conf` configuration file.

8. After the universal forwarder is up and running (and after you have ensured that migration worked correctly), uninstall the old forwarder.

Troubleshoot forwarding

Troubleshoot the universal forwarder with Splunk Enterprise

Receiver doesn't accept new connections on its receiving port

If the internal queue on the receiving indexer gets blocked, the indexer shuts down the receiving/listening (`splunktcp`) port after a specified interval of being unable to insert data into the queue. Once the queue is again able to start accepting data, the indexer reopens the port.

However, sometimes (on Windows machines only) the indexer is unable to reopen the port once its queue is unblocked. To remediate, you must restart the indexer.

If you find you have this issue, you can set the `stopAcceptorAfterQBlock` attribute in inputs.conf on the receiver to a higher value, so that it does not close the port as quickly. This attribute determines the amount of time the indexer waits before closing the port. The default is 300 seconds (five minutes).

If you are using load-balanced forwarders, they will switch their data stream to another indexer in the load-balanced group based to their time-out interval, set in outputs.conf with the `writeTimeout` attribute. This results in automatic failover when the receiving indexers have blocked queues.

Confusing the receiving and management ports

As part of setting up a forwarder, you specify the receiver `hostname/IP_address` and receiving `port`. The forwarder uses these to send data to the receiver. Be sure to specify the port that you designated as the receiving port at the time the receiver was configured. If you mistakenly specify the management port, the receiver will generate an error similar to this:

```
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error = error:140760FC:SSL
routines:SSL23_GET_CLIENT_HELLO:unknown protocol
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - ACCEPT_RESULT=-1 VERIFY_RESULT=0
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error for fd from HOST:localhost.localdomain,
IP:127.0.0.1, PORT:53075
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error = error:140760FC:SSL
routines:SSL23_GET_CLIENT_HELLO:unknown protocol
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - ACCEPT_RESULT=-1 VERIFY_RESULT=0
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error for fd from HOST:localhost.localdomain,
IP:127.0.0.1, PORT:53076
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error = error:140760FC:SSL
routines:SSL23_GET_CLIENT_HELLO:unknown protocol
splunkd.log:03-01-2010 13:35:28.654 ERROR TcpInputFd - ACCEPT_RESULT=-1 VERIFY_RESULT=0
splunkd.log:03-01-2010 13:35:28.654 ERROR TcpInputFd - SSL Error for fd from HOST:localhost.localdomain,
IP:127.0.0.1, PORT:53077
splunkd.log:03-01-2010 13:35:28.654 ERROR TcpInputFd - SSL Error = error:140760FC:SSL
routines:SSL23_GET_CLIENT_HELLO:unknown protocol
splunkd.log:03-01-2010 13:35:28.654 ERROR TcpInputFd - ACCEPT_RESULT=-1 VERIFY_RESULT=0
```

Receiver indexer closes receiving socket

If a receiving indexer's queues become full, it closes the receiver socket to prevent additional forwarders from connecting to it. If a forwarder with load-balancing enabled can no longer forward to that receiver, it sends its data to another indexer on its list. If the forwarder does not employ load-balancing, it holds the data until you resolve the problem.

The receiver socket reopens automatically when the queue gets unclogged.

Typically, a receiver gets behind on the data flow because it can no longer write data due to a full disk or because it is itself attempting to forward data to another Splunk Enterprise instance that is not accepting data.

The following warning message will appear in `splunkd.log` if the socket gets blocked:

```
Stopping all listening ports. Queues blocked for more than N seconds.
```

This message will appear when the socket reopens:

```
Started listening on tcp ports. Queues unblocked.
```

Release Notes

Known issues

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

Date filed	Issue number	Description
2018-04-10	SPL-153251	Universal Forwarder txz package cannot be installed on FreeBSD 11.1 Workaround: 1. Use pkg install instead of pkg add OR 2. Install package by untarring tgz file to /opt/splunkforwarder
2015-04-14	SPL-99687, SPL-129637	Splunk universal forwarder is 7-10 days behind recent Windows Security and system log events. Workaround: To mitigate this, edit the following stanza in inputs.conf: [WinEventLog://Security] evt_resolve_ad_obj = 0.
2015-04-07	SPL-99316	Universal Forwarders stop sending data repeatedly throughout the day Workaround: In limits.conf, try changing file_tracking_db_threshold_mb in the [inputproc] stanza to a lower value.
2014-08-05	SPL-88396	After configuring a client name for a deployment client, the name is not shown in the Forwarder Management UI Workaround: Create a server class, where you can see the client name, and use that group when you add data.

Fixed issues

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

8.0.4

Version 8.0.4 was released on May 21, 2020. This release fixes the following universal forwarder issue.

Date resolved	Issue number	Description
2020-03-31	SPL-185540, SPL-183953	Batch Stanza deleting file upon restart/read completion

8.0.3

Version 8.0.3 was released on April 1, 2020. This release fixes the following universal forwarder issue.

Date resolved	Issue number	Description
2020-02-27	SPL-184043, SPL-157269	High CPU usage originating from Splunk UF on macOS devices

8.0.2

Version 8.0.2 was released on February 11, 2020. No new universal forwarder issues are fixed in this release.

8.0.1

Version 8.0.1 was released on December 12, 2019. This release fixes the following universal forwarder issue.

Date resolved	Issue number	Description
2019-11-25	SPL-171961	Unpatched universal forwarders that process structured data, process data locally, or encounter unknown file types with a monitor input experience problems with timestamp extraction beginning on January 1, 2020. See Timestamp recognition of dates with two-digit years fails beginning January 1, 2020 for information and solutions.

8.0.0

Version 8.0.0 was released on October 22, 2019. No new universal forwarder issues are fixed in this release.

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.