



# Splunk Universal Forwarders

By: Ryan Stewart

## Installing Splunk Universal Forwarder for Windows

In this training session, I'll install the Splunk Universal Forwarder in its default configuration to facilitate the sending of Windows logs to Splunk.



### 1. Prepare for Installation:

- Go to the Windows computer.
- Download the Splunk Universal Forwarder setup file.

## Splunk Universal Forwarder 9.0.0.1

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

### Choose Your Installation Package

Windows	Linux	Mac OS	Free BSD	Solaris	AIX
64-bit	Windows 10 , Windows 11 Windows Server 2012, 2012 R2, 2016, 2019, 2022		.msi	75.41 MB	Download Now 
32-bit	Windows 10		.msi	62.49 MB	Download Now 

### 2. MD5 Verification:

- Read the Splunk General Terms and download the MD5 checksum.
- Open the MD5 file and verify the checksum using PowerShell:

```
```powershell
Get-FileHash .\splunkforwarder-9.0.0.1-9e907cedecb1-x64-release.msi -Algorithm md5
```
```

```
PS C:\Users\nucl3arsnake\Downloads> Get-FileHash .\splunkforwarder-9.0.0.1-9e907cedecb1-x64-release.msi -Algorithm md5
```

| Algorithm | Hash                             | Path                             |
|-----------|----------------------------------|----------------------------------|
| MD5       | 183A09C64537832701320609E665E3E7 | C:\Users\nucl3arsnake\Downloa... |

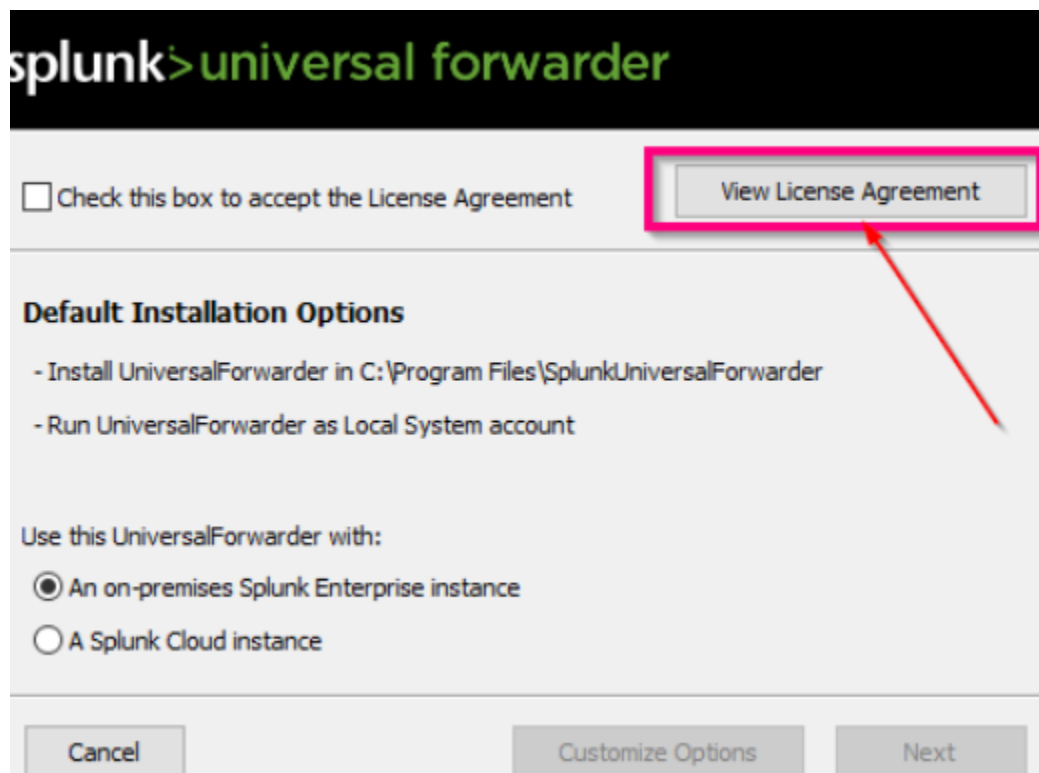
- Confirm that the calculated MD5 matches the provided checksum.

### 3. Launch Setup:

- Launch the setup file and read the License Agreement.

### 4. License Agreement:

- Accept the License Agreement.



- Select "an on-premises Splunk Enterprise instance" for on-premise server installation.

### 5. Configuration:

- Use the default configuration.
- Provide a username for the Universal Forwarder.

UniversalForwarder Setup

splunk>universal forwarder

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:  
localadmin

☒ Generate random password

Password:  
[Empty field]

Confirm password:  
[Empty field]

Cancel Back Next

- Specify the IP or Hostname and port (usually 9997) of the receiving indexer. Use the IP if there is no DNS in your lab.

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

**Receiving Indexer**

Hostname or IP  
192.168.10.1 : 9997

*Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com* *default is 9997*

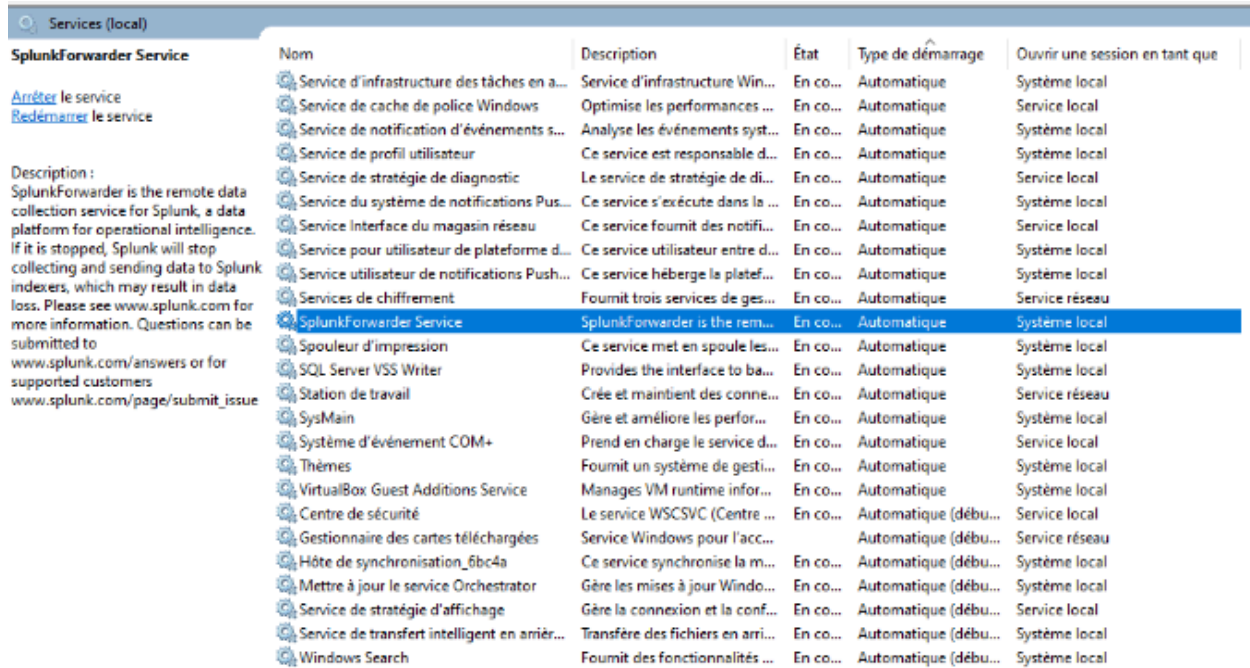
Cancel Back Next

## 6. Installation:

- Launch the installation.

## 7. Check Universal Forwarder Installation:

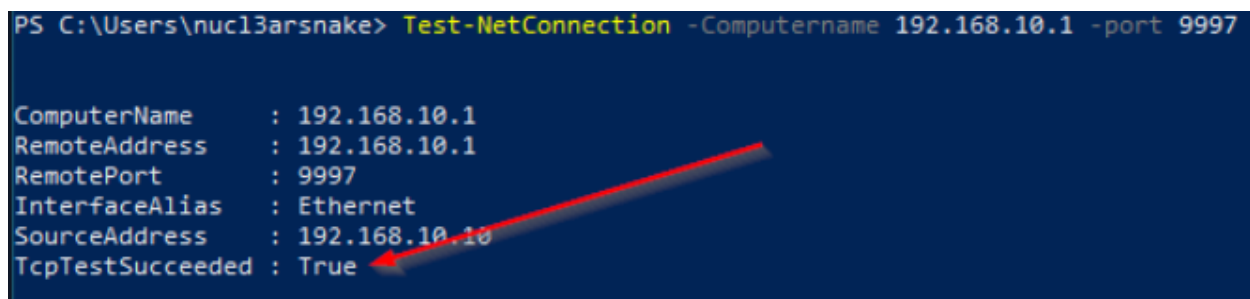
- Open services.msc and confirm that the "SplunkForwarder Service" is running.



- Use PowerShell to check if communication is open:

powershell

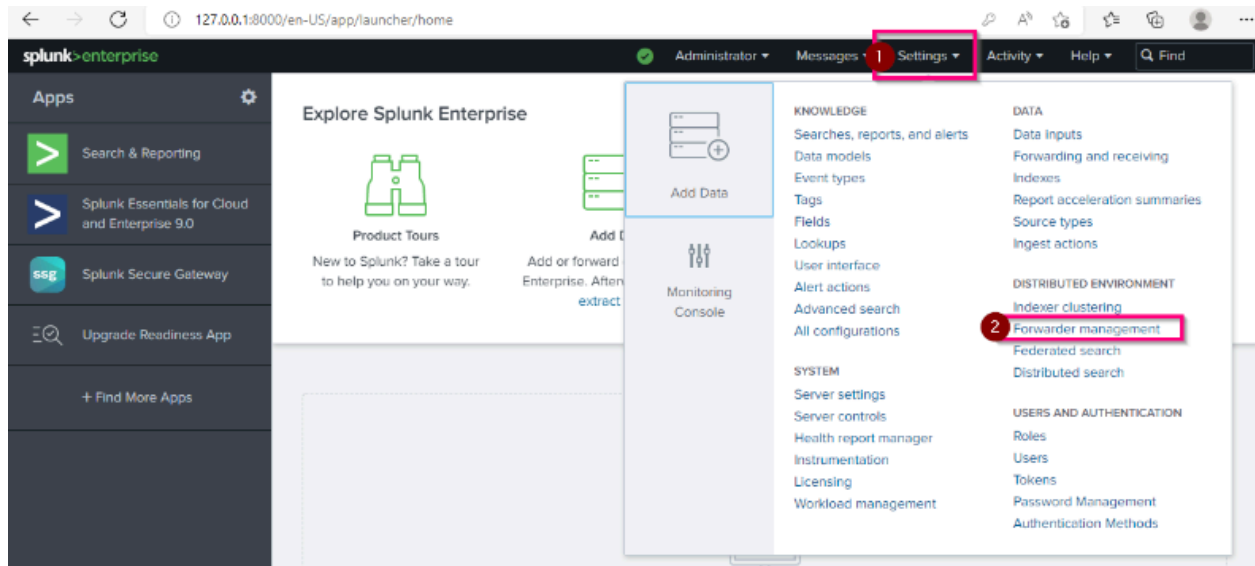
Test-NetConnection -Computername Splunk\_IP -port 9997



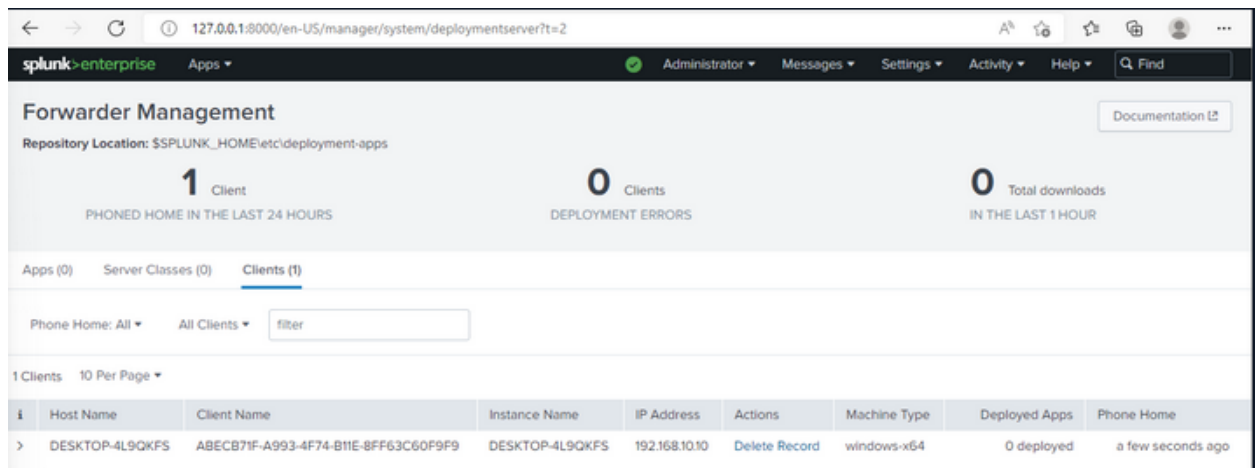
\*Congratulations, Splunk Universal Forwarder for Windows has been successfully installed.\*

## 8. Verify on Splunk:

- Go to your Splunk Server.
- Navigate to Settings > Forwarder management.



- Confirm that your Windows computer is visible on this page.



- If the computer is not visible after a few minutes, restart the Splunk Universal Forwarder service and check the connection between the client and server.