**Installation on Windows Servers**

* Download the forwarder from [splunk.com](https://www.splunk.com/en_us/download/universal-forwarder.html)
* For Windows:
  + Install it, and specify **ds.splunk.wustl.edu:8089** on the screen that asks about a deployment server
* Once the forwarder has phoned home to the cluster, assign the appropriate deployment apps
* Help the customer configure etc/system/local/inputs.conf to define what data goes into their database
  + If they have a lot of identical devices we could put a custom input.conf into their deployment app and save them a bit of work

**Installation on Linux Servers**

* Download a current version of the Universal Forwarder: <https://www.splunk.com/en_us/download/universal-forwarder.html>
* sudo yum localinstall splunkforwarder.rpm
* cd /opt/splunkforwarder/bin
* sudo ./splunk start --accept-license
  + Enter a username (admin) and a randomly-generated secure password. This user/pass is specific to Splunk itself and does not create an OS-level user.
  + You'll need to save this password for the next five minutes or so.
* sudo ./splunk stop
  + Yes, you're stopping it immediately after starting it. The above was required to accept the license.
* sudo ./splunk enable boot-start -systemd-managed 1
  + If you prefer not to use systemd, omit the last couple parameters, leaving only "enable boot-start"
* sudo ./splunk set deploy-poll **ds.splunk.wustl.edu:8089**
  + This step will require the user/pass provided above but should never be needed after this point.
  + In some cases, the user/pass aren't required here – we're still working out when that happens, and why. (I believe that installing and running as root negates the requirement for a credential here.)
* sudo ./splunk start

After a few minutes, the forwarder should phone into our deployment server and download additional configuration. Per-logging-source configuration may also be needed but is outside the scope of this document.

**Manual UF Update**

* sudo yum localinstall new.rpm
  + The RPM update normally stops the service
* sudo /opt/splunkforwarder/bin/splunk start --accept-license
  + This *should*restart the service
* sudo systemctl status SplunkForwarder
  + (verify that the forwarder is running properly etc)

**File Permissions and Ownership Concerns**

We have chosen to run Linux forwarders as the root user in most cases, to simplify management. If you want to run Splunk as a non-root user, you'll need to take a few extra steps.

* After installing or updating the forwarder RPM, you'll need to chown -R splunk:splunk /opt/splunkforwarder
* When you enable boot-start, you can add the -user=splunk flag to specify a username
* You'll have to be sure that this user has the right permissions to read the log files you're ingesting.
  + On NTS syslog, for instance, we added the splunk user to the "adm" group.
  + FACLs and SELinux may also come into play; if we run into cases like that we'll add them here.

**Installation on Ubuntu**

* Download a current version of the Universal Forwarder: <https://www.splunk.com/en_us/download/universal-forwarder.html>
* Install is using the below commands based on your Operating system
  + sudo yum localinstall splunkforwarder.rpm
  + sudo dpkg –i splunkforwarder-package.deb
* cd /opt/splunkforwarder/bin
* sudo ./splunk start --accept-license
  + Enter a username (admin) and a randomly-generated secure password. This user/pass is specific to Splunk itself and does not create an OS-level user.
  + You'll need to save this password for the next five minutes or so.
* sudo ./splunk stop
  + Yes, you're stopping it immediately after starting it. The above was required to accept the license.
* sudo ./splunk enable boot-start -systemd-managed 1
  + If you prefer not to use systemd, omit the last couple parameters, leaving only "enable boot-start"
* sudo ./splunk set deploy-poll ds.splunk.wustl.edu:8089
  + This step will require the user/pass provided above, but should never be needed after this point.
  + In some cases, the user/pass aren't required here – we're still working out when that happens, and why. (I believe that installing and running as root negates the requirement for a credential here.)
* sudo ./splunk restart

After a few minutes, the forwarder should phone into our deployment server and download additional configuration. Per-logging-source configuration may also be needed but is outside the scope of this document.

**Manual UF Update**

* sudo yum localinstall new.rpm
  + The RPM update normally stops the service
* sudo /opt/splunkforwarder/bin/splunk start --accept-license
  + This *should*restart the service
* sudo systemctl status SplunkForwarder
  + (verify that the forwarder is running properly etc)

**File Permissions and Ownership Concerns**

We have chosen to run Linux forwarders as the root user in most cases, to simplify management. If you want to run Splunk as a non-root user, you'll need to take a few extra steps.

* After installing or updating the forwarder RPM, you'll need to chown -R splunk:splunk /opt/splunkforwarder
* When you enable boot-start, you can add the -user=splunk flag to specify a username
* You'll have to be sure that this user has the right permissions to read the log files you're ingesting.
  + On NTS syslog, for instance, we added the splunk user to the "adm" group.
  + FACLs and SELinux may also come into play; if we run into cases like that, we'll add them here.

**Installation on Windows Desktops**

* This should be on the domain
* Open Software Center
* Install the Splunk Universal Forwarder package
  + it will be up to date and have all items preconfigured.

**Installation on Windows Desktops**

* This is currently in QA
  + This will also be something that’s preconfigured for machines that are enrolled into JAMF

<https://www.splunk.com/en_us/download/universal-forwarder.html>