



Scribbler

Windows Agent

USER GUIDE

Reach us

support@syskeysoftlabs.com | sales@syskeysoftlabs.com

www.syskeysoftlabs.com

Follow us



Copyright

© 2020 Syskey Softlabs Pvt Ltd.

Trademarks

Windows and Windows Server are either trademarks or registered trademarks of their respective owners in the United States and/or other countries.

Contents

Scribbler Windows Agent	2
Installing Scribbler Windows Agent.....	2
Configuring Scribbler Windows Agent.....	3
How to configure Windows Event Logs	3
How to set Event Log Filter	4
How to configure Windows Firewall Logs.....	8
How to forward Windows logs to Syslog Server	9
Reference Links	10

Scribbler Windows Agent

Scribbler Windows Agent is one of the easiest and light weighted tools for gathering Windows Logs from Windows machines. It enables system administrators to easily monitor key metrics and change activities over the windows environment.

Scribbler Windows Agent collects Windows Logs in real-time and forward to Scribbler Log Manager or any available Syslog servers over RFC5424 format.

Scribbler Windows Agent collects:

- **Windows Event Logs**
- **Windows Firewall Logs**

Installing Scribbler Windows Agent

Scribbler supports flexible deployment options. It can either be installed on windows running on a Virtual Machine (VM) or on a bare metal server.

The Scribbler solution is distributed as an installable MSI package and installs in just few steps as mentioned below

Procedure

1. Run the installation package and follow the on-screen instructions to install pre-requisites
2. Read and accept the license agreement
3. Click next and continue the installation.
4. Desktop icon is available for the users to open the application anytime after the installation.

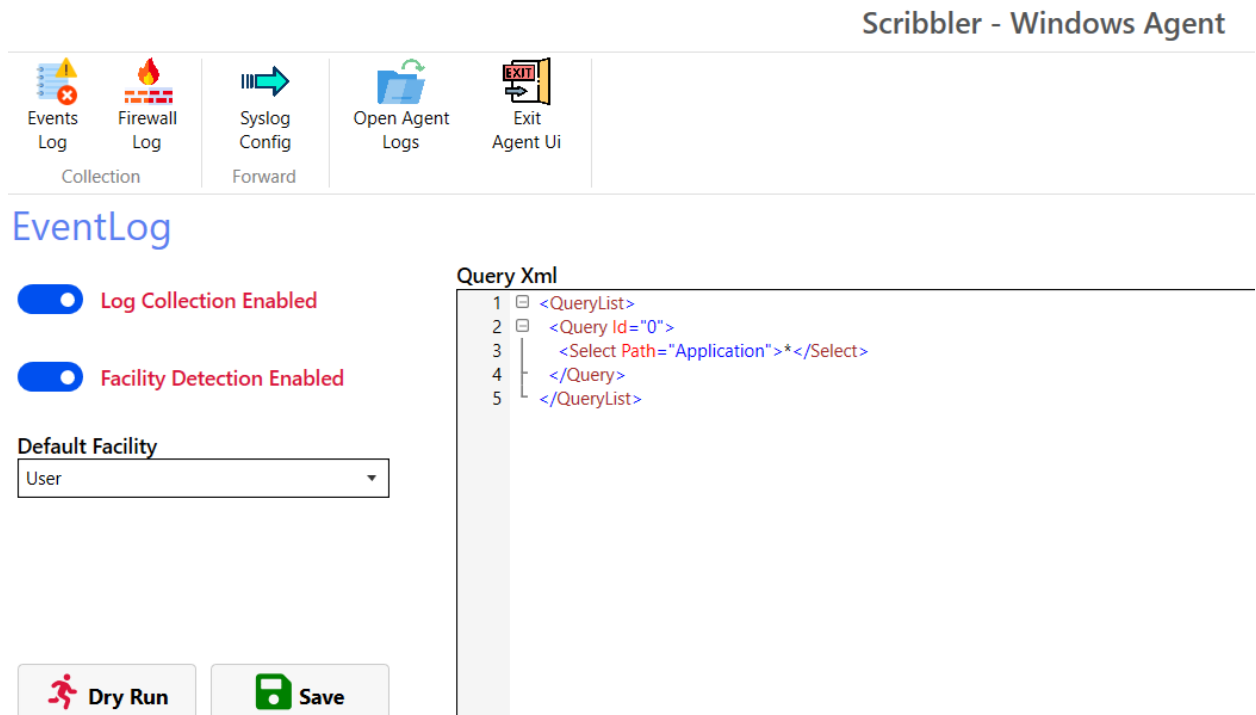
Configuring Scribbler Windows Agent

How to configure Windows Event Logs

Configure the input options to enable Scribbler Windows Agent to collect Event Logs from the Windows machines.


Procedure

1. In the top navigation pane, click on **EventsLog** tab



The screenshot shows the 'Scribbler - Windows Agent' interface. At the top right, the title 'Scribbler - Windows Agent' is displayed. Below the title is a navigation bar with five icons: 'Events Log' (Collection), 'Firewall Log' (Forward), 'Syslog Config' (Forward), 'Open Agent Logs' (Open Agent Logs), and 'Exit Agent Ui' (Exit Agent Ui). The main content area is titled 'EventLog'. On the left, there are two toggle switches: 'Log Collection Enabled' (checked) and 'Facility Detection Enabled' (checked). Below these is a 'Default Facility' dropdown menu set to 'User'. At the bottom left, there are two buttons: 'Dry Run' (with a red running person icon) and 'Save' (with a green floppy disk icon). On the right, there is a 'Query Xml' section with a text area containing the following XML code:

```
1 <QueryList>
2   <Query Id="0">
3     <Select Path="Application">*</Select>
4   </Query>
5 </QueryList>
```

2. **Enable Log Collection** – Click on Toggle switch to Enable/Disable EventLog collection
3. **Enable Facility Detection** –Enable this feature to allow Scribbler to Auto Detect the Facility of the incoming logs.
4. **Disable Facility Detection** –Disable this feature for Scribbler Not to Auto Detect the Facility of the incoming logs. In this case, Default Facility chosen by user will be applied all the time.
5. Click 

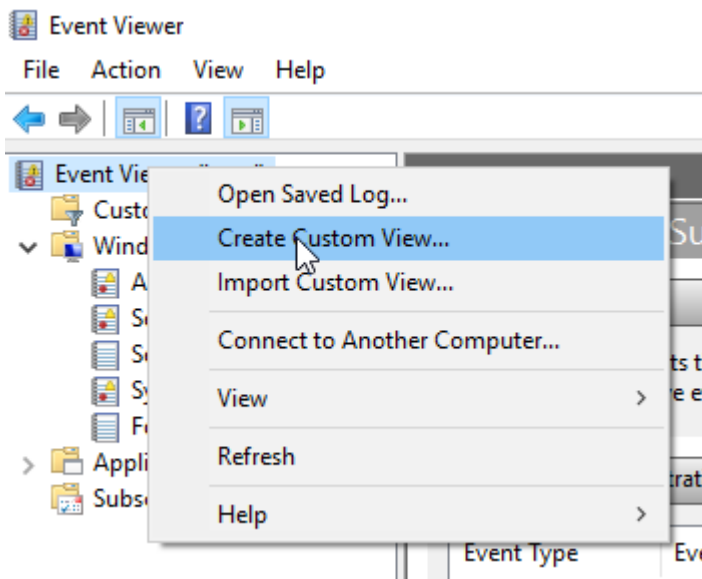
How to set Event Log Filter

Event Log filters decide which logs to be forwarded to Scribbler Log Manager/Any Syslog Server over RFC5424. The application reads all the logs and forwards based on the configured filters.

Setting filters are quite easy for the users as it is possible to utilize existing custom-view feature of the windows event viewer.

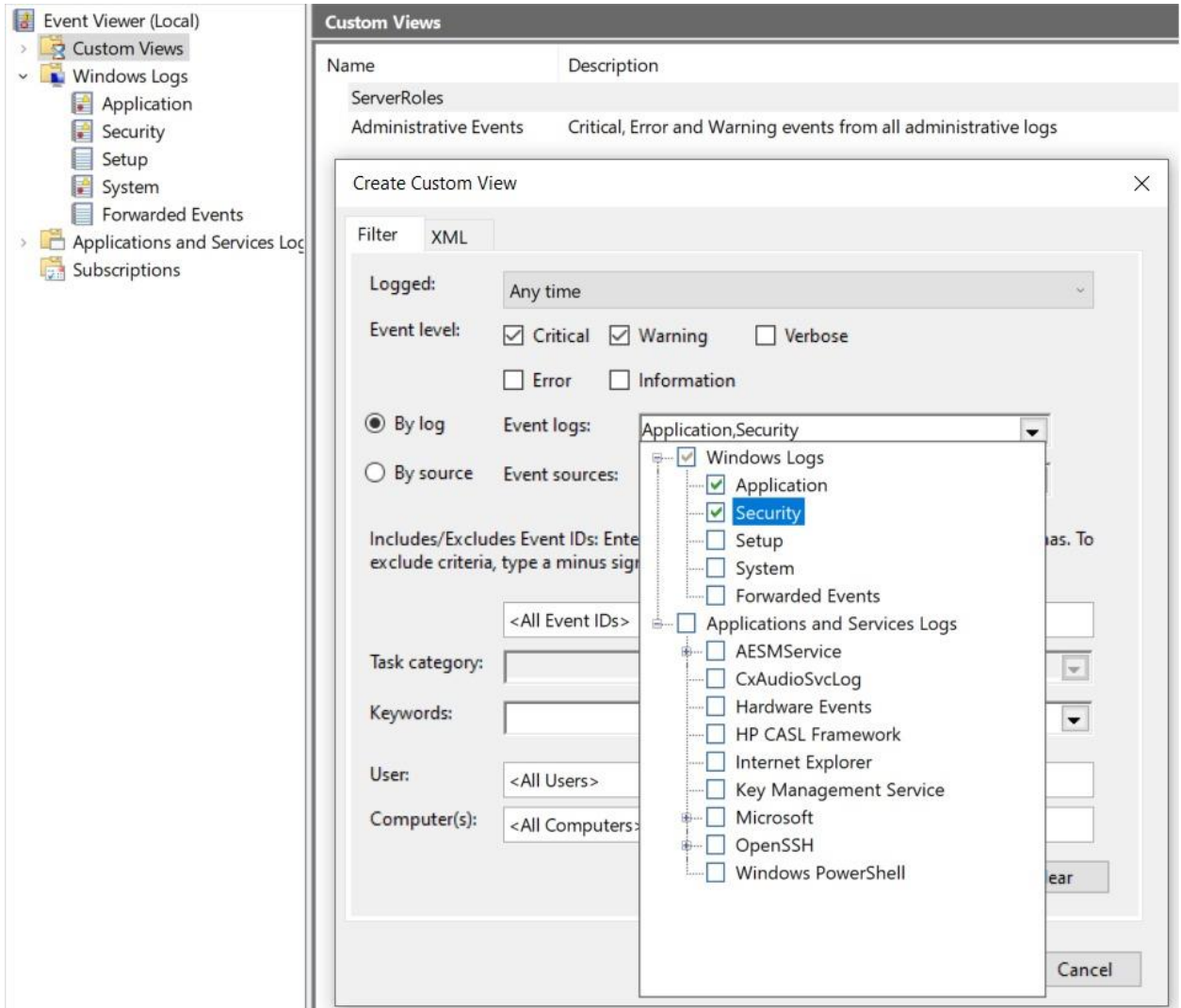
Procedure

1. Open **Windows Event Viewer** of the host machine and right click to find **“Create Custom View”** option

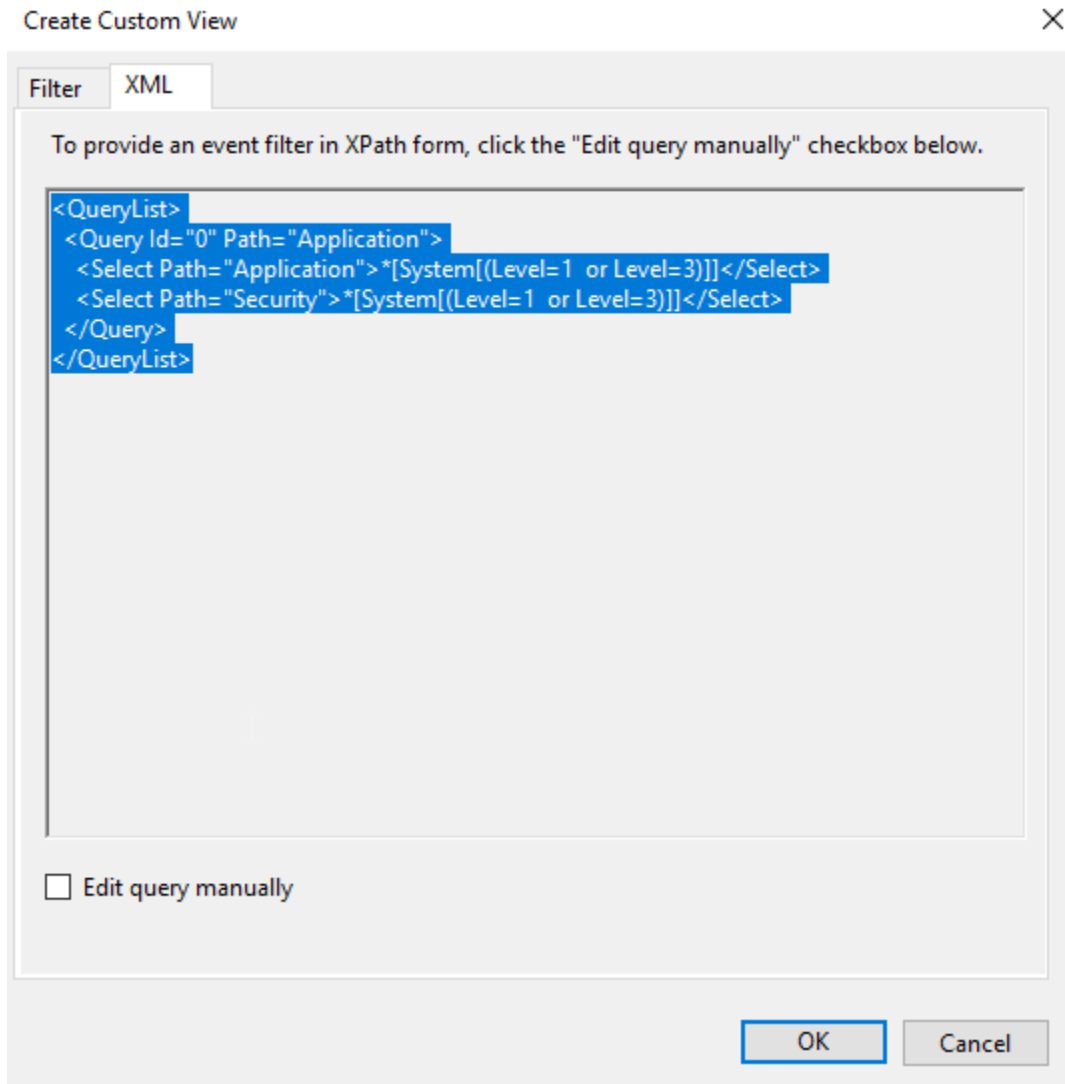


2. Click on **“Create Custom View”**

3. Set the Desired filters based on **Event Level, By Log, By Source, Event ID and Keywords**.

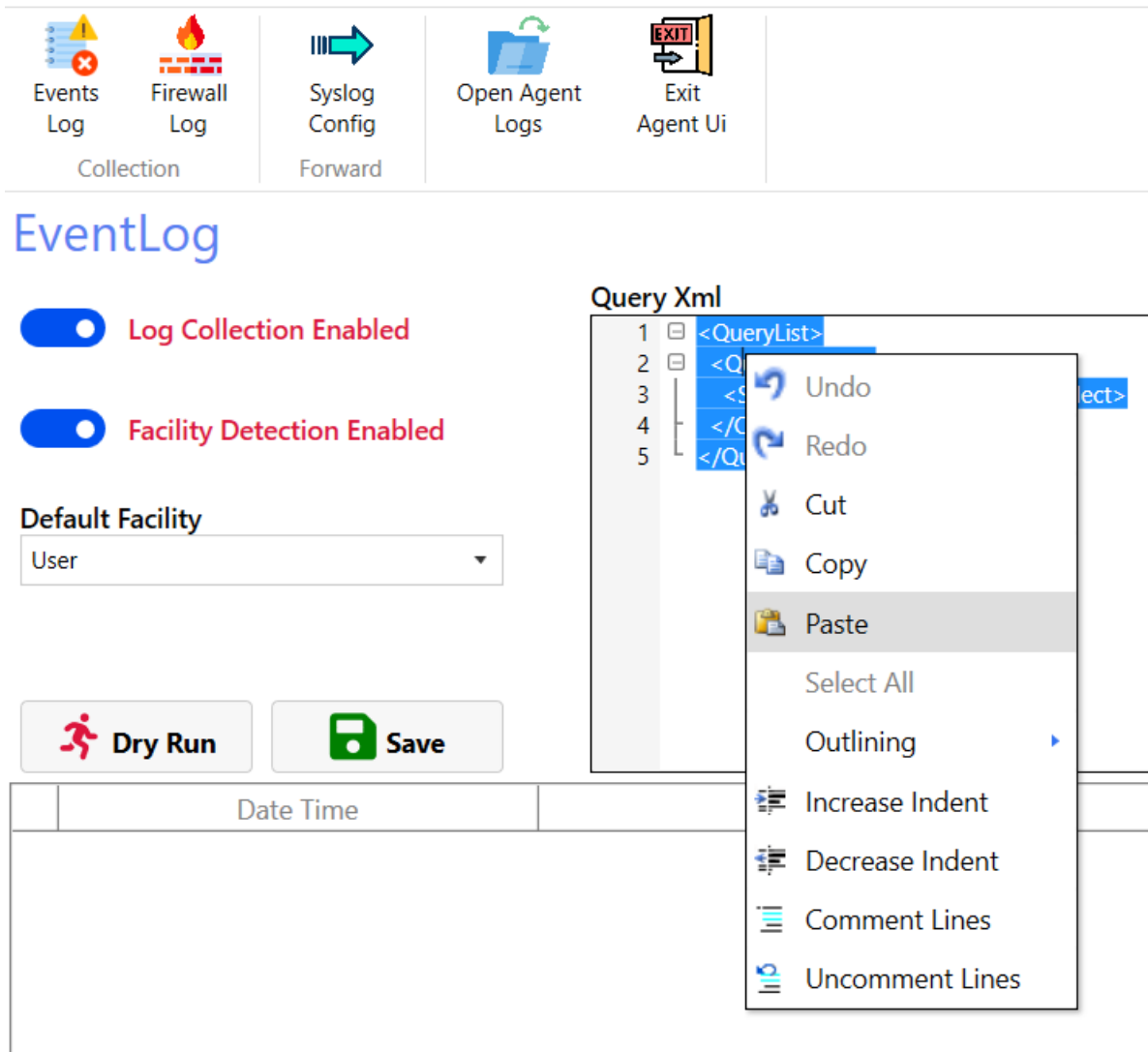


4. After configuring all required filter options, Click on “XML” tab



5. Select and Copy the “XML” query from Windows Event Viewer-Custom View

6. Paste on the “Scribbler Windows Agent-EventLog” XML query tab.



The screenshot displays the Scribbler Windows Agent interface. At the top, there are five icons representing different log sources: Events Log, Firewall Log, Syslog Config, Open Agent Logs, and Exit Agent Ui. Below these is the 'EventLog' section, which includes two toggle switches for 'Log Collection Enabled' and 'Facility Detection Enabled', both currently turned on. A 'Default Facility' dropdown menu is set to 'User'. At the bottom of this section are 'Dry Run' and 'Save' buttons. To the right, the 'Query Xml' editor shows a tree view with a context menu open over the '<QueryList>' element. The context menu options include Undo, Redo, Cut, Copy, Paste (highlighted), Select All, Outlining, Increase Indent, Decrease Indent, Comment Lines, and Uncomment Lines.

7. Click  and there we go

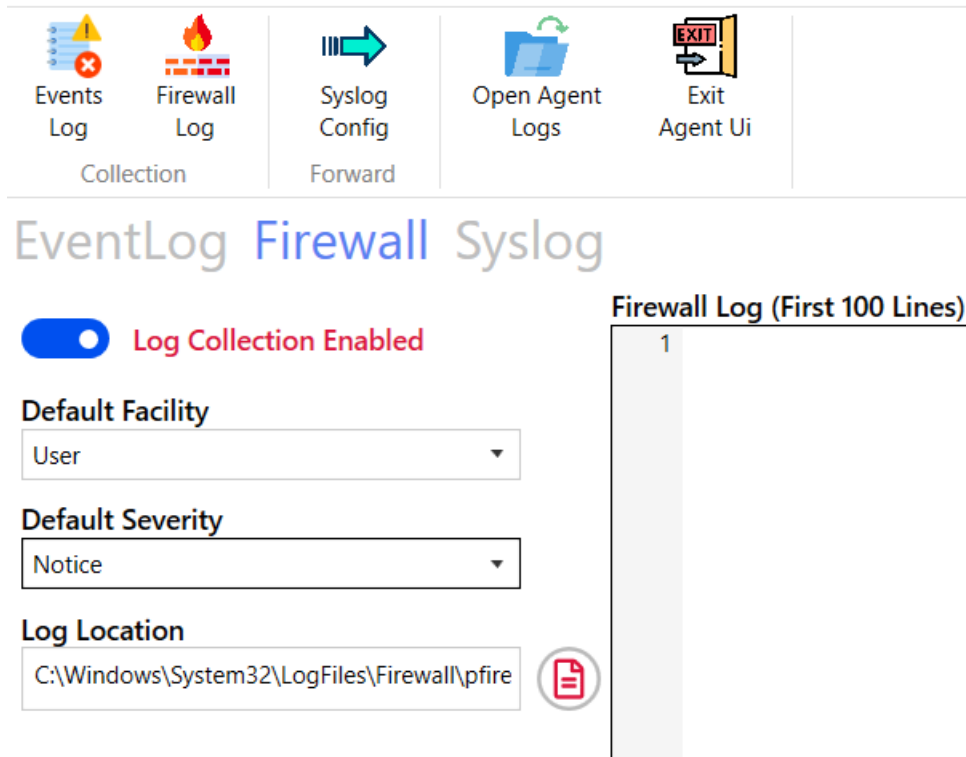
Note: Use the same Copied Query in **Scribbler Windows Agents** hosted on other similar windows machines (if any with same filter configurations)

How to configure Windows Firewall Logs


Configure the input options to enable Scribbler Windows Agent to collect Firewall Logs from the Windows machines.

Procedure

1. In the top navigation pane, click on **FirewallLog** tab



The screenshot shows the Scribbler Windows Agent interface. At the top, there is a navigation pane with icons for 'Events Log', 'Firewall Log', 'Syslog Config', 'Open Agent Logs', and 'Exit Agent Ui'. Below this, the 'Firewall Log' configuration screen is displayed. It features a toggle switch for 'Log Collection Enabled' which is turned on. Below the toggle are three dropdown menus: 'Default Facility' set to 'User', 'Default Severity' set to 'Notice', and 'Log Location' set to 'C:\Windows\System32\LogFiles\Firewall\pfire'. To the right of the configuration fields is a preview window titled 'Firewall Log (First 100 Lines)' which currently shows a single line with the number '1'. A 'Save' button is visible at the bottom of the configuration area.

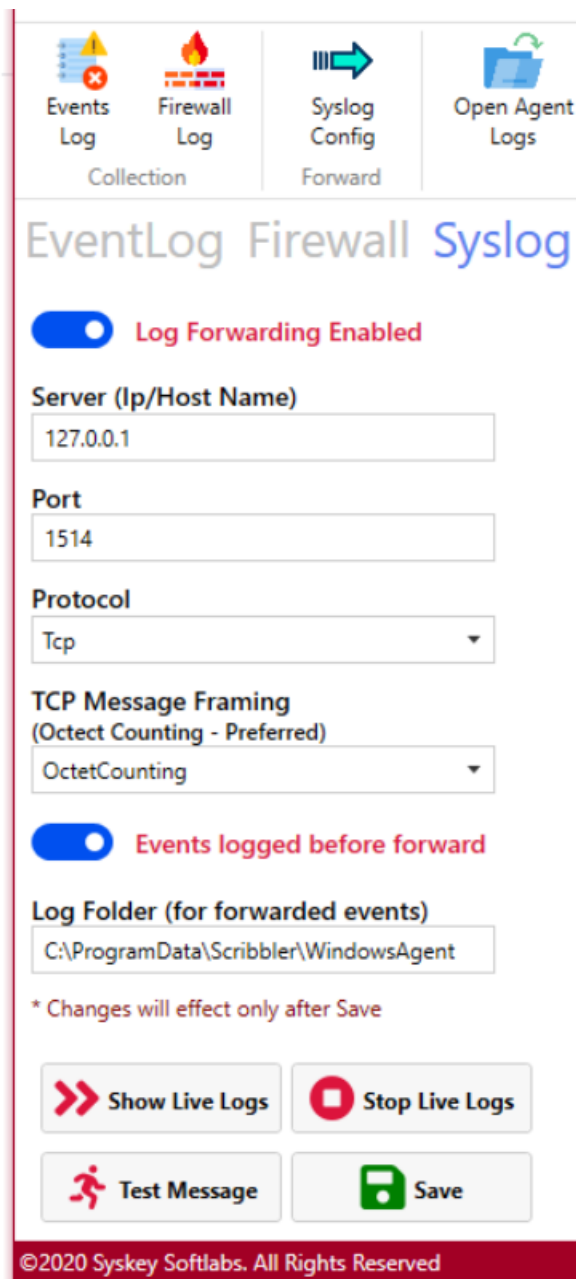
2. **Enable Log Collection** – Click on Toggle switch to Enable/Disable FirewallLog collection
3. Choose **Default Facility** to be applied for the collected Firewall Logs
4. Choose **Default Severity** to be applied for the collected Firewall Logs
5. Default path of the Log Location is selected by Scribbler automatically. If please choose/change only if the Logs are recorded in a different location
6. Click 

How to forward Windows logs to Syslog Server

Configure Scribbler Windows Agent to forward system Windows logs to a syslog server over Syslog protocol in RFC5424 format.

Procedure

1. In the top navigation pane, Click on **Syslog Config Tab**



Events Log Firewall Log Syslog Config Open Agent Logs

Collection Forward

EventLog Firewall **Syslog**

Log Forwarding Enabled

Server (Ip/Host Name)
127.0.0.1

Port
1514

Protocol
Tcp

TCP Message Framing
(Octect Counting - Preferred)
OctetCounting

Events logged before forward

Log Folder (for forwarded events)
C:\ProgramData\Scribbler\WindowsAgent


* Changes will effect only after Save

>> Show Live Logs **Stop Live Logs**

Test Message **Save**

©2020 Syskey Softlabs. All Rights Reserved

2. Switch the Toggle switch to Enable Log Forwarding option
3. Specify the IP address, network protocol and port number of the Syslog Server.
4. Select the method for TCP framing. The available options are **Octet Counting** and **Non-Transparent Framing**.
5. Switch the Toggle switch to Enable/Disable local recording of logs in a specified folder.

6. Click Test message option to test the sample message from Scribbler Agent to the syslog Server
7. Click on **Show Live Logs** to see the real time logs flowing towards the Syslog Server.
8. Click  Save.

Reference Links

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc722404\(v=ws.11\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc722404(v=ws.11)?redirectedfrom=MSDN)

[https://docs.microsoft.com/en-us/previous-versions//aa385231\(v=vs.85\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions//aa385231(v=vs.85)?redirectedfrom=MSDN)