Seqrite Endpoint Security 7.60

SyslogAgent Tool – SIEM Integration

Document Version 1.0

Copyright Information

Trademarks

Contents

SyslogAgent Tool

Abstract

This document contains usage information about SyslogAgent tool for Seqrite Endpoint Security (EPS).

Overview

The SyslogAgent is an independent tool that is used to integrate Seqrite Endpoint Security (EPS) with SIEM (Security Information and Event Management) applications.

The SyslogAgent tool helps you to push all the events logs from EPS Server to the configured SIEM server.

Requirement

Operating System Requirement

- Microsoft Windows 8 and above

  For windows 8.1

  If the OS is Windows 8.1 (32-bit or 64-bit), you need to download and install a latest packager from the following link

  https://docs.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170

  After successful installation of the above package, you can install the SyslogAgent tool.

Seqrite Endpoint Security

- Seqrite Endpoint Security 7.60 Service Pack 5 and above

Prerequisite

EPS 7.60 SP5 Server is installed with one of the following flavors/editions:

  - Business
  - Total
  - Enterprise Suite

- SIEM Server is installed

Tool Information

File Name	MD5 Checksum
SQSYSAGINST.EXE	7571e65a0f9f6b3b5d0d390190a777bf

The SyslogAgent tool works with many SIEM vendors that support CEF and LEEF formats. Few supporting vendors are mentioned below for your reference.

- IBM Security QRadar
- SolarWinds Papertrail
- ManageEngine
- Securonix

Usage Information

Download and execute the tool on the EPS server from which the data needs to be pushed.

After executing the tool, provide credentials of the SIEM Server. Then, set the schedule for pushing the data and select the events of which the data will be pushed to the SIEM server.

You can view the event logs on the configured SIEM server.

Installing SyslogAgent Tool

To install SyslogAgent tool, follow these steps.

1. Download SyslogAgent tool from the following link,

   https://dlupdate.quickheal.com/builds/seqrite/760/en/SyslogAgent/SQSYSAGINST.EXE

2. Execute **SQSYSAGINST.EXE** file.

   The SyslogAgent tool is installed.

Using SyslogAgent tool

To push the events data to the SIEM server, follow these steps.

1. Execute **SQSYSAGINST.EXE** file. The SyslogAgent Configuration window appears as shown below (Figure 1). Set all the Syslog server configuration and event selection in the window.

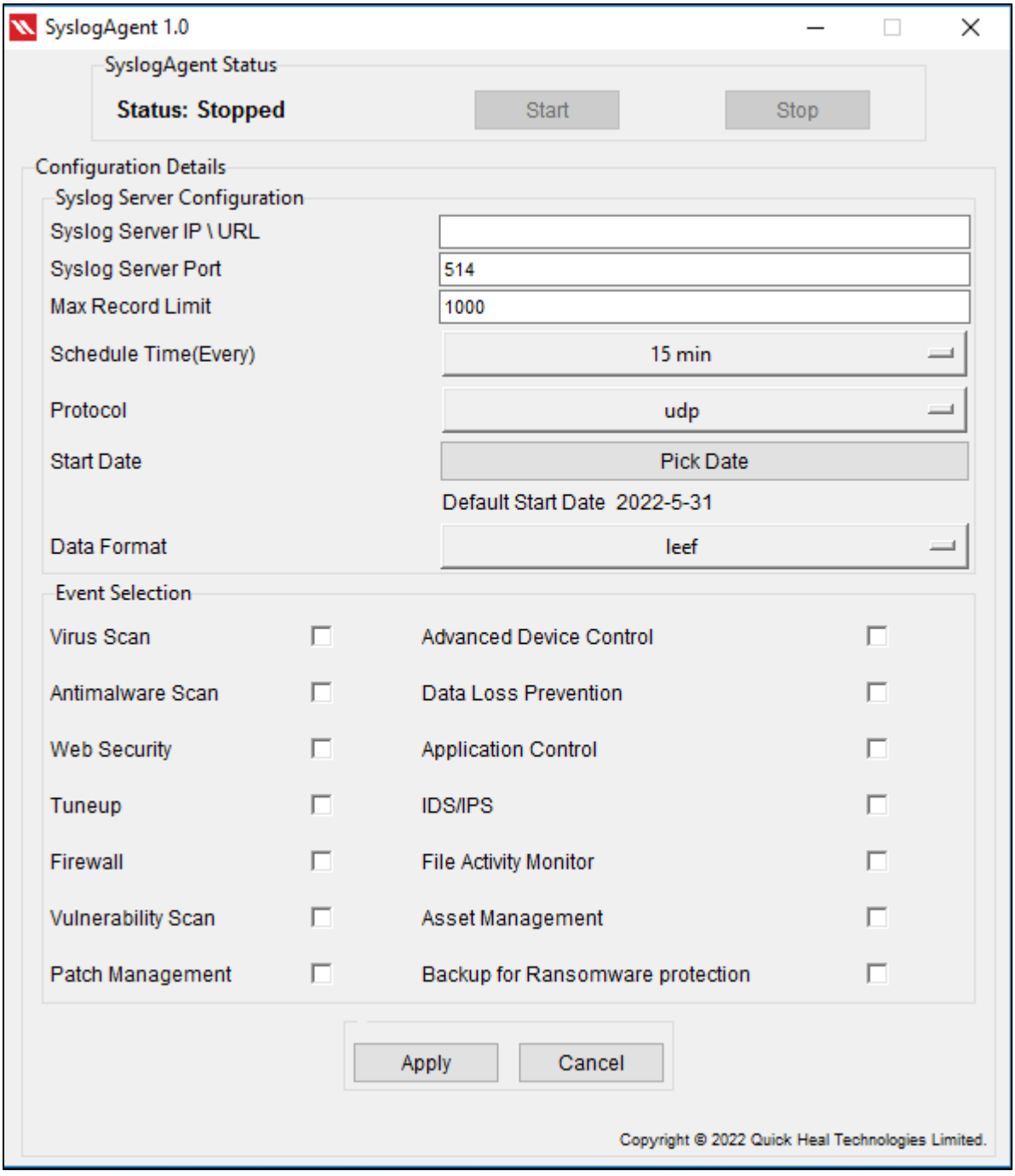

Figure 1

1. Enter **Syslog Server IP\URL**.
2. Enter **Syslog Server Port** number.
3. Enter **Max Record Limit**. This number of records will be pushed to the SIEM server.
4. Select **Schedule Time** from the list. Records will be pushed as per selected schedule time.

5. Select **Protocol** either UDP or TCP.
6. Select **Start Date** with the calendar control.
7. Select **Data format** either LEEF or CEF.

   Note: The data formats supported are LEEF (Log Event Extended Format) and CEF (Common Event Format) only.
8. In the Event Selection section, select the events as required.
9. Click **Apply**. The configuration success message appears.

   The SyslogAgent service will start automatically as per set schedule.

Updating Configuration

To update the configuration, follow these steps.

1. Run SyslogAgentUI.exe from the path, <installation directory>\Seqrite\Endpoint Security 7.60\Admin.

   The SyslogAgent Configuration window appears. (Figure 1)
2. Edit the information.
3. Click **Apply**.

Uninstalling SyslogAgent Tool

To uninstall the SyslogAgent tool manually, follow these steps.

1. You need to check status of Seqrite SyslogAgent service. Before uninstalling, the service must be stopped.

   To check the status of the service, launch the SyslogAgentUI.exe file from <installation directory>\Seqrite\Endpoint Security 7.60\Admin.
2. If the status of service is Running, click **Stop** to stop the service.
3. Open the command line as an Administrator and run the following command

   `SC DELETE "Seqrite SyslogAgent"` (Ensure you put **double quotes** here)

   This command will uninstall the SyslogAgent service only. Installation files will not be deleted from EPS installation directory. These files will be deleted only when you uninstall the EPS Server.
4. If you want to reinstall the SyslogAgent tool, then first manually remove the previously installed SyslogAgent tool files mentioned below and then reinstall.

   Keep Self Protection OFF while removing files.

   - <Installation directory>\Seqrite\Endpoint Security 7.60\Admin
     - siem_win_service.exe, SyslogAgentUI.exe, sql_res.ini, syslogagent_sp.sql

- <Installation directory>\Seqrite\Endpoint Security 7.60\Admin\config
    - siem_log_config.ini, SiemConfig.json