

# LogZilla Syslog Agent for Windows

## Introduction

LZ Syslog Agent is a Windows service that sends Windows event log messages to a syslog server. Syslog is a widely used protocol of event notification and LZ Syslog Agent allows Windows machines to be part of this environment.

## Features

This program supports the following:

- Simple configuration and ease of use.
- Select of specific event logs
- Configuration of primary and secondary LogZilla recipient servers
- Configuration of optional TLS transport for log messages
- Optional ignoring specified Windows event IDs
- Optional “tail”-ing of specified file

## History

Parts of this Syslog Agent are based the Datagram Syslog Agent, which in turn was based on SaberNet's NTSyslog. The bulk of the work is Copyright © 2021 by [LogZilla Corporation](#).

## Installation

The LZ Syslog Agent programs are installed by executing the LogZilla\_SyslogAgent\_6.23.0.0.msi file.

## Prerequisites

The LZ Syslog Agent configuration program, SyslogAgentConfig.exe, requires .NET Framework 4.6.2 or later. The LZ Syslog Agent service, SyslogAgent.exe, has no prerequisites.

## Configuration

The operation of the LZ Syslog Agent service is controlled by registry settings. These can be maintained with the LZ Syslog Agent configuration program, SyslogAgentConfig.exe. This program always runs as administrator.

The screenshot shows the Syslog Agent Configuration window with the following sections and annotations:

- Servers:**
  - Primary LogZilla server: mylogzilla.company.com (Annotation: Button to choose PEM cert files points to the Select Primary Cert button)
  - Primary Use TLS: ☒ (Annotation: Optional: send events to second server points to the Secondary LogZilla server field)
  - Secondary LogZilla server: 11.22.44.55 (Annotation: Optional: send events to second server points to the field)
  - Secondary Use TLS: ☐ (Annotation: Optional: send events to second server points to the field)
- Event Logs:**
  - Application: ☒
  - HardwareEvents: ☐
  - Internet Explorer: ☐
  - Key Management Service: ☐
  - Microsoft: ☐
  - OpenSSH: ☒
    - Admin: ☐
    - Operational: ☒
  - Security: ☒
  - Setup: ☐
  - SMSApi: ☐
  - System: ☒
- Event Selection:**
  - Poll interval: 10
  - Ignore event ids: 4624,4625
- Message Content:**
  - Look up account IDs: ☒ (Annotation: Optional: add JSON key-value pairs points to the Extra key-values field)
  - Facility: Local 4
  - Severity: Dynamic
  - Extra key-values: "bldg":"12a","dept":"accounting"
- Debug Logging:**
  - Debug Log Level: WARNING
  - Debug Log File Name: syslogagent.log (Annotation: Optional: log verbosity and file points to the field)
- File Watcher (tail):**
  - File Name: C:\Users\Public\Documents\logfile.log (Annotation: Optional: add log messages by "tail"-ing given file points to the field)
  - Program Name: LoggerApp (Annotation: (tail descriptive name) points to the field)
  - Choose File: Button

LogZilla Syslog Agent version 6.22.0.0

Save Restart

Agent service is running

### Servers

The address and port for the primary Syslog server, and optionally for a secondary server can be entered. The address can be either a host name or an IP address.

### Secondary LogZilla server

There is an option to send messages to a secondary LogZilla server. If selected, every message successfully sent to the primary server will also be sent to the secondary server.

## **Primary / Secondary Use TLS**

There is an option to use TLS to send messages to one or both LogZilla servers. If selected, every message sent to the primary or secondary server will use a TLS communications link.

## **Select Primary / Secondary Cert**

These buttons are used to select (PEM format) certificate files for the TLS communications to the primary or secondary server. When the button is clicked a window will pop up allowing selection of the file from which the cert is to be read. Please note that once the cert is read and imported (using the button) that certificate information is copied into the LogZilla settings and the source cert file is no longer used. If desired the cert information that LogZilla uses can be directly edited in the files `primary.cert` and `secondary.cert` in the LogZilla directory.

## **Event Logs**

A list of all event logs on the local system is displayed. Messages in the event logs that are checked will be sent to the server.

## **Poll Interval**

This is the number of seconds between each time the event logs are read to check for new messages to send.

## **Look up Account IDs**

Looking up the domain and user name of the account that generated a message can be expensive, as it may involve a call to a domain server, if the account is not local. To improve performance, this look up can be disabled and messages will be sent to the server without any account information.

## **Ignore Event Ids**

To reduce the volume of messages sent, it is possible to ignore certain event ids. This is entered as a comma-separated list of event id numbers.

## **Facility**

The selected facility is included in all messages sent.

## **Severity**

By selecting 'Dynamic', the severity for each message is determined from the Windows event log type. Otherwise, the selected severity is included in all messages sent.

## **Extra Key-Values**

This configures whether any supplemental key-value pairs will be included with the log messages, for processing by LogZilla rules. Key-value pairs should be separated by commas.

In addition to the manually specified key-values, LogZilla includes some default key-value pairs for use in the LogZilla rules:

- "EventID" : "nnnn" contains the Windows event id
- "EventLog" : "xxx" ... contains the name of the event log that produced the message
- "\_source\_type" : "WindowsAgent" identifies this program as the sender of the message

- “\_log\_type”: “eventlog” OR “\_log\_type”: “file” ... indicates whether the log message originated in a Windows event log or originated from the “tail” operation

### **Log Level**

This configures the “level” of log messages produced by the Syslog Agent. The “level” means the type or importance of a given message. Any given log level will produce messages at that level and those levels that are more important. For example if “RECOVERABLE” is chosen, the Syslog Agent will also produce log messages of levels “FATAL” and “CRITICAL”. Logging is optional, so this can be left set to “None”.

### **Log File Name**

This configures the path and name of the file to which log messages will be saved. If a path and directory are specified that specific combination will be used for the log file, otherwise the log file will be saved in the directory with the SyslogAgent.exe file. If log level is set to “None” this will be blank.

### **File Watcher (tail)**

The agent has the capability to “tail” a specified text file – this means that the agent will continually read the end of the given text file and send each new line that is appended to that text file as a separate message to the LogZilla server. A program name should be specified here to indicate the source of those log messages.

### **Save**

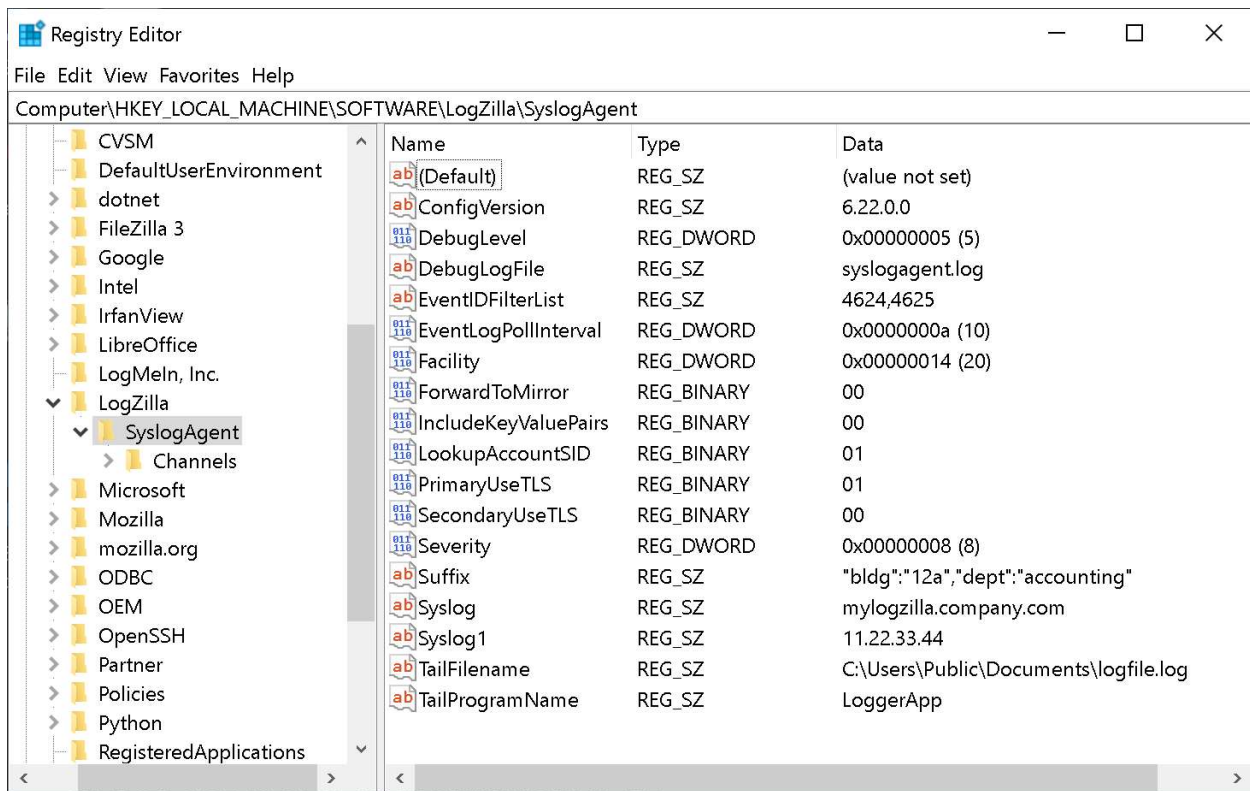
The configuration settings are stored in the registry.

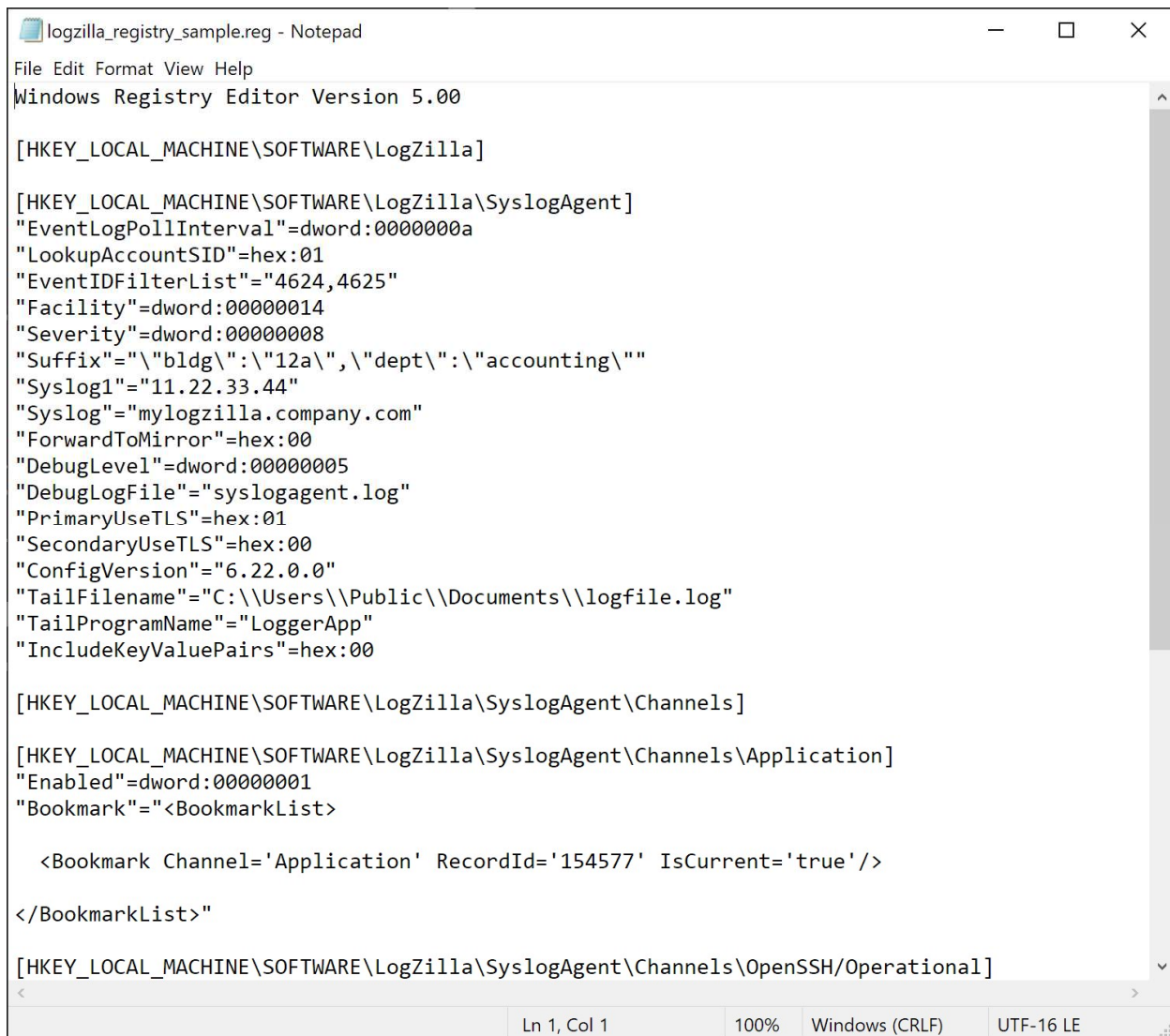
### **Restart**

If the syslog agent service is running, it must be restarted to pick any changes made in the configuration settings.

## **Registry Data**

The settings are stored in the registry at HKEY\_LOCAL\_MACHINE\SOFTWARE\Logzilla\SyslogAgent. There are sub-keys for each event log selected.





```
logzilla_registry_sample.reg - Notepad
File Edit Format View Help
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla]

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla\SyslogAgent]
"EventLogPollInterval"=dword:0000000a
"LookupAccountSID"=hex:01
"EventIDFilterList"="4624,4625"
"Facility"=dword:00000014
"Severity"=dword:00000008
"Suffix"="\bldg\":"12a\","dept\":"accounting\"
"Syslog1"="11.22.33.44"
"Syslog"="mylogzilla.company.com"
"ForwardToMirror"=hex:00
"DebugLevel"=dword:00000005
"DebugLogFile"="syslogagent.log"
"PrimaryUseTLS"=hex:01
"SecondaryUseTLS"=hex:00
"ConfigVersion"="6.22.0.0"
"TailFilename"="C:\\Users\\Public\\Documents\\logfile.log"
"TailProgramName"="LoggerApp"
"IncludeKeyValuePairs"=hex:00

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla\SyslogAgent\Channels]

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla\SyslogAgent\Channels\Application]
"Enabled"=dword:00000001
"Bookmark"="<BookmarkList>

    <Bookmark Channel='Application' RecordId='154577' IsCurrent='true' />

</BookmarkList>"

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla\SyslogAgent\Channels\OpenSSH\Operational]
```

Settings can be maintained on one machine and loaded onto another machine by exporting them to a text file. This is done by right-clicking on the SyslogAgent node and selecting 'Export', or using the command line:

```
regedit /E sample.reg "HKEY_LOCAL_MACHINE\SOFTWARE\Logzilla\SyslogAgent"
```

The settings are loaded on the target machine with the command line:

```
regedit /S sample.reg
```

If the Syslog Agent service has been run on the source machine, the registry may contain information about the last messages processed, and these lines should be deleted before loading the settings on to another machine.

## Operation

After the Syslog Agent has been installed as a Windows service, it can be started and stopped with the Windows Services control panel, or with the command line:

```
net start "LZ Syslog Agent"
```

and

```
net stop "LZ Syslog Agent"
```

For testing, the Syslog Agent can be run from the command line. The command prompt must be run as administrator.

```
syslogagent -console
```

or

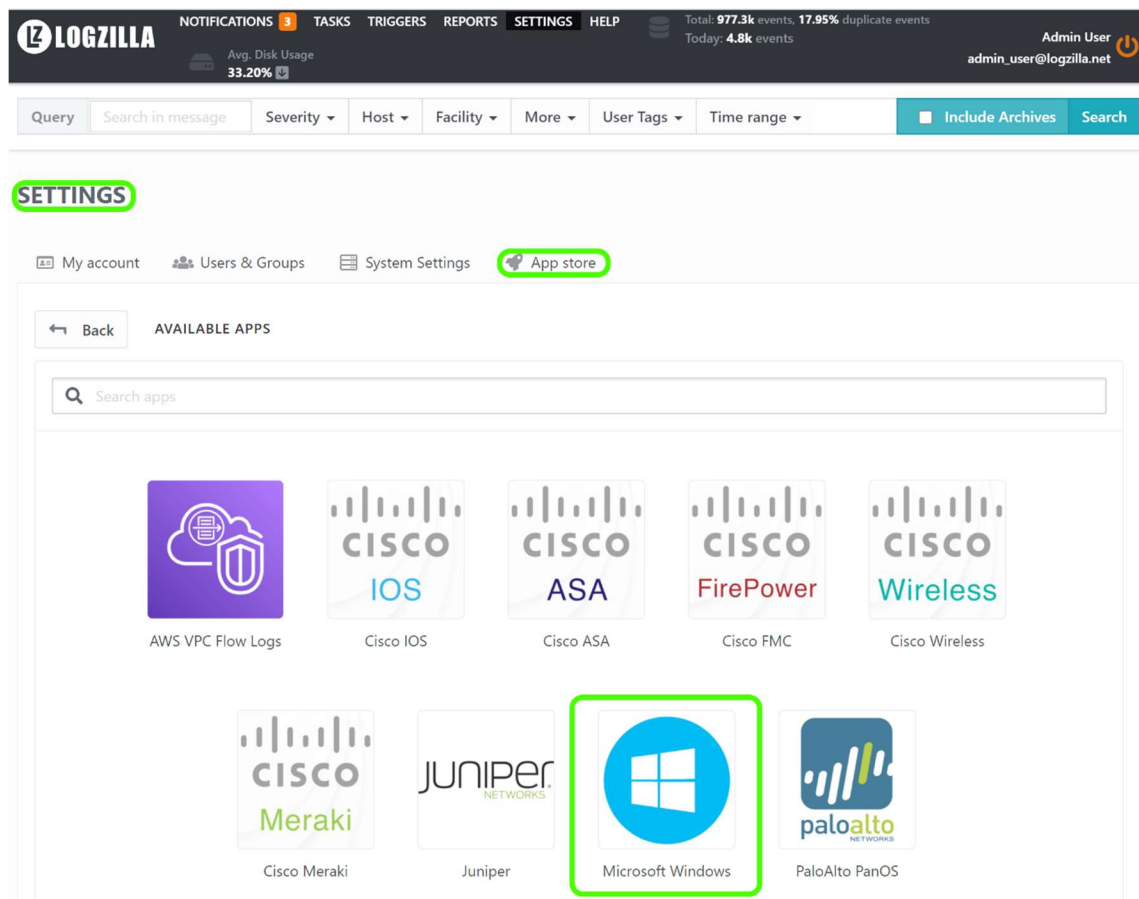
```
syslogagent -console -debug
```

to print debugging information.

To stop a test run, type the 'esc' key.

## LogZilla Configuration

In order for LogZilla to make use of the Windows Syslog Agent the LogZilla rule for the agent must be installed. The preferred means of accomplishing this is by installing the *MS Windows* app from the LogZilla appstore, by going to Settings -> App store then choosing Microsoft Windows and then choosing Install.



Once the Microsoft Windows appstore application has been installed LogZilla should correctly receive and display log messages from the Windows Syslog Agent.