Kiwi SyslogGen

A Freeware Syslog message generator for Windows

by SolarWinds, Inc.

Kiwi SyslogGen is a free Windows Syslog message generator which sends Unix type Syslog messages to any PC or Unix Syslog Daemon. Excellent for testing your Kiwi Syslog Server setup. Supports TCP syslog messages for emulating PIX firewall messages.

Table of Contents

1 Kiwi SyslogGen

A Freeware Syslog Message Generator for Windows.

Latest version available from: http://www.kiwisyslog.com

Kiwi SyslogGen sends Unix type Syslog messages created from the GUI to a host running a Syslog Server.

Kiwi SyslogGen can be used to test a Syslog Server setup and diagnose communication problems.

Features

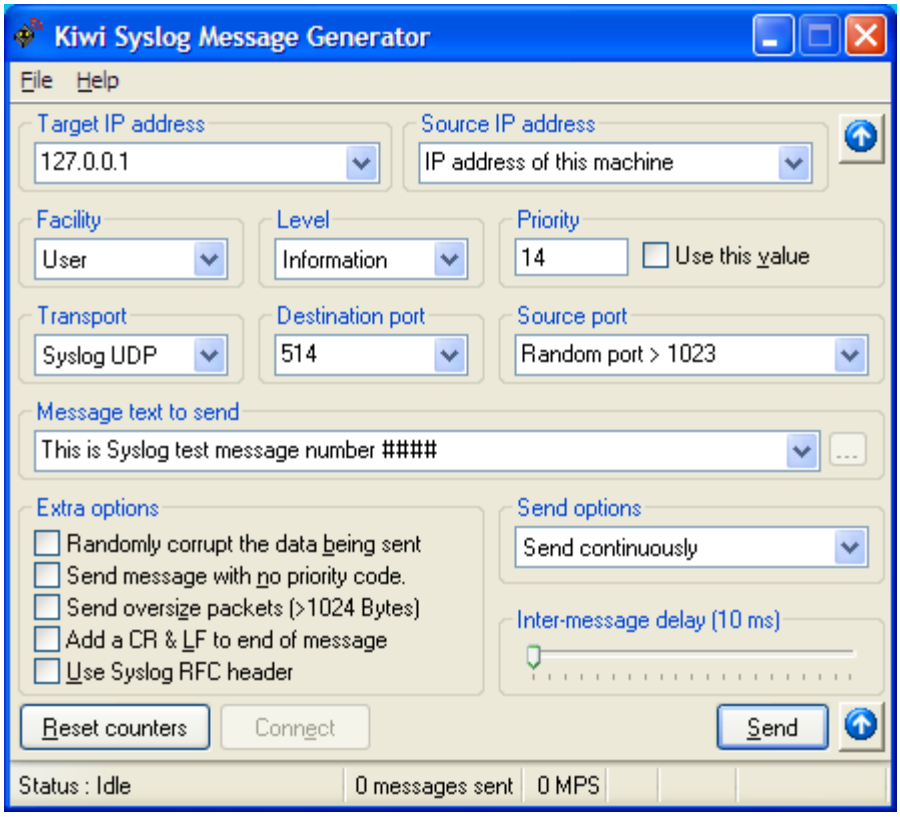
- GUI Interface
- Sends standard Unix Syslog messages (or enhanced messages compatible with Kiwi Syslog Server)
- Fast and simple to use
- Free to use for as long as you like
- Fully test your Syslog Server setup
- Create BSD Syslog Daemon RFC3164 compliant message headers
- Send messages using either UDP or TCP protocol
- Can send sequentially numbered messages
- Can replay syslog messages from an Ethereal capture file

Message creation options

- Priority selection of any Facility and Level including random
- Ready made messages or user entered text
- Frequency of delivery (once, every second, every minute, continuously or burst mode)
- Message proxying compatible with Kiwi Syslog Server*
- Random corrupt packets can be generated to test the robustness of the receiving Syslog Server server

* Message proxying allows messages to go from one Syslog Server to another and still retain the originator's IP address in the host name field.

2 The SyslogGen GUI



2.1 Target IP Address

The target IP address is the machine you want to send the Syslog messages to. The target machine must be running a Syslog Server program in order for the messages to be received.

Kiwi Syslog Server is a freeware Syslog Server for Windows and is available from:
http://www.kiwisyslog.com

The target host address can be specified either as a standard IP address or as a host name.
To send a message to the local machine use the localhost address of 127.0.0.1

Examples:
127.0.0.1
192.168.1.1
10.0.30.23
logginghost.company.com

2.2 Source IP Address

The source IP address is normally left as the default of "IP address of this machine"

When Kiwi Syslog Server forwards a message to another Syslog Server, it adds a tag to the message text to indicate the original sending host of the message. The message can be sent through multiple relays without loosing the identity of the original message sender.
The tag 'original address=192.168.0.1' is added to the text straight after the <PRI> value. If the 'Use Syslog RFC header' option is checked, the tag is added after the Syslog header.
When you specify a different address as the source IP address, the value is inserted into the 'original address=' tag. If "IP address of this machine" is specified, no original address tag is inserted into the text.
Kiwi Syslog Server automatically removes the tag before logging or forwarding the messages.

Entering a specific IP address

You can type over the selected list options and use a specific IP address. The source IP address must be specified as a standard IP address NOT as a host name.

Examples:
IP address of this machine (Default)
192.168.0.1
10.0.0.25
logginghost.company.com
192.168.1.? (This will generate a random host between 192.168.1.1 and 192.168.1.254)

IP address of this machine

No additional 'original address=' tag is inserted into the message text. The message will originate from this host.

Random Class C addresses

Automatically generates a random class C IP address for each message it sends. This is useful for testing the DNS resolver on the Syslog Server. Each message will appear to come from a different host and will require reverse DNS resolution.

Random host on this subnet

This option takes the IP address of the current machine and generates a random value from 1 to 254 for the 'host' portion of the IP address (assumes a class C mask). For example, if your machine address is 192.168.1.100. Random addresses will be picked between 192.168.1.1 and 192.168.1.254.

2.3 Facility

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value. The priority is enclosed in "<>" delimiters.

A BSD Unix Syslog message looks like this:
<PRI>HEADER MESSAGE
The priority is a value from 0 to 191 and is not space or leading zero padded.
For more information on the Syslog message format, please read the RFC.

The Facility value is a way of determining which process of the machine created the message. Since the Syslog protocol was originally written on BSD Unix, the Facilities reflect the names of Unix processes and Daemons.
The priority value is calculated using the following formula:
Priority = Facility * 8 + Level

The list of Facilities available:

```
0     kernel
1     user
2     mail
3     daemon
4     authorization
5     syslogd
6     line printer subsystem
7     news
8     UUCP
9     cron
10    security
11    FTP
12    NTP
13    log audit
14    log alert
15    clock daemon
16    local use 0  (local0)
17    local use 1  (local1)
18    local use 2  (local2)
19    local use 3  (local3)
20    local use 4  (local4)
21    local use 5  (local5)
22    local use 6  (local6)
23    local use 7  (local7)
```

If you are receiving messages from a Unix system, it is suggested you use the "user" Facility as your first choice. Local0 through to Local7 are not used by Unix and are traditionally used by networking equipment. Cisco routers for example use Local6 or Local7.

2.4 Level

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value. The priority is enclosed in "<>" delimiters.

A BSD Unix Syslog message looks like this:
<PRI>HEADER MESSAGE
The priority is a value from 0 to 191 and is not space or leading zero padded.
For more information on the Syslog message format, please read the RFC.

The priority value is calculated using the following formula:
Priority = Facility * 8 + Level

The list of severity Levels:

```
0     Emergency: system is unusable
1     Alert: action must be taken immediately
2     Critical: critical conditions
3     Error: error conditions
4     Warning: warning conditions
5     Notice: normal but significant condition
6     Informational: informational messages
7     Debug: debug-level messages
```

Recommended practice is to use the 'Notice' Level for normal messages.

2.5 Priority value

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value. The priority is enclosed in "<>" delimiters.

A BSD Unix Syslog message looks like this:
<PRI>HEADER MESSAGE
The priority is a value from 0 to 191 and is not space or leading zero padded.
For more information on the Syslog message format, please read the RFC.

The priority value is calculated using the following formula:
Priority = Facility * 8 + Level

To manually set a particular priority number, enter a number into the Priority value field and check the 'Use this value' box. This value will be sent in the <PRI> field of the Syslog message. This allows you to use values above 191 (up to 255). Values above 191 are illegal and could cause unknown results.

2.6 Transport

Kiwi Syslog Server can listen for UDP messages and TCP messages. Normally Syslog messages are sent using UDP. Some networking devices such as the Cisco PIX firewall can send messages using TCP to ensure each packet is received and acknowledged by the Syslog Server.

When sending messages using UDP the destination port is usually 514
When sending messages using TCP the destination port is usually 1468

When selecting to send using TCP, the Extra option: Add CR and LF to end of message is automatically selected as well. Messages sent via TCP need a delimiter such as this at the

end of a message to allow the receiving program to readily determine the end of each message.

2.7 Destination Port

Kiwi Syslog Server can listen for UDP messages and TCP messages. Normally Syslog messages are sent using UDP. Some networking devices such as the Cisco PIX firewall can send messages using TCP to ensure each packet is received by the Syslog Server.

When sending messages using UDP the destination port is usually 514
When sending messages using TCP the destination port is usually 1468

2.8 Source Port

Each message that is sent must have a source port. Normally this is automatically generated by the sending device. SyslogGen allows you to specify the source port if you want. Normally you would leave this option set to 'Random port > 1023'. SyslogGen will then allocate the source port for you each time.

Although in the Syslog RFC it is recommended that a source port should be the same as the destination port, it is not always possible to do this with Winsock (Windows Sockets). As an alternative, the RFC recommends that the source port be a consistent value for each message.

SyslogGen won't let you set the Source port the same as the Destination port because of the Winsock limitations.

2.9 Message text options

This drop down list allows you to select the message text to send. You can replace the text with any message text you want to send. Just type over the existing text.

Ready made messages:

The following 'canned' messages are available:
This is a test message generated by Kiwi SyslogGen
The quick brown fox jumps over the lazy dog
ALL YOUR BASE ARE BELONG TO US*

*http://www.planettribes.com/allyourbase/index.shtml

This is Syslog test message number

This sends sequenced messages that allow you to see if a message has been missed at the receiving Syslog Server.
Kiwi Syslog Server automatically looks for this sequenced message text and will beep if a message is missed.
Message numbers start at 1 and go to 999999. They then start back at 1 again.
To reset the sequence number back to 1, press the 'Reset counters' button.

Test user connected to website...

Test user connected to website http://###.###.###.###/index.html
This will generate a random IP address in place of the hashes. This can be used to test the DNS resolution options of the Syslog Server.

MultiLine text message

When this option is selected, a popup window will ask you to enter a multi line text message. Normally Syslog messages should only contain a single line of text so they can be read easily. When a multi line message is sent, each line is terminated with a carriage return and line feed.

Random string of text

This generates a random length message of random text characters. This is useful to see if the Syslog Server is capable of displaying all the random information.

From tab delimited text file

When this option is selected you can specify the text file to read from by pressing the … button.
The text file is expected to be a tab delimited text file created by Kiwi Syslog Server.

The fields should be:
`Date Time <TAB> Priority <TAB> Hostname <TAB> Message text`

Only the 4th field (Message text) is used, all other fields are ignored. This is useful for replaying messages already received by Kiwi Syslog Server.

From a Hex byte code text file. (One packet per line)

When this option is selected you can specify the text file to read from by pressing the … button.
The text file is expected to contain a series of 2 digit hexadecimal values separated by a space. Each line represents a separate message. Each line must begin with the string "HEX=" followed by the hexadecimal characters.

For example:
HEX=31 32 33 41 42 43

This will be sent out as "123abc"

From a Ethereal capture file

When this option is selected you can specify the text file to read from by pressing the … button.
Kiwi SyslogGen will scan the Ethereal capture file for any UDP syslog messages sent to port 514. Each valid syslog message found will be sent sequentially. When the last message in the file is sent, it will loop back to the beginning of the file and start again.

More information on Ethereal can be found at: www.ethereal.com

If you check the option called "Send message with no priority code", the messages will be sent using the priority value found in the capture file. With this option unchecked, the priority value will be what ever is set in the GUI options.

2.10 Extra options

Randomly corrupt the data being sent

This option will randomly change a character of the message to a random value. This is used to test the ability of the Syslog Server to handle unexpected data. In real life, if the data is corrupted the UDP or TCP checksum would fail the test and the packet would be dropped by Winsock before it ever reached the Syslog Server.

Send message with no priority code

The BSD Unix Syslog RFC states that each message must start with a valid priority code delimited by '<>'. Some network devices do not obey this rule and simply send the messages on UDP port 514 without a priority code.
This option can be used to see how the Syslog Server handles illegal messages.

Send oversize packets

Normally, Syslog messages must not exceed 1024 bytes in total length. This option pads the end of the message with 4096 space characters to see how the Syslog Server handles it.
Messages should be either dropped or truncated.

Add CR and LF to end of message

Normally Syslog messages don't contain carriage return or line feed characters. Some network devices such as the Cisco PIX firewall terminate the message text with a CR and LF. This option allows you to simulate this type of device by adding a CR and LF to the end of each message.

Use Syslog RFC header

This option ensures that the correct BSD Syslog header is used for the message.
More info about the format of the header can be found in the BSD Syslog RFC.

The HEADER part contains a timestamp and an indication of the host name or IP address of the device.
The HEADER contains two fields called the TIMESTAMP and the HOSTNAME.
The TIMESTAMP will immediately follow the trailing ">" from the PRI part and single space characters MUST follow each of the TIMESTAMP and HOSTNAME fields.
HOSTNAME will contain the host name, as it knows itself. If it does not have a host name, then it will contain its own IP address.
The TIMESTAMP field is the local time and is in the format of:
"Mmm dd hh:mm:ss" (without the quote marks).

The MSG part has two fields known as the TAG field and the CONTENT field. The value in the TAG field will be the name of the program or process that generated the message.

The CONTENT contains the details of the message. This has traditionally been a free form message that gives some detailed information of the event. The TAG is a string of ABNF alphanumeric characters that MUST NOT exceed 32 characters. Any non-alphanumeric character will terminate the TAG field and will be assumed to be the starting character of the CONTENT field. Most commonly, the first character of the CONTENT field that signifies the conclusion of the TAG field has been seen to be the left square bracket character ("["), a colon character (":"), or a space character

Kiwi SyslogGen uses the following format for its messages:
<PRI>Jul 10 12:00:00 192.168.1.1 SyslogGen MESSAGE TEXT

The TAG field is "SyslogGen"
The host name is specified as an IP address

2.11 Send message options

- Send message once
- Send once a second
- Send once a minute
- Send continuously
- 100 packet burst every 10 seconds
- 500 packet burst every 10 seconds

When the 'Send continuously' option is used the inter-message delay can be set by using the slider control.

The 100 and 500 packet burst mode is a "best effort" approach. SyslogGen tries to send as many messages as it can in a burst. This could overload the output buffers and packets could be dropped by routers between SyslogGen and the Syslog Server.

2.12 Inter-message delay

The inter-message delay slider sets the number of milliseconds between each message. This only applies when the send message options is set to 'Send continuously'

The value in milliseconds is indicated by the tool tip text as you move the slider. Setting the delay to 1000 will send a message every second. Setting the delay to 200 will send 5 messages per second etc.

2.13 Reset counters

When the message text option is set to "This is Syslog test message number ####" each message contains a sequence number in place of the hashes.
To reset this count back to 0000 press the reset counters button.

When the message text option is set to read data from a file, the Reset counters button will reset the pointer to the beginning of the file. The next message sent will be the first line of the text file selected.

2.14 Connect

The connect button is only used when TCP transport is selected. Before a message can be sent, the TCP connection must be established first. If you press the Send button before making a connection, SyslogGen will attempt to make the connection automatically. Use the connect button to connect and disconnect the TCP session to the Syslog Server.

If the TCP connection is disconnected remotely you will hear a sound and the status display will indicate that the connection was terminated remotely.

2.15 Send message button

This button stops and starts the sending of messages.

2.16 Window size

The  button toggles the window size. The small window size option gives you more space on the screen. This can be used when you have set all the options and only want to stop and start the message sending.

The small window size mode looks like:

Index

- K -