

Standard Operating Procedure

On

**SPLUNK UNIVERSAL FORWARDER**

**INSTALLATION SETUP**

**Security Operations Centre**

**GITC**

**Issue Date: 01/03/2021**

**Version: 2.0**

**Reference Number: S-1**

**Data Classification**

**(As per Data Governance Policy)**

Disclaimer – Please use the below link to access the ISO 9001:2015 compliance instructions –

<https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/documented_information.pdf>

<The ‘Table of Contents’ can be updated through ‘Update Table’ feature made available by clicking on the table>

**Table of Contents**

[1. Introduction 4](#_Toc56702406)

[1.1 Purpose of the Document 4](#_Toc56702407)

[1.2 Prerequisites 4](#_Toc56702408)

[1.3 Scope 4](#_Toc56702409)

[1.4 Document Audience 4](#_Toc56702410)

[1.5 Policy Reference No 4](#_Toc56702411)

[1.6 Version Control 4](#_Toc56702412)

[2. Role of the Department/s 5](#_Toc56702413)

[3. Procedure/Process Flow [To be followed by Application Owner] 6](#_Toc56702414)

[3.1 Objectives 6](#_Toc56702415)

[3.2 Inputs 6](#_Toc56702416)

[3.3 Activities 6](#_Toc56702417)

[3.4 Outputs 9](#_Toc56702418)

[4. Tasks of the Department 11](#_Toc56702419)

[4.1 Purpose 11](#_Toc56702420)

[4.2 Definitions 11](#_Toc56702421)

[4.3 Responsibility 11](#_Toc56702422)

[4.4 Requirements 11](#_Toc56702423)

[4.5 Tools & Information 11](#_Toc56702424)

[4.6 Exception handling 11](#_Toc56702425)

[5. Reference 12](#_Toc56702426)

[6. Troubleshooting/FAQs 13](#_Toc56702427)

[6.1 Port Validation 13](#_Toc56702428)

[7. Do’s & Don’ts 14](#_Toc56702429)

[7.1 Do’s 14](#_Toc56702430)

[7.2 Don’ts 14](#_Toc56702431)

[8. Escalation Matrix [To be filled by Bank] 15](#_Toc56702432)

[8.1 Escalation Level 1 15](#_Toc56702433)

[8.2 Escalation Level 2 15](#_Toc56702434)

[8.3 Escalation Level 3 15](#_Toc56702435)

[Annexure A 16](#_Toc56702436)

[Glossary 17](#_Toc56702437)

# Introduction

The universal forwarder (agent) is a dedicated, streamlined version of Splunk Enterprise (SIEM) that contains only the essential components needed to forward data. This agent is required to be installed on the server where the data source resides.

While it does not have a Web interface, you can still configure, manage, and scale it by editing configuration files.

## Purpose of the Document

The purpose of this document is to provide instructions for downloading, installing and configuring agent on the client server where the data resides. The agent is a separate installation package. The most notable benefit is that it uses significantly fewer hardware resources.

## Prerequisites

Following are the prerequisites for agent installation.

1. Access to the server where the agent is required to be installed.

2. Port 8089 communication (bi-directional) from client to Cluster master and Deployment servers.

3. Port 9997 communication (unidirectional) from client to indexers.

## Scope

The agent is light weight and is required to be installed on the client server (from which the data has to be sent to SIEM) so that the data can be sent on the SIEM Setup.

## Document Audience

The document is intended for Application Owners to install Agents on the client (server from which data has to be forwarded to SIEM)

## Policy Reference No

(Define policy reference no. corresponding to the procedure, if any)

## Version Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Status** | **Revision Details** |
| 31/10/2020 | 1.0 |  |  |  |
| 6/11/2020 | 1.1 |  |  |  |
| 01/03/2021 | 2.0 |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Role of the Department/s

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No | **ACTION** | **ACTION OWNER** | **TIMELINE** |
| 1. | Share the details of the IT assets as per the prescribed format to be integrated with the SIEM | AO | T |
| 2. | Upload the asset details into the Asset management tool as provided by the AO | SOC Integration Team | T + 0 |
| 3. | Share the IPs of the receiving servers with relevant integration documentation. | SOC Integration Team | T + 0 |
| 4. | Initiate FAR | AO | T + 0 |
| 5. | Review of FAR | SOC Integration Team | T + 0 |
| 6. | Post FAR Implementation, integration steps to be performed per the integration documentation shared prior. | AO | T + 1 |
| 7. | Verification of integration | SOC Integration Team | T + 1 |
| 8. | Upload the asset details | SOC Integration Team | T + 1 |
| 9. | Share screenshot of successful integration with the AO | SOC Integration Team | T + 1 |

# Procedure/Process Flow [To be followed by Application Owner]

## Objectives

The Objective of the procedure is to install agent and send data to SIEM Deployment. After installation of the Splunk agent (Forwarder) it will be configured to collect the data form the server and forward it to SIEM deployment.

## Inputs

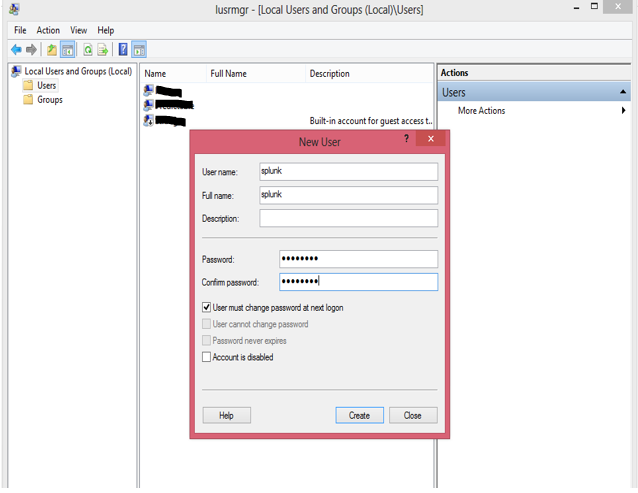
1. The agent package will be available on the repository provided by the SOC Team.
2. FAR approval confirmation will be provided by SOC Team along with the deployment server details which will be required during the forwarder installation.

## Activities

* + 1. **Download the package.**

Download the agent from the repository location. The package would be available in .msi format.

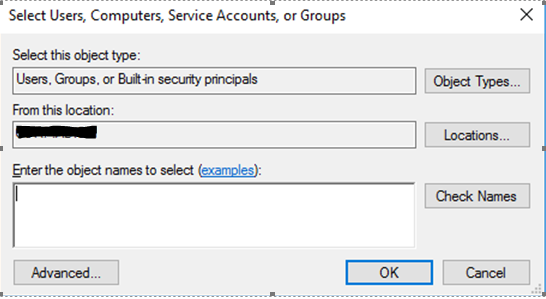
* + 1. **Create a local user account**
  1. Run a command lusrmgr.msc
  2. Go to users, right click on user, new user.
  3. Uncheck “User must change password at next logon”
  4. Check “Password never expires”

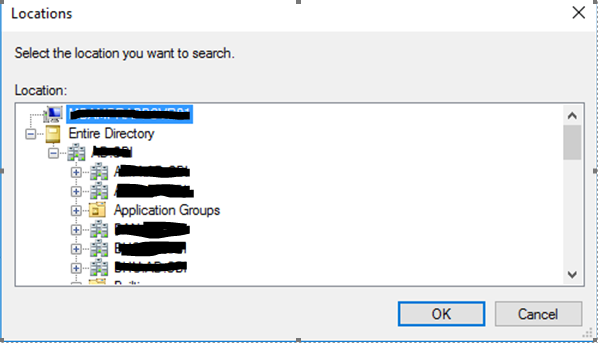


* 1. Add the user splunk to the “Event Log Reader” Group

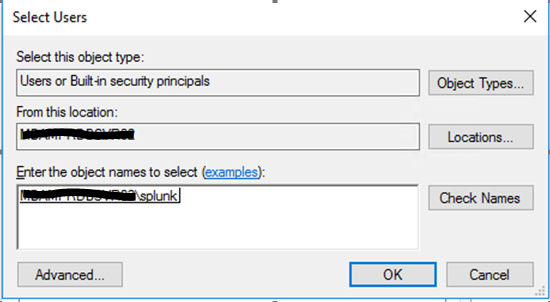
Click on Groups >> Select “Event Log Readers” group >> right click on the “event log reader” group >> Click on Add to group. >> Event log reader properties dialog box will appear >> Add created splunk user .

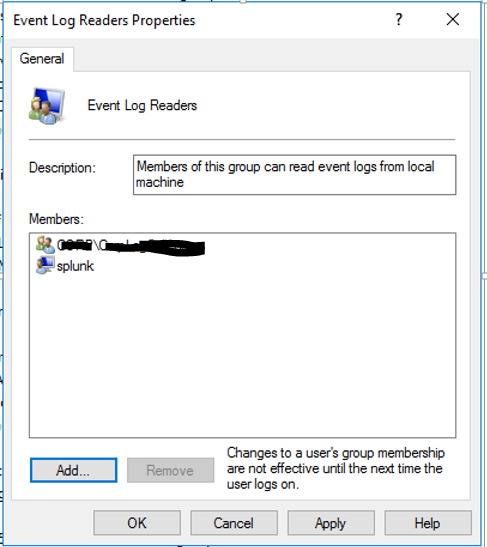
* 1. Go to locations, select the device name (which will mentioned at the top)





The object name will be in the format Computername\username

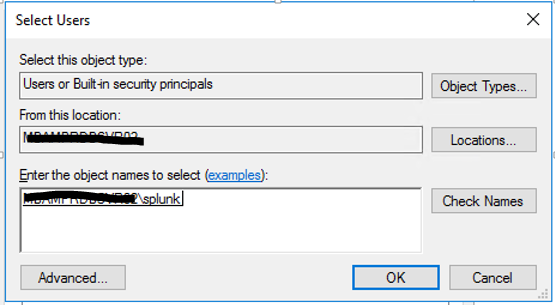


Splunk user should appear in Event Log Readers group.  
  


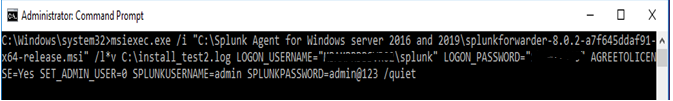
**3.3.3 Installation of Agent**

1. Run **command prompt** as administrator.

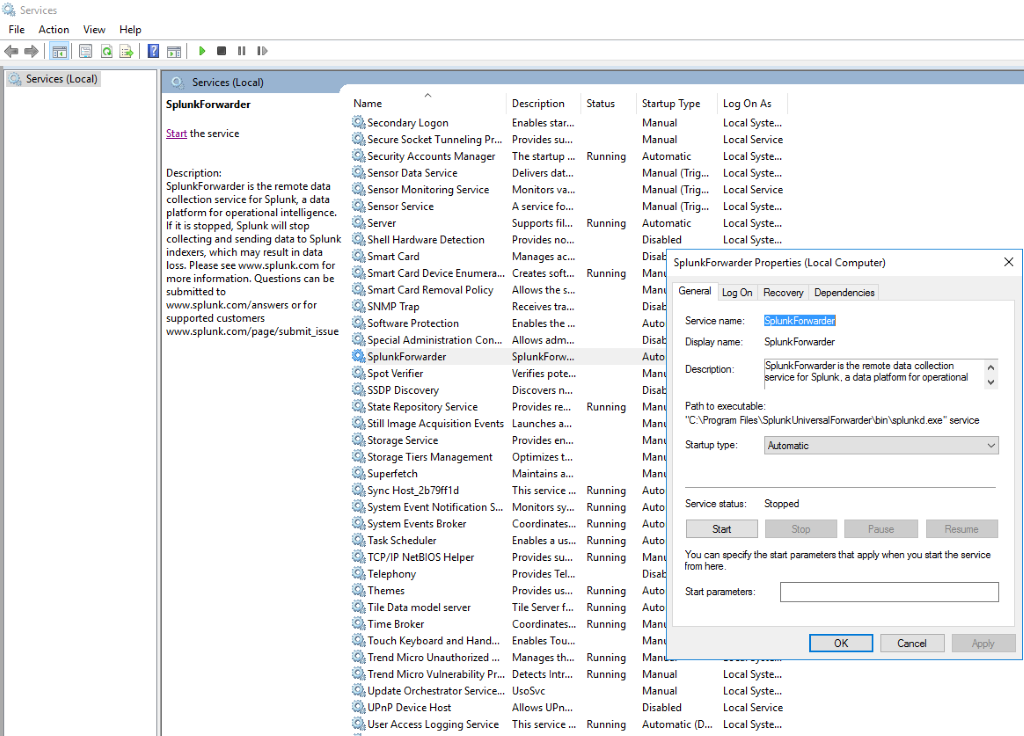
1. Run the following command where **<path to installed msi file>** specifies the directory location of the .msi agent file.   
     
     
   msiexec.exe /i <path to Splunk universal forwarder .msi file> /l\*v C:\SplunkForwarderinstallation.log LOGON\_USERNAME="<computername\user>" LOGON\_PASSWORD=<password> AGREETOLICENSE=yes SET\_ADMIN\_USER=0 SPLUNKUSERNAME=admin SPLUNKPASSWORD=<splunk\_password> /quiet  
     
     
   LOGON\_USERNAME : splunk  
   LOGON\_PASSWORD : Password for splunk local user

Computername : Windows server computer name. Refer below screenshot for sample  
  


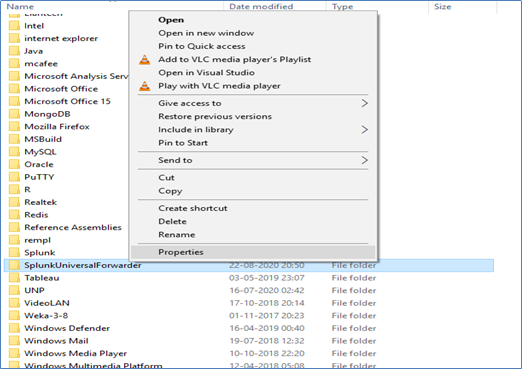
Below is the example

msiexec.exe /i "C:\Splunk Agent for Windows server 2016 and 2019\splunkforwarder-8.0.2-a7f645ddaf91-x64-release.msi" /l\*v C:\Forwarder\_install.log LOGON\_USERNAME="ABCDEFGH01\splunk" LOGON\_PASSWORD="password" AGREETOLICENSE=Yes SET\_ADMIN\_USER=0 SPLUNKUSERNAME=admin SPLUNKPASSWORD=admin@123 /quiet  
  


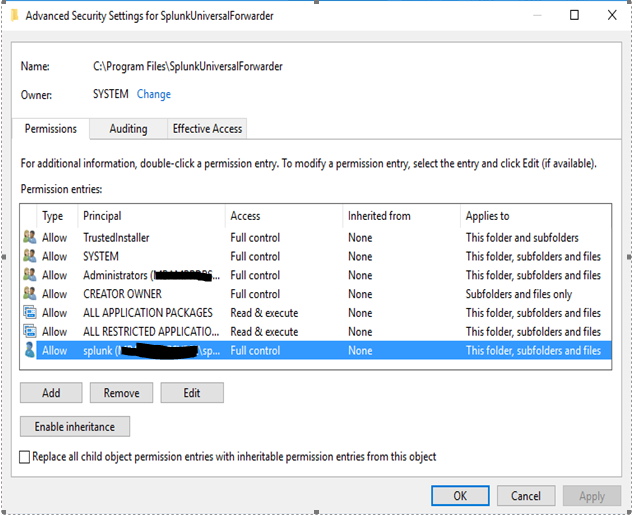
This will silently install Splunk.  This process will take few minutes.

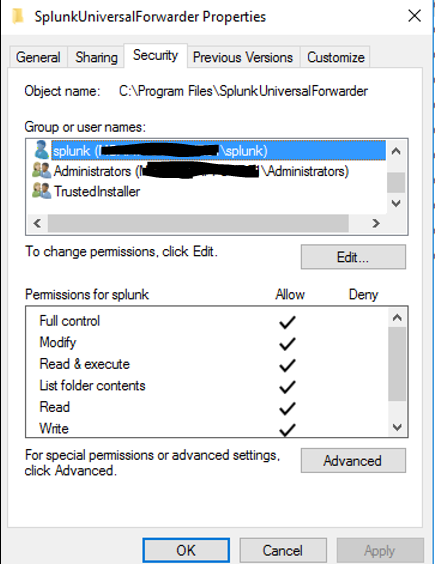
1. Once the setup is complete, open services.  
     
   **splunkForwarder** service should appear in services with logon type as splunk user. Do not start the service if not already started.  
     
   

1. Grant full control to Splunk forwarder installation directory (**C:\Program Files\SplunkUniversalForwarder**). This can be done by going through properties.



1. Go to security tab >> Click on advanced





* + 1. **Setup Splunk configurations:**

1. Open cmd and run the command

cd C:\Program Files\SplunkUniversalForwarder

1. To set the deployment server, run the command

.\splunk set deploy-poll <deploymentserver>:8089



**Note: The deployment server has to be added based on the deployment-server details provided by SOC team.**

Once the command is executed, it will ask for credentials. Provide the credentials that were created when installing the agent (application user created)

1. Stop and start the SplunklForwarderservice to apply the above changes.

1. The splunk forwarder service should be running.

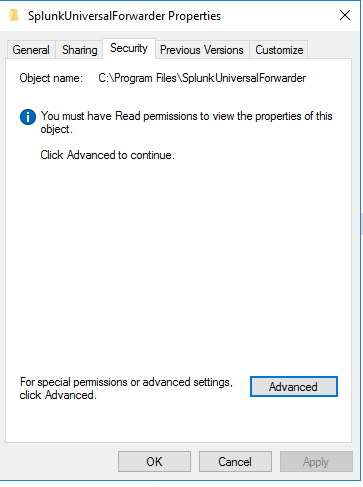
1. To validate the setting applied run the following command

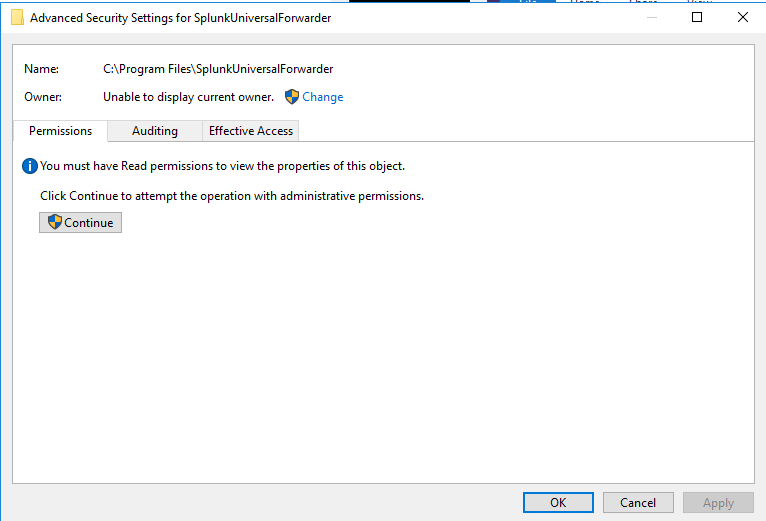
splunk show deploy-poll



**Please Note**: Files to be monitored which are present in other directory by Splunk should have read access to the Splunk user. You can do this by right clicking on the file >> Properties >> Security. Add the user and give the splunk user **Read permissions**.

SplunkUniversalForwarder Security tab





## Outputs

## Go to the services and Check splunkforwarder service status

* 1. If any errors are found refer the troubleshooting section.
  2. Once all the steps are completed, update the SOC Team with confirmation of forwarder installation.

# Tasks of the Department

## Purpose

To successfully install Splunk forwarder and forward logs to Splunk deployment. Splunk universal forwarder is setup on a remote server (Where the log resides) and is configured to forward the logs to Splunk Indexers (Where the logs will be stored).

## Definitions

The Splunk Agent will send the data to Splunk. Splunk Agent is installed on the remote server and the Splunk (Indexer) to which the agent will be forwarding data is on a different server.

## Responsibility

Once the Forwarder is installed by the Application Owner, SOC team will validate the data integration and give confirmation over the same.

## Requirements

To confirm successful integration, FAR approval and installation of Splunk agent validation will be done by SOC team.

## Tools & Information

## Exception handling

# Reference

This section provides the reference documents for Splunk Agent Installation.

[https://docs.Splunk.com/Documentation/Forwarder/latest/Forwarder/Installanixuniversalforwarder](https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Installanixuniversalforwarder)

# Troubleshooting/FAQs

Refer the below troubleshooting steps:

## Port Validation

Run the following command for Port validation:

1. For indexer communication
   * + The following command is used to check the connectivity of the indexer with the port 9997.
     + Indexer connectivity with the port 9997 is needed because via 9997 the logs are forwarded to the intended indexer.
     + The best practice scenario is to use the following command and check the host.

Index=\_internal

* + - If the forwarded data is not being indexed on the indexer, the following command can be used to test the connectivity.

tracert <indexerip> -p 9997

* + - Cluster master connectivity is needed to check since cluster master has the indexer list with it.
    - If any indexer is not reachable it can be checked within cluster master.
    - Telnet indexer to check the connectivity of your server with indexer

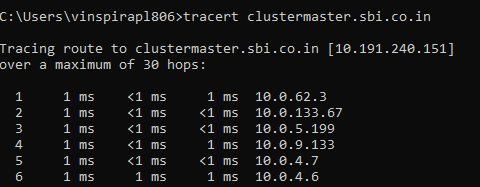


1. For Deployment server communication
   * + The following command is used to test the connectivity of the deployment server.
     + The deployment server connectivity and the port 8089 is needed because the it’s a two-way port. The deployment server sends configuration via this port and the forwarder phonehomes the deployment server via the same port.
     + If any configuration is distributed by the deployment server which are not found in the forwarder, the following command can be used to test the connectivity.
     + The deployment server also shows the deployment clients connected to it.
     + If in case the deployment server shows the indexer is down it can be checked in the cluster master.

tracert <deploymentserver> -p 8089

1. For Clustermaster Communication
   * + The following command is used to check the connectivity of the cluster master.
     + Cluster master connectivity is needed to check since cluster master has the indexer list with it.
     + If any indexer is not reachable it can be checked within cluster master.

tracert clustermaster.sbi.co.in –p 8089



* + - Telnet cluster master to check the connectivity of your server to the cluster master

C:\Users\vinspirapl806\AppData\Local\Microsoft\Windows\INetCache\Content.Word\telnet cluster manager.png

1. Telnet the connection between the host and splunk servers.
   * 1. telnet deploymentserver<1,2,3,4,5>.sbi.co.in 8089
     2. telnet clustermaster.sbi.co.in 8089

If facing above issue while connecting the servers, check if the DNS server IP is present.

# Do’s & Don’ts

## Do’s

* + 1. Confirm the deployment server details from the SOC Team.
    2. In the above document, all the commands with details in “< >” are required to be modified by application owner based on the environment.
    3. Use FQDN of the deployment server.

## Don’ts

* + 1. Do not specify IP Address of Splunk Deployment server.

# Escalation Matrix [To be filled by Bank]

## Escalation Level 1

The point of contact for level 1 escalation. The details should include –

Name

Designation

Email Id

Contact Number

## Escalation Level 2

The point of contact for level 2 escalation. The details should include –

Name

Designation

Email Id

Contact Number

## Escalation Level 3

The point of contact for level 3 escalation. The details should include –

Name

Designation

Email Id

Contact Number

# Annexure A

# Glossary