Kiwi Syslog Server

A Syslog Server for Windows

SolarWinds, Inc.

Kiwi Syslog Server is a Syslog Server for the Windows platform. It receives, logs, displays and forwards Syslog messages from hosts such as routers, switches, Unix hosts and any other syslog enabled device. There are many customisable options available.

Features include: PIX firewall, LinkSys home firewall, SNMP Trap and TCP support. A Service Edition is available for use on 2K/XP/2k3/Vista/2K8/2K8 R2/2K12/2K12 R2.



Table of Contents

Foreword 0

Part I Kiwi Syslog Server 1

1 Features in the licensed version ... 1
2 Features in the free version ... 3
3 How to purchase the licensed version ... 3
4 Initial Setup of Kiwi Syslog Server ... 4
Overview - Getting Started ... 4
5 Feedback - Comments or Bugs ... 4
6 End User License Agreement (EULA) ... 4

Part II The main display window 9

1 The main display window ... 9
2 File menu ... 10
Setup ... 10
Send Test message to local host (Ctrl-T) ... 10
Purge ... 11
Debug options ... 11
Create Tech-Support File (Zip) ... 11
Export settings to INI file ... 11
Exit ... 12
3 Edit menu ... 12
Select All ... 12
Copy selected items to the clipboard ... 12
4 View menu ... 12
View syslog statistics ... 12
View e-mail log file ... 12
View error log file ... 12
Adjust width to fit screen ... 12
Clear display ... 13
Highlighting Options ... 13
Choose font ... 14
5 Manage menu ... 15
Manage menu ... 15
Install the Syslogd service ... 15
Uninstall the Syslogd service ... 15
Start the Syslogd service ... 15
Stop the Syslogd service ... 15
Ping the Syslogd service ... 15
Show the Syslogd service state ... 16
Debug options menu ... 16
Display the service version ... 16
Get diagnostic information ... 16
Reset the Syslogd service ... 16
Clear the service DNS Cache ... 16

©2014 SolarWinds, Inc.

Apply new settings to Syslogd service ... 16
Retrieve last messages ... 17
Send keep alive ... 17
Enable Service Debug Mode ... 17
6 Help menu ... 17
Context based Help (F1) ... 17
Help Topics ... 17
Online FAQ ... 17
Purchase the licensed version ... 17
Enter license details (F2) ... 17
Make a suggestion or report a bug ... 17
Check for update... ... 18
About Kiwi Syslog Server ... 18
Part III Configuring the Syslog properties 18
1 Guide to initial Syslog Server Setup ... 18
2 How to navigate using the keyboard ... 18
3 Rules / Filters / Actions ... 19
How the rule engine works ... 19
Filter types ... 19
Simple filter ... 19
Complex filter ... 20
Regular Expression filter ... 21
IP Address Range filter ... 24
IP Subnet Mask filter ... 25
Priority filter ... 26
Time of Day filter ... 27
Time Interval filter ... 28
Threshold filter ... 29
Timeout filter ... 30
Importing and Exporting a filter definition ... 30
Input source ... 31
Action - Display ... 31
Action - Log to file ... 31
Action - Log to file ... 31
AutoSplit values ... 31
Log file formats ... 35
Log File Rotation ... 37
Action - Forward to another host ... 38
Action - Play a sound ... 40
Action - Run external program ... 40
Action - E-mail message ... 42
Insert message content or counter ... 43
Action - Send Syslog message ... 44
Action - Log to ODBC database ... 45
Action - Log to Database ... 45
Problems logging when running as a Service ... 48
Action - Log to NT Event log ... 48
Action - Log to NT Event log ... 48
Setting the log insertion type ... 48
Action - Send pager or SMS message via NotePage Pro ... 49
Action - Send ICQ instant message ... 50

©2014 SolarWinds, Inc.

Action - Send SNMP Trap ... **52**
Action - Stop processing message ... **53**
Action - Run Script ... **53**
Tutorial - creating your first script ... 55
The script variables ... 57
The script functions ... 60
The scripting dictionaries ... 67
Script examples ... 70
PIX message lookup ... 70
All the variables - (Info function) ... 72
JScript escape characters ... 72
Action - Log to Syslog Web Access ... **73**
Action - Reset Flags/Counters ... **73**
4 Setup - Schedules ... **73**
How the scheduler works ... **73**
On a schedule ... **76**
On application/service startup ... **79**
On application/service shutdown ... **80**
Archive task ... **80**
Clean-up task ... **85**
Run Program task ... **88**
Run Script task ... **90**
Schedule Report ... **92**
5 Setup - Formatting ... **92**
Custom file formats ... **92**
Custom DB formats ... **93**
6 Setup - DNS Resolution ... **95**
Resolve the address of the sending device ... **95**
Remove the domain name (show only the host name) ... **95**
Resolve IP addresses found within the syslog message text ... **95**
DNS query timeout ... **96**
Setup - DNS Setup ... **97**
Internal IP address - Name Resolution ... 97
External IP address - Name Resolution ... 98
Setup - DNS Cache ... **98**
The local DNS cache ... 98
Cache settings ... 98
7 Setup - Modifiers ... **99**
Syslog message modifiers ... **99**
8 Setup - Scripting ... **100**
9 Setup - Appearance ... **101**
Wallpaper ... **101**
10 Setup - E-mail options ... **101**
E-mail setup options ... **101**
An example Alarm message ... **103**
An example Statistics message ... **104**
11 Setup - Alarm thresholds ... **104**
Notify by Mail ... **104**
Audible Alarm ... **105**
Run Program ... **105**
12 Setup - Input options ... **105**

©2014 SolarWinds, Inc.

Setup - Input options ... 105
Inputs - UDP ... 105
Inputs - TCP ... 106
Inputs - Secure (TLS) Syslog ... 107
Inputs - SNMP ... 108
Beep on every message received ... 110
Cisco PIX Firewall (TCP) ... 111
Inputs - Keep-alive ... 111
13 Setup - Display ... 112
Always on top ... 112
Rows of scrolling display ... 112
Minimize to System Tray on start-up ... 113
Use 3D titles ... 113
Use dd-mm-yyyy date format (non US format) ... 113
Show messages per hour in title bar ... 113
Blink System Tray Icon when receiving messages ... 113
Word wrap ... 113
Adjust column widths automatically ... 113
14 Enabling SSL ... 113
15 Setup - Product Updates ... 114
16 How the Test button works ... 115
Part IV The Syslog statistics window 116
1 The Syslog statistics window ... 116
2 1 Hour history ... 116
3 24 Hour history ... 116
4 Severity ... 116
5 Top 20 Hosts ... 117
6 Counters ... 117
Part V Kiwi Syslog Server Service Edition 118
1 Kiwi Syslog Server Service requirements ... 118
2 Installing Kiwi Syslog Server as a Service ... 118
3 Managing the service edition ... 119
4 Troubleshooting the Service edition ... 120
5 Upgrading to a new version of Kiwi Syslog Server NT Service ... 120
Upgrading to a new version of Kiwi Syslog Server NT Service ... 120
Steps to remove existing version ... 121
Steps to installing the new version ... 121
Part VI Configuring Syslog enabled devices 121
1 Configuring Log Forwarder to capture Windows Event logs ... 121
2 Configuring a 3Com NetServer ... 122
3 Configuring a 3Com Total Control Chassis ... 122
4 Configuring an Alliant Cellular Gateway ... 123

©2014 SolarWinds, Inc.

5 Configuring an Allied Telesyn router ... 124
6 Configuring an Arris Cable Modem Termination System ... 124
7 Configuring an Extreme Summit switch ... 124
8 Configuring a Barracuda Spam Firewall ... 125
9 Configuring a Bay Networks device ... 125
10 Configuring a Bintech access router ... 128
11 Configuring a BuffaloTech AirStation Router ... 129
12 Configuring a Checkpoint FW-1 firewall ... 129
13 Configuring a Cisco 3000 series VPN concentrator ... 129
14 Configuring a Cisco Catalyst switch ... 130
15 Configuring a Cisco PIX ... 130
16 Configuring a Cisco Router ... 131
17 Configuring a Cisco Wireless device (Aironet) ... 131
18 Configuring a D-Link DFL-700 firewall ... 132
19 Configuring a DLink DL-840V router ... 132
20 Configuring a FortiGate Anti-Virus Firewall ... 132
21 Configuring a FREESCO router/firewall ... 133
22 Configuring a HP JetDirect Printer ... 133
23 Configuring a Intertex ADSL router ... 134
24 Configuring a Linksys firewall ... 134
25 Configuring a Linksys wireless VPN router ... 134
26 Configuring a Lucent router ... 135
27 Configuring a Meinberg time server ... 135
28 Configuring a Netgear / ZyXEL RT311/RT314 ... 136
29 Configuring a Netgear ADSL Firewall Router DG834 ... 137
30 Configuring a Netgear FVS318 VPN Firewall ... 137
31 Configuring a Netgear RP114 Router ... 137
32 Configuring a NetScreen firewall ... 138
33 Configuring a Nortel Networks router ... 139
34 Configuring the Pack X IDScenter ... 139
35 Configuring a SnapGear SOHO+ ... 140
36 Configuring a SonicWall firewall ... 140
37 Configuring a Symantec Firewall/VPN 200 ... 141
38 Configuring a Unix machine ... 141
39 Configuring a VegaStream Telephony Gateway ... 142
40 Configuring a Watchguard Firebox to work with DShield ... 142
41 Configuring a WatchGuard SOHO firewall ... 143
42 Configuring a W-Linx MB Broadband router ... 143
43 Configuring a ZyXEL ZyWALL 10 ... 143

©2014 SolarWinds, Inc.

Part VII Configuring SNMP Trap generating devices 144

1 Configuring Cisco IOS SNMP Trap support ... 144

Part VIII The Syslog Server error and e-mail logs 144

1 The error log ... 144
2 To view the error log file ... 144
3 The SMTP mail log ... 144
4 To view the e-mail log file ... 145

Part IX The Syslog Protocol 145

1 Syslog Facilities ... 145
2 Syslog Levels ... 146
3 Syslog Priority values ... 147
4 Transport ... 147
5 Syslog RFC 3164 header format ... 147
6 The Kiwi Reliable Delivery Protocol (KRDP) ... 148
KRDP Error Messages ... 150

Part X Troubleshooting 151

1 Troubleshooting ... 151
2 Running on Windows XP SP2 or Windows 2003 Server SP1 ... 151

Part XI Advanced Information 152

1 Registry settings for Kiwi Syslog Server ... 152
Display - Enabled columns ... 152
Display - Default row height ... 153
Statistics mail delivery time ... 153
Service - Start/Stop Timeout ... 154
Service - Properties Update Timeout ... 154
Service - Inter-App communication port ... 155
Service - Dependencies ... 155
Service - Debug start-up ... 156
DNS - Disable wait when busy ... 157
DNS - Max cache size ... 158
DNS - Cache Failed Lookups ... 158
DNS Setup - DNS/NetBIOS queue buffer burst coefficient ... 159
DNS Setup - DNS/NetBIOS queue buffer clear rate ... 159
DNS Setup - DNS/NetBIOS queue limit ... 160
DNS Setup - Debug Mode ... 160
Message buffer size ... 161
E-mail - Additional subject text ... 161
E-mail - Additional body text ... 162
E-mail - Limiting the messages sent ... 163
File write caching ... 164
File logging - Date separator character ... 166
File logging - Time separator character ... 167

©2014 SolarWinds, Inc.

File logging - Encoding format ... 168
Script Editor ... 169
Script Timeout ... 169
Database Command Timeout ... 170
Archiving - Replacement character ... 170
Archiving - Separation character ... 171
Archiving - Use Old Archive Naming Convention ... 172
Archiving - Archive Temp Path ... 172
Archiving - Enable Temp File ... 173
Error Log Folder ... 173
Mail Log Folder ... 174
KRDP - ACK timer ... 174
KRDP - Keep Alive timer ... 175
KRDP - Disk cache folder ... 175
KRDP - Rx Debug ... 175
KRDP - Tx Debug ... 176
KRDP - Queue size ... 176
KRDP - Queue Max MB Size ... 177
KRDP - AutoConnect ... 177
KRDP - Connect time ... 178
KRDP - Send speed ... 178
KRDP - IdleTimeout ... 179
KRDP - Add SeqNum ... 179
Syslogd Process Priority ... 180
Originating Address - Custom Start and End tags ... 181
Rules - Maximum Rule Count ... 182
Database Logger - Cache Clear Rate ... 182
Database Logger - Cache Timeout ... 183
Database Logger - Disable Database Cache ... 183
Statistics Report – No of Hosts to Show ... 184

2 Command-line arguments ... 184

Start-up Debug ... 184
Service - Install Service ... 185
Service - Uninstall Service ... 185

3 Automating the installation of Kiwi Syslog Server ... 186

4 Using an INI file to automatically configure the settings ... 186

5 Ports used by Kiwi Syslog Server ... 187

Part XII Other Kiwi Software 187

1 Kiwi CatTools ... 187

2 Kiwi SyslogGen ... 187

3 Kiwi Logfile Viewer ... 188

4 Kiwi Secure Tunnel ... 188

5 Kiwi Harvester ... 188

Index 0

©2014 SolarWinds, Inc.

1 Kiwi Syslog Server

Kiwi Syslog™ Server

A Syslog Server for Windows

Program copyright 1998 - 2014 SolarWinds, Inc. All rights reserved.

Latest version available from: www.kiwisyslog.com

Support: http://www.kiwisyslog.com/support/

Kiwi Syslog Server receives syslog messages from network devices, and displays them in real-time.

Syslog messages can then be processed using events like:

- Display the message in the scrolling window
- Logging the message to a text file
- Forward the message to another syslog server
- Log to an ODBC database
- Log to the NT Application Event Log
- E-mail the message to someone via SMTP
- Triggering a sound alarm
- Running an external program such as a paging notification system
- Send an SNMP Trap message
- Page someone using NotePager Pro
- Log to Kiwi Syslog Web Access

Actions can be performed on received messages. Messages can be filtered by host name, host IP address, priority, message text or time of day.

The installation package allows you to install Kiwi Syslog Server in one of two ways:

- As a Windows Service for use on Windows XP, Windows 2003, Windows Vista, Windows 2008, Windows 7,Windows 8, Windows 2008 R2, Windows 2012 or Windows 2012 R2
- As a Standard interactive Windows application for use on Windows XP, 2003, Vista, 2008, Windows 7, Windows 8, Windows 2008 R2, Windows 2012 or Windows 2012 R2

The Standard application runs interactively and only operates while a user is logged on to the system.

The Service runs as an automatic Windows Service. Installing Kiwi Syslog Server as a service means that a user does not need to be logged on to the system for Kiwi Syslog Server to operate.

The Kiwi Syslog Service Manager program provides the interface to configure and manage the Windows NT service.

The BSD Syslog protocol is defined in RFC 3164.
http://community.roxen.com/developers/idocs/rfc/rfc3164.html

1.1 Features in the licensed version

Logging to Kiwi Syslog Web Access:

- Gives users the ability to view their Syslog data from anywhere on the network.
- Allows users to save Web Access views using custom filters and highlighting rules.

Additional Auto Split log file options:
- Host name
- Host IP address
- Domain name
- WELF format tags in message text
- Input Source (TCP/UDP/SNMP)

Additional filtering options:
- Filter on IP address, host name or message text.
- Filter out unwanted host messages or take a different logging action depending on the host name.
- Filter on messages containing specific keywords.

Additional actions
- Powerful scripting engine for filtering, parsing, custom statistics and performing subsequent actions
- Log to an ODBC-compliant database. (Access/SQL/Oracle/MySQL/Informix etc)
- Write logs to the Windows NT application Event Log
- Play the sound file of your choice when the filter conditions are met.
- Forward the received Syslog messages via e-mail.
- Send a Syslog message to another host when the filter conditions are met.
- Send an SNMP trap (Version 1 or Version 2)
- Send ICQ Instant message
- Send a pager or SMS message via NotePager Pro
- Run an external program of your choice when the filter conditions are met.
- Pass values from the received Syslog message to an external program, e-mail message or Syslog message, such as:

  - Message text
  - Time of message
  - Date of message
  - Hostname
  - Facility
  - Level
  - Alarm threshold values
  - Current Syslog statistics

Additional buffering:
- A buffer for 20,000 Syslog messages to ensure you don't miss messages under heavy load.
- A buffer for 1000 e-mail messages to ensure all e-mail gets through under heavy load or if the mail server is unavailable temporarily.

Additional DNS capabilities:
- Resolve all IP addresses contained in the message text to hostnames
- Either replace the IP address with the hostname, or place the hostname next to the IP address
- The DNS cache will hold up to 20,000 entries. Supports maximum 1000000 by making an entry "DNSCacheMaxSize" with the value "1000000" in the Registry.
- The DNS pre-emptive lookup can spawn up to 200 threads.

Additional alarm options:
- Play the sound file of your choice when an alarm condition is reached.
- Run an external program when an alarm condition is reached. This could be a pager or SMS program.

Benefits of using the Registered version:
- Greater flexibility in managing and inspecting log files produced by Kiwi Syslog Server. Particularly in larger networks, the ability to provide timely and relevant status and event information is of great value to the network manager. The additional Auto Split log file options support this ability by easy and natural segregation of incoming messages into unique log files. These can then be used to create reports on specific devices, events, conditions, or other items of specific interest to your organisation.

- Additional Filtering options for greater and simpler control of subsequent actions. A large number of additional actions that can be automatically initiated as a result of incoming messages, filters, and rules. In particular, the increase in notification methods meets the needs of an increasingly mobile business culture.

©2014 SolarWinds, Inc.

- A much larger buffering capacity. This increased capacity greatly increases the scale of the network that can be supported, as well as more reliably handling peak busy periods or message spikes.

The free version of Kiwi Syslog Server includes the following features.

1.2 Features in the free version

The free version of Kiwi Syslog Server includes the following features:

- Limited to 5 devices
- GUI based syslog manager
- 10 virtual displays for organizing your messages
- Message logging or forwarding of all messages, or based on priority or time of day.
- Auto Split the log file by priority or time of day
- Receives messages via UDP, TCP or SNMP
- Forwards messages via UDP or TCP
- Messages per hour alarm notification with audible sound or e-mail
- Log file size alarm notification with audible sound or e-mail
- Daily e-mailing of syslog traffic statistics
- Minimizes to the system tray
- Maintains source address when forwarding messages to other syslog hosts
- Syslog statistics with graph of syslog trends (Last 24 hrs/Last 60 mins.)
- Syslog message buffering ensuring messages are not missed under heavy load
- DNS resolution of source host IP addresses with optional domain removal
- DNS caching of up to 100 entries to ensure fast lookups and minimize DNS lookups
- Pre-emptive DNS lookup using up to 10 threads
- Comes with 5 cool skins to change the look of the program
- Selectable display font, display color, and background wallpaper
- Available as an NT Service
- RFC3164 send and receive options
- Context based help

See what features the Licensed version offers.

1.3 How to purchase the licensed version

To purchase your copy of Kiwi Syslog Server visit the Kiwi Syslog Server website at:

http://www.kiwisyslog.com/how-to-buy.aspx

Alternatively, you can click the **Help | About** menu on Kiwi Syslog Server and then use the link provided, to take you to the registration page.

©2014 SolarWinds, Inc.

1.4 Initial Setup of Kiwi Syslog Server

Kiwi Syslog Server is designed to be as flexible and as easy to use as possible. For this reason it is extremely easy to initially setup.

To setup Kiwi Syslog Server all you need to do is install the application in the desired location on your system. By default it will listen for syslog messages that are sent to UDP port 514.

For the basic configuration no further setup is required.

To have Kiwi Syslog Server receive syslog messages you will need to configure your sending network devices to send their information to the IP address of the system that Kiwi Syslog Server is installed on.

Instructions on how to configure most devices can be found in the Configuring syslog enabled devices section.

If you have a device that sends syslog messages that is not listed in this section then please send the setup information to http://www.kiwisyslog.com/support/ for inclusion in the next help file release.

1.4.1 Overview - Getting Started

By default when Kiwi Syslog Server is installed it contains a single Rule that has no Filters. This means that all syslog messages that arrive are processed by the Actions in this Rule. The Rule contains two separate Actions: a "Display" Action which displays all information received to Display00 'in real time'; and a "Log to File" Action. This Action logs all the information to a file called "SyslogCatchall.txt" which is located in the \Logs directory of your Kiwi Syslog installations folder.

This is a very basic initial setup for Kiwi Syslog Server. If this Rule is turned off or deleted, no messages will be displayed or logged to file.

To manage your syslog messages, you can create further filters and actions that will allow you to process the messages to your own requirements.

1.5 Feedback - Comments or Bugs

If you have any comments about this program or improvements you would like to see in the next version, please feel free to contact the author via e-mail on: http://www.kiwisyslog.com/support/

Please also check the Thwack (SolarWinds community) website forums at: http://thwack.solarwinds.com/community/tools_tht/kiwi-syslog

1.6 End User License Agreement (EULA)

SOLARWINDS
END USER LICENSE AGREEMENT

This End User License Agreement (the “Agreement”) is hereby entered into and agreed upon by you, either an individual or an entity, and its Affiliates (defined below) (“You” or “Company”) and **SolarWinds Worldwide, LLC** (“SolarWinds Worldwide”) for the Software (as defined below).

1. DEFINITIONS.

©2014 SolarWinds, Inc.

1.1 "Affiliates" means an entity controlled by, under common control with, or controlling such party, where control is denoted by having fifty percent (50%) or more of the voting power (or equivalent) of the applicable entity. Subject to the terms and conditions of this Agreement, Affiliates may use the license granted hereunder. All references to SolarWinds shall be deemed to be references to SolarWinds and its Affiliates, and all references to Company, You, or Your shall be deemed to be references to Company and its Affiliate(s).

1.2 "**Computer**" means the hardware, if the hardware is a single computer system, whether physical or virtual, or means the computer system with which the hardware operates, if the hardware is a computer system component.

1.3 "Documentation" means the user documentation provided by SolarWinds Worldwide to You on the use of the Software. For the avoidance of doubt, any installation guide or end user documentation not prepared or provided by SolarWinds; any online community site; or feedback does not constitute Documentation.

1.4 "**Software**" means the object code versions of the product, together with the updates, new releases or versions, modifications or enhancements, owned and provided by SolarWinds Worldwide to You pursuant to this Agreement.

2. GRANT OF LICENSE.

2.1 Production License. Upon payment of the applicable fees for the Software and continuous compliance with the terms and conditions of this Agreement, SolarWinds Worldwide hereby grants You a limited, perpetual, nonexclusive, nontransferable license to use the object code of the Software and Documentation in Your facility subject to the terms contained herein:

a) For each Software license key that You purchase from SolarWinds Worldwide, You may: (i) use the Software on any single Computer, unless the Documentation clearly indicates otherwise; and (ii) copy the Software for back-up and archival purposes, provided any copy must contain all of the original Software's proprietary notices and a notice that it will not be used for transfer, distribution or sale.

b) The Software is in use on a Computer when it is loaded into temporary memory or installed in permanent memory (hard drive, CD-ROM or other storage device). You agree to use Your reasonable efforts to prevent and protect the contents of the Software and Documentation from unauthorized use or disclosure, with at least the same degree of care that You use to protect Your own confidential and proprietary information, but in no event less than a reasonable degree of care under the circumstances. You agree that You will register this Software only with SolarWinds and that You will only install a Software license key obtained directly from SolarWinds.

2.2 Software Evaluation License. If the Software is provided to You for evaluation purposes, SolarWinds Worldwide grants to You a nonexclusive, limited, royalty-free, nontransferable evaluation license to use the Software solely for evaluation prior to purchase (an "Evaluation License"). The Evaluation License shall terminate on the end date of the pre-determined evaluation period or immediately upon notice from SolarWinds at its sole discretion. Notwithstanding any other provision contained herein, Software provided pursuant to an Evaluation License is provided to You "AS IS" without indemnification, support, or warranty of any kind, express or implied. Except to the extent such terms conflict with the specific Evaluation License terms set forth in this Section, all other terms of this End

©2014 SolarWinds, Inc.

User License shall apply to Software licensed under an Evaluation License.

2.3 High Availability and/or Disaster Recovery Purpose License. If You are obtaining a redundant version of the Software solely for high availability and/or disaster recovery purposes for use on Your disaster recovery Computer, You represent and warrant that (i) You may actively run the redundant version of the Software on a Computer, provided it is not running on a primary production Computer, unless (a) the primary production Computer related to the primary production version of the Software fails, (b) the Software or Computer associated with the primary production license is being upgraded or replaced, or (c) other temporary reasons that disrupt all or a material part of Your business operations; (ii) You will not utilize the redundant version of the Software to monitor any items not being monitored by the primary production Computer; and (iii) You will promptly get the primary production Computer hosting the primary production license license operating correctly in order to support Your daily activities.

3. LICENSE RESTRICTIONS.

3.1 You may not: (i) provide, make available to, or permit other individuals to use the Software or Documentation, except under the terms listed above, either in whole or part; (ii) modify, translate, reverse engineer, decompile, disassemble, create derivative works, or otherwise attempt to derive the source code based upon the Software or Documentation; (iii) copy, reproduce, republish, upload, post, or transmit the Software or Documentation (except for back-up or archival purposes, which will not be used for transfer, distribution, or sale); (iv) license, sell, rent, lease, transfer, sublicense, distribute, or otherwise transfer rights to the Software or Documentation; (v) remove any proprietary notices or labels on the Software or Documentation; or (vi) license the Software if You are a direct competitor of SolarWinds for the purposes of monitoring the Software's availability, performance, or functionality or for any other benchmarking or competitive purposes. Any such forbidden use shall immediately terminate Your license to the Software. The Software, including its monitoring, managing, recording, playback, and download features, are intended only for use with public domain or properly licensed third party materials. You might need a third party license to create, copy, download, record or save third-party media or content files for playback by this Software or to serve or distribute such files to be played back by the Software. All responsibility for obtaining such a license is Yours, and SolarWinds shall not be responsible for Your failure to do so.

3.2 SolarWinds Trademarks. You may not delete, remove, hide, move or alter any trademark, logo, icon, image or text that represents the company name of SolarWinds, any derivation thereof, or any icon, image, or text that is likely to be confused with the same. All representations of the company name or mark "SolarWinds" or any of its Affiliates' names or marks must remain as originally distributed regardless of the presence or absence of a trademark, copyright, or other intellectual property symbol or notice.

3.3 Export Restrictions. The Software and Documentation delivered to You under this Agreement are subject to U.S. export control laws and regulations and may also be subject to import and export laws of the jurisdiction in which it was obtained, if outside the U.S. You shall abide by all applicable export control laws, rules and regulations applicable to the Software and Documentation. You agree that You will not export, re-export, or transfer the Software or Documentation, in whole or in part, to any country, person, or entity subject to U.S. export restrictions. You specifically agree not to export, re-export, or transfer the Software or Documentation (i) to any country to which the U.S. has embargoed or restricted the export of goods or services, or to any national of any such country, wherever located, who intends to transmit or transport the products back to such country; (ii) to any person or

©2014 SolarWinds, Inc.

entity who You know or have reason to know will utilize the Software or portion thereof in the design, development, production or use of nuclear, chemical or biological materials, facilities, or weapons; or (iii) to any person or entity who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government.

3.4 Compliance with Applicable Laws. The Software and Documentation are protected by the intellectual property laws and other laws of the United States and international laws and treaties, including intellectual property laws. You agree that You shall use the Software and Documentation solely in a manner that complies with all applicable laws in the jurisdictions in which You use the Software and Documentation, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

4. RIGHTS RESERVED. THE SOFTWARE IS LICENSED, NOT SOLD. Use herein of the word "purchase" in conjunction with licenses, license keys, or the Software shall not imply a transfer of ownership. Unless as conveyed herein, this Agreement does not grant You any rights, title, or interest in or to Software, Documentation, trademarks, service marks, or trade secrets, or corresponding intellectual property (including without limitation any images, photographs, animations, video, audio, music, and text incorporated into the Software, the accompanying printed materials, and any copies of the Software) of SolarWinds or its suppliers, and all rights, title, and interest in and to the Software, Documentation, and corresponding intellectual property shall remain the property of SolarWinds, its suppliers, or are publicly available. All rights not expressly granted under this Agreement are reserved by SolarWinds, its suppliers, or third parties. All title, rights, and interest in and to content, which may be accessed through the Software, is the property of the respective owner and may be protected by applicable intellectual property laws and treaties. This Agreement gives You no rights to such content, including use of the same. SolarWinds agrees that the data and information (including without limitation, computer software, computer database, computer software documentation, specifications, design drawings, reports, blueprints, and the like) generated by the Software from Your proprietary data and information shall be and remain Your sole property.

5. DATA RIGHTS. You agree that SolarWinds will collect and track technical and related information about You and Your use of the Software, which may include Your internet protocol address, hardware identifying information, operating system, application software, peripheral hardware, and Software usage statistics to assist with the necessary operation and function of the Software, the provision of updates, support, invoicing, marketing by SolarWinds or its agents, and research and development. As a reminder, SolarWinds Privacy Policy can be found here (http://www.solarwinds.com/privacy.aspx), and SolarWinds may update its Privacy Policy from time to time.

6. LIMITED WARRANTY. SolarWinds Worldwide warrants to You that for a period of thirty (30) days following the initial purchase and delivery of the Software to You that the Software will perform substantially in conformance with the Documentation. SolarWinds Worldwide does not warrant that the Software will meet all of Your requirements or that the use of the Software will be uninterrupted or error-free. The foregoing warranty applies only to failures in operation of the Software that are reproducible in standalone form and does not apply to: (i) Software that is modified or altered by You or any third party that is not authorized by SolarWinds Worldwide; (ii) Software that is otherwise operated in violation of this Agreement or other than in accordance with the Documentation; or (iii) failures that are caused by other software or hardware products. To the maximum extent permitted under applicable law, as SolarWinds' and its suppliers' entire liability, and as Your exclusive

©2014 SolarWinds, Inc.

remedy for any breach of the foregoing warranty, SolarWinds Worldwide will, at its sole option and expense, promptly repair or replace any Software that fails to meet this limited warranty or, if SolarWinds Worldwide is unable to repair or replace the Software, refund to You the applicable license fees paid upon return, if applicable, of the nonconforming item to SolarWinds Worldwide. The warranty is void if failure of the Software has resulted from accident, abuse, or misapplication. Any replacement Software under this limited warranty will be warranted for thirty (30) days.

EXCEPT AS EXPRESSLY STATED IN THIS SECTION, TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, SOLARWINDS IS PROVIDING AND LICENSING THE SOFTWARE TO YOU "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

7. INTELLECTUAL PROPERTY INDEMNIFICATION. SolarWinds Worldwide will indemnify and hold You harmless from any third party claim brought against You that the Software, as provided by SolarWinds Worldwide to You under this Agreement and used within the scope of this Agreement, infringes or misappropriates any U.S. patent, copyright, trademark, trade secret, or other intellectual property rights of a third party, provided (i) use of the Software by You is in conformity with the Agreement and Documentation; (ii) the infringement is not caused by modification or alteration of the Software or Documentation; and/or (iii) the infringement was not caused by a combination or use of the Software with products not supplied by SolarWinds. SolarWinds Worldwide's indemnification obligations are contingent upon You: (i) promptly notifying SolarWinds Worldwide in writing of the claim; (ii) granting SolarWinds Worldwide sole control of the selection of counsel, defense, and settlement of the claim; and (iii) providing SolarWinds Worldwide with reasonable assistance, information and authority required for the defense and settlement of the claim. This Section states SolarWinds' entire liability (and shall be Company's sole and exclusive remedy) with respect to indemnification to Company.

8. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL SOLARWINDS, ITS DIRECTORS, OFFICERS, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE TO YOU (WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE) (I) FOR MORE THAN THE AMOUNT OF LICENSE FEES THAT YOU HAVE PAID TO SOLARWINDS IN THE PRECEDING (12) TWELVE MONTHS FOR THE APPLICABLE SOFTWARE OR (II) FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE,OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS, LOST BUSINESS OPPORTUNITIES, LOSS OF USE OF THE SERVICE OFFERING, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, LOST SAVINGS, OR OTHER ECONOMIC DAMAGE , ARISING OUT OF THIS AGREEMENT OR THE USE OR INABILITY TO USE THE SOFTWARE OR DOCUMENTATION, EVEN IF SOLARWINDS OR A DEALER AUTHORIZED BY SOLARWINDS HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9. Third Party Programs. To the extent the Software is bundled with third party software programs; these third party software programs are governed by their own license terms, which may include open source or free software licenses. Nothing in this Agreement limits an end user's rights under, or grants the end user rights that supersede, the terms of any such third party software.

10. CHOICE OF LAW AND VENUE. This Agreement shall be governed by the laws of

©2014 SolarWinds, Inc.

the State of Texas and of the United States, without regard to any conflict of laws provisions, except that the United Nations Convention on the International Sale of Goods shall not apply. The parties agree that the provisions of the Uniform Computer Information Transactions Act shall not apply to this Agreement. You hereby consent to jurisdiction of the courts of both the state or federal courts of Texas.

11. COUNTERPARTS AND FACSIMILE SIGNATURE. This Agreement may be executed in counterparts, each of which shall be deemed an original and all of which shall constitute one and the same instrument. The Parties may exchange signature pages by facsimile and such signatures shall be effective to bind the Parties.

12. COMPLETE AGREEMENT. This Agreement constitutes the entire agreement between the Parties and supersedes all prior or contemporaneous communications, agreements and understandings, written or oral, with respect to the subject matter hereof including without limitation the terms of any party or any purchase order issued in connection with this Agreement. If any provision of this Agreement is held to be unenforceable, that shall not affect the enforceability of the remaining provisions. This Agreement shall not be amended or modified except in a writing signed by authorized representatives of each party.

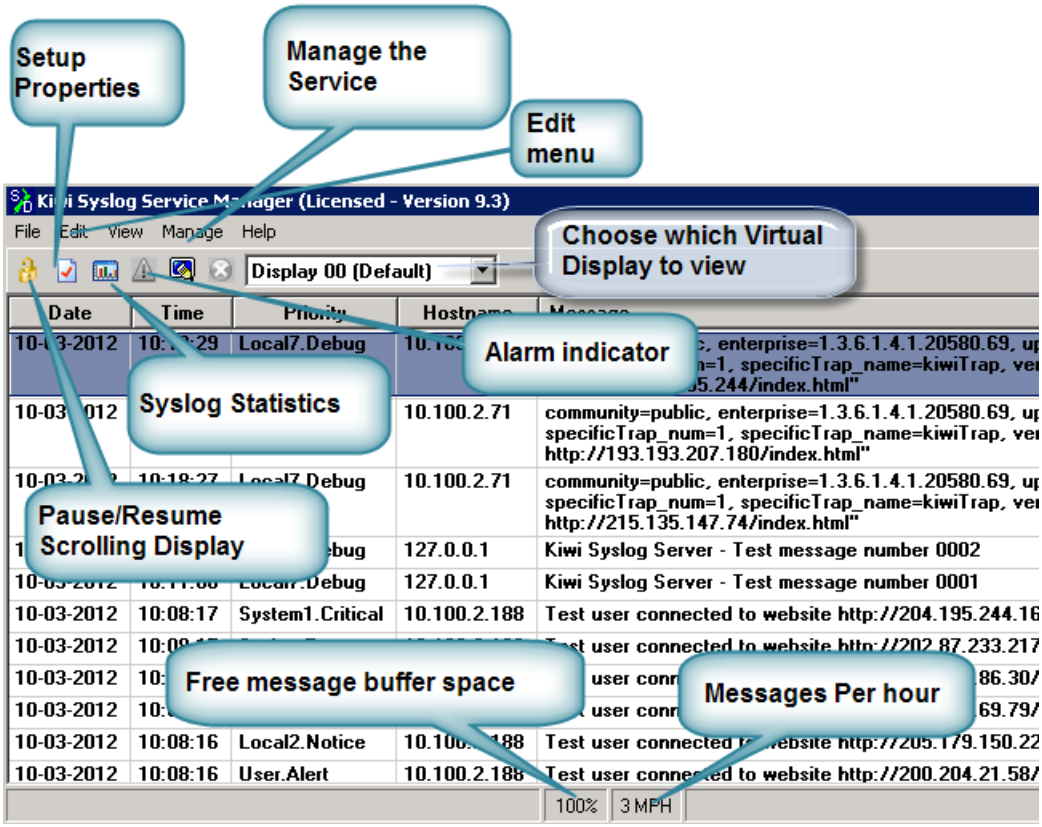
13. RESTRICTED RIGHTS. SolarWinds' Software is provided to non-DOD agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the government is subject to the restrictions as set forth in subparagraph "C" of the Commercial Computer Software – Restricted Rights clause at FAR 52.227-19. In the event the sale is to a DOD agency, the government's rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202. Manufacturer is SolarWinds Worldwide, LLC, 7171 Southwest Parkway, Building 400, Austin, Texas 78735.

2 The main display window

2.1 The main display window

When started, the main display for Kiwi Syslog Server looks like:

©2014 SolarWinds, Inc.



2.2 File menu

2.2.1 Setup

Opens the Kiwi Syslog Server Setup window. This is where you setup the syslog configuration.

2.2.2 Send Test message to local host (Ctrl-T)

This will send a UDP syslog message to 127.0.0.1 (localhost) to ensure the program is functioning correctly. The message is sent to the same port as the Syslog is listening on. To test the TCP setup of the program, please use SyslogGen from http://www.kiwisyslog.com/products/

The test message sent will look like this:

Kiwi Syslog Server - Test message number 0001

The number at the end will increment by one each time the test is performed.

©2014 SolarWinds, Inc.

2.2.3 Purge

Allows you to clear the contents of:

- The e-mail log (InstallPath\SendMailLog.txt)
- The error log (InstallPath\Errorlog.txt)
- The internal syslog message queue (up to 1000 messages)
- The internal e-mail queue (up to 1000 messages)
- The failed MIB lookup file (InstallPath\MIBs\UnknownOIDs.txt)

2.2.4 Debug options

Allows the following options:

- Enable Syslog Debug (Logs all raw received data to InstallPath\Syslogd-debug.txt)
- Reset Syslog socket (closes the listening socket, clears the data and enables listening again)
- View the message buffer (show the messages held in the queue)
- View the mail messages buffer (show the messages held in the queue)
- Create a Tech-support zip file

2.2.4.1 Create Tech-Support File (Zip)

This menu option will create a Tech-support zip file, suitable for sending to SolarWinds for diagnostic purposes.

The file that is created, (C:\Program Files\Syslogd**Syslogd_TechSupport.zip**), can contain any or all of the following files:

- **ErrorLog.txt** - Syslog Server Error Log (Errorlog0.txt may also be present for error logs > 1MB in size)
- **Syslog_Server_Settings.ini** - Syslog Server Settings file
- **Syslog_Diagnostics.txt** - Syslog Server diagnositic report file
- **DNS-debug.txt** - Syslog DNS/NetBIOS verbose debugging file
- **Syslogd-debug.txt** - Syslog received messages debug file
- **Syslogd_Startup.txt** - Syslog (Standard Edition) Start-up debug file
- **Syslogd_Service_Startup.txt** - Syslog Service (Service Edition) Start-up debug file
- **Syslogd_Manager_Startup.txt** - Syslog Manager (Service Edition) Start-up debug file
- **KRDP_Sessions.ini** - Kiwi Reliable Delivery Protocol (KRDP) Sessions file
- **CacheSettings.ini** - Kiwi Reliable Delivery Protocol (KRDP) cache settings file
- **install.log** - Kiwi Syslog Server (Standard/Service Edition) Installer log file
- **StaticHosts.txt** - DNS name resolution static hosts file
- **Unknown_OID_list.txt** - MIB lookup unknown or unresolved OID list
- **Standard-YYYYMMDDHHNNSS-DebugLogN.txt** - Syslog Debug versions only: Standard edition verbose debug file
- **Manager-YYYYMMDDHHNNSS-DebugLogN.txt** - Syslog Debug versions only: Service edition (Manager) verbose debug file
- **Service-YYYYMMDDHHNNSS-DebugLogN.txt** - Syslog Debug versions only: Service edition (Service) verbose debug file

2.2.5 Export settings to INI file

Provides the ability to save the program configuration information to an INI file.

This file can then be transferred to another system and the configuration information imported into Kiwi Syslog Server by using the **File | Setup | Defaults/Import/Export** menu option.

If you have a problem that you wish to advise SolarWinds support staff, please use this option to export your INI settings, then send the zipped attachment to: http://www.kiwisyslog.com/support/

©2014 SolarWinds, Inc.

2.2.6 Exit

Surprisingly enough, this closes the program. If you are running the Standard Edition, once the program is closed, no more messages will be received or logged. If you would like to continue receiving, logging and actioning messages when you have logged off the system, you will need to install Kiwi Syslog Server as a Service by choosing this option during the installation process.

The ability to install the program as a Windows Service is only available on Windows XP Professional, Windows 2003, Windows 7 and Windows 2008 (STD and R2).

If you are installing Kiwi Syslog Server on an operating system that is not listed above then the option to "Install Kiwi Syslog Server as a Service" will not be available at installation time.

When the Display option "**Minimize to system tray on [X] close button**" is checked, the normal X close button in the top right hand corner of the form will not close the program. Instead the program must be closed from the **File | Exit** menu or from the System Tray popup menu.

2.3 Edit menu

2.3.1 Select All

This option will select all the syslog messages in the current display.

Once you have used this option you can copy the selected messages to the clipboard by using the "Copy selected items to the clipboard" menu option, or by pressing Ctrl-C.

2.3.2 Copy selected items to the clipboard

Allows the currently selected syslog messages to be copied to the clipboard.

To choose a selection, pause the display, highlight the desired message cells and then press Ctrl-C to copy to the clipboard.

2.4 View menu

2.4.1 View syslog statistics

Shows the Syslog Statistics window containing the message counters and trend graphs.

2.4.2 View e-mail log file

Displays the log file of mail messages sent using Windows Notepad.

The mail log file is: InstallPath\SendMailLog.txt

2.4.3 View error log file

Displays the log file of logging errors using Windows Notepad.

The error log file is: InstallPath\Errorlog.txt

2.4.4 Adjust width to fit screen

Adjusts the main Syslog window width to fit snugly across the screen.

©2014 SolarWinds, Inc.

2.4.5 Clear display

Removes all messages from the selected scrolling display.

2.4.6 Highlighting Options

This feature is only available in the licensed version.

The highlighting options available in Kiwi Syslog Server enable the user to specify a set of highlighting rules which will be applied to each message that is displayed in the Kiwi Syslog Display-grid. Highlighting rules are evaluated from the top-down, and any Syslog messages which match a given rule will have the given highlight-effects applied.

Highlight Items:

Lists the highlighting rules that will be applied to each syslog message that is to be displayed, the syslog message field that will be searched, the string pattern that will be searched for, and the effect to be applied. Each rule can be activated/deactivated by respectively checking/unchecking the checkboxes leftmost on each row of the list. The list of fields available in the 'fields' drop-down box are the same as the fields that are available on the Kiwi Syslog main display grid. (ie. Date, Time, Priority, Hostname, Message). Highlighting rules can be added/deleted by clicking the buttons on the toolbar to the right of the highlights list. Rule precedence can be changed in this toolbar as well, by clicking the up/down arrows.

Note: That the first time you access the Highlighing Options, you may be prompted "No highlighting rules have been found. Do you want to create some default rules based on Syslog Priorities?". As the prompt implies, if you answer yes to this question some default rules based on Syslog Priority will be created for you. These default rules are shown in *figure 1* below.

String to match:

The string pattern that will be searched for in the selected syslog message field.

Regular Expression	If checked, this option specifies if the string to match is a regular expression. (see Regular Expression Reference)
Invert Match	If checked, this option specifies that the effect will be applied only if a match is NOT found.
Ignore Case	If checked, the search pattern (string to match) will be treated as case insensitive.

Highlight Effects:

Apply Foreground Color	If checked, the foreground color selected will be applied, and override any existing foreground color. If unchecked, the current foreground color will be used.
Apply Background Color	If checked, the background color selected will be applied, and override any existing background color. If unchecked, the current background color will be used.
Bold Font	If checked, the font weight will be bold.
Italic Font	If checked, the font style will be italicised.
Underline Font	If checked, the font will be underlined.
Selected Icon	The icon that will be shown if the effect is to be applied to the current syslog message.

Icons:

©2014 SolarWinds, Inc.

The Icons shown in *figure 1* are (by default) built into Kiwi Syslog. Additional icons can be added by dropping them in the <Program Files>\Syslogd\Icons directory. The icon list is loaded at startup, so if you have added new icons you will need to restart Kiwi Syslog for the new icons to be displayed in this list.

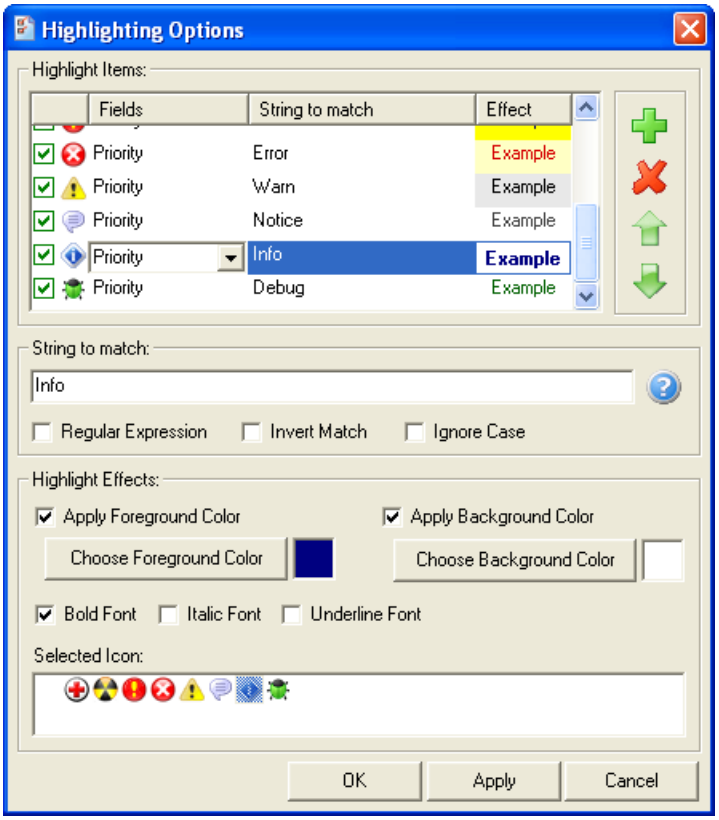


Figure 1 - Kiwi Syslog Server Highlighting Options

2.4.7 Choose font

Allows you to select a new font name, style, and colour to be used for displayed messages.

If non ASCII characters appear in the display as blanks or square blocks, it means that the font doesn't contain the required Unicode character glyph.

Microsoft Office comes with a font called "Arial MS Unicode". This font contains all of the Unicode glyphs that you are ever likely to want. Unfortunately, this font is not redistributable and is only available to you if you own Microsoft Office.

Alternatively, various free Unicode fonts are available from:

http://www.unicode.org and http://www.travelphrases.info/gallery/all_fonts.html

Most of the free fonts only contain subsets of glyphs. You will need to choose the best font that contains all the language glyphs you are wanting to display.

©2014 SolarWinds, Inc.

2.5 Manage menu

2.5.1 Manage menu

This menu only appears in the Service Edition

From the Kiwi Syslog Server Service Manager you can manage and control the service part of the program.

2.5.2 Install the Syslogd service

This allows you to install the Kiwi Syslog Server as an service if you are using, Windows XP or Windows 2003, Windows Vista, Windows 2008, Windows 7,Windows 8, or Windows 2008 R2.

You only need to install the service once.

After installing the service, you need to start it, using the **Manage | Start the Syslogd Service** menu option, so that it becomes active.

2.5.3 Uninstall the Syslogd service

This allows you to uninstall the Kiwi Syslog Server service.

Remember to stop the service before you try and uninstall it!

Once uninstalled, you can remove the application with the **Control Panel | Add / Remove programs** applet.

2.5.4 Start the Syslogd service

This starts the Syslogd service.

When the service is started (running) it will receive, log and forward messages.

To see if the service is alive and well, use the **Manage | Ping the Syslog service** menu.

2.5.5 Stop the Syslogd service

This stops the Syslogd service.

While the service is stopped the program is not running, therefore no messages are logged or displayed.

The service will not respond to 'Pings' from the Manager or any other form of communication.

Note: it can take up to 20 seconds to stop the service.

2.5.6 Ping the Syslogd service

This sends a test message to the Syslogd service and waits for a response. If no response is received after 5 seconds the Service is either stopped or not installed.

The results can be seen in the status bar at the bottom of the main window.

©2014 SolarWinds, Inc.

The message "The Syslogd Service is Alive!" will be displayed when a response to the ping is received.

2.5.7 Show the Syslogd service state

This checks the current state of the service.

The possible results are: Uninstalled, Running, Stopped or Not Responding.

2.5.8 Debug options menu

2.5.8.1 Display the service version

To ensure that the service version is the same as the Service Manager version, you can ask the service to display its version number.

The version number will appear in the status bar window.

2.5.8.2 Get diagnostic information

At some stage you may need to troubleshoot the service, this option causes the service to send all its information to the Service Manager.

The data is stored on the clipboard for pasting into e-mail or notepad.

If you experience problems with the operation of the Kiwi Syslog Server service, it would be a good idea to check the diagnostic info provided by this option.

2.5.8.3 Reset the Syslogd service

OK, no program or OS is perfect, so at some stage the service might get itself tied up and confused for whatever reason. This option allows you to kick-start the service and get things re-initialized again.

There is no harm in using this option, just be aware that a few messages might be dropped while the service restarts.

This option should take about 3 seconds to complete.

Only the receiving socket is reset, i.e. the Winsock part of the service.

2.5.8.4 Clear the service DNS Cache

Because the service can resolve IP addresses to hostnames it also has a DNS cache to reduce network traffic.

When you clear the DNS cache on the service manager it also clears the cache on the service.

This option is provided to allow you to manually force a clear of the service cache.

2.5.8.5 Apply new settings to Syslogd service

This forces the service to read the current Syslogd settings from the registry and start using them.

You can use this option when you want to ensure that the new settings have been applied.

A message in the status bar will indicate if the service successfully used the new settings.

©2014 SolarWinds, Inc.

2.5.8.6 Retrieve last messages

This asks the service to send all the messages currently held in the virtual displays. This is done automatically when the Service Manager starts.

2.5.8.7 Send keep alive

The Service Manager sends keep alive messages to the service every minute. This lets the service know that it should forward the messages to an active Service Manager. If the service does not receive a keep alive for 3 minutes it will stop forwarding the messages to the Service Manager. This allows the CPU utilization and network traffic to be kept to a minimum when the Service Manager is not running.

This option sends a keep alive message to the service. This function is for debug purposes only.

2.5.8.8 Enable Service Debug Mode

The service manager logs the syslog messages to <Program Files>\Syslogd\Syslogd-debug.txt file.

Debug mode will be disabled when restarting the service.

2.6 Help menu

2.6.1 Context based Help (F1)

Opens this help file.

2.6.2 Help Topics

Opens this help file to the contents page.

2.6.3 Online FAQ

Opens your default web browser to the support section providing you with access to FAQ and Knowledge Base articles - http://www.kiwisyslog.com/support/

2.6.4 Purchase the licensed version

Takes you to http://www.kiwisyslog.com/downloads.aspx where you can purchase the licensed version of the program.

2.6.5 Enter license details (F2)

Displays your current license details.

2.6.6 Make a suggestion or report a bug

Opens a feedback dialogue allowing you to make a suggestion or report a bug to SolarWinds.

You will need to supply an SMTP mail server address, your e-mail address, and your name. An e-mail will be generated and sent to http://www.kiwisyslog.com/support/

©2014 SolarWinds, Inc.

Alternatively, you can use the feedback form on the web site at: http://www.kiwisyslog.com/support/

2.6.7 Check for update...

Opens the product update notification dialogue, and checks the Solarwinds website for available product updates.

If an updated version of Kiwi Syslog Server is available, then "What's New" in the update is displayed along other relevant update details, and "Download Update" button.

Note:
- This dialog may be permanently supressed by checking the "Don't tell me about this again" option.
- For information about disabling the product update checking altogether, see Setup - Product Updates

2.6.8 About Kiwi Syslog Server

Opens the **About Kiwi Syslog Server** window.

This form displays the copyright information, version, license information, and links to the Kiwi Syslog Server website.

3 Configuring the Syslog properties

3.1 Guide to initial Syslog Server Setup

When you run Kiwi Syslog Server for the first time, the default action settings are used. This will ensure that all messages are seen on the display and captured to a log file called "SyslogCatchAll.txt" which is located in the \Logs directory of your Kiwi Syslog Server installation folder.

You can modify these settings by using the **File | Setup** menu option or pressing Ctrl-P.

You can return to the default settings at any time by using the **Load default Rules and Settings** button found under the **File | Setup | Defaults/Import/Export** menu option.

3.2 How to navigate using the keyboard

Delete	**Delete** selected Rule, Filter, Action or Archive schedule.
Insert	**Add** a new Rule, Filter, Action or Archive schedule. (Item selected must be Rules, Filters, Actions or Archiving)
Ctrl-V	**Paste** copied Rule, Filter, Action or Archive schedule. (Item selected must be Rules, Filters, Actions or Archiving)
Ctrl-C	**Copy** selected Rule, Filter, Action or Archive schedule.
F2	**Rename** selected Rule, Filter, Action or Archive schedule.
F4	**Auto-name** Filter, Action or Archive schedule
Home	**Move cursor to top** of tree
End	**Move cursor to bottom** of tree

©2014 SolarWinds, Inc.

Enter	**Collapse** or expand the tree at currently selected position. (Same as double clicking with the mouse)
Space bar	**Enable or Disable** selected Rule, Filter, Action or Archive schedule.
Shift + Up Arrow	**Move** selected Rule, Filter, Action or Archive schedule up one position.
Shift + Dn Arrow	**Move** selected Rule, Filter, Action or Archive schedule down one position.

3.3 Rules / Filters / Actions

3.3.1 How the rule engine works

It is possible to define up to 100 rules. Each rule can contain up to 100 filters and 100 actions.

When a syslog message is received it is processed by each rule in turn. Starting at the top rule and working down. The order of the rules can be adjusted up or down using the toolbar buttons.

For each rule, the message is matched against the specified filters. Starting from the top most filter and working down. If any of the filter conditions fail, the program stops processing that rule and moves on to the next rule. If all the filter conditions are met, that is they all return TRUE, then the program will perform the specified action or actions for that rule, in order starting at the top most action and working down.

Once all the actions for that rule have been completed, the program will process the next rule in the list. When all rules have been processed, the program waits for the next syslog message to be received, then starts processing the new message from the top most rule.

Each rule, filter or action can be given a descriptive name. To edit the name, press F2 or use the right-click menu. The names do not have to be unique, but should describe their function. The name can be a maximum of 25 characters in length.

When no filters are defined for a rule, all messages are passed.

By default, the initial setup contains a single rule named Default. No filters are defined. This ensures all messages are passed. The two default actions of "Display" and "Log to file" are used. This ensures that by default, all messages are displayed and logged to a file called "SyslogCatchAll.txt" which is located in the \Logs directory of your Kiwi Syslog Server installation folder.

To Add/Delete/Rename rules, Filters and Actions, please refer to How to navigate using the keyboard

3.3.2 Filter types

3.3.2.1 Simple filter

Overview
A simple one line filter. It is useful for matching a single or multiple strings of text or IP addresses in the incoming message. By including multiple quoted search strings, it is possible to match String-A OR String-B.

Include: "link up" "link down"
Matches on either "link up" or "link down"

Details
The simple filter allows you to specify a single line of text to match. Each search string must be contained by double quotes. Multiple quoted search strings can be placed next to each other on the same line. The filter will then match any of the strings specified. This is an implicit OR relationship.

The [C] button selects a case sensitive or case in-sensitive string search.
The [S] button selects a sub-string search or an exact, whole string match.

Examples:

©2014 SolarWinds, Inc.



If the message text contains any of the listed words anywhere in the message, the filter result will be true.

Notice the [S] button is pressed, indicating a sub-string search. This means the search strings can appear anywhere in the text.

All strings must be contained in double quotes. Items can be listed next to each other and will be OR'd together.

The filter above reads as:

If any of the message text contains the text "POP3" or "SMTP" or "MAPI" in upper or lower case, the filter will be true.



If the message text exactly matches the specified string in the same case, the filter result will be true.

Notice the [S] button is raised, indicating the search string must exactly match the message text, character for character.

Notice the [C] button is pressed, indicating the case must match exactly as specified.

The filter above reads as:

If the message text is "The link is down" in the same case, the filter will be true.

3.3.2.2 Complex filter

Overview
A more complex multi-line filter. It allows complex include/exclude matching for text and IP addresses. By including multiple quoted search strings, it allows for Boolean operations on the search strings.

Allows for AND, OR, NOT-OR, NOT-AND and exclusion matching.

Details
The complex filter allows you to specify multiple search strings. Search strings can be linked together in the form of [(A or B) and (C or D)] but not [(E or F) and (G or H)].

Each search string must be contained by double quotes. Multiple quoted search strings can be placed next to each other on the same line. The filter will then match any of the strings specified. This is an implicit OR relationship.

The [C] button selects a case sensitive or case in-sensitive string search.
The [S] button selects a sub-string search or an exact, whole string match.

The filter matching process will ignore any blank fields.

Leaving the first two fields blank and specifying text in the third and or fourth fields can perform exclusion matching. In this case, if the text is NOT matched the result will be true.

Examples:

©2014 SolarWinds, Inc.



Notice the [S] button is pressed, indicating a sub-string search. This means the search strings can appear anywhere in the text.

All strings must be contained in double quotes. Items can be listed next to each other and will be OR'd together.

The filter above reads as:

If any of the message text contains the text "fox" or "quick" or "hello" and also contains "over" or "the", but does not contain "hello" and "brown" (in upper or lower case), the filter will be true.



This is an example of an exclusion filter:

If the text does NOT contain the words "chicken" or "duck" then the result will be true.
Notice the first two fields are left blank. These fields will be ignored during the filter processing.

Notes:

The "And:" fields can be left blank if they are not required.

If the "And:" fields contain values, the field above it must also contain data.

3.3.2.3 Regular Expression filter

Overview
Allows the use of Unix type regular expression matching. Useful for matching ranges of numbers, letters or symbols in the text. Allows maximum control over what is searched for within the text, including specifying the location within the text to match.

Allows for AND, OR, NOT OR, NOT AND, and exclusion matching.

Details
The regular expression filter allows you to specify Unix type regular expression arguments to tightly control what and where text is matched.

Each search string must be contained by double quotes. Multiple quoted search strings can be placed next to each other on the same line. The filter will then match any of the strings specified. This is an implicit OR relationship.

The [C] button selects a case sensitive or case in-sensitive string search.

The filter matching process will ignore any blank fields.

©2014 SolarWinds, Inc.

Leaving the first two fields blank and specifying text in the third and or fourth fields can perform exclusion matching. In this case, if the text is NOT matched the result will be true.

Example:



All strings must be contained in double quotes. Items can be listed next to each other and will be OR'd together.

The filter above reads as:

If the message text starts with "The" (case sensitive) and ends with "dog" but does not contain "chicken" and "Duck" then the result will be true.



This is an example of an exclusion filter:

If the message text does NOT contain the word "The" at the start and the word "dog" at the end then the result will be true.
Notice the first two fields are left blank. These fields will be ignored during the filter processing.

Notes:

The "And:" fields can be left blank if they are not required.

If the "And:" fields contain values, the field above it must also contain data.

Regular Expression Syntax:

Special characters and sequences are used in writing patterns for regular expressions. The following table describes and gives an example of the characters and sequences that can be used:

Char	Description
^	Beginning of a string.
$	End of a string.
.	Any character.
?	Repeat previous character zero or one time. For example, "10?" matches "1" and "10".
*	Repeat previous character zero or more times. For example, "10*" matches "1", "10", "1000", etc.

©2014 SolarWinds, Inc.

+ Repeat previous character one or more times. For example, "10+" matches "10", "1000", etc.

**** Escape next character. This is required to any of the special characters that are part of the syntax. For example "\.*\+\\" matches ".*+\". It is also required to encode some special non-printable characters (such as tabs) listed below.

x|y Matches either *x* or *y*. For example, "z|wood" matches "z" or "wood". "(z|w)oo" matches "zoo" or "wood".

{*n*} *n* is a nonnegative integer. Matches exactly *n* times. For example, "o{2}" does not match the "o" in "Bob," but matches the first two o's in "foooood".

{*n*,} *n* is a nonnegative integer. Matches at least *n* times. For example, "o{2,}" does not match the "o" in "Bob" and matches all the o's in "foooood." "o{1,}" is equivalent to "o+". "o{0,}" is equivalent to "o*".

{ *n* , *m* } *m* and *n* are nonnegative integers. Matches at least *n* and at most *m* times. For example, "o{1,3}" matches the first three o's in "fooooood." "o{0,1}" is equivalent to "o?".

[*xyz*] A character set. Matches any one of the enclosed characters. For example, "[abc]" matches the "a" in "plain".

[^ *xyz*] A negative character set. Matches any character not enclosed. For example, "[^abc]" matches the "p" in "plain".

[*a-z*] A range of characters. Matches any character in the specified range. For example, "[a-z]" matches any lowercase alphabetic character in the range "a" through "z".

[^ *m-z*] A negative range characters. Matches any character not in the specified range. For example, "[m-z]" matches any character not in the range "m" through "z".

\b Matches a word boundary, that is, the position between a word and a space. For example, "er\b" matches the "er" in "never" but not the "er" in "verb".

\B Matches a non-word boundary. "ea*r\B" matches the "ear" in "never early".

\d Matches a digit character. Equivalent to [0-9].

\D Matches a non-digit character. Equivalent to [^0-9].

\f Matches a form-feed character.

\n Matches a newline character.

\q Quote character or ASCII value of 34

\r Matches a carriage return character.

\s Matches any white space including space, tab, form-feed, etc. Equivalent to "[\f\n\r\t\v]".

\S Matches any nonwhite space character. Equivalent to "[^ \f\n\r\t\v]".

\t Matches a tab character.

\v Matches a vertical tab character.

\w Matches any word character including underscore. Equivalent to "[A-Za-z0-9_]".

\W Matches any non-word character. Equivalent to "[^A-Za-z0-9_]".

\num Matches *num*, where *num* is a positive integer. A reference back to remembered matches. For example, "(.)\1" matches two consecutive identical characters.

\ *n* Matches *n*, where *n* is an octal escape value. Octal escape values must be 1, 2, or 3 digits long. For example, "\11" and "\011" both match a tab character. "\0011" is the equivalent of "\001" & "1". Octal escape values must not exceed 256. If they do, only the first two digits comprise the expression. Allows ASCII codes to be used in regular expressions.

©2014 SolarWinds, Inc.

\x*n* Matches *n*, where *n* is a hexadecimal escape value. Hexadecimal escape values must be exactly two digits long. For example, "\x41" matches "A". "\x041" is equivalent to "\x04" & "1". Allows ASCII codes to be used in regular expressions.

For example:

```
"^stuff"                      ' any string starting with "stuff"
"stuff$"                      ' any string ending with "stuff"
"o.d"                         ' "old", "odd", "ord", etc
"o[ld]d"                      ' "old" or "odd" only
"o[^l]d"                      ' "odd", "ord", but not "old"
"od?"                         ' "o" or "od"
"od*"                         ' "o", "od", "odd"
"od+"                         ' "od", "odd", etc
"\."                          ' decimal point (needs escape character)
"[A-Z][a-z]*"                 ' any uppercase word
"[0-9]+"                      ' any stream of digits
"[1-9]+[1-9]*"                ' any stream of digits not starting with zero
"[+\-]?[0-9]*[\.]?[0-9]*"     ' any number with optional sign and decimal point
                              '(needs two escape characters)
"dst=\qLOCAL MACHINE\q"       ' finds occurrence of "dst="LOCAL MACHINE""
"dst=\x22LOCAL MACHINE\x22"   ' finds occurrence of "dst="LOCAL MACHINE""; Hex(22) = ASCII 34,
or (")
"(z|w)oo"               ' finds occurances of "zoo" or "woo"
```

3.3.2.4 IP Address Range filter

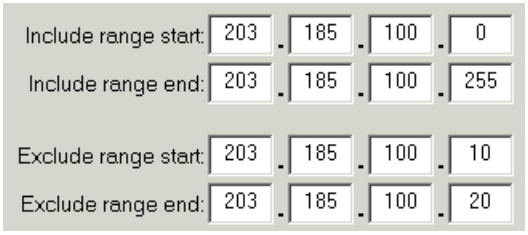
Overview
Matches on a range of IP addresses. Great for including or excluding a range of host addresses.

Details
The IP Address Range filter allows you to specify a range of IP addresses to include or exclude.

Either the 'Include' or 'Exclude' range can be left blank, but not both.

If the 'Include' range is left blank the filter works in exclusion mode. If the IP address falls in the range of the 'Exclude' values, the result is true.

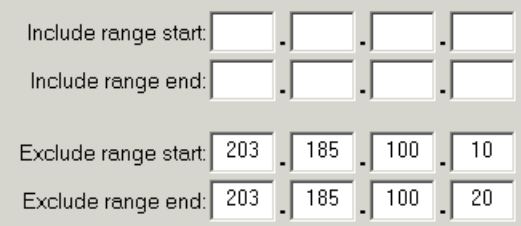
Examples:



The filter above reads as:

If the IP address falls within the range of 203.185.100.0 to 203.185.100.255 and is not between 203.185.100.10 and 203.185.100.20 then the result will be true.

©2014 SolarWinds, Inc.



This is an example of an exclusion filter:

If the IP address does NOT fall within the range of 203.185.100.10 to 203.185.100.20 then the result will be true.

3.3.2.5 IP Subnet Mask filter

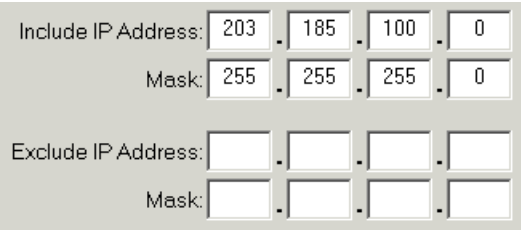
Overview
Allows the use of subnet masking to define the included/excluded host addresses.

Details
The IP Subnet Mask filter allows you to specify a range of IP addresses to include or exclude based on mask matching.

Either the 'Include' or 'Exclude' fields can be left blank, but not both.

If the 'Include' fields is left blank the filter works in exclusion mode. If the IP address falls in the range of the 'Exclude' values, the result is true.

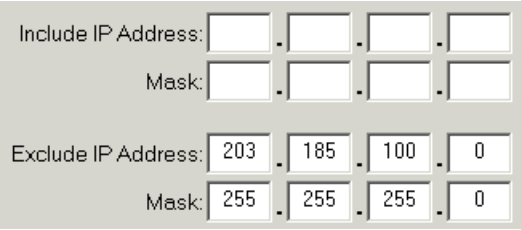
Examples:



The IP address specified is logically AND'd with the specified Mask and then compared with the message host IP address. If the two addresses are on the same "subnet" then the result is true.

The filter above reads as:

If the IP address falls within the range of 203.185.100.0 to 203.185.100.255 then the result will be true.



This is an example of an exclusion filter:

If the IP address does NOT fall within the range of 203.185.100.0 to 203.185.100.255 then the result will be true.

©2014 SolarWinds, Inc.

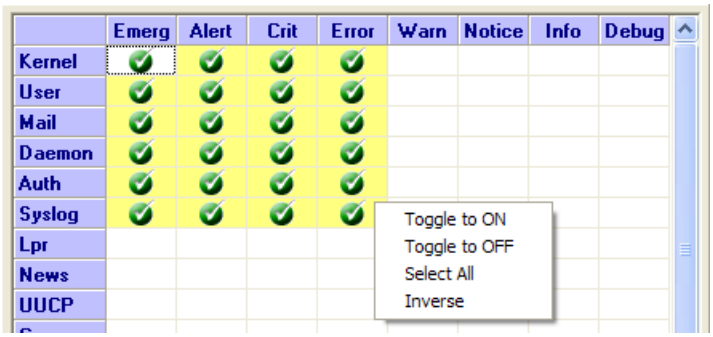
3.3.2.6 Priority filter

Overview
Allows the selection of priority values to be matched against the incoming message priority.

Details
Each incoming message contains a Priority value. This value is made up of a Facility and Level. You can specify which priorities will cause the filter result to be true.

To select a priority, double click the grid cross referenced by Facility and Level. A green tick indicates a match on that priority will cause the filter result to be true.

Use the mouse to select columns or rows, and then right click to show the popup options menu.

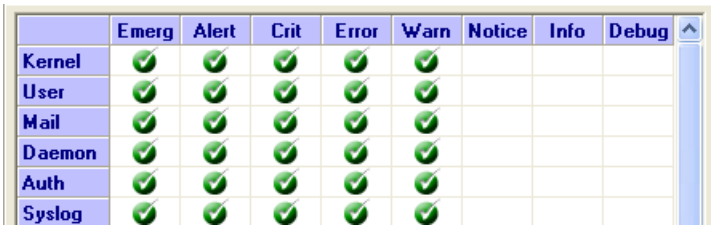


Setting a green tick in all of the priority values ensures a match will occur no matter what the message priority value. If you want to match all priority values it is not necessary to use a filter at all. The absence of a priority filter means that all priorities are passed anyway.

Inverse will invert all the currently enabled boxes to become blank and visa versa. (Inversing the enabled boxes will essentially create an exclusion filter.)

Use the Select All menu to select every priority, then use Toggle to OFF or ON to toggle the green ticks.

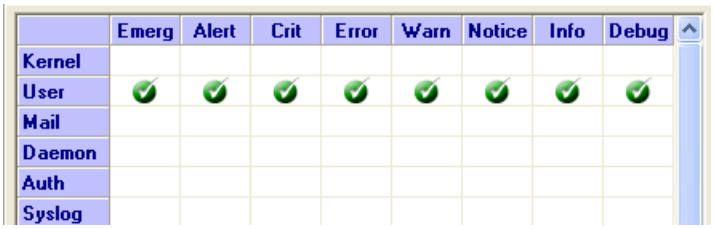
Examples:



The filter above reads as:

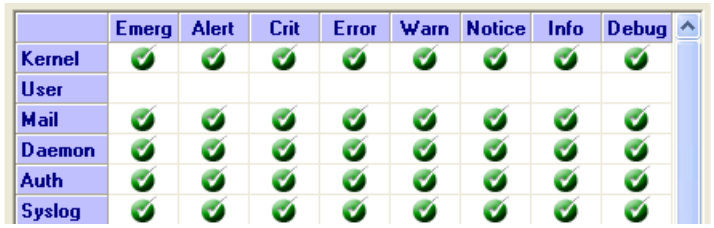
Any message with a Level of Warning or higher on any Facility will cause the result to be true.

©2014 SolarWinds, Inc.



The filter above reads as:

Any message with a Facility of User on any Level will cause the result to be true.



The filter above is an example of an exclusion filter and reads as:

Any message with a Facility that is NOT User on any Level will cause the result to be true.

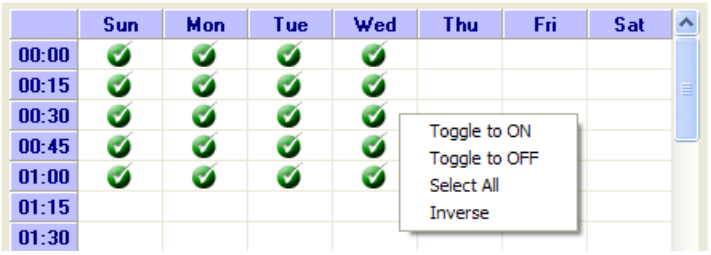
3.3.2.7 Time of Day filter

Overview
This filter matches the current time of day against the times specified in the matrix and allows or denies an action.

Details
This filter allows you to include or exclude certain times of the day.

To select a time of day (in ¼ hour segments), double click the grid cross referenced by Time and Day. A green tick indicates a match on that time and day will cause the filter result to be true.

Use the mouse to select columns or rows, and then right click to show the popup options menu.



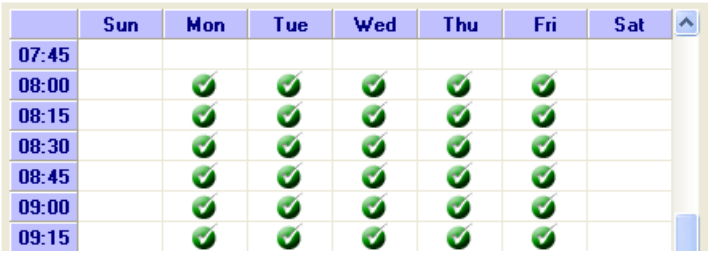
Enabling all of the time and day values ensures a match will occur no matter what time or day the message arrives. Having no time of day filter defined will also ensure that messages will pass for all times of the day.

Inverse will invert all the currently enabled boxes to become blank and visa versa. (Inversing the enabled boxes will essentially create an exclusion filter.)

Use the Select All menu to select every time segment, then use Toggle to OFF or ON to toggle the green ticks.

Examples:

©2014 SolarWinds, Inc.



The filter above reads as:

Any message that arrives from Monday 8am to Friday 9am will cause the result to be true.

A business hours filter could be created by selecting Monday to Friday from 8am until 5pm. Using the inverse option on a particular configuration will create an exclusion filter. For example, not Monday to Friday from 8am to 5pm.

3.3.2.8 Time Interval filter

Overview
This filter will trigger once, then wait for a set time interval before triggering the filter again.

The Flags/Counters filters need to be placed after all the other filter types in the rule. This is so the other filters can be processed first.

Details
The time interval filter is useful when you are using a notify action such as "send e-mail message" to notify you when a particular message text is found (for example "link down"). If the link goes up and down many times a minute, you would normally receive an e-mail alert for each "link down" event. The time interval filter can fire once, then wait for X minutes before alerting you again.

Example of a link down notification using the time interval filter:

```
Rule: Link down notify
  Filters
    Filter: Field=Hostname, Type=Simple.
            Include: "central-router.company.com" [S]
    Filter: Field=Msg Text, Type=Simple.
            Include: "link down" [S]
    Filter: Field=Flags/Counters, Type=Time interval
            Fire this event once, then wait for 15 minutes before firing again.
  Actions
    Action: Send E-mail message
            E-mail body: The link has gone down, please call the helpdesk.
            Alert - %MsgText
```

When a message arrives from the host "central-router.company.com" that contains the words "link down" in the text, the first filter (Message text) will be true. The Time interval filter is then processed. The first time the Time interval filter is processed, the result will be true, and the actions that follow will be performed. A countdown timer using the specified value is started. In the above example it is 15 minutes. If another message arrives from the same host that contains the words "link down", the first filter (Message text) will again be true. If the countdown timer has not reached zero, the Time interval filter will return false and the actions following will not be performed.

This filter may also be used to reduce the amount of notification e-mail sent to you when an attack occurs. For example, you might want to know when the text "port scan detected" is received, but you only want to be notified once every hour, not every time the message is received. Use the time interval filter to trigger once, then wait for 60 minutes before triggering again.

The internal counter for the Time Interval filter can be reset, by using the Reset Flags/Counters Action.

©2014 SolarWinds, Inc.

3.3.2.9 Threshold filter

Overview
This filter will trigger only when the preceding filters have been met X times in Y seconds.

The Flags/Counters filters need to be placed after all the other filter types in the rule. This is so the other filters can be processed first.

Details
The Threshold filter is useful when you only want to know about an event when it reaches a certain level. For example, you may receive the occasional message containing the text "port scan detected", but you only want to be alerted to it when it occurs 5 times within a minute. This would indicate that there is someone persistently scanning your network.

Another example would be to watch for failed login attempts. If the text "login failed" occurred more than 5 times within 30 seconds then it could indicate a brute force login attempt.
Example of a link down notification using the time interval filter:

```
Rule: Failed login
  Filters
    Filter: Field=Hostname, Type=Simple.
            Include: "unixhost.company.com" [S]
    Filter: Field=Msg Text, Type=Simple.
            Include: "login failed" [S]
    Filter: Field=Flags/Counters, Type=Threshold
            Filter is true if event occurs 10 times in 120 seconds.
  Actions
    Action: Send E-mail message
            E-mail body: Intruder Alert – Login failed 10 times in 2 minutes.
            Alert - %MsgText
```

When 10 messages arrive from the host "central-router.company.com" that contains the words "login failed" in the text within 120 seconds, the filter will be true. If the filter is true, the actions below it will be performed.

This filter may also be used to reduce the amount of notification e-mail sent to you. You can use it to set the Threshold at which you want to be notified.

Maintain individual threshold counts for each host address
If checked, this setting means that Kiwi Syslog Server will maintain a separate internal threshold count for each host that sends a message.
What this means, is that instead of keeping a general threshold count of messages sent 'X times in Y seconds', Kiwi Syslog Server records a count of messages sent 'X times in Y seconds from host Z'.

The following example highlights the usage of this setting, in notifying an administrator via email when 'port-flapping' is detected on a device over and above a certain threshold. One email is received for each device that is above the threshold. The host or device that caused the threshold event to fire can be reported using **'%MsgHost'.**

```
Rule: Link Up
  Filters
    Filter: Field=Msg Text, Type=Simple
            Include: "Link Up" [S]
    Filter: Fields=Flags/counters, Type=Threshold
            Filter is true is event occurs 10 times in 120 seconds,
            maintain individual threshold counts for each host address.

  Actions
    Action: Send E-mail message
            E-mail body: Port Flapping Detected - Link Up message on device '%MsgHost'
received 10 times in 2 minutes.
            Device - %MsgHost
            Alert - %MsgText
```

The internal counter for the Threshold filter can be reset, by using the Reset Flags/Counters Action.

©2014 SolarWinds, Inc.

3.3.2.10 Timeout filter

Overview
This filter will trigger only when the preceding filters have not been met X times in Y minutes.

The Flags/Counters filters need to be placed after all the other filter types in the rule. This is so the other filters can be processed first.

Details
The Timeout filter is useful for monitoring syslog devices and notifying you when things go quiet. For example, the firewall might normally generate at least 200 messages per hour. If the amount of messages suddenly dropped to only 10 messages in the hour, or even stopped sending messages at all, you could be alerted to the inconsistency via e-mail.

This filter is different from the other flags/counters filters in that it is not fired by an incoming message. It is actually fired by a count down timer due to a lack of messages. Therefore when this filter is fired, no current message is associated with the event. Instead an informational message is created and passed to any actions below the filter. The message is in the following format:

Priority: Local7.Debug (191)
HostIP: 127.0.0.1 (localhost)
MsgText: The rule 'Rule name here' has only been matched X times in Y minutes. The threshold was set for Z times.

```
Rule: Firewall Monitor
  Filters
    Filter: Field=Hostname, Type=Simple.
            Include: "firewall.company.com" [S]
    Filter: Field=Flags/Counters, Type=Timeout
            Filter is true if event doesn't occur 1 times in 5 minutes.
    Filter: Field=Time of Day, Type= Time of Day
            Monday to Friday 8:00 a.m. to 6:00 p.m.

  Actions
    Action: Send E-mail message
            E-mail body: Firewall is not alive
            Alert - %MsgText
```

%MsgText will read:
The rule 'Firewall Monitor' has only been matched 0 times in 5 minutes. The threshold was set for 1 times.

When no messages arrive from the host "firewall.company.com" in 5 minutes, the count down timer will fire. The filters that follow the Timeout filter will be tested and if they pass (the time is between 8:00 a.m. and 6:00 p.m.), the actions will be performed. Remember that this filter is not triggered by a particular message like the other filters, it is triggered when the countdown timer elapses. An informational message is created and used as the current message. Actions can then use this informational message in the alerts etc.

The internal counter for the Timeout filter can be reset, by using the Reset Flags/Counters Action.

3.3.2.11 Importing and Exporting a filter definition

It is possible to export a filter definition to a file for later use or sharing with another person. Use the Import and Export buttons to manage the filters.

Select the Import button to choose a filter to import. A file opening dialogue will prompt for a KSD file to import.

Select the Export button to save the selected filter to a file. Filter files are given an extension of **.KSR**

If you have created a useful filter definition that you think others will want to use, please e-mail the exported filter definition file to http://www.kiwisyslog.com/support/ so it can be made available on the Kiwi Syslog Server web site.

©2014 SolarWinds, Inc.

3.3.2.12 Input source

Overview

This filter will trigger when the input source of the current message matches one of the selected input sources of the filter.

Avaible selections

- UDP
- TCP
- SNMP
- Keep-alive
- TLS/Syslog

Details

To filter for UDP messages only:
Check the UDP checkbox, and ensure that the other checkboxes are not checked.

To filter for TCP messages only:
Check the TCP checkbox, and ensure that the other checkboxes are not checked.

To filter for SNMP messages only:
Check the SNMP checkbox, and ensure that the other checkboxes are not checked.

To filter for Keep-alive messages only:
Check the Keep-alive checkbox, and ensure that the other checkboxes are not checked.

To filter for TLS/Syslog messages only:
Check the TLS/Syslog checkbox, and ensure that the other checkboxes are not checked.

3.3.3 Action - Display

This will display the message on the screen.

Choose one of the 25 virtual displays to send the message to. You can then choose which display to view from the drop down list on the main syslog Server display.

You can rename the displays to something more meaningful by using the **File | Setup | Display** menu option, then choosing the display from the "Modify display names" dropdown, entering a new name into the field provided, then pressing the "Update" button.

3.3.4 Action - Log to file

3.3.4.1 Action - Log to file

This will log the message to the specified file in the file format you select.

Fill in the **Log file name** field with the absolute path and filename to use for the log file, or use the […] button to browse for a file.

The default log file name is "SyslogCatchAll.txt"
The default path is "InstallPath\Logs\" where InstallPath is the folder that Kiwi Syslog Server is installed in.

3.3.4.2 AutoSplit values

Using AutoSplit values can eliminate the need to use filters and actions to split incoming messages into multiple log files.

To use the AutoSplit values, place the cursor at the point you want to insert the new value and then click the

©2014 SolarWinds, Inc.

"Insert AutoSplit value" link and choose from the menu items. The new variable will be placed at the current cursor position.

When a message is received, the variable will be replaced with a value from the message. For example % PriLevAA will be replaced with the message Priority level.

The AutoSplit values can be used anywhere within the path or log file name, as long as the result would make a valid file name.

Some examples:

To split the messages into separate files based on the day of the month.

C:\Logs\MyLogFile%DateD2.txt

The %DateD2 part would be replaced by the current day of the month. If it was the 23rd of the month, the message would be written to:
C:\Logs\MyLogFile23.txt

Any number of AutoSplit values can be used within the path or file name.

To split the messages based on priority level and current date, use:
C:\Logs\%PriLevAA\MyLogFile-%DateISO.txt

The resulting path and file name would look like this:
C:\Logs\Debug\MyLogFile-2002-04-09.txt

Or you could split the messages based on the sending host, then break each host into priority level
C:\Logs\%HostName.%HostDomain\MyLogFile-%PriLevAA.txt

The resulting path and file name would look like this:
C:\Logs\myhost.mycompany.com\MyLogFile-Debug.txt

If you are using the Run Script action, you can use any of the VarCustom or VarGlobal fields as an autosplit item.

Rather than remembering the %variable names, just use the menu items to insert the values.

Here are a list of all the currently available AutoSplit values:

Date values

Menu name: ISO Date (YYYY-MM-DD)
Parameter: %DateISO
Explanation: International formatted date in the format YYYY-MM-DD. Leading zeros, always 10 characters in length.
Example: 2002-10-15

Menu name: Year (YYYY)
Parameter: %DateY4
Explanation: 4 digit year, always 4 characters in length.
Example: 2002

Menu name: Year (YY)
Parameter: %DateY2
Explanation: 2 digit year, always 2 characters in length.
Example: 02

Menu name: Month (MM) with leading zero
Parameter: %DateM2
Explanation: 2 digit month with leading zero, always 2 characters in length.
Example: 12

Menu name: Month (MMM) in English
Parameter: %DateM3
Explanation: 3 character month in English, always 3 characters in length. First letter is in upper case. (Jan, Feb, Mar, Apr…)

©2014 SolarWinds, Inc.

Example: Nov

Menu name: Date (DD) with leading zero
Parameter: %DateD2
Explanation: 2 digit day of the month with leading zero, always 2 characters in length.
Example: 05

Menu name: Day (DDD) in English
Parameter: %DateD3
Explanation: 3 character day of the week in English, always 3 characters in length. First letter is in upper case. (Sun, Mon, Tue…)
Example: Fri

Time values

Menu name: Hour (HH) with leading zero
Parameter: %TimeHH
Explanation: 2 digit hour, always 2 characters in length. 24 hour display. 3 p.m. = 15
Example: 14

Menu name: Minute (MM) with leading zero
Parameter: %TimeMM
Explanation: 2 digit minute, always 2 characters in length.
Example: 59

Menu name: AM/PM indicator (AM or PM)
Parameter: "%TimeAMPM
Explanation: 2 character time of day indicator. Always 2 characters in length. 00:00 to 11:59 = AM. 12:00 to 23:59 = PM
Example: AM

Priority values

Menu name: Level (Alpha)
Parameter: %PriLevAA
Explanation: The message priority level as a word. Debug, Notice, Info…
Example: Critical

Menu name: Facility (Alpha)
Parameter: %PriFacAA
Explanation: The message priority facility as a word. Local1, News, Cron…
Example: User

Menu name: Level (2 digit numeric)
Parameter: %PriLev00
Explanation: The message priority level as a 2 digit number. 00 to 07
Example: 05

Menu name: Facility (2 digit numeric)
Parameter: %PriFac00
Explanation: The message priority facility as a 2 digit number. 00 to 23
Example: 23

Menu name: Priority (3 digit numeric)
Parameter: %Pri000
Explanation: The message priority as a 3 digit number. 000 to 191
Example: 016

IP Address values (Only in the registered version)

Menu name: IP Address (4 octets, zero padded)
Parameter: %IPAdd4
Explanation: The IP address of the device that sent the message. Each octet is zero padded. Always 15 characters in length
Example: 192.168.001.024

©2014 SolarWinds, Inc.

Menu name: IP Address (3 octets, zero padded)
Parameter: %IPAdd3
Explanation: The first 3 octets of the IP address of the device that sent the message. Each octet is zero padded. Always 11 characters in length.
Example: 192.168.001

Menu name: IP Address (2 octets, zero padded)
Parameter: %IPAdd2
Explanation: The first 2 octets of the IP address of the device that sent the message. Each octet is zero padded. Always 7 characters in length.
Example: 203.056

Host name values (Only in the registered version)

Menu name: Hostname (no domain)
Parameter: %HostName
Explanation: The host name of the device that sent the message. Just the host name, no domain name is included.
Example: sales-router

Menu name: Domain (no host)
Parameter: %HostDomain
Explanation: The domain name suffix of the device that sent the message. Just the domain name, no host name is included.
Example: mycompany.co.nz

Menu name: Reversed domain (no host)
Parameter: %HostDomRev
Explanation: The domain name suffix of the device that sent the message, in reverse order. Just the domain name, no host name is included.
Example: nz.co.mycompany

Message Text - WELF format (Only in the registered version)

WELF format is the WebTrends Extended Logging Format. This format is used by many firewalls such as, GNATBox, SonicWall, CyberWallPlus, NetScreen etc. Each field within the message text is prefixed with a identifying tag. Such as fw= for the firewall name, src= for the source of the packet being logged. More fields will be added into the AutoSplit list later. Contact http://www.kiwisyslog.com/support/ if you need one added.

Menu name: Firewall name (WELF format)
Parameter: %TextFW
Explanation: The name of the firewall that created the message.
Example: protector

Menu name: Source address (WELF format)
Parameter: %TextSrc
Explanation: The source IP address of the packet being logged by the firewall. (Not zero padded, unless this has been done by the firewall already)
Example: 192.168.1.6

Menu name: Destination address (WELF format)
Parameter: %TextDst
Explanation: The destination IP address of the packet being logged by the firewall. (Not zero padded, unless this has been done by the firewall already)
Example: 203.57.12.1

Menu name: Protocol (WELF format)
Parameter: %TextProto
Explanation: The protocol of the packet being logged by the firewall.
Example: http

Menu name: Serial Number(WELF format)
Parameter: %TextSn
Explanation: The Serial number of the device as in WELF Message
Example: abcdDDDXSD

©2014 SolarWinds, Inc.

Input Source values (Only in the registered version)

Menu name: Input Source (UDP/TCP/SNMP)
Parameter: %InpSrc
Explanation: Identifies the input source of the message. (The listening method that received the message)
Example: UDP

Custom/Global script fields (Only in the registered version)

Menu name: VarCustom01 to VarCustom16
Parameter: %VarCustom01 to %VarCustom16
Explanation: There are 16 custom fields that can be modified by the Run Script action. If these fields have not been modified by the script, they will be blank. Be aware that a blank autosplit value may result in an invalid file name. The custom field values are cleared when a new message arrives. They are only valid for the current message. To store values longer than a single message, use VarGlobal fields.
Example: Any value that the script creates can be used.

Menu name: VarGlobal01 to VarGlobal16
Parameter: %VarGlobal01 to %VarGloabl16
Explanation: There are 16 global fields that can be modified by the Run Script action. If these fields have not been modified by the script, they will be blank. Be aware that a blank autosplit value may result in an invalid file name. The global fields retain their value between messages.
Example: Any value that the script creates can be used.

3.3.4.3 Log file formats

There are various standard formats available from the drop down list that will change the way the fields and message content are logged to the specified file. If the file format you want to use is not included, you can create your own format. Just add a new Custom File Format under the Formats option and then set the fields as desired. Then choose this new custom field from the drop down list in the Log to file action (the custom formats appear at the end of the list, after the standard and reserved formats.)

The following standard file formats are included with the program:

Kiwi format ISO yyyy-mm-dd (Tab delimited)
Format: DateTime (YYYY-MM-DD HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

Example: 2002-07-22 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format ISO UTC yyyy-mm-dd (Tab delimited)
Format: UTC DateTime (YYYY-MM-DD HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

Example: 2002-07-22 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format mm-dd-yyyy (Tab delimited)
Format: Date (MM-DD-YYYY) [TAB] Time (HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

Example: 07-22-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format dd-mm-yyyy (Tab delimited)
Format: Date (DD-MM-YYYY) [TAB] Time (HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

©2014 SolarWinds, Inc.

Example: 22-07-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format UTC mm-dd-yyyy (Tab delimited)
Format: UTC Date (MM-DD-YYYY) [TAB] UTC Time (HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

Example: 07-22-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format UTC dd-mm-yyyy (Tab delimited)
Format: UTC Date (DD-MM-YYYY) [TAB] UTC Time (HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

Example: 22-07-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Comma Separated Values yyyy-mm-dd (CSV)
Format: DateTime (YYYY-MM-DD HH:MM:SS),Priority (Facility.Level),Host name,Message text

Example: 2002-07-22 12:34:56,Local5.Debug,firewall-inside,"prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64"

Comma Separated Values UTC yyyy-mm-dd (CSV)
Format: UTC DateTime (YYYY-MM-DD HH:MM:SS),Priority (Facility.Level),Host name,Message text

Example: 2002-07-22 12:34:56,Local5.Debug,firewall-inside,"prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64"

BSD Unix syslog format
Format: DateTime (Mmm DD HH:MM:SS) [SPACE] Host name [SPACE] Message text (PID tag followed by message content)

Example: Jul 22 12:34:56 [SPACE] firewall-inside [SPACE] amd[308]: key sys: No value component in "rw, intr"

XML tagged format
Format: <Message><DateTime> DateTime (YYYY-MM-DD HH:MM:SS) </DateTime><Priority> Priority (Facility.Level) </Priority><Source_Host> Host name </Source_Host><MessageText> Message Text </MessageText></Message>

Example: <Message><DateTime>2002-07-23 21:53:35</DateTime><Priority>Local7.Debug</Priority><Source_Host>firewall-inside</Source_Host><MessageText> prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64</MessageText></Message>

RnRsoft ReportGen format
Format: rnrsoft [TAB] Date (YYYY-MM-DD) [TAB] Time (HH:MM:SS) [TAB] Host name [TAB] Level (numeric 0-7) [TAB] Message text

Example: rnrsoft [TAB] 2002-07-23 [TAB] 22:02:51 [TAB] firewall-inside [TAB] 7 [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

More information on ReportGen for SonicWall, PIX, GNATbox and Netscreen can be found at: www.reportgen.com

WebTrends format
Format: WTsyslog [SPACE] Date (YYYY-MM-DD) [SPACE] Time (HH:MM:SS) [SPACE] ip=Host address (a.b.c.d) [SPACE] pri=Level (numeric 0-7) [SPACE] Message text

©2014 SolarWinds, Inc.

Example: WTsyslog [2001-11-12 12:44:45 ip=192.168.168.1 pri=6] <134>id=firewall time="2001-11-15 08:43:42" fw=192.168.1.1 pri=6 src=192.168.1.34 proto=http

More information on Webtrends firewall suite can be found at: http://www.netiq.com/products/fwr

Cisco PIX PFSS format (Raw logging)
Format: <Priority value (0-191)>Message text

Example: <191>Built outbound TCP connection 12004 for faddr grc.com/80 gaddr 192.168.2.2/4120 laddr 192.168.1.1/4391

3Com 3CDaemon format (BSD space delimited)
Format: DateTime (Mmm DD HH:MM:SS) [SPACE] Host address [SPACE] Message text

Example: Jul 22 12:34:56 [SPACE] 192.168.1.1 [SPACE] key sys: No value component in "rw,intr"

Raw - Message text only (no priority)
Format: Message text only

Example: Built outbound TCP connection 12004 for faddr grc.com/80 gaddr 192.168.2.2/4120 laddr 192.168.1.1/4391

Sawmill format ISO yyyy-mm-dd (Tab delimited)
Format: DateTime (YYYY-MM-DD HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

Example: 2002-07-22 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

More information on Sawmill log processing software can be found at: www.sawmill.net

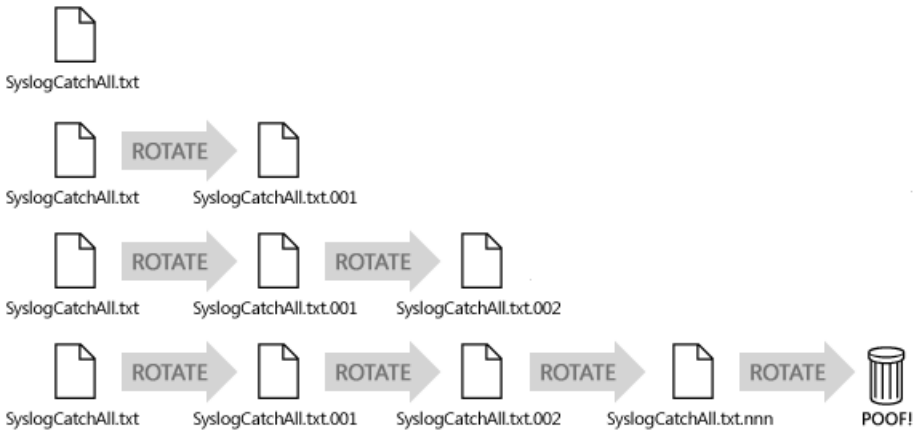
3.3.4.4 Log File Rotation

This feature is only available in the licensed version.

Log file rotation ensures that log files do not grow indefinately. It allows us to keep a reasonable, finite amount of log data araound.
This can be a necessary consideration if disk space is at a premium or limited for whatever reason.
File rotation is the usual solution to disk space problems.

After a log file has reached a specific size or age, the current log file is moved to another name, eg. logfile.txt.001. The logging process is then continued into an empty file. Whenever the next file size or age is reached the process is repeated, first moving logfile.txt.001 to logfile.txt.002, and then moving the current log file to logfile.txt.001. This process is repeated until the set number of log files in the rotation have been created. The oldest file at that point is discarded. (see illustration below)

©2014 SolarWinds, Inc.



Log File Rotation options within Kiwi Syslog Server's Log to file Action:

Enable Log File Rotation
If this option is checked then the log file will be rotated in the manner described above.
If not, then log file rotation will not occur and data will be logged to the file as normal.

Total number of log files
This specifies the total number of log files in the rotation set. The number of log files created during file rotation will never exceed this number.
e.g. If set to '4', once all log files have been created they will be named <logfile>, <logfile.001>, <logfile.002>, and <logfile.003>

Maximum log file size
Select this option if you want to ensure that no single log file in the rotation set exceeds a certain size. The size of each file can be specified in bytes, kilobytes, megabytes or gigabytes.

Maximum log file age
Select this option if you want to ensure that no single log file in the rotation set exceeds a certain age. The age of each file can be specified in minutes, hours, days, weekdays, weeks, months, quarters or years.

3.3.5 Action - Forward to another host

This will forward the received message to another Syslog host using the UDP or TCP syslog protocol.

Destination IP address or hostname

This is where you specify the remote host IP address or hostname to forward the messages to.

You can send messages to multiple hosts by separating each hostname or IP address with a comma.

For example: Myhost.com, SecondHost.net, 203.75.21.3

Protocol

Syslog messages can be sent using UDP (default), TCP, or KRDP.

The Kiwi Reliable Delivery Protocol (KRDP) works between two Kiwi Syslog Servers to reliably deliver syslog messages over a TCP transport.

New Port

This specifies the port number to send the message to. Recommended values are:
UDP: Port 514

©2014 SolarWinds, Inc.

TCP: Port 1468 or port 601
KRDP: Port 1468

New Facility/New Level

This allows you to force all outgoing messages to use a new Facility or Level. In most cases this option should be set to "- No change -". This will forward messages with the same Facility and Level that they arrived with.

KRDP connection identifier

This specifies the unique name assigned to the KRDP connection. Each connection between the source and destination syslog Server needs to be identified. When the connection is broken and re-established, the sequence numbers can be exchanged and any lost messages can be resent. A separate set of message sequence numbers are kept against each connection identifier.

Examples are: Source:RemoteOffice1 or SyslogServer1

The string of text used will uniquely identify the source of the connection to the destination syslog Server.

If you have more than one "Forward to another host" action configured, you can use the same connection identifier on all actions. This will mean that only a single KRDP connection is made between the source and destination syslog Servers. If you specify a different connection identifier, multiple KRDP sessions will be created.

To ensure that the identifier is unique, we recommend the use of the %MACAddress variable. This variable will be replaced by the first MAC address of the machine.

Examples are: Source:RemoteOffice1-%MACAddress
When running, the ID would look like: Source:RemoteOffice1-AA-BB-CC-DD-EE-FF-00
The MAC Address is globally unique to each network card.

Send with RFC3164 header information

This will add the standard RFC3164 header information to the outgoing message. The format is:

<Priority>Date Hostname PID Message text

The Priority is a value between 0 and 191
The Date is in the format of Mmm DD HH:NN:SS (July 4 12:44:39). Note there is no year specified.
The PID is a program identifier up to 32 characters in length

Retain the original source address of the message

Normally, the syslog protocol is unable to maintain the original senders address when forwarding/relaying syslog messages. This is because the senders address is taken from the received UDP or TCP packet.

The way Kiwi Syslog gets around this problem is to place tags in the message text that contains the original senders address. By default, the tags looks like Original Address=192.168.1.1. That is, the "Original Address=" tag, followed by the IP address, followed by a space delimiter.

These tags are only inserted if the "Retain the original source address of the message" option is checked.

These tags can also be overidden by way of two registry settings, named OriginalAddressStartTag and OriginalAddressEndTag.
For more information on overiding the default originating address start and end tags, please see - Originating Address - Custom Start and End tags

Note: If the "Spoof Network Packet" option is used, then the "Original Address=" tag will not be used. The Syslog packet will be fowarded to the destination address as though it has been sent from the originating IP address.

Use a fixed source IP address

©2014 SolarWinds, Inc.

This option will use a fixed IP address in the Original Address= tag. This can be useful when you want to identify all outgoing messages as from a particular host. For example, if you have many remote syslog Servers sending messages to one central location. If each of the remote syslogs use the 10.0.0.x address range, all the received messages will appear from the same host. Specifying a different source IP address for each remote syslog could help in identifying the incoming messages better.

Note: If the "Spoof Network Packet" option is used, then the "Original Address=" tag will not be used. The Syslog packet will be fowarded to the destination address as though it has been sent from the specified fixed IP address.

Spoof Network Packet
This feature is only available in the licensed version, requires WinPcap 4.1+ installation

This option only applies to syslog messages forwarded via UDP protocol.
The network packet will be spoofed to appear as though the fowarded message has come directly from the originating devices' IP address, and not the address of the Syslog Server. Kiwi Syslog Server will use the **Selected Network Adapter** to send the spoofed UDP/IP packet.

Important Note:
This option also requires that WinPcap version 4.1 and above is installed. WinPcap (Windows Packet Capture library) is available for download from: WinPcap, The Packet Capture and Network Monitoring Library for Windows

Test button

Use the **Test** button to send a test Syslog message to the host(s) specified.

3.3.6 Action - Play a sound

This feature is only available in the licensed version.

The specified sound will be played whenever a message matches the filters set above.

Specify a sound filename to play in the **Sound file name** field or use the "**...**" browse button to select a file.

A number of sample sound files are included in the \sounds folder. To hear the sound file play, press the **Test** button.

3.3.7 Action - Run external program

This feature is only available in the licensed version.

This will execute an external program whenever a message is received which passes the filters set above.

Please note that a new instance of the external program is launched for every message, so this may become a problem if messages arrive faster than the external program exits. It is especially true if Syslog is installed as a service, in which case the external program is launched by the service inside the non- interactive Windows session. The only way to see that the program is running is by using Task Manager. So if not used carefully this action may lead to the computer being flooded with multiple instances of the external program.

Details of the message and other Syslog statistics can be passed to the external program as command-line arguments.
Specify the external program filename by filling in the **Program file name** field or press the "**...**" browse button to browse for a program.
Specify the command line options you would like to pass to the program in the **Command line options** field.
Press the "**?**" button to see syntax for passing message details and Syslog statistics to the external program.

Insert message content or counter

©2014 SolarWinds, Inc.

To pass program variables, counters, script fields and statistics to the external program, click on the Insert message content or counter link and choose an option from the popup menu. More details on the values can be found here.

This option allows you to choose a variable from a popup menu. The variable is then replaced with the current value before the program is run. For example %MsgText is replaced with the text of the current syslog message. Just position your cursor in the command line options text line and click the hyperlink. A popup menu will be displayed so you can choose the variable you want.

Example command line options:

"555-1234", "Syslog - A link has gone down - %MsgAll"
Or: "Warning, message received from host %MsgHost at %MsgTime"

Process Priority
Sets the priority of the new windows process that will be created.

Acceptable values are:
LOW_PRIORITY
BELOW_NORMAL_PRIORITY
NORMAL_PRIORITY (default)
ABOVE_NORMAL_PRIORITY
HIGH_PRIORITY
REALTIME_PRIORITY (Caution: REALTIME priority can cause system lockups)

AboveNormal
Indicates a process that has priority above Normal but below High.

BelowNormal
Indicates a process that has priority above Idle but below Normal.

High
Specify this class for a process that performs time-critical tasks that must be executed immediately. The threads of the process preempt the threads of normal or idle priority class processes. An example is the Task List, which must respond quickly when called by the user, regardless of the load on the operating system. Use extreme care when using the high-priority class, because a high-priority class application can use nearly all available CPU time.

Low
Specify this class for a process whose threads run only when the system is idle. The threads of the process are preempted by the threads of any process running in a higher priority class. An example is a screen saver. The idle-priority class is inherited by child processes.

Normal
Specify this class for a process with no special scheduling needs.

RealTime
Specify this class for a process that has the highest possible priority. The threads of the process preempt the threads of all other processes, including operating system processes performing important tasks. For example, a real-time process that executes for more than a very brief interval can cause disk caches not to flush or cause the mouse to be unresponsive.

Window Mode
Sets the window mode of the process if that process has a user interface. This setting has no effect on processes that do not have a user interface. This setting is unavailable if running Syslog Server as a service.

Acceptable values are:
Hide
Normal
Minimized
Maximized

Wait for program initialization to complete before continuing
When checked, this option means that Syslog will wait for the new process to complete it's initialization. It does this by waiting until the new process signals that it is idle.
Note: This is a blocking operation. Kiwi Syslog will not process messages any further; until it receives the

©2014 SolarWinds, Inc.

InputIdle signal from the process. Because of this, there is an additional option which specifies how long Kiwi Syslog should wait for the process to initialize. Once this time interval has elapsed, Kiwi Syslog assumes that the process started correctly.
This setting is useful is you are interacting with the process at a later stage, and you want to be sure that the process has started.

3.3.8 Action - E-mail message

This feature is only available in the licensed version.

This action will send an e-mail message to the recipients specified whenever a Syslog message is received that matches the filters set.

Details from the Syslog message received and other Syslog statistics can be included in the e-mail subject or message body. In effect this program can be used as a Syslog to e-mail converter.

Firstly, ensure that you have set the SMTP server and format of the Email (HTML/Plain text) options via the e-mail options.

Specify the e-mail recipient's address in the **E-mail recipient** field. More than one address can be specified. Each address must be separated by a comma.

Specify the From address in the **E-mail From** field. Make sure that when you use secured mailing(SSL/TLS), the from address keyed in 'Email setup' and 'Email message' Action are same.

Specify the e-mail subject in the **E-mail subject** field. (Single line only). The **Max subject length** option can be used to ensure that only a limited number of characters are sent in the subject line.

Specify the e-mail message in the **E-mail message** field. (Multiple lines may be used). If this message is intended for an e-mail to pager gateway, then the message body part of the e-mail may not be used. In this case you can just leave it blank. Most paging systems only have limited space so they only use the subject part of the message. The **Max message length** option can be used to limit the amount of data sent in the message body. If you have used the variable %MsgText in the message body and a large syslog message arrives, it may be too large to send via e-mail. You can limit the message body length to a more manageable length.

The **Test** button will send a test e-mail message to the specified recipients. The content of the test message can be modified by pressing the **Test Setup** button.

Insert message content or counter
To pass program variables, counters, script fields and statistics into the message or subject, click on the Insert message content or counter link and choose an option from the popup menu. More details on the values can be found here.

This option allows you to choose a variable from a popup menu. The variable is then replaced with the current value before the message is sent. For example %MsgText is replaced with the text of the current syslog message. Just position your cursor in the subject or message text line and click the hyperlink. A popup menu will be displayed so you can choose the variable you want.

Example subject field: Syslog Alert from %MsgHost

Example message body field: Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

To set Kiwi Syslog Server to act as a Syslog message to e-mail converter use the %MsgAll keyword in the message body text to pass all of the received Syslog message information into the e-mail message.

Be aware, that if you are getting a lot of messages, then you could cause congestion on your e-mail server. The e-mail buffer will hold 1000 messages before a message is lost, this will help when many Syslog messages are received at once and the mail server is busy.

E-mail is queued for a minute before sending. This is more efficient than having to reconnect to the mail server each time a message needs to be sent. The messages are queued for a minute and then delivered in a batch.

©2014 SolarWinds, Inc.

E-mail Delivery Options
This option allows the importance, priority and sensitivity flags of the e-mail message to be specified. The e-mail recipients will recieve the messages with the various importance/priority/sensitivity levels set accordingly.
Importance: Unspecified (Default) / High / Normal / Low
Priority: Unspecified (Default) / Normal / Urgent / Non-Urgent
Sensitivity: Unspecified (Default) / Personal / Private / Confidential

Expand <013><010> in message
This option will expand any carriage return and line feed characters that have previously been replaced with <013> and <010>.

If the replace non printable characters with ASCII value option is set, any CR and LF characters appearing in the syslog message are replaced. It is sometimes useful to have them expanded back again when forwarded via e-mail as it makes the text more readable.

3.3.8.1 Insert message content or counter

This option allows you to choose a variable or counter from a popup menu. The variable is then replaced with the current value before the message is sent. For example %MsgText is replaced with the text of the current syslog message. Clicking on a popup menu item will place the %variable name at the current cursor position.

Example subject field: Syslog Alert from %MsgHost

List of variables and their function.

Menu name: All of the message
Parameter: %MsgAll
Explanation: The whole message as it appears on the display. Including the time, date, priority and message text. Each field is space delimited.
Example: 2005-10-10 11:28:04 Local7.Debug host.company.com This is a test message

Menu name: Date
Parameter: %MsgDate
Explanation: The date the message arrived in the format YYYY-MM-DD
Example: 2005-02-18

Menu name: Time
Parameter: %MsgTime
Explanation: The time the message arrived in the format HH:MM:SS
Example: 22:30:16

Menu name: Facility
Parameter: %MsgFacility
Explanation: The facility of the message in text format.
Example: Local7, Mail

Menu name: Level
Parameter: %MsgLevel
Explanation: The level of the message in text format.
Example: Debug, Info

Menu name: Host address of sender
Parameter: %MsgHost
Explanation: The host IP address of the sending device.
Example: 192.168.1.1

Menu name: The message text
Parameter: %MsgText
Explanation: The message text part of the syslog message
Example: This is a test message

Menu name: Alarm min msg threshold
Parameter: %MsgAlarmMin
Explanation: The threshold level set for the minimum message count alarms

©2014 SolarWinds, Inc.

Example: 100 (messages per hour minimum)

Menu name: Alarm max msg threshold
Parameter: %MsgAlarmMax
Explanation: The threshold level set for the maximum message count alarms
Example: 5000 (messages per hour maximum)

Menu name: Alarm disk space threshold
Parameter: %MsgAlarmDisk
Explanation: The threshold level set for the minimum disk space remaining in MB
Example: 90 (MB)

Menu name: Message count this hour
Parameter: %MsgThisHour
Explanation: The number of messages received so far this hour.
Example: 254

Menu name: Message count last hour
Parameter: %MsgLastHour
Explanation: The number of messages received in the last hour
Example: 254

Menu name: Machine MAC address
Parameter: %MACAddress
Explanation: The MAC address value of the first network adaptor found.
Example: AA-BB-CC-DD-EE-FF-00

Menu name: Rule Name
Parameter: %RuleName
Explanation: The name of the Rule which triggered this action.
Example: EmailAction

Custom/Global/Statistics fields (Only in the registered version)

Menu name: VarCustom01 to VarCustom16
Parameter: %VarCustom01 to %VarCustom16
Explanation: There are 16 custom fields that can be modified by the Run Script action. If these fields have not been modified by the script, they will be blank. Be aware that a blank autosplit value may result in an invalid file name. The custom field values are cleared when a new message arrives. They are only valid for the current message. To store values longer than a single message, use VarGlobal fields.
Example: Any value that the script creates can be used.

Menu name: VarGlobal01 to VarGlobal16
Parameter: %VarGlobal01 to %VarGloabl16
Explanation: There are 16 global fields that can be modified by the Run Script action. If these fields have not been modified by the script, they will be blank. Be aware that a blank autosplit value may result in an invalid file name. The global fields retain their value between messages.
Example: Any value that the script creates can be used.

Menu name: VarStats01 to VarStats16
Parameter: %VarStats01 to %VarStats16
Explanation: There are 16 statistics fields that can be modified by the Run Script action. The statistics fields retain their value between messages. You can modify the names associated with the statistics fields and their initial value from the Script options section on the setup window. The custom statistics values are viewable on the statistics display and on the daily statistics e-mail.
Example: Any value that the script creates can be used.

3.3.9 Action - Send Syslog message

This feature is only available in the licensed version.

This will send a Syslog message to the hosts specified, whenever a message is received and passes the filters set above.

©2014 SolarWinds, Inc.

Details of the received message and other Syslog statistics can be included in the outgoing Syslog message.

This can be used to relay selected Syslog messages on to another host with extra information, or with your own text added to the message.

Specify a destination IP address or host name in the **Hostname or IP address** field.

Press the "**?**" button next to the **Hostname or IP address** field to see the host name syntax.

Multiple host names can receive the forwarded message.

Each host name or IP address must be separated by a comma.

I.e. Myhost.com, SecondHost.net, 203.75.21.3

Specify the new facility and level you wish to forward the message to, by selecting from the **New facility** and **New level** lists. (By default the message will be sent out on the same facility and level it came in on, but you can change this if you want to.)

Press the **Test** button to send a test Syslog message to the addresses specified.

Insert message content or counter
To pass program variables, counters, script fields and statistics into the new syslog message, click on the Insert message content or counter link and choose an option from the popup menu. More details on the values can be found here.

This option allows you to choose a variable from a popup menu. The variable is then replaced with the current value before the message is sent. For example %MsgText is replaced with the text of the current syslog message. Just position your cursor in the syslog message text line and click the hyperlink. A popup menu will be displayed so you can choose the variable you want.

Example message text field: Syslog Alert from %MsgHost
Or: Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

3.3.10 Action - Log to ODBC database

3.3.10.1 Action - Log to Database

This feature is only available in the licensed version.

This will log the message to the table specified by the Data Link connection string.

Data link connection string
Press the **Browse** (...) button to create or edit Data link properties.

The Data Link Properties dialog box opens, displaying the following tabs: Provider, Connection, Advanced, and All.

- On the Provider tab, select a database provider.
- On the Connection tab, either select the data source name (DSN) of an available Provider, or enter a custom connection string. Valid DSNs for providers that are pre-defined on your system are displayed in the Use Data Source drop-down list.

  The "Test Connection" button can be used to validate that the connection properties supplied are correct.
- Use the Advanced tab to view and set other initialization properties for your data.

Click "OK" when done.

Database Table name

©2014 SolarWinds, Inc.

A valid database table name must be specified. The table specified must contain field names that match the selected database format. If the field sizes are too small, the data could be truncated when written to the database.

The default table name used is Syslogd.

To test the Log to Database action, press the **Test** button. A message will indicate if the action was successful, or details of any error that occurred will be displayed.

Database type/field format
Choose from the list of default database types or create your own format by clicking on the **Edit custom format** button.

The default database types are:

- Access
- SQL
- MySQL
- Oracle

The default database table design is as follows.

Microsoft Access database

Field	Name	Type	Size
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	Text	30
Hostname	MSGHOSTNAME	Text	255
Message text	MSGTEXT	Memo	1024

SQL database (Microsoft SQL and generic SQL)

Field	Name	Type	Size
Date	MSGDATE	DateTime	10
Time	MSGTIME	DateTime	8
Priority	MSGPRIORITY	VarChar	30
Hostname	MSGHOSTNAME	VarChar	255
Message text	MSGTEXT	VarChar	1024

MySQL database

Field	Name	Type	Size
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	VarChar	30
Hostname	MSGHOSTNAME	VarChar	255
Message text	MSGTEXT	Text	1024

Oracle database

Field	Name	Type	Size
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	VarChar2	30
Hostname	MSGHOSTNAME	VarChar2	255
Message text	MSGTEXT	VarChar2	1024

Notes:
If the database file is opened exclusively by another process, Kiwi Syslog Server may not be able to write new records to the database.

Some example ODBC databases are available for download from: http://www.kiwitools.com/downloads/

©2014 SolarWinds, Inc.

Syslog_ODBC_Samples.zip

The zip file contains information and sample databases that you can use as a guide to help you setup ODBC logging on your own system.

Create table button
This button will attempt to create the specified table in the database referenced by the DSN. Any existing table will be deleted and the contents lost. The new table will be created with the field names and types specified by the database type you have selected. If all goes well and the new table is created, you will see a confirmation message. If there is a problem creating the table, an error message will be displayed so you can work on correcting the problem.

Query table button
This button will attempt to retrieve the last 5 entries in the table specified. The DSN type must be set to allow dynamic access. Forward only databases can't be read correctly since the "Move previous" command is issued to the database.

The data returned will be displayed in notepad. You can then get some information on the table structure and the data contained in the last 5 fields.

Example of information returned by the query:

```
Field name      Type            Size  Data
---------------+---------------+-----+----->
MsgDate         adDBTimeStamp     16 28/03/2005
MsgTime         adDBTimeStamp     16 14:45:16
MsgPriority     adVarWChar        30 Local7.Debug
MsgHostname     adVarWChar       255 host.company.com
MsgText         adLongVarWChar  1024 This is a test message from Kiwi Syslog Server
```

Edit custom format button
If a custom format is selected from the database type drop down list, then pressing this button will take you to the custom format selected. If no custom format is selected, then you will be taken to the "Custom DB formats" option where you can create a new format of your choice.

Show SQL commands button:
This button will generate the SQL commands used to create and insert data into the selected table. The commands generated are dependent on which database format is selected. You can use these commands to generate the database table schema in your database application. Alternatively, you can have Kiwi Syslog Server create the table for you by pressing the "Create table" button.

Example of SQL commands generated:

```
Database type: Access database
Database name: Kiwi Access format ISO yyyy-mm-dd

SQL command to create the table:
CREATE TABLE Syslogd (MsgDate DATE,MsgTime TIME,MsgPriority TEXT(30),MsgHostname TEXT(255),
MsgText MEMO)

SQL INSERT command example:
INSERT INTO Syslogd (MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText) VALUES ('2005-03-
28','14:58:04','Local7.Debug','host.company.com','This is a test message from Kiwi Syslog
Server')
```

Connection Inactivity timeout:
This value controls how long the database connection is kept open after the last message has been sent. Because opening and closing the connection can be the slowest part of logging to a database, the connection is kept open while data is actively being logged. If no more messages have been logged before the timeout value expires, the database connection will be closed. As soon as a new message arrives, the connection will be reopened. The default for this setting is 600 seconds (10 minutes). Using a value of 0 will ensure that the connection will never time out. The maximum value is 86400 seconds (1 day).

Run debug command button:

©2014 SolarWinds, Inc.

If there is a problem logging to the database, you can use this button to diagnose the problem. A separate window is displayed where you can enter the SQL command to be executed on the database. If the command fails, a detailed error message will be displayed in the results field. By default, the current INSERT statement that is used for the database type selected will be displayed in the query field. This statement can be modified to test particular variations of the statement.

This option may not be used to run a query on the database. Only error information is returned to the results field. It is not possible to run a Select From statement for example and obtain the results back. All that will be returned is an indication if the statement executed correctly or not.

By using the **Show SQL commands** button, you can obtain the correct syntax to use in the debug test.

Custom fields
Custom fields are for use by the run script action. By writing a parsing script, the syslog message text can be broken down into various sub fields. The values can then be assigned to the 16 custom fields and then logged to a database. Because each device manufacturer creates syslog messages in a different format, it is not possible to create a generic parser that will break up the message text into separate fields. A custom script must be written to parse the message text and then place it in the custom database fields. Example parsing scripts can be found in the \Scripts sub folder.

It is also possible to use the scripting function ActionLogToODBC to send SQL statements and raw data to a database connection.

3.3.10.2 Problems logging when running as a Service

When testing the ODBC logging from the Service Manager, the program is running as the current user (probably "Administrator").

When the Service logs to an ODBC database, it is running as the "Local System" user by default.

If your test messages work but the service does not, try changing the Service logon to "Administrator" instead of "Local System".

This can be changed with the Services applet under Control Panel.

You may also want to check the box that allows the program to interact with the desktop.

3.3.11 Action - Log to NT Event log

3.3.11.1 Action - Log to NT Event log

This feature is only available in the licensed version.

This will log the syslog message to the NT application event log whenever a message is received and passes the filters set above.

The NT event log has five logging levels: Error, Warning, Information, Success and Failure.

Select a logging level from the drop down list. Messages will then be logged to the NT event log with this level.

3.3.11.2 Setting the log insertion type

When the message is inserted into the Event Log it can be done in three ways.
The messages are logged as follows:
Single insertion string.
%1 is replaced with:
Date – Tab – Time – Priority – Tab – Hostname – Tab – Message

©2014 SolarWinds, Inc.

5 Tab delimited insertion strings
%1 Tab %2 Tab %3 Tab %4 Tab %5
%1 = Date
%2 = Time
%3 = Priority
%4 = Hostname
%5 = Message

5 Space delimited insertion strings
%1 Space %2 Space %3 Space %4 Space %5
%1 = Date
%2 = Time
%3 = Priority
%4 = Hostname
%5 = Message

Press the **Test** button to test the NT event logging action. When running on a non NT system like Windows 95/98, no message will be logged and an error message will appear.

Note: By default, when viewing the NT event log with the NT event log viewer, the log type is set to show System events. To show Application events, you need to check the Application item in the Log menu of the NT Event viewer.

3.3.12 Action - Send pager or SMS message via NotePage Pro

This feature is only available in the licensed version.

This action will send a pager, SMS or e-mail message via the NotePagerPro application. For this to work, you must have first purchased and installed NotePager Pro from http://www.notepager.com. NotePager Pro is an inexpensive but very powerful paging and SMS gateway application.

Benefits of using NotePager Pro include:

- Group messaging capabilities
- Multiple carrier support including cellular and paging carriers
- Supports internet paging protocols including SNPP, WCTP and SMTP
- Supports scheduled messaging, repeating messages, and pre-programmed messages

Click here to download NotePager Pro now.

When a message is passed to NotePager Pro, it places the messages in the sending queue. NotePager Pro will check the queue periodically and then send them via the method you have specified. This could be via SNPP, e-mail, modem, TAPI, or what ever paging interface you have configured.

By using the "Insert message content or counter" link, details from the Syslog message received and other Syslog statistics can be included in the pager message to be sent.

Send Page To:
Select a recipient from the drop down list. The list is automatically populated from the NotePager Pro Recipients and Groups database. If no names are available in the drop down list, then NotePager Pro has not been installed correctly. You can choose either a single recipient, or a group of recipients to send to. For example: Send to: Joe, or Send To: All-Network-Staff.

Message From:
This can be any descriptive name you like. If the recipient is configured in NotePager Pro to receive the message via e-mail, the From name you specify will be prepended to the default domain you have configured. For example, if NotePager Pro is configured with the default domain of "company.com", when you send a message from "Syslog", it will appear as if the message came from "Syslog@company.com"

Message:

©2014 SolarWinds, Inc.

This is where you place any message text you want to have appear in the pager or SMS message. Normally this is set to %MsgText. This will be replaced by the message text from the original syslog message.
Other variables can be used in the message. Click on the "Insert message content or counter" hyperlink to display the popup menu of available variables. The **Max message length** option can be used to limit the amount of data sent in the message. If you have used the variable %MsgText in the message body and a large syslog message arrives, it may be too large to send via a pager. You can limit the message body length to a more manageable length.

If your pager is only capable of receiving numeric messages, you will need to specify a number in the message field instead of %MsgText. You will have to determine a series of codes that mean something to you. For example, 1=link up, 2=link down, 9=Router unreachable etc.

Test Button:
The **Test** button will send a test pager message to the recipient specified. The content of the test message can be modified by pressing the **Test Setup** button.

Insert message content or counter
To pass program variables, counters, script fields and statistics into the pager message, click on the Insert message content or counter link and choose an option from the popup menu. More details on the values can be found here.

This option allows you to choose a variable from a popup menu. The variable is then replaced with the current value before the message is sent. For example %MsgText is replaced with the text of the current syslog message. Just position your cursor in the subject or message text lines and click the hyperlink. A popup menu will be displayed so you can choose the variable you want.

Example message field:
Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

3.3.13 Action - Send ICQ instant message

This feature is only available in the licensed version.

****** This feature is currently disabled because of changes to the ICQ WWW paging system. We aim to have a replacement paging system very soon. ******

This action will send an ICQ instant message to the ICQ number specified whenever a Syslog message is received that matches the filters set.

The alert will appear on ICQ as an incoming WWPager message. The user can then read and close the ICQ alert.

The message is sent via the ICQ web based interface. This is currently a free service. The ICQ client can be downloaded for free from http://www.icq.com.

Delivery of the message is not guaranteed and is performed on a best effort basis. ICQ limits the frequency of pager messages to around 1 every 2 seconds. Pager messages being sent faster than this will probably be lost.

To be able to use this feature, the program must be able to directly connect to the ICQ web server on port 80 using standard http. Transparent proxies are not an issue. This feature will not work via a firewall that blocks direct port 80 access. The destination web site address is http://wwp.icq.com. This address may need to be added to the firewall access list for direct access.

Details from the Syslog message received and other Syslog statistics can be included in the message subject or message body.

ICQ number:
This must be a valid ICQ number to send the page to.

©2014 SolarWinds, Inc.

From name:
This can be any descriptive name you like. This name will appear as the Nickname on the ICQ message.

From e-mail address:
This address should be a valid return address. It is shown in the E-mail address field on the ICQ message.

Subject:
This line is used to indicate the subject of the message. Normally this is set to %MsgHost. This will be replaced by the host name of the device that sent the original syslog message.
Other variables can be used in the subject line. Click on the "Insert message content or counter" hyperlink to display the popup menu of available variables. The **Max subject length** option can be used to ensure that only a limited number of characters are sent in the subject line.

Message:
This is where you place any message text you want to have appear in the ICQ message. Normally this is set to %MsgText. This will be replaced by the message text from the original syslog message.
Other variables can be used in the message body. Click on the "Insert message content or counter" hyperlink to display the popup menu of available variables. The **Max message length** option can be used to limit the amount of data sent in the message body. If you have used the variable %MsgText in the message body and a large syslog message arrives, it may be too large to send via ICQ. You can limit the message body length to a more manageable length.

Expand <013><010> in message
This option will expand any carriage return and line feed characters that have previously replaced with <013> and <010>. If the replace non printable characters with ASCII value option is set, any CR and LF characters appearing in the syslog message are replaced. It is sometimes useful to have them expanded back again when forwarded via ICQ as it makes the text more readable.

Example pager message:
Below is an indication of what the ICQ pager message will look like.

```
Nickname: Syslog Server
E-mail: syslog@company.com
Sender IP: xxx.xxx.xxx.xxx
Subject: firewall.company.com
Firewall Alert - Unauthorized login attempt: User=Administrator
```

The **Test** button will send a test ICQ pager message to the ICQ number specified. The content of the test message can be modified by pressing the **Test Setup** button.

Insert message content or counter
To pass program variables, counters, script fields and statistics into the ICQ pager message, click on the Insert message content or counter link and choose an option from the popup menu. More details on the values can be found here.

This option allows you to choose a variable from a popup menu. The variable is then replaced with the current value before the message is sent. For example %MsgText is replaced with the text of the current syslog message. Just position your cursor in the subject or message text lines and click the hyperlink. A popup menu will be displayed so you can choose the variable you want.

Example subject field: Syslog Alert from %MsgHost

Example message body field:
Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

©2014 SolarWinds, Inc.

3.3.14 Action - Send SNMP Trap

This feature is only available in the licensed version.

This action will send an SNMP trap to the IP Address specified, whenever a Syslog message is received that matches the filters set.

You can create a new Action by right-clicking on the **File | Setup | Action** item, or by highlighting it and clicking the "**Add New item**" button on the tool-bar.

The following parameters apply to the "**Send SNMP trap**" option:

Destination IP address
The IP address of the system that will be receiving the SNMP trap.

Message text
The content of the SNMP trap to be forwarded. This field can contain all of the standard message variables, and these can be selected by clicking on the **Insert message content or counters** link (just above the **Message text** field)

Agent IP address
The IP address that will appear as the source of the SNMP trap. By default this is set to "The original sender" but can be set to "From this machine" (i.e. the address of the machine running the Kiwi Syslog Server)

Generic type
A value from 0 to 6 that indicates the type of trap to be sent. This field only applies for version 1 traps.

The values are:

0 Cold Start
1 Warm Start
2 Link Down
3 Link Up
4 Authentication Failure
5 EGP Neighbor Loss
6 Enterprise Specific

These can be selected from the drop down menu.

Version
The SNMP version (v1 or v2) supported by the system receiving the SNMP traps from your Kiwi Syslog Server.

Enterprise OID
This is a dotted numerical value (1.3.6.1.x.x.x.x) that represents the MIB enterprise of the SNMP trap. This field only applies for version 1 traps. Version 2 traps have the Enterprise value bound as the second variable in the message.

If the Generic Type is set to 6 it indicates an Enterprise type trap. In this case the Specific Trap value needs to be considered.

Variable OID
This is a dotted decimal value (1.3.6.1.x.x.x.x) that represents that MIB variable of version 2 SNMP traps.

Community
This is like a password that is included in the trap message. Normally this value is set to values such as "public", "private" or "monitor".

©2014 SolarWinds, Inc.

Specific type
This is a value that indicates the condition that caused the trap to be sent. In version 2 traps, this condition will be unique to the MIB defined for the particular device sending the trap (or syslog message).

Remote port
The port to which the SNMP trap will be sent. The default is set to 162.

If you change this setting, you will need to configure the receiving device to "listen" for SNMP traps on the same port number.

3.3.15 Action - Stop processing message

When fired this action causes Kiwi Syslog Server to stop processing the current message any further.

This means that the message in question will not be tested against any further Rules.

3.3.16 Action - Run Script

This action will run the specified script which will allow you to perform filtering or parsing on the current message.

A step by step example of creating and using a script can be found in the tutorial.

Script file rules
The script must always contain a function called **Main()**. No parameters are passed to the function, but a return value of "OK" must be passed back to indicate that the script ran successfully. If any value other that "OK" is returned, Syslog will assume an error has occurred in the script and place an entry in the error log. The value returned from the script function will also be included in the error log for later diagnoses.

Example (VBScript):

```
Function Main()

' Your code goes here


' Set the return value
Main = "OK"

End Function
```

Each of the script variables available can be accessed from the Fields object.

Script file name
The script file is a standard text file that contains the script commands. The file name can have any extension, but .txt is used by default for ease of editing with Notepad.

Script description
This field can contain any descriptive text you like. Its purpose is to briefly describe the function of the script

Script Language
Windows Script provides two script engines, Visual Basic® Scripting Edition and Microsoft JScript®

VBScript - A variation of Visual Basic or VBA (Visual Basic for Applications) used in MS Word and Excel. This language is easy to learn and has a rich feature set.

JScript - A variation of Java Script used in web pages. If you are familiar with Java Script then this may be your language of choice.

Both languages offer similar functionality and speed, so the choice on which to use is up to personal

©2014 SolarWinds, Inc.

preference. However we have found through our tests that if your script is performing mainly string manipulation then JScript appears to be faster in most cases.

More info on VBScript can be found at:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/vtoriVBScript.asp

More info on JScript can be found at:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/js56jsoriJScript.asp

It is also possible to add additional scripting languages such as Perl or Python.

To do this you will need to install the Active Scripting engines for any new languages that you want to script in.

For information on using PerlScript please visit:
http://www.activestate.com/Products/ActivePerl

For information on using Python please visit:
http://www.activestate.com/Products/ActivePython

To download and for further information on ActiveScriptRuby please visit:
http://arton.hp.infoseek.co.jp/index.html

Edit script button
This will open the script file in Notepad and allow you to view/modify the code. If you modify the code, make sure you save the changes. The script can then be tested by pressing the Test button.

Test button
This will attempt to run the specified script. The script must contain a function named Main(). This is the only function called by Syslog. A return value of "OK" must be passed back from the Main() function to tell Syslog that the script ran successfully.

If an error occurs while trying to run the script, a message box will be displayed indicating the error description and the line number on which it occurred. If the script runs successfully and you have the "show test results" option checked, a before and after dump of the variables will be shown. This will show you any changes that have been made to the variables by your script.

When scripts are tested from the **Kiwi Syslog Server Setup** window (**Test** button pressed) they are not cached. Each script is freshly loaded before it is run.

Show test results option
If the script runs successfully and you have the "show test results" option checked, a before and after dump of the variables will be shown. This will show you any changes that have been made to the variables by your script.

Script file caching
During normal operation, the script files are cached after they have been read from disk. This improves the program speed and saves a lot of additional disk accessing. If you are modifying the script externally and saving it back to disk, the changes will not take effect until you restart the program.

If you are running Kiwi Syslog Server as a standard interactive application you can flush the script file cache and cause the program to reload the files from disk by using the File | Debug options | Clear the script file cache menu option. Or by pressing Ctrl-F8 from the main syslog window.

If you are running Kiwi Syslog Server as a service then this option is not available. To flush the script file cache you will need to stop and restart the service via the Manage menu.

Remember you will need to flush the cache each time you want the new script file to be read from disk.

Field Read/Write permissions
For reasons of security and speed, access to the message/scripting variables can be restricted. Each time a script is run, the message fields are copied to the script variables and back again upon completion of the script. Because the copying takes time and uses CPU cycles, limiting the read/write access to only the

©2014 SolarWinds, Inc.

variables you want to use will improve the speed of the program.

When you enable read access for a group of fields, their values will copied into the script variables and will readable from within the script.

When you enable write access for a group of fields, their values will copied from the script variables and will replace the equivalent program fields.

The fields are divided into groups based on the likelihood of usage within a script.

More details on each of the fields can be found here

Common fields
VarFacility
VarLevel
VarInputSource
VarPeerAddress
VarPeerName
VarPeerDomain
VarCleanMessageText

Other fields
VarDate
VarTime
VarMilliSeconds
VarSocketPeerAddress
VarPeerAddressHex
VarPeerPort
VarLocalAddress
VarLocalPort
VarPriority
VarRawMessageText

Custom fields
VarCustom01 to VarCustom16

The following script variables are always available for read and write access by the script.

Inter-script fields
VarGlobal01 to VarGlobal16

Custom Statistics fields
VarStats01 to VarStats16

Control and counter fields
ActionQuit
SecondsSinceMidnight
SecondsSinceStartup

Triggering a script on a regular basis.
By enabling the Keep-alive input function, a message will be injected on a regular interval. This message can be used to trigger the scripting action.

3.3.16.1 Tutorial - creating your first script

This tutorial will show you how to create your own script and use it to search and replace text within a syslog message.

The scripting action requires the program to be registered.

©2014 SolarWinds, Inc.

Step 1. Create the script action...
Create a new rule called "Replace text"
Add a new Run Script action.
Set the script file name to: ReplaceText.txt
Set the script description to: Replaces occurrences of "cat" with "dog".
Set the script language to VBScript
Set the field read/write permissions to:
Common fields: Read=Yes, Write=Yes
Other fields: Read=No, Write=No
Custom fields: Read=No, Write=No
Press the Edit Script button to open the file in notepad. Since the file doesn't exist, you will be prompted to create a new file.

Copy and paste the following script file into Notepad and then click the File | Save menu on notepad.

```
Function Main()

' Replace cat with dog within the message text field
Fields.VarCleanMessageText = Replace(Fields.VarCleanMessageText, "cat", "dog")

' Return OK to tell syslog that the script ran correctly.
Main = "OK"

End Function
```

Step 2. Create the actions...
Add a new Log to file action
Set the file name to "MyCustomLog.txt" in the folder of your choice.
Leave the file format as default.
Click the action and then press F4 to auto name the action "Log to file"
Add a new Display action
Leave the display number as default.
Click the action and then press F4 to auto name the action "Display"

The Run script action should be above the display and log to file actions. If not, you can move it up the list by selecting the action and using the ^ toolbar button.

Your rule should look like this:

```
Rules
  Rule: Replace Text
    Filters
    Actions
      Run Script
      Display
      Log to file
```

Step 3. Test the script...
Select the Run Script action.
Click the Test Setup button.
Change the message text to read: The cat sat on the mat.
Click the Show action button
Check the Show test results check box
Press the Test button

Once the script runs, the results will be opened in Notepad. There you will be able to see all the script variables. Check the VarCleanMessageText field and you should see the word "cat" has been changed to "dog".

Step 4. Test the script with SyslogGen.
Apply the new rule changes by clicking OK on the Kiwi Syslog Server Setup window. You will then have just the main syslog window showing.
Download SyslogGen from http://www.kiwisyslog.com/downloads.aspx
Install it on the same machine as the Syslog Server
Set the send options to "send message once"
Set the destination to localhost (127.0.0.1).

©2014 SolarWinds, Inc.

Set the message text to be: This is a test. The cat sat on the mat.
Press the Send button
You should now see the message appear on the display "This is a test. The dog sat on the mat."

3.3.16.2 The script variables

A number of variables are passed to and from the script. Depending on the read/write permissions you set for the action, the variables can be modified and returned for use in the syslog program.

The variables and functions are passed via a globally accessible object named "Fields". To access a variable or function, simply prefix the word "Fields." to the variable or function name.

Common fields

Fields.VarFacility
Details: The Facility value of the message.
Type: Integer (0-32767)
Range: 0 to 23. Click here for a list of facilities.

Fields.VarLevel
Details: The level value of the message.
Type: Integer (0-32767)
Range: 0 to 7. Click here for a list of levels

Fields.VarInputSource
Details: The input source of the message.
Type: Integer (0-32767)
Range: 0 to 4. 0=UDP, 1=TCP, 2=SNMP, 3 = KeepAlive, 4 = TLS/Syslog

Fields.VarPeerAddress
Details:
The IP address of the sending device in nnn.nnn.nnn.nnn format. If the message has been forwarded from another syslog collector, this value will contain the original senders address.

Case A.
Firewall device (192.168.1.1) ---> First syslog collector (192.168.1.2) ---> This syslog collector (192.168.1.3)
The field value would be 192.168.1.1.

Case B.
Firewall device (192.168.1.1) ---> This syslog collector (192.168.1.3)
The field value would be 192.168.1.1.

Type: String
Format: nnn.nnn.nnn.nnn Values are not zero padded.
Example: 192.168.1.67

Fields.VarPeerName
Details:
The host name of the sending device. This field will only contain resolved host name if the DNS lookup options are enabled and the lookup was successful. Otherwise it will contain the same value as VarPeerAddress in the format nnn.nnn.nnn.nnn. The name identifies the host portion of the fully qualified domain name (FQDN), it does not contain the domain suffix.
Type: String
Format: myhost

Fields.VarPeerDomain
Details:
The domain name portion of the resolved FQDN. This is just the domain suffix, it does not contain the host

©2014 SolarWinds, Inc.

name. This field will only contain a value if the DNS lookup options are enabled and the lookup was successful. Otherwise it will contain an empty string ("").
Type: String
Format: mydomain.com

Fields.VarCleanMessageText
Details:
The message text after it has been modified (header removed, DNS lookups, original address removed, Cisco date removed etc).
Type: String
Example:
%SEC-6-IPACCESSLOGP: list 101 denied udp 10.0.0.3 (firewall) (137) -> 216.7.14.105 (webserver.company.com) (137), 1 packet

Other fields

Fields.VarDate
Details: The date the message was received
Type: String (10 bytes)
Format: YYYY-MM-DD
Example: 2005-03-17

Fields.VarTime
Details: The time the message was received
Type: String (8 bytes)
Format: HH:MM:SS
Example: 23:10:04

Fields.VarMilliSeconds
Details: The time the message was received in milliseconds past the second.
Type: String (3 byte)
Range: 000 to 999
Format: nnn (three bytes, zero padded)

Fields.VarSocketPeerAddress
Details: The IP address of the device, or the closest collector that sent the message.

Case A.
Firewall device (192.168.1.1) ---> First syslog collector (192.168.1.2) ---> This syslog collector (192.168.1.3)
The field value would be 192.168.1.2.

Case B.
Firewall device (192.168.1.1) ---> This syslog collector (192.168.1.3)
The field value would be 192.168.1.3.

Type: String
Format: nnn.nnn.nnn.nnn. Values are not zero padded.
Example: 192.168.1.67

Fields.VarPeerAddressHex
Details:
The IP address of the device that sent the message converted to an 8 digit hex value.
The hex address is used for the IP Mask and IP Range filters. If you are making changes to the VarPeerIPAddress and want to use the IP Mask or Range filters, you will also need to make changes to the VarPeerAddressHex field too.
Type: String (8 bytes)
Range: 00000000 to FFFFFFFF
Example: C0A80102 (192.168.1.2 converted to 2 byte zero padded hex)

Fields.VarPeerPort
Details: The UDP/TCP port that the message was sent from.
Type: Integer (0-65535)
Range: 0 to 65535
Typically: A value greater than 1023

©2014 SolarWinds, Inc.

Fields.VarLocalAddress
Details: The IP address that the message was sent to on this machine.
Type: String
Examples: 127.0.0.1, 192.168.1.2

Fields.VarLocalPort
Details: The local machine UDP/TCP port that received the message
Type: Integer (0-65535)
Range: 0 to 65535
Typically: 514 for UDP, 1468 for TCP, 162 for SNMP

Fields.VarPriority
Details: The message priority value.
Type: Integer (0-32767)
Range: 0 to 191

Fields.VarRawMessageText
Details:
The message as it was received before modification (includes <pri> tag, original address etc).
This field is read only. Changing the field within the script will not modify the equivalent program variable.

Custom fields

These fields are dynamic and are cleared with each new message. These fields can be used to hold the results of your script so they can be used in Log to file or Log to Database actions. The fields can also be passed to actions as parameters using the %VarCustom01 **Insert message content or counter** option or via the AutoSplit syntax. A good use for these fields would be breaking a message up into separate fields via the script and then logging them to file or database in the separate fields.

There are 16 custom fields available. Values from 1 to 9 are zero padded (VarCustom01 not VarCustom1).

Fields.VarCustom01 to **Fields.VarCustom16**

Inter-script fields

These fields are static and do not change with each message. These fields can be used to pass values from one script to another or hold values for modification by the same script at a later time. The values can also be passed to actions as parameters using the %VarGlobal01 **Insert message content or counter** option or via the AutoSplit syntax.

There are 16 global fields available. Values from 1 to 9 are zero padded (VarGlobal01 not VarGlobal1).

Fields.VarGlobal01 to **Fields.VarGlobal16**

Custom Script fields

These fields are static and do not change with each message. These fields can be used to hold your own custom statistics and counters. The values can also be passed to actions as parameters using the % VarStats01 **Insert message content or counter** option.

The current field values can be viewed from the Statistics view window under the Counters tab. The custom stats are also included in the daily statistics e-mail.

The names and initial values of the Statistics fields can be set from the Scripting option

There are 16 custom statistics fields available. Values from 1 to 9 are zero padded (VarStats01 not VarStats1).

Fields.VarStats01 to **Fields.VarStats16**

Control and timing fields

Fields.ActionQuit
Details:
This field can be set to determine what occurs after the script has been run. A value of 0 means the program

©2014 SolarWinds, Inc.

continues on to the next action in the rule. A value of 1 to 99 means skip the next n actions within this rule (1=skip the next 1 action, 3=skip the next 3 actions). A value of 100 means jump to the next rule. A value of 1000 means skip all rules and stop processing this message. A value of 0 is assumed if no value is set.
Type: Integer (0-32767)
Range: 0 to 1000
Enum: 0=No skip, 1-99=skip next n actions, 100=skip to next rule, 1000=stop processing message.

Fields.SecondsSinceMidnight
Details: The number of seconds elapsed since Midnight
Type: Long (0-2 billion)
Range: 0 to 86400

Fields.SecondsSinceStartup
Details: The number of seconds elapsed since the program was started.
Type: Long (0-2 billion)

3.3.16.3 The script functions

A number of built in functions are available from the Fields object. More functions will be added to future releases to help improve the functionality of the scripting engine.

To use a built in function, simply access the function name prefixed with the Fields object. Pass any parameters needed and the result will be returned.

Built-in functions of the "Fields" object

Fields.IsValidIPAddress(IPAddress as string) as Boolean
Function: Checks the string passed to it and returns true if the string has a valid IP address format.
Input parameters: IPAddress as string
Return value: Boolean (true/false)

Example usage:
```
If Fields.IsValidIPAddress(Fields.VarPeerAddress) = True then
   Fields.VarCustom01 = Fields.VarPeerAddress
End if
```

Fields.ConvertIPtoHex(IPAddress As String) As String
Function: Converts an IP address to 8 byte hex format.
Input parameters: IPAddress as string
Return value: 8 byte hex value

Example usage:
```
If Fields.IsValidIPAddress(Fields.VarPeerAddress) = True then
   Fields.VarCustom01 = Fields.ConvertIPToHex(Fields.VarPeerAddress)
End if
```

Fields.GetDailyStatistics() As String
Function: Returns the daily statistics page as a CRLF delimited string.
Input parameters: None
Return value: String

Example usage:
```
MyStats = Fields.GetDailyStatistics()
```

The resulting string can then be written to a file or e-mailed etc.

Fields.ConvertPriorityToText(PriorityValue)
Function: Converts a message priority value to a text representation of the facility.level.

©2014 SolarWinds, Inc.

Input parameters: Priority value
Range: 0 to 191
Return value: Facility.Level as text string
Example: A value of 191 returns "Local7.Debug"
Example usage:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
' Use the date and time from the current message
With Fields
     MsgDate = .VarDate & " " & .VarTime
     MsgText = "This is a test message from the scripting action"
     Data = MsgDate & vbtab & .ConvertPriorityToText(.VarPriority) & vbtab & _
            .VarPeerAddress & vbtab & MsgText
     Call .ActionLogToFile(Filename, Data)
End with
```

Fields.ActionPlaySound(SoundFilename As String, RepeatCount as Long)
Function: Plays a beep or specified wav file. Can be repeated for x times or until cancelled.
Input parameters: SoundFilename as string, RepeatCount as long
Return value: None

Specifying a empty string ("") for SoundFilename will result in the system beep sound.

RepeatCount options:
0 = repeat until cancelled (Cancel by pressing flashing bell on main display window)
1 to 100 = repeat specified number if times, or until cancelled manually

When the repeat count is greater than 1, the wav file or beep sound will be played at 5 second intervals.

Example usage:

```
' Play the squeak sound 5 times
Call Fields.ActionPlaySound("C:\Program Files\Syslogd\Sounds\Squeak.wav", 5)

' Play the squeak sound until cancelled
Call Fields.ActionPlaySound("C:\Program Files\Syslogd\Sounds\Squeak.wav", 0)

' Play the system beep sound 10 times
Call Fields.ActionPlaySound("", 10)

' Play the system beep sound until cancelled
Call Fields.ActionPlaySound("", 0)
```

Fields.ActionSendEmail(MailTo, MailFrom, MailSubject, MailMessage , [MailImportance] , [MailPriority] , [MailSensitivity])
Function: Sends an e-mail to the addresses specified
Return value: None

Importance, Priority and Sensitivity E-mail Delivery Option parameters are optional.

E-mail Delivery Options
These parameters allow for the importance, priority and sensitivity flags of the e-mail message to be specified.

The e-mail recipients will recieve the messages with the various importance/priority/sensitivity levels set accordingly.

MailImportance: 0 - Unspecified (Default)
1 - High
2 - Normal
3 - Low

MailPriority: 0 - Unspecified (Default)
1 - Normal
2 - Urgent
3 - Non-Urgent

MailSensitivity: 0 - Unspecified (Default)
1 - Personal

©2014 SolarWinds, Inc.

2 - Private
3 - Confidential

To send the message to multiple addresses, separate each address with a comma.
E.g.:

MailTo = "user1@company.com,user2@company.com,user3@company.com"

Example usage: Send e-mail to joe@company.com, use default importance, priority and sensitivity

```
MailTo = "joe@company.com"
MailFrom = "server@company.com"
MailSubject = "This is a test of the scripting action"
MailMessage = "This is a test mail message" & vbCrLf & "Multiple lines."

Call Fields.ActionSendEmail(MailTo, MailFrom, MailSubject, MailMessage)
```

Example usage: Send e-mail to joe@company.com, High importance, Urgent priority, Confidential sensitivity

```
MailTo = "joe@company.com"
MailFrom = "server@company.com"
MailSubject = "This is a test of the scripting action"
MailMessage = "This is a test mail message" & vbCrLf & "Multiple lines."
MailImportance = 1
MailPriority = 2
MailSensitivity = 3

Call Fields.ActionSendEmail(MailTo, MailFrom, MailSubject, MailMessage, MailImportance,
MailPriority, MailSensitivity)
```

Fields.ActionLogToFile(Filename, Data, [RotateLogFile] , [RotationType] , [NumLogFiles] , [Amount] , [Unit])
Function: Opens the specified log file and appends the Data to the end of the file.
Return value: None

This function can be used to log messages to file in your own format.

AutoSplit syntax values can be used in the filename if you want.
To have the filename contain the current hour of the day, use %TimeHH

Example: Filename = "C:\Program files\Syslogd\Logs\TestLog%TimeHH.txt"

Example usage:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
MsgPriority = "Local7.Info"
MsgHostAddress = Fields.VarPeerAddress
' Use the date and time from the current message
MsgDate = Fields.VarDate & " " & Fields.VarTime
MsgText = "This is a test message from the scripting action"
Data = MsgDate & vbtab & MsgPriority & vbtab & MsgHostAddress & vbtab & MsgText

Call Fields.ActionLogToFile(Filename, Data)
```

Note: this example requires that Read permission be enabled for "Other fields". This gives the script read access to the VarDate and VarTime variables.

Log File Rotation:

For more information on Log File Rotation in Kiwi Syslog Server, please see Log File Rotation

The parameters RotateLogFile, RotationType, NumLogFiles, Amount and Unit are all optional and only need to be specified if logging to a rotated log file.

RotateLogFile: 0 = Do not rotate log file

©2014 SolarWinds, Inc.

1 = Rotate log file

RotationType: 0 = Rotate log files when **log file size** exceeds the amount specified by Amount and Unit
1 = Rotate log files when **log file age** exceeds the amount specified by Amount and Unit

NumLogFiles: The number of log files to be used in the rotation.

Amount: For RotationType=0 : Amount is a file size.
For RotationType=1 : Amount is a file age.

Unit For RotationType=0 : Unit relates to the size of the file and specifies whether the Amount is Bytes, KB, MB, etc.

0 = Bytes
1 = Kilobytes
2 = Megabytes
3 = Gigabytes

For RotationType=1: Unit relates to the age of the file and specifies whether the Amount is Minutes, Days, Weeks, etc.

0 = Minutes
1 = Hours
2 = Days
3 = Weekdays
4 = Weeks
5 = Months
6 = Quarters
7= Years

Example Usage:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
MsgPriority = "Local7.Info"
MsgHostAddress = Fields.VarPeerAddress
' Use the date and time from the current message
MsgDate = Fields.VarDate & " " & Fields.VarTime
MsgText = "This is a test message from the scripting action"
Data = MsgDate & vbtab & MsgPriority & vbtab & MsgHostAddress & vbtab & MsgText

RotateLogFile = 1       'Rotate this log
RotationType = 0  'Using File size rotation -
NumLogFiles = 4   'Use up to 4 log files
Amount = 1000           'Each log file no more than 1000
Unit = 0          'bytes in length

Call Fields.ActionLogToFile(Filename, Data, RotateLogFile, RotationType, NumLogFiles, Amount,
Unit)
```

Example Usage (2):

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
MsgPriority = "Local7.Info"
MsgHostAddress = Fields.VarPeerAddress
' Use the date and time from the current message
MsgDate = Fields.VarDate & " " & Fields.VarTime
MsgText = "This is a test message from the scripting action"
Data = MsgDate & vbtab & MsgPriority & vbtab & MsgHostAddress & vbtab & MsgText

RotateLogFile = 1       'Rotate this log
RotationType = 1  'Using File age rotation -
NumLogFiles = 12  'Use up to 12 log files
Amount = 1        'Each log file no more than 1
Unit = 5          'month old

Call Fields.ActionLogToFile(Filename, Data, RotateLogFile, RotationType, NumLogFiles, Amount,
Unit)
```

Fields.ActionSendSyslog(Hostname, Message, Port, Protocol)
Function: Sends a syslog Message to Hostname on Port via Protocol.
Return value: None

©2014 SolarWinds, Inc.

Hostname: Text string containing the hostname or IP address of the remote host.
Message: Text string containing the priority tag and syslog message text
Port: Integer between 1 and 65535 (514 is the standard syslog port)
Protocol: Integer between 0 and 1 (0=UDP, 1=TCP)

This function can be used to send syslog messages to another syslog host via the UDP or TCP protocol.

Example usage:

```
Hostname = "10.0.0.1" ' Remote syslog host
Priority = 191        ' Local7.Debug
Port = 514            ' Use the standard syslog port
Protocol = 0          ' 0=UDP, 1=TCP
' Construct the syslog message by adding <PRI> value to the front of the text
Message = "<" + Cstr(Priority) + ">" + "This is an example of a syslog message"

Call Fields.ActionSendSyslog(Hostname, Message, Port, Protocol)
```

Fields.ActionSpoofSyslog(AdapterAddress, SrcAddress, DstAddress, DstPort, Message)
Function: Sends a spoofed Syslog Message (UDP only) to DstAddress on Port DstPort.
Return value: None

AdapterAddress: Text string containing the IP or MAC address of the network adapter that the message will be sent from.
(Can be an IP Addres:- ie "192.168.0.1", or MAC address:- ie. "00:50:56:C0:00:08")
SrcAddress: Text string containing the hostname or IP address of the source of the message (actual or spoofed)
DstAddress: Text string containing the hostname or IP address of the remote (receiving) host.
DstPort: Integer between 1 and 65535 (514 is the standard syslog port)
Message: Text string containing the priority tag and syslog message text

This function can be used to send syslog messages to another syslog host via the UDP protocol.

Example usage:

```
AdapterAddress = "192.168.1.100"        ' Adapter Address (Can be IP Address- ie "192.168.0.1", or MAC address - ie. "00:50:56:C0:00:08")
SrcAddress = "192.10.10.1"              ' Source of message
DstAddress = "10.0.0.1"                 ' Destination of message
DstPort = 514                           ' Use the standard syslog port
Priority = 191                    ' Local7.Debug

' Construct the syslog message by adding <PRI> value to the front of the text
Message = "<" + Cstr(Priority) + ">" + "This is an example of a syslog message"

Call Fields.ActionSpoofSyslog(AdapterAddress, SrcAddress, DstAddress, DstPort, Message)
```

Important Note:
This option also requires that WinPcap version 4.1 and above is installed. WinPcap (Windows Packet Capture library) is available for download from: WinPcap, The Packet Capture and Network Monitoring Library for Windows

Fields.ActionLogToFileWithCache(Filename, Data, [RotateLogFile] , [RotationType] , [NumLogFiles] , [Amount] , [Unit])
Function: Writes data to the specified log file. This function uses a write cache to improve performance. The cache is flushed every 100 messages or 5 seconds, which ever comes first. The cache settings can be adjusted via registry settings. This function is exactly the same as ActionLogToFile, except that it uses a write cache. We recommend the use of the write caching function when you are receiving more than 10 messages per second.
Return value: None

This function can be used to log messages to file in your own format.

AutoSplit syntax values can be used in the filename if you want.
To have the filename contain the current hour of the day, use %TimeHH

Example: Filename = "C:\Program files\Syslogd\Logs\TestLog%TimeHH.txt"

©2014 SolarWinds, Inc.

Example usage:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
MsgPriority = "Local7.Info"
MsgHostAddress = Fields.VarPeerAddress
' Use the date and time from the current message
MsgDate = Fields.VarDate & " " & Fields.VarTime
MsgText = "This is a test message from the scripting action"
Data = MsgDate & vbtab & MsgPriority & vbtab & MsgHostAddress & vbtab & MsgText

Call Fields.ActionLogToFileWithCache(Filename, Data)
```

Note: this example requires that Read permission be enabled for "Other fields". This gives the script read access to the VarDate and VarTime variables.

Log File Rotation:

For more information on Log File Rotation in Kiwi Syslog Server, please see Log File Rotation

The parameters RotateLogFile, RotationType, NumLogFiles, Amount and Unit are all optional and only need to be specified if logging to a rotated log file.

RotateLogFile: 0 = Do not rotate log file
1 = Rotate log file

RotationType: 0 = Rotate log files when **log file size** exceeds the amount specified by Amount and Unit
1 = Rotate log files when **log file age** exceeds the amount specified by Amount and Unit

NumLogFiles: The number of log files to be used in the rotation.

Amount: For RotationType=0 : Amount is a file size.
For RotationType=1 : Amount is a file age.

Unit For RotationType=0 : Unit relates to the size of the file and specifies whether the Amount is Bytes, KB, MB, etc.

0 = Bytes
1 = Kilobytes
2 = Megabytes
3 = Gigabytes

For RotationType=1: Unit relates to the age of the file and specifies whether the Amount is Minutes, Days, Weeks, etc.

0 = Minutes
1 = Hours
2 = Days
3 = Weekdays
4 = Weeks
5 = Months
6 = Quarters
7= Years

Example Usage:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
MsgPriority = "Local7.Info"
MsgHostAddress = Fields.VarPeerAddress
' Use the date and time from the current message
MsgDate = Fields.VarDate & " " & Fields.VarTime
MsgText = "This is a test message from the scripting action"
Data = MsgDate & vbtab & MsgPriority & vbtab & MsgHostAddress & vbtab & MsgText

RotateLogFile = 1       'Rotate this log
RotationType = 0  'Using File size rotation -
NumLogFiles = 4   'Use up to 4 log files
Amount = 1000           'Each log file no more than 1000
Unit = 0          'bytes in length
```

©2014 SolarWinds, Inc.

```
Call Fields.ActionLogToFileWithCache(Filename, Data, RotateLogFile, RotationType, NumLogFiles,
Amount, Unit)
```

Example Usage (2):

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
MsgPriority = "Local7.Info"
MsgHostAddress = Fields.VarPeerAddress
' Use the date and time from the current message
MsgDate = Fields.VarDate & " " & Fields.VarTime
MsgText = "This is a test message from the scripting action"
Data = MsgDate & vbtab & MsgPriority & vbtab & MsgHostAddress & vbtab & MsgText

RotateLogFile = 1       'Rotate this log
RotationType = 1  'Using File age rotation -
NumLogFiles = 12  'Use up to 12 log files
Amount = 1        'Each log file no more than 1
Unit = 5          'month old

Call Fields.ActionLogToFileWithCache(Filename, Data, RotateLogFile, RotationType, NumLogFiles,
Amount, Unit)
```

Fields.ActionDeleteFile(Filename)
Function: Attempts to delete the specified file.
Return value: None

This function can be used to delete a log file to ensure a fresh start.

This function does not support wildcards, a specific file name must be specified. No confirmation is required, so be careful when using this function.

Example usage:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
Call Fields.ActionDeleteFile(Filename)
```

Fields.ActionDisplay(DisplayNumber, TabDelimitedMessage)
Function: Displays a message to the specified virtual display number.
Return value: None

This function can be used to display messages on the screen in your own format.

The TabDelimitedMessage must contain 5 tab delimited fields. The contents of each field can be anything you like. The normal display fields are: Date TAB Time TAB Priority TAB Hostname TAB Message.

Example usage:

```
With Fields
      MsgPriority = ConvertPriorityToText(.VarPriority)
      MsgHostAddress = .VarPeerAddress
      ' Use the date and time from the current message
      MsgDate = .VarDate & " " & .VarTime
      MsgText = "This is a test message from the scripting action"
      Display = MsgDate & vbtab & MsgTime & vbtab & MsgPriority & vbtab &_
                MsgHostAddress & vbtab & MsgText
      Call .ActionDisplay(0, Display)
End with
```

Fields.ActionLogToODBC(DSNString, TableName, InsertStatement, Timeout)
Function: Passes the InsertStatement to the database specified by DSNString and TableName. The timeout specifies how many seconds to keep the database connection open when idle.

Return value: For success, an empty string is returned. Otherwise the error is passed back as a string value.

This function can be used to log messages to a database in your own format. The connection to the database is held open internally to the program. This avoids the overhead of creating and breaking the connection each

©2014 SolarWinds, Inc.

time data is sent. If no further data is sent to the database, once the timeout period has elapsed, the connection will be closed. The next time data needs to be sent, the connection will be reopened.

Example usage:

In the case of this example, a System DSN called "KiwiSyslog" has been created and points to a MS Access database. The SQL insert statement syntax changes slightly depending on the database type being written to. The example here has only been tested on MS Access 97 and 2000.

This example assumes that a table called "Syslogd" has already been created and contains all the required fields.

```
MyDSN = "DSN=KiwiSyslog;"
MyTable = "Syslogd"
MyFields = "MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText"

' MS Access DB SQL INSERT command example:
' INSERT INTO Syslogd (MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText)
' VALUES ('2004-08-08','13:26:26','Local7.Debug','host.company.com',
' 'This is a test message from Kiwi Syslog Server')

With Fields
     ' Construct the insert statement
     SQLcmd = "INSERT INTO " & MyTable & " (" & MyFields & ") VALUES (" & _
     Quote(.VarDate) & "," & Quote(.VarTime) & "," & _
     Quote(.ConvertPriorityToText(.VarPriority)) & "," & _
     Quote(.VarPeerAddress) & "," & Quote(.VarCleanMessageText) & ")"
     ' Log the data to database using DSN, Table, SQLcmd and Timeout of 30 seconds
     .VarCustom01 = .ActionLogToODBC(MyDSN, MyTable, SQLcmd, 30)
     ' VarCustom01 now holds the return value from the function.
End with

Function Quote(Data)
    ' Replace all occurrences of ' with '' to escape existing quotes
    ' Wrap data with single quotes
    Quote = "'" & Replace(Data, "'", "''") & "'"
End Function
```

Note: This example requires that Read permission is enabled for "Other fields". This gives the script read access to the .VarDate and .VarTime variables.

Note: There are more example scripts installed in the \Scripts sub folder.

3.3.16.4 The scripting dictionaries

New to version 8.1 of Kiwi Syslog Server, the Dictionaries collection allows for the creation of (named) dictionaries that store data key and item pairs. The data stored in these dictionaries is persistant, in that it exists for the lifetime of the application. Dictionaries have essentially the same scope as the VarGlobal variables in the Fields namespace.

A named **Dictionary** is the equivalent of a PERL associative array. Items, which can be any form of data, are stored in the array. Each item is associated with a unique key. The key is used to retrieve an individual item and is usually a integer or a string, but can be anything except an array.

All dictionary methods and properties are accessible through the "dictionaries" namespace.

Built in functions of the "Dictionaries" object

StoreItem(**dicName** As String, **dicKey** As String, **dicItem** As Variant)

The **StoreItem** method stores a key, item pair to a named dictionary.

dicName Required. The name of the dictionary. If **dicName** does not exist, it will be created.
dicKey Required. The key associated with the item being stored. If **dicKey** does not exist, it will be created.
dicItem Required. The item associated with the key being stored.

©2014 SolarWinds, Inc.

```
eg.   Call Dictionaries.StoreItem("MyDictionary", "MyKeyName", "MyItemValue")
```

The .AddItem() and .UpdateItem() methods have been supplanted as of version 8.1.4 of Kiwi Syslog Server, by the .StoreItem() method. However, to ensure backwards compatibility the usage of .AddItem() and .UpdateItem() will continue to be supported.

AddItem(**dicName** As String, **dicKey** As String, **dicItem** As Variant)

The **AddItem** method adds a key, item pair to a named dictionary. An error will occur if the key **dicKey** already exists in the dictionary **dicName**.

dicName Required. The name of the dictionary. If **dicName** does not exist, it will be created.
dicKey Required. The key associated with the item being added.
dicItem Required. The item associated with the key being added.

```
eg.   Call Dictionaries.AddItem("MyDictionary", "MyKeyName", "MyItemValue")
```

UpdateItem(**dicName** As String, **dicKey** As String, **dicItem** As Variant)

The **UpdateItem** method updates the item associated with key **dicKey** to the value in **dicItem**. Only the dictionary **dicName** is affected. An error will occur if dictionary **dicName** does not exist, or if key **dicKey** does not exist.

dicName Required. The name of the dictionary.
dicKey Required. The key associated with the item being updated.
dicItem Required. The new item to be updated.

```
eg.   Call Dictionaries.UpdateItem("MyDictionary", "MyKeyName", "MyNewItemValue")
```

RemoveItem(**dicName** As String, **dicKey** As String)

The **RemoveItem** method removes a key, item pair from the dictionary **dicName**. An error will occur if dictionary **dicName** does not exist, or if key **dicKey** does not exist.

dicName Required. The name of the dictionary.
dicKey Required. The key associated with the item being removed.

```
eg.   Call Dictionaries.RemoveItem("MyDictionary", "MyKeyName")
```

RemoveAll(**dicName** As String)

The **RemoveAll** method removes all key, item pairs from the dictionary **dicName**. An error will occur if dictionary **dicName** does not exist.

dicName Required. The name of the dictionary.

```
eg.   Call Dictionaries.RemoveAll("MyDictionary")
```

Delete(**dicName** As String)

The **Delete** method deletes the entire dictionary **dicName**. An error will occur if dictionary **dicName** does not exist.

dicName Required. The name of the dictionary being deleted.

```
eg.   Call Dictionaries.RemoveItem("MyDictionary", "MyKeyName")
```

©2014 SolarWinds, Inc.

DeleteAll()

The **DeleteAll** method deletes all dictionaries.

```
eg.   Call Dictionaries.DeleteAll()
```

GetItemCount(**dicName** As String) As Long

The **GetItemCount** property returns the number of items in the dictionary **dicName**. An error will occur if dictionary **dicName** does not exist.

dicName Required. The name of the dictionary.

```
eg.   ItemCount = Dictionaries.GetItemCount("MyDictionary")
```

GetItem(**dicName** As String, **dicKey** As String) As Variant

The **GetItem** property returns an item for a specified key **dicKey** in dictionary **dicName**. An error will occur if dictionary **dicName** does not exist, or if key **dicKey** does not exist.

dicName Required. The name of the dictionary.
dicKey Required. The key associated with the item being fetched.

```
eg.   MyItem = Dictionaries.GetItem("MyDictionary", "MyKeyName")
```

ItemExists(**dicName** As String, **dicKey** As String) As Boolean

The **ItemExists** property returns **True** if the specified key **dicKey** exists in the dictionary **dicName**. An error will occur if dictionary **dicName** does not exist.

dicName Required. The name of the dictionary.
dicKey Required. The key associated with the item being fetched.

```
eg.   If Dictionaries.ItemExists("MyDictionary", "MyKeyName") Then
            ...
      End If
```

GetKeys(**dicName** As String) As Variant

The **GetKeys** property returns an **array** containing all the keys in the dictionary **dicName.** An error will occur if dictionary **dicName** does not exist.

dicName Required. The name of the dictionary.

```
eg.   MyKeyArray = Dictionaries.GetKeys("MyDictionary")
      For i = 0 to UBound(MyKeyArray)
            ThisKey = MyKeyArray(i)
            ...
      Next
```

GetItems(**dicName** As String) As Variant

The **GetItems** property returns an **array** containing all the items in the dictionary **dicName.** An error will occur if dictionary **dicName** does not exist.

dicName Required. The name of the dictionary.

```
eg.   MyItemArray = Dictionaries.GetItems("MyDictionary")
      For i = 0 to UBound(MyItemArray)
```

©2014 SolarWinds, Inc.

```
        ThisItem = MyItemArray(i)
        ...
    Next
```

Error Reference:

Function Name	Error Description
GetName()	Script Error executing .GetName() - Dictionary does not exist
Delete()	Script Error executing .Delete() - Dictionary [x] does not exist
AddItem()	Script Error executing .AddItem() - Dictionary Key [x] already exists in dictionary [y]
UpdateItem()	Script Error executing .UpdateItem() - Dictionary Key [x] does not exist in dictionary [y]
	Script Error executing .UpdateItem() - Dictionary [x] does not exist
RemoveItem()	Script Error executing .RemoveItem() - Dictionary Key [x] does not exist in dictionary [y]
	Script Error executing .RemoveItem() - Dictionary [x] does not exist
RemoveAllItems()	Script Error executing .RemoveAllItems() - Dictionary [x] does not exist
GetItemCount()	Script Error executing .GetItemCount() - Dictionary [x] does not exist
GetItems()	Script Error executing .GetItems() - Dictionary [x] does not exist
GetKeys()	Script Error executing .GetKeys() - Dictionary [x] does not exist
GetItem()	Script Error executing .GetItem() - Dictionary Key [x] does not exist in dictionary [y]
	Script Error executing .GetItem() - Dictionary [x] does not exist
ItemExists()	Script Error executing .ItemExists() - Dictionary [x] does not exist

3.3.16.5 Script examples

The scripts included in this help file will help you get started. More scripts and tutorials are being added to the Kiwi Syslog Server web site at www.kiwisyslog.com.

The program also includes a selection of sample scripts that show you how to play sounds, send e-mail and log to file etc. These scripts can be found in the \Scripts sub folder off the install folder.

If you have created a custom parsing script or something that would be useful to others, please send a copy of the script to http://www.kiwisyslog.com/support/ and we will add it to the web site for others to download.

3.3.16.5.1 PIX message lookup

The function below checks the message for specific PIX message numbers and passes the explanation to a custom message field. The custom fields can then be used in a "Send e-mail" action.

The values used in this script are found on the Cisco web site at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/syslog/pixemsgs.htm

Run Script action setup.
Common fields: Read=yes
Custom fields: Write=yes

Rules setup

```
Rules
  Rule: Lookup PIX msg
    Filters
      Filter: Host IP address: Simple: Match PIX firewall address
    Actions
      Action: Run Script: Lookup PIX msg
      Action: Send e-mail
              To: helpdesk@company.com:
              Subject: Problem with PIX
```

©2014 SolarWinds, Inc.

```
            Body: %MsgText
                Explanation: %VarCustom01
                Action to take: %VarCustom02


Function Main()

' Set the return value to OK
Main = "OK"

' By default, skip to the next rule, don't take the actions that follow
' If we exit the function before we get to the end, the default 'skip to next rule'
' will be used.
Fields.ActionQuit = 100

' Example of a PIX message
' %PIX-4-209004: Invalid IP fragment...

Dim M ' Message
Dim E ' Explanation
Dim A ' Action

' Copy message to local variable for speed
M = Fields.VarCleanMessageText

' If message length is too short, exit function
If Len(M) < 15 then exit function

' Grab the first 15 chrs
M = Left(M,15)

' Check the message is a valid PIX message
If Mid(M,1,5) <> "%PIX-" then exit function

' Add any additional checks you want to perform here

' Grab the important part ("4-209004")
M = Mid(M,6,8)

E = ""
A = ""

' Now lookup the values and create an explanation and action for each match
Select Case M
  Case "4-209004"
       E = "An IP fragment is malformed. The total size of the reassembled IP packet exceeds
the maximum possible size of 65,535 bytes"
      A = "A possible intrusion event may be in progress. If this message persists, contact
the remote peer's administrator or upstream provider."
  Case "2-106012"
      E = "This is a connection-related message. A IP packet was seen with IP options.
Because IP options are considered a security risk, the packet was discarded."
      A = "A security breach was probably attempted. Check the local site for loose source or
strict source routing."

' Insert other values to lookup here

End Select

' Exit if we don't have any values to pass
If len(E) = 0 then exit function
If len(A) = 0 then exit function

' Pass the Explanation and Action to take to the custom variables
Fields.VarCustom01 = E
Fields.VarCustom02 = A

' Since we have a valid match, we want to execute the send e-mail action which follows.
' Setting ActionQuit to 0 means we won't skip any actions.
Fields.ActionQuit = 0

End function
```

©2014 SolarWinds, Inc.

3.3.16.5.2 All the variables - (Info function)

The function below shows all the available field variables. This function can be pasted into your script as a reference.

Note: All the variables are remarks and will not be executed if the function is called.

```
Function Info()

' // Common fields
' VarFacility
' VarLevel
' VarInputSource
' VarPeerAddress
' VarPeerName
' VarPeerDomain
' VarCleanMessageText

' // Other fields
' VarDate
' VarTime
' VarMilliSeconds
' VarSocketPeerAddress
' VarPeerAddressHex
' VarPeerPort
' VarLocalAddress
' VarLocalPort
' VarPriority
' VarRawMessageText (Read only)

' // Custom fields
' VarCustom01 to VarCustom16

' // Inter-Script fields
' VarGlobal01 to VarGlobal16

' // Custom Stats fields
' VarStats01 to VarStats16

' // Control and timing fields
' ActionQuit
'   0=No skip, 1-99=skip next n actions within rule,
'   100=skip to next rule, 1000=stop processing message
'
' SecondsSinceMidnight
' SecondsSinceStartup

' // Functions and Actions
' IsValidIPAddress(IPAddress as string) as boolean
' ConvertIPtoHex(IPAddress as string) as string

' ActionPlaySound(SoundFilename as string, RepeatCount as long)
'   RepeatCount 0=until cancelled, 1-100=repeat x times
'   Soundfilename ""=system beep, "wav file name"=play wav file

' ActionSendEmail(MailTo as String, MailFrom as string, MailSubject as string, MailMessage as
string)
'   Sends an e-mail message to the addresses specified in MailTo


End function
```

3.3.16.5.3 JScript escape characters

JScript provides escape sequences that you can include in strings to create characters that you cannot type directly. Each of these sequences begins with a backslash. The backslash is an escape character that informs the JScript interpreter that the next character is special.

Escape sequence	Meaning

©2014 SolarWinds, Inc.

\b	Backspace
\f	Form feed (rarely used)
\n	Line feed (newline)
\r	Carriage return. Use with the line feed (\r\n) to format output.
\t	Horizontal tab
\v	Vertical tab (rarely used)
\'	Single quote (')
\"	Double quote (")
\\	Backslash (\)
\n	ASCII character represented by the octal number n. *
\xhh	ASCII character represented by the two-digit hexadecimal number hh.
\uhhhh	Unicode character represented by the four-digit hexadecimal number hhhh.

* The value of n must be in the range 0 to 377 (octal).

Any escape sequence not included in this table simply codes for the character that follows the backslash in the escape sequence. For example, "\a" is interpreted as "a".

Since the backslash itself represents the start of an escape sequence, you cannot directly type one in your script.

If you want to include a backslash, you must type two sequential characters (\\).

For example. 'The log file path is C:\\Program Files\\Syslogd\\Logs\\SyslogCatchAll.txt'

The single quote and double quote escape sequences can be used to include quotes in string literals.

For example. 'The caption reads, \"This is a test message from \'Kiwi SyslogGen\'.\"'

3.3.17 Action - Log to Syslog Web Access

This action will log syslog events to Kiwi Syslog Web Access, if installed.

3.3.18 Action - Reset Flags/Counters

This action will reset all the internal counters used by the Threshold, Timeout and Time Interval filters configured under Rules.

3.4 Setup - Schedules

To enable log archiving, click the **Schedules** option and then right click to add a new schedule. Alternatively, click the **Schedules** option and then the [**New**] button in the toolbar.

There can be up to 100 custom schedules in the list. Each one is actioned sequentially. If two schedules are set for the same time, the top most schedule is actioned first and the next in the list and so on.

You can enable or disable a schedule at any time by using the check box to the left of the schedule name.

The name used for each custom schedule is up to you. They don't have to be unique, but should describe what the schedule does or when it occurs.

3.4.1 How the scheduler works

The Kiwi Syslog Server integrated scheduler allows you to run various tasks; at a specified time or interval, or when Kiwi Syslog Server starts-up or shuts-down.
It is a fully functional scheduling tool, with the ability to run task specific to Kiwi Syslog Server (eg. Log

©2014 SolarWinds, Inc.

Archiving, Log Clean-ups or Running a Kiwi Syslog Script action), as well as the ability to run any other Windows process or program.

The schedule frequencies available range from a one-off process, through to yearly (annual) tasks and every discernable interval in between, including minute-to-minute, daily, weekly, monthly, etc. Schedule exceptions can also be added to exclude certain dates, such as public holidays, scheduled network outage times, etc. **Figure 3;** shows a sample Scheduled Archive task.

There are four task types that can be run:

- Archive
- Clean-up
- Run Program
- Run Script

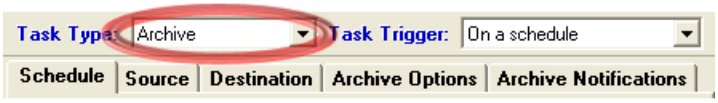


Figure 1 *- Shows the Schedule Task Type, selectable from the drop-down at the top of the schedule options screen.*

And (depending on each task-type) these may be triggered:

- On a schedule
- At application/service start up
- At application/service shutdown



Figure 2 *- Shows the Scheduled Task Trigger, selectable from the drop-down at the top of the schedule options screen.*

©2014 SolarWinds, Inc.

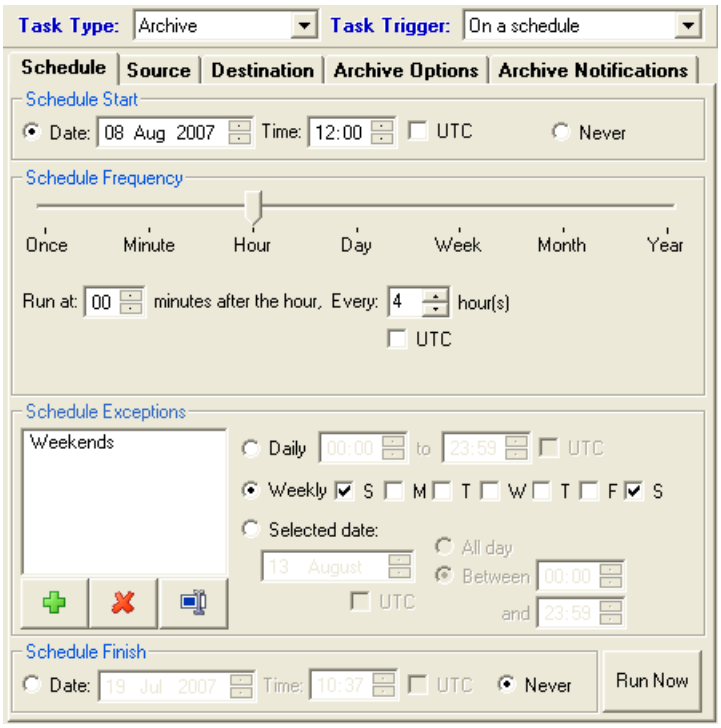
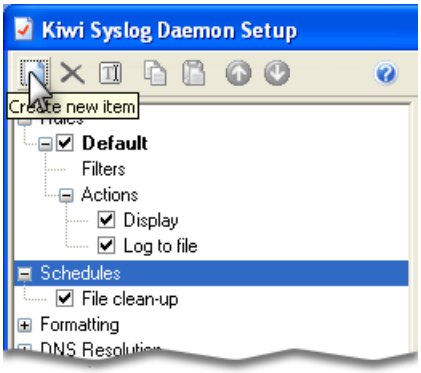


Figure 3 *- Scheduled Archive Task, runs 4 hourly; except on weekends.*

Add a Schedule:

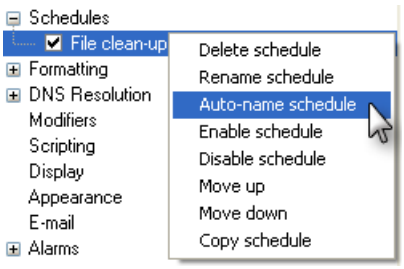
To create a new schedule, select the "Schedules" node in the Kiwi Syslog Server Setup properties tree, and click the "Create new item" button in the toolbar.



Other Schedule selection options:

When a schedule is selected, there are various options that are available through the schedules context menu (or through the toolbar at the top-right of the Setup window).

©2014 SolarWinds, Inc.



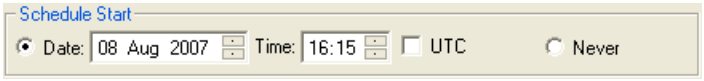
To access the schedules context menu, right-click on a selected schedule.

3.4.2 On a schedule

When creating a new schedule, the following options are available to be set:

- The schedule start date and time
- The schedule frequency
- The schedule finish date and time
- The schedule exceptions (if any)

Schedule Start:



This is the date and time that the scheduled task will be active from. It is entirely acceptable to set this date to a future date, but as a consequence; the schedule remains inactive until the set date has passed. Similarly, setting the schedule to "Never" start; means that the scheduled task remains inactive (and is effectively disabled). As with any of the schedule options, dates and times can be specified as UTC (Coordinated Universal Time).

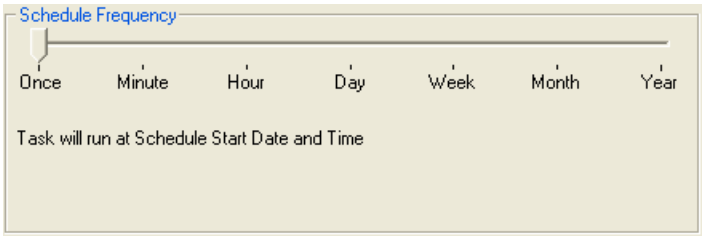
Schedule Frequency:

There are seven distinct schedule frequencies:

- Once
- Minute
- Hour
- Day
- Week
- Month
- Year

Each schedule frequency has it's own set of options, each of which can be summarized as follows:

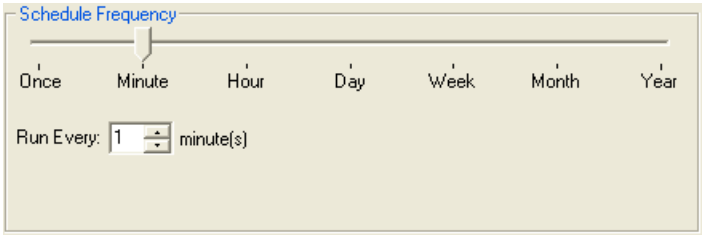
Schedule Frequency - Once:



The task will be run once and only once, at the date and time set in the "Schedule Start" options.

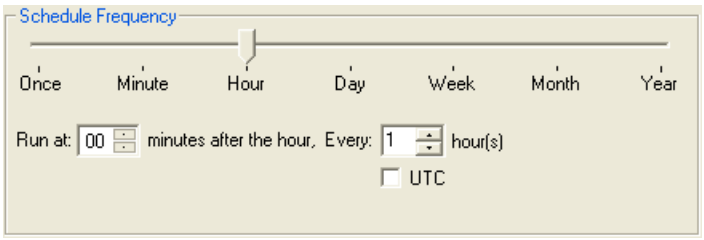
©2014 SolarWinds, Inc.

Schedule Frequency - Minute:



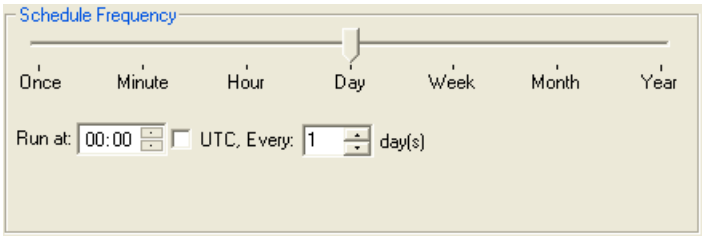
The task will be run every N minutes.
In the figure above, the task has been set to run every single minute.
(eg. 00:00, 00:01, 00:02, 00:03, ... , 23:59)

Schedule Frequency - Hour:



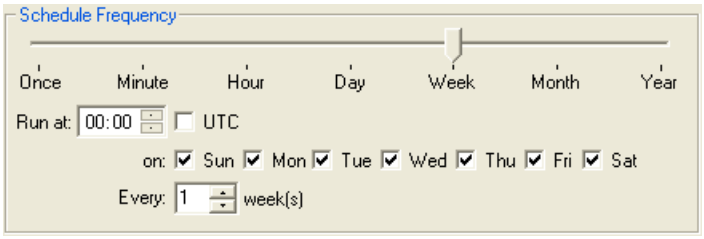
The task will be run every X hours, at N minutes past the hour.
In the figure above, the task has been set to run every single hour, at zero minutes past the hour.
(eg. 00:00, 01:00, 02:00, 03:00, ... , 23:00)
As with any of the schedule options, dates and times can be specified as UTC (Coordinated Universal Time).

Schedule Frequency - Day



The task will be run every X days, at exactly HH:MM.
In the figure above, the task has been set to run every single day, at exactly midnight.
(eg. 2007-08-30 00:00, 2007-08-31 00:00, 2007-09-01 00:00, ...)
As with any of the schedule options, dates and times can be specified as UTC (Coordinated Universal Time).

Schedule Frequency - Week:

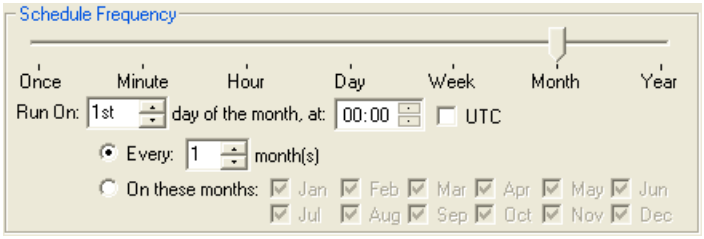


The task will be run every X weeks, on the specified days of the week, at exactly HH:MM.
In the figure above, the task has been set to run every single week, on every day of the week, at exactly midnight.
(eg. Sunday at 00:00, Monday at 00:00, Tuesday at 00:00, ...)

©2014 SolarWinds, Inc.

As with any of the schedule options, dates and times can be specified as UTC (Coordinated Universal Time).

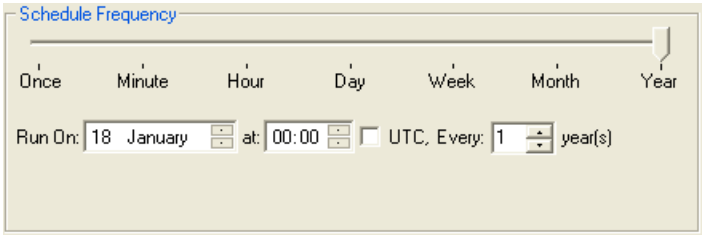
Schedule Frequency - Month



The task will be run on the Nth day of the month at exactly HH:MM, either:
- every N months, or
- on the specified months only.

In the figure above, the task has been set to run on the 1st day of every single month, at exactly midnight.
(eg. 1st January at 00:00, 1st February at 00:00, 1st March at 00:00, ... , 1st December at 00:00)
As with any of the schedule options, dates and times can be specified as UTC (Coordinated Universal Time).

Schedule Frequency - Year:



The task will be run on the Nth of month X, at exactly HH:MM, every N years.
In the figure above, the task has been set to run on the 18th of January at exactly midnight, every single year.
(eg. 18th January 2008 at 00:00, 18th January 2009 at 00:00, 18th January 2010 at 00:00, ...)

Schedule Finish:

Scheduled tasks only run they are when active. Whether or not a schedule is active, is determined by the start and finish dates.
In the case of the Schedule Finish date and time, the scheduled task will be run up until the schedule finish date.
If set to "Never", then the schedule will be active indefinately.

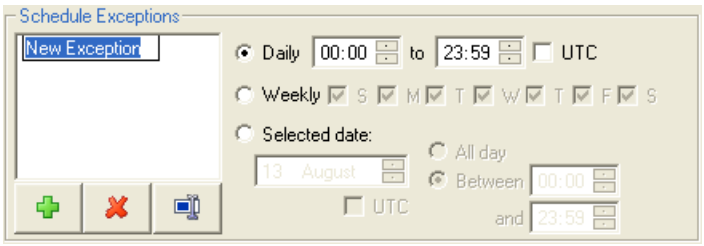
Schedule Exceptions:

There are three types of schedule exceptions:

Daily exceptions:
These occur every day, between two specifc times of day.
As with any of the schedule options, dates and times can be specified as UTC (Coordinated Universal Time).
eg. The following figure shows a New Daily Exception, that occurs every day between 00:00 and 23:59 (ie. all day)

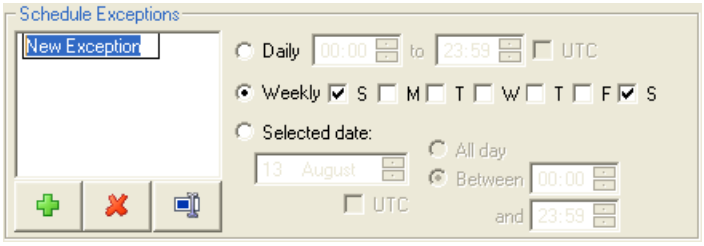
*The scheduled task will **not** run between these times of day.*

©2014 SolarWinds, Inc.



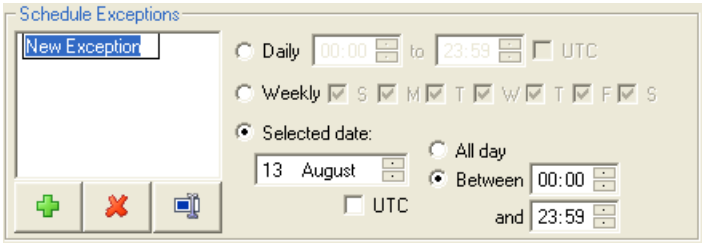
Weekly exceptions:
These occur on one or more days of the week
eg. The following figure shows a New Weekly Exception, that occurs on Saturday and Sunday every week.

*The scheduled task will **not** run on these days.*



Selected Date exceptions:
These occur on a specific day, either all day, or between two specific times of day.
As with any of the schedule options, dates and times can be specified as UTC (Coordinated Universal Time).
eg. The following figure shows a New Selected Date Exception, that occurs on the 13th August, between 00:00 and 23:59.

*The scheduled task will **not** run on the 13th of August between these times of day.*



3.4.3 On application/service startup

The selected task-type will run as soon as Kiwi Syslog Server has started.

Task types that are supported by this trigger are:
- Archive
- Clean-up
- Run-Program
- Run-Script

©2014 SolarWinds, Inc.

3.4.4 On application/service shutdown

The selected task-type will run as part of Kiwi Syslog Server's shut-down process.

Task types that are supported by this trigger are:
- Run-Script

3.4.5 Archive task

The Archive task replaces and extends the old Kiwi Syslog Server Archive functionality (in versions prior to 8.3.0). It allows you to copy or move logs from one location to another, compress the files into individual or single archives, encrypt those archive(s), create multi-part archive(s), create file or archive hashes, run external programs, and much more. Following the completion of an archive task, notification can be sent via e-mail, or a web-based report created on disk.

Any archive task can be scheduled to occur over any interval or at any date and time desired, or at application/service start-up.
Whether an archive task is scheduled or not, it consists of the following four parts:

- Source
- Destination
- Archive Options
- Archive Notification

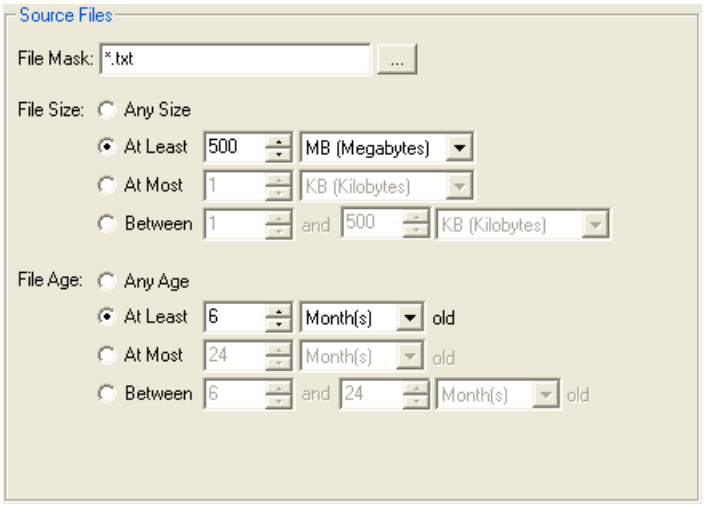
Source:

Source Location:



The Source Location specifies the root folder from which files will be moved or copied. If the "Include subdirectories" option is checked, then all subfolders in the root folder will be included in the file processing. If unchecked, only files that exist in the source location will be processed.

Source Files:



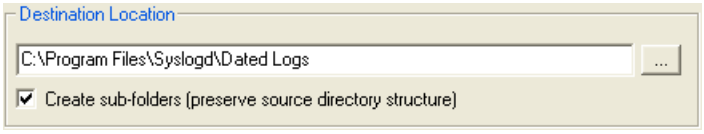
The Source Files section defines which files will be included in the task processing.
Files that match the specified file mask, file size, and file age criteria are included in processing, those that

©2014 SolarWinds, Inc.

do not match the criteria are excluded.
eg. In the figure above, *.txt files that are at least 500 MB AND at least 6 months old are processed.

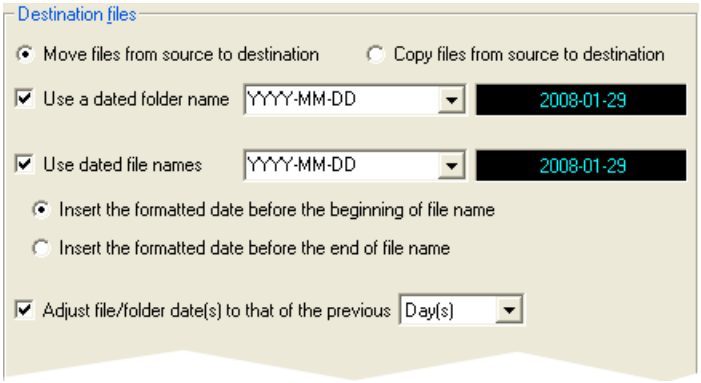
Destination:

Destination Location:



The Destination Location specifies where files matching the source file criteria will be copied or moved to.
If the "Build subfolders" option is checked, then directory structure that exists in the source location will be preserved.
If the "Build subfolders" option is not checked, then the file paths will be "flattened" and any directory structure that exists at the source will be lost.

Destination Files:



The Destination Files section determines how files will be transferred from source to destination.

Move/Copy files from source to destination:

Selecting "Copy Files from Source to Destination" leaves existing files intact at the source. Selecting "Move Files from Source to Destination" means that files are deleted from the source location once they have been copied.

When copying or moving files from the source to the destination, an optional date-time stamp can be added.

Use a dated file name:

The "Use dated file names" option adds a date-time stamp (in the specified format) to each file as it is moved or copied. The formatted date-time stamp will be inserted into the destination file name at the location specified, either:

- Before the beginning of the filename, ie. DATETIMESTAMP-filename.log, or
- Before the end of the filename, ie. filename-DATETIMESTAMP.log

Use a dated folder names:

The "Use a dated folder name" option adds a date-time stamped root folder at the destination, into which all matching files will be moved/copied.

Adjust file/folder date(s) to that of the previous ... :

With either date-time stamp option, the target date used can be adjusted to the previous day, week, month, or year.

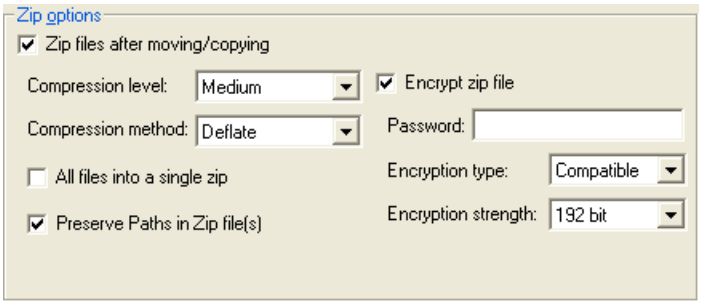
©2014 SolarWinds, Inc.

This setting is particularly useful when running a scheduled archive at the beginning of a new period, whilst having the archived logs reflect the fact that they contain information from the *previous* period.

eg. Consider a scheduled archive task, set to occur every day at midnight: This setting will adjust the current date, so that the target file is named to reflect; that the *contents* of the archived logs contain data from the *previous* day.

Archive Options:

Zip Options:



Zip files after moving/copying:

If selected, a zip file containing the destination files will be created.

Compression Level:

None
No compression. Files are stored in the zip file as raw data.

Low
Minimum compression. This setting takes the least amount of time to compress data. For the Deflate compression method, when compared to the Medium setting, this setting usually gives noticeably faster compression times in exchange for about 1% to 15% larger compressed files.

Medium
Normal compression. This is the best balance between the time it takes to compress data and the compression ratio achieved (this statement applies to both to the Deflate and the Burrows Wheeler (BWT) compression methods).

High
Maximum compression. This setting achieves the best compression ratios that the compression algorithm is capable of producing. For the Deflate compression method, when compared to the Medium setting, this setting significantly increases compression time for only slightly smaller compressed files. We recommend that you use this setting only when you really need to achieve the smallest possible files and when compression time is totally unimportant.

Compression Method:

Stored
No compression or decompression should be applied at all.

Deflate
Use the Deflate compression method. This algorithm provides fast compression and decompression speeds and achieves pretty good compression.

Deflate 64
Use the Deflate64™ compression method. This method takes longer to compress data than Deflate, however it provides better compression.

©2014 SolarWinds, Inc.

BurrowsWheeler
Use the BWT compression method. This algorithm often provides superior compression on many popular file types such as database, picture, text and executable files. It takes longer to compress or uncompress data with this algorithm vs. the standard Deflate algorithm.

All files into a single Zip:

If selected, this option ensures that all files in the destination location will be achived into a single zip file. If not selected, a zip file will be created for each file in the destination location.

Encrypt Zip file:

If selected, zip file encryption will be applied to each and every zip file created, with the password, encryption type, and encryption strength specified.

Encryption password:

The Encryption Password property contains the case-sensitive password to be used for encrypting or decrypting files.
The password specified in the applies to all the files being zipped.
If the Encryption Password property is empty, ie. if no password is provided, then any newly zipped files will not be encrypted.
Passwords can be up to 79 characters long.

Encryption Type:

Compatible
Traditional zip encryption (weak)

WinZip AES
WinZip 9.0's AES encryption (strong)

Encryption Strength:

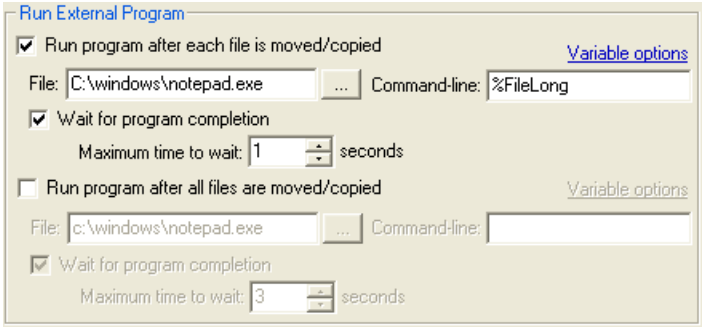
The Encryption Strength property allows you to specify the strength of the encryption (in bits). Does not apply to the "Compatible" encryption type.

Preserve Paths in Zip file(s):

The Preserve Paths property allows you to specify whether or not the created zip file(s) include path information from the destination files.

Archive Options:

Run External Program:



Run program after each file is moved/copied:

The selected Windows program will be executed **after each file** has been moved or copied from the source location to the destination.

©2014 SolarWinds, Inc.

The command-line parameters specified will be passed to the selected executable.

Wait for program completion:

The time to wait for program completion. Programs or processes that are still running after this period of time has elapsed; will be terminated.

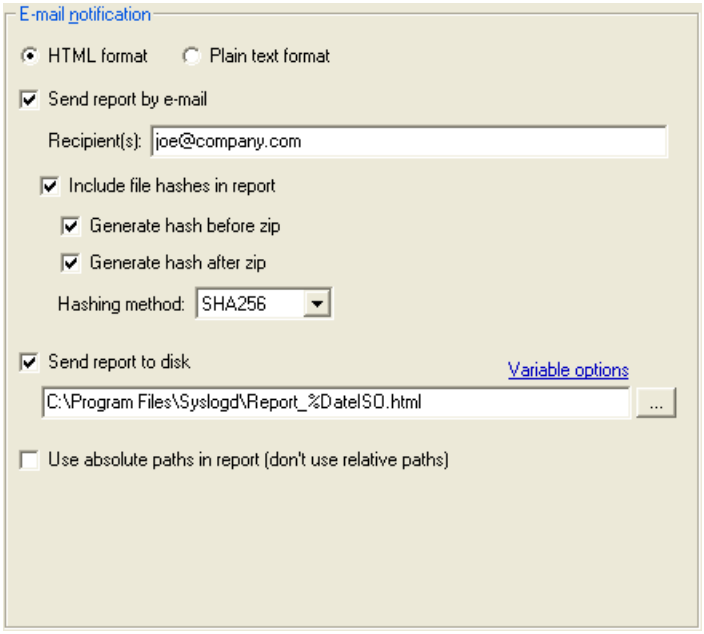
Run program after all files are moved/copied:

The selected Windows program will be executed **after all files** have been moved or copied from the source location to the destination.
The command-line parameters specified will be passed to the selected executable.

Wait for program completion:

The time to wait for program completion. Programs or processes that are still running after this period of time has elapsed; will be terminated.

Archive Notification:



E-mail format:

The archive report can be generated and sent in either HTML or plain-text format.

Send Report by e-mail:

If selected, an e-mail containing the archive report will be sent to the e-mail address specified in the "Recipient(s)" field.

Recipient(s):

Comma or semi-colon delimited list of e-mail addresses, which are to receive copies of the archive report.

Include file hashes in report:

If selected, a file hash value will be generated for each file processed.

Generate Hash before zip:

©2014 SolarWinds, Inc.

A hash value will be generated from the source file, before it is zipped. Hash values will be included in the report that is generated.

Generate Hash after zip:

A hash value will be generated from any zip files that are created as part of the archiving process. Hash values will be included in the report that is generated.

Hashing Method:

Specifies the type of Hash that will be generated from the file.

MD5
MD5 (Message Digest Algorithm 5) is a secure hash algorithm developed by R. Rivest in 1991 at RSA Data Security, Inc. The algorithm takes a message of arbitrary length and produces a 128-bit message digest. MD5 is a popular hash algorithm and it is considered reasonable secure. However, some people have reported potential weaknesses in it. It is also reported that it is possible to build a special-purpose machine to find a plaintext matching given hash-value in a few weeks.

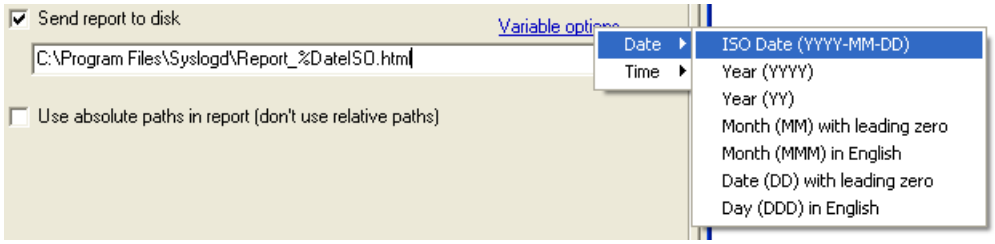
SHA1
The SHA-1 (Secure Hash Algorithm 1) was proposed by the U.S. National Institute for Standards and Technology (NIST) for certain U.S. federal government applications. The algorithm takes a message of arbitrary length and produces a 160-bit message digest. Compared to 128-bit hash functions, the 160-bit hash-value of SHA-1 provides increased security against brute-force attacks. SHA-1 is considered stronger than MD5.

SHA256
SHA256 (or SHA-2 as it is known, Secure Hash Algorithm 2 (256)) was proposed by the U.S. National Institute for Standards and Technology (NIST) for certain U.S. federal government applications. The algorithm takes a message of arbitrary length and produces a 256-bit message digest. The SHA-2(256) algorithm was designed to produce outputs that provide security comparable to that projected for the Advanced Encryption Standard (AES).

Send Report to disk:

If selected, an file containing the archive report will be sent to disk using the file name and path specified.

Variable options:



Selected variables will be inserted into the file path. This aides in creating dated or date-time stamped report files, to avoid overwriting the same report file each time an archive task is run.

Use absolute paths in report (don't use relative paths):

If selected, the report that is generated (either to disk or e-mail) will show full file paths instead of relative paths, which are the default.

3.4.6 Clean-up task

The Clean-up task removes (deletes) files from a the source location, that match the criteria specified.

Any Clean-up task can be scheduled to occur over any interval or at any date and time desired, or at

©2014 SolarWinds, Inc.

application/service start-up.
Whether an Clean-up task is scheduled or not, it consists of the following three parts:

- Source
- Clean-up Options
- Clean-up Notification

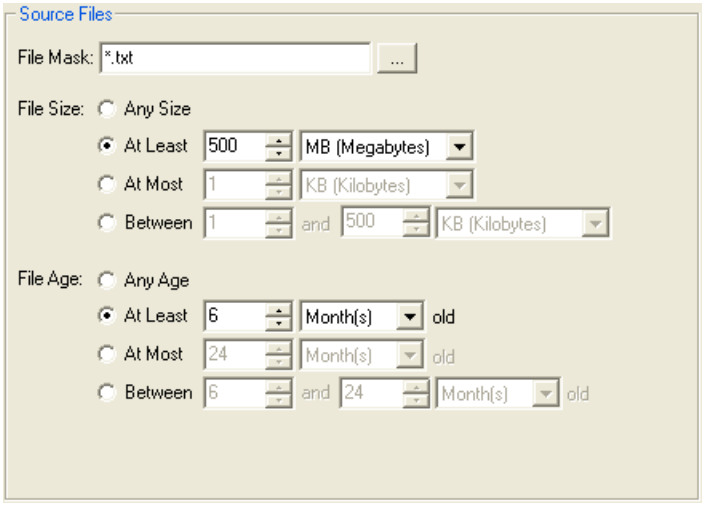
Source:

Source Location:



The Source Location specifies the root folder from which files will be cleaned-up. If the "Include subdirectories" option is checked, then all subfolders in the root folder will be included in the file processing. If unchecked, only files that exist in the source location will be processed.

Source Files:



The Source Files section defines which files will be included in the task processing.
Files that match the specified file mask, file size, and file age criteria are included in processing, those that do not match the criteria are excluded.
eg. In the figure above, *.txt files that are at least 500 MB AND at least 6 months old are processed.

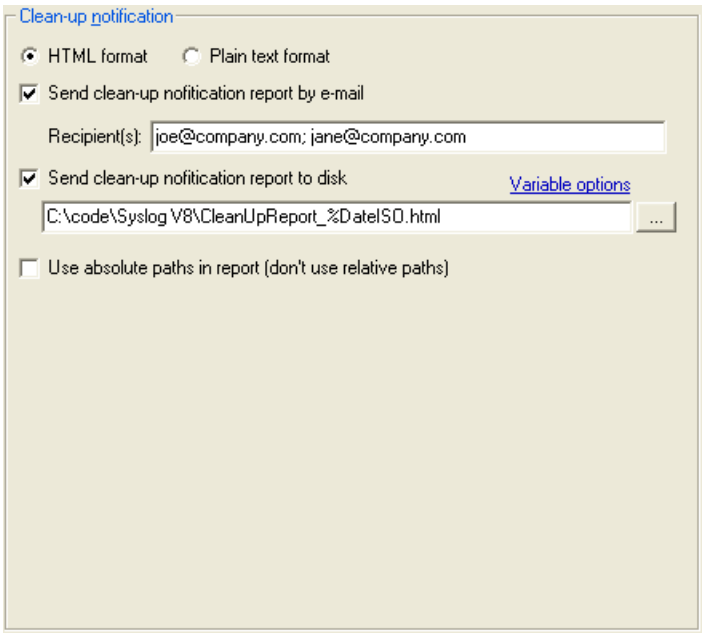
Clean-up Options:

Remove empty folders:

If selected, empty folders from the source location will be deleted as well.

Clean-up Notification:

©2014 SolarWinds, Inc.



E-mail format:

The clean-up report can be generated and sent in either HTML or plain-text format.

Send Clean-up Notification Report by e-mail:

If selected, an e-mail containing the clean-up report will be sent to the e-mail address specified in the "Recipient(s)" field.

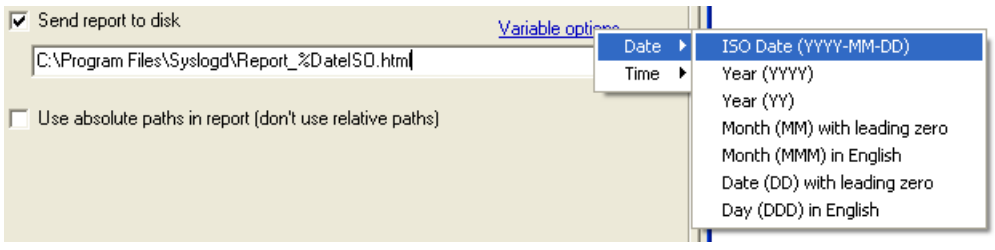
Recipient(s):

Comma or semi-colon delimited list of e-mail addresses, which are to receive copies of the clean-up report.

Send Clean-up Notification Report to disk:

If selected, an file containing the clean-up report will be sent to disk using the file name and path specified.

Variable options:



Selected variables will be inserted into the file path. This aides in creating dated or date-time stamped report files, to avoid overwriting the same report file each time a clean-up task is run.

Use absolute paths in report (don't use relative paths):

If selected, the report that is generated (either to disk or e-mail) will show full file paths instead of relative paths, which are the default.

©2014 SolarWinds, Inc.

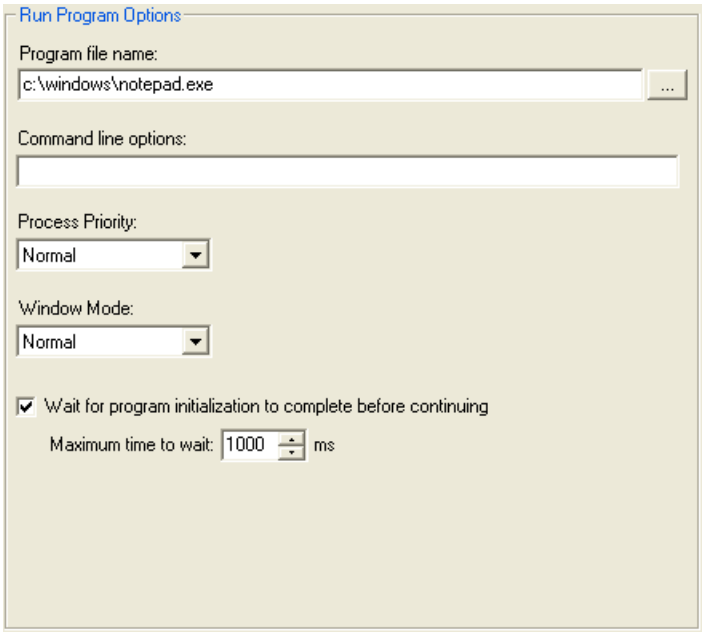
3.4.7 Run Program task

The Run Program task allows you to execute any Windows program, process or batch file, etc.

Any Run Program task can be scheduled to occur over any interval or at any date and time desired, or at application/service start-up.
Whether a Run Program task is scheduled or not, it consists of the following two parts:

- Run Program Options
- Run Program Notification

Run Program Options:



Program file name:
The program or process that will be executed by Windows.

Command line options:
The command line parameters that will be passed to the executable.

Process Priority:
Sets the priority of the new windows process that will be created.

Acceptable values are:
- LOW_PRIORITY
- BELOW_NORMAL_PRIORITY
- NORMAL_PRIORITY (default)
- ABOVE_NORMAL_PRIORITY
- HIGH_PRIORITY
- REALTIME_PRIORITY (Caution: REALTIME priority can cause system lockups)

AboveNormal
Indicates a process that has priority above Normal but below High.

BelowNormal
Indicates a process that has priority above Idle but below Normal.

High
Specify this class for a process that performs time-critical tasks that must be executed immediately. The

©2014 SolarWinds, Inc.

threads of the process preempt the threads of normal or idle priority class processes. An example is the Task List, which must respond quickly when called by the user, regardless of the load on the operating system. Use extreme care when using the high-priority class, because a high-priority class application can use nearly all available CPU time.

Low
Specify this class for a process whose threads run only when the system is idle. The threads of the process are preempted by the threads of any process running in a higher priority class. An example is a screen saver. The idle-priority class is inherited by child processes.

Normal
Specify this class for a process with no special scheduling needs.

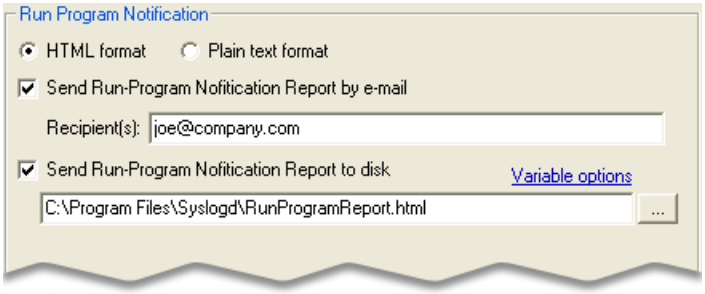
RealTime
Specify this class for a process that has the highest possible priority. The threads of the process preempt the threads of all other processes, including operating system processes performing important tasks. For example, a real-time process that executes for more than a very brief interval can cause disk caches not to flush or cause the mouse to be unresponsive.

Window Mode:
Sets the window mode of the process if that process has a user interface. This setting has no effect on processes that do not have a user interface.

Acceptable values are:
- Hide
- Normal
- Minimized
- Maximized

Wait for program initialization to complete before continuing
When checked, this option means that Syslog will wait for the new process to complete it's initialization. It does this by waiting until the new process signals that it is idle. This setting is useful is you are interacting with the process at a later stage, and you want to be sure that the process has started.

Run Program Notification:



E-mail format:

The Run Program report can be generated and sent in either HTML or plain-text format.

Send Run Program Notification Report by e-mail:

If selected, an e-mail containing the Run Program report will be sent to the e-mail address specified in the "Recipient(s)" field.

Recipient(s):

Comma or semi-colon delimited list of e-mail addresses, which are to receive copies of the Run Program report.

©2014 SolarWinds, Inc.

Send Run Program Notification Report to disk:

If selected, an file containing the Run Program report will be sent to disk using the file name and path specified.

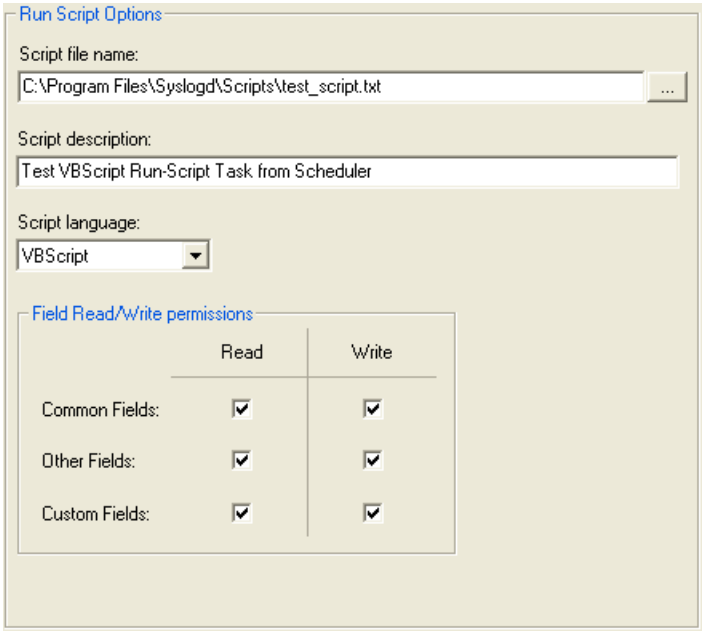
3.4.8 Run Script task

The Run Script task allows you to run a Kiwi Syslog Server Run-Script.

Any Run Script task can be scheduled to occur over any interval or at any date and time desired, at application/service start-up or shutdown.
Whether a Run Script task is scheduled or not, it consists of the following two parts:

- Run Script Options
- Run Script Notification

Run Script Options:



Script file name
The script file is a standard text file that contains the script commands. The file name can have any extension, but .txt is used by default for ease of editing with Notepad.

Script description
This field can contain any descriptive text you like. Its purpose is to briefly describe the function of the script

Script Language
Windows Script provides two script engines, Visual Basic® Scripting Edition and Microsoft JScript®

VBScript - A variation of Visual Basic or VBA (Visual Basic for Applications) used in MS Word and Excel. This language is easy to learn and has a rich feature set.

JScript - A variation of Java Script used in web pages. If you are familiar with Java Script then this may be your language of choice.

©2014 SolarWinds, Inc.

Both languages offer similar functionality and speed, so the choice on which to use is up to personal preference. However we have found through our tests that if your script is performing mainly string manipulation then JScript appears to be faster in most cases.

More info on VBScript can be found at:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/vtoriVBScript.asp

More info on JScript can be found at:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/js56jsoriJScript.asp

It is also possible to add additional scripting languages such as Perl or Python.

To do this you will need to install the Active Scripting engines for any new languages that you want to script in.

For information on using PerlScript please visit:
http://www.activestate.com/Products/ActivePerl

For information on using Python please visit:
http://www.activestate.com/Products/ActivePython

To download and for further information on ActiveScriptRuby please visit:
http://arton.hp.infoseek.co.jp/index.html

Field Read/Write permissions
For reasons of security and speed, access to the message/scripting variables can be restricted. Each time a script is run, the message fields are copied to the script variables and back again upon completion of the script. Because the copying takes time and uses CPU cycles, limiting the read/write access to only the variables you want to use will improve the speed of the program.

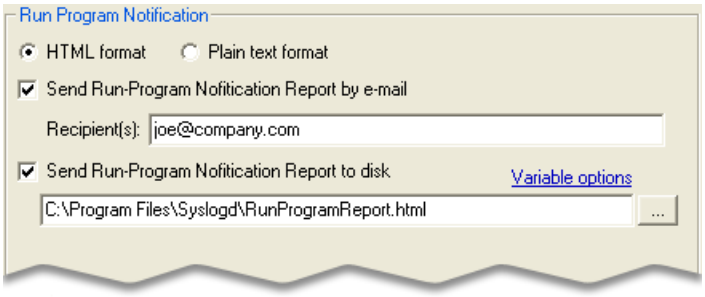
When you enable read access for a group of fields, their values will copied into the script variables and will readable from within the script.

When you enable write access for a group of fields, their values will copied from the script variables and will replace the equivalent program fields.

The fields are divided into groups based on the likelihood of usage within a script.

More details on each of the fields can be found here

Run Script Notification:



E-mail format:

The Run Script report can be generated and sent in either HTML or plain-text format.

Send Run Script Notification Report by e-mail:

If selected, an e-mail containing the Run Script report will be sent to the e-mail address specified in the

©2014 SolarWinds, Inc.

"Recipient(s)" field.

Recipient(s):

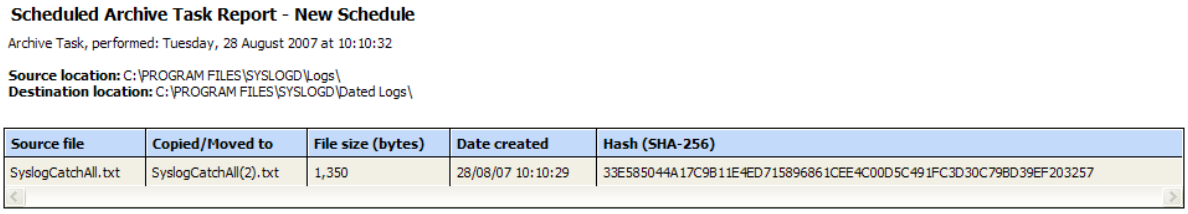
Comma or semi-colon delimited list of e-mail addresses, which are to receive copies of the Run Script report.

Send Run Script Notification Report to disk:

If selected, an file containing the Run Script report will be sent to disk using the file name and path specified.

3.4.9 Schedule Report

Sample HTML Report:



Scheduled Archive Task Report - New Schedule

Archive Task, performed: Tuesday, 28 August 2007 at 10:10:32

Source location: C:\PROGRAM FILES\SYSLOGD\Logs\
Destination location: C:\PROGRAM FILES\SYSLOGD\Dated Logs\

Source file	Copied/Moved to	File size (bytes)	Date created	Hash (SHA-256)
SyslogCatchAll.txt	SyslogCatchAll(2).txt	1,350	28/08/07 10:10:29	33E585044A17C9B11E4ED715896861CEE4C00D5C491FC3D30C79BD39EF203257

Sample plain-text report:

```
Kiwi Syslog Server - Scheduled Archive Task Report - Archive on a schedule
Archive Task, performed: Friday, 24 August 2007 at 16:10:01

Source location: C:\Program Files\Syslogd\Logs\
Destination location: C:\Program Files\Syslogd\Dated logs\

File 1:
Source file: SyslogCatchAll.txt
Copied/Moved to: 2007-08-24\SyslogCatchAll2007-08-24(2).txt
File size (bytes): 259,509,414
Date created: 24/08/2007 4:10:01 p.m.
Hash (SHA-256): D6034A75FCA28DEAA839D8536839B9745C1DAF2BEA4F6ADCC5D06B86C05D3BAE
```

3.5 Setup - Formatting

3.5.1 Custom file formats

If you would like to log your data in a different format to the standard formats available, this option will allow you to create your own custom file logging format from the fields available.

Creating a new custom format
To create a new custom file format, select the "Custom file formats" option then right click to choose "add new custom file format". Alternatively, you can use the "New" tool bar button at the top of the form.

Once a custom file format has been created, it will be available from the "Log File Format" dropdown in the "Log to File" actions. The custom file formats appear at the very end of the drop down list.

Changing the order of fields

©2014 SolarWinds, Inc.

The order in which the fields are written to the file can be changed by simply dragging the field checkboxes into a new order. When the mouse is over the checkbox text, the mouse cursor will change to a drag-drop cursor. Just click, drag and then drop to change the order as you want. The order shown will be used when creating the log file entry.

Enabling a Field
All the available fields are listed in the "Log file fields" area. Just check the fields you want to be written to the log file.

Date and Time formats
The format for the Date, Time and Date-Time fields can be chosen from the drop down options on the right hand side of the screen. Choose the format that best suites your location.

Field Delimiter
Each field is normally separated by a specific and unique delimiting character. Tab characters are the most common delimiters used for syslog files.

Qualifier
Each field can be enclosed in quotes, or double quotes etc. This is especially useful when the delimiter is set to use a comma character.

Adjust time to UTC
If you would like the date and time stamps in your log files to be adjusted to UTC (GMT) time, then simply check this box. The current time difference (in hours) between your system and UTC is shown in brackets.

Custom fields
Custom fields are for use by the run script action. By writing a parsing script, the syslog message text can be broken down into various sub fields. The values can then be assigned to the 16 custom fields and then logged to a file. Because each device manufacturer creates syslog messages in a different format, it is not possible to create a generic parser that will break up the message text into separate fields. A custom script must be written to parse the message text and then place it in the custom fields. Example parsing scripts can be found in the \Scripts sub folder. If you have checked the Custom field checkbox, all 16 custom fields will be written to the log file. Each custom field is separated by the selected delimiter character.

Example of fields and their values:

```
Field name        Example
-------------------------------------------------------->
Date                    28/01/2005
Time              16:12:54
Date-Time         28/01/2005 16:12:54
Milliseconds            123
TimeZone          -13 hrs
Facility          Local7
Level             Debug
Priority          Local7.Debug
HostAddress       192.168.0.1
Hostname          host.company.com
InputSource       UDP
Message Text         This is a test message from Kiwi Syslog Server
Custom                  Custom01 Custom02 Custom03 etc
```

3.5.2 Custom DB formats

Creating a new custom format
To create a new custom database format, select the "Custom DB formats" option then right click to choose "add new custom DB format". Alternatively, you can use the "New" tool bar button at the top of the form. Initially the database type will show "Access database", choose your database type from the drop down list. If your database type is not shown, choose "Unknown format" and modify the fields to suit your database type.

Changing the order of fields
The order in which the fields are created in the database can be changed by simply dragging the field function cell and dropping it above or below other cells. When the mouse is moved over the dark grey "Function" cells, the mouse cursor will change to a drag-drop cursor. Just click, drag and then drop to change the order as you

©2014 SolarWinds, Inc.

want. The order shown will be used when creating the database table and also when inserting data into the table.

Field function
The database field functions are listed in the first column. The next column containing the checkboxes allows you to enable or disable a particular field. If the field is not checked, it will not be included in the database INSERT statement or used when creating the database table.

Field names
The Field name column is editable so you can choose a suitable name for your field. The default field names are known to work on all databases. If you change the date field to a name of "DATE" for example, this may cause a problem with some database types because "DATE" is a reserved word. By using MSG at the beginning of the field name, you can avoid using reserved words.

Field size
When creating a database it is important to specify the field size so that the largest data element can fit into the field. Some field types do not need a size specified since it is implied by the field type. For example, a field type of Time is always assumed to be a size of 8 bytes. The size value is also needed by the program when it comes time to log data to the database. As the data is passed to the database via an INSERT statement, the data is trimmed to the specified field size. This avoids any errors caused by data that is too large for the field. For example, if you have specified the message text field to be 255 bytes, but a message arrives that is 300 bytes, the data will be trimmed back to 255 bytes before being logged.

Field type
Each field type must be matched to the type of data being logged. If you are not sure of the correct data type to use it is safe to use "VarChar" in most cases. When the data type cell is edited, a drop down combo will show allowing you to choose from a list of known data types. You can choose your own type instead of one from the list, by simply typing the value into the cell. The data types shown in the list are specific to the database format selected. For example, "Text" in Access becomes "VarChar" in SQL.

Custom fields
Custom fields are for use by the run script action. By writing a parsing script, the syslog message text can be broken down into various sub fields. The values can then be assigned to the 16 custom fields and then logged to a database. Because each device manufacturer creates syslog messages in a different format, it is not possible to create a generic parser that will break up the message text into separate fields. A custom script must be written to parse the message text and then place it in the custom database fields. Example parsing scripts can be found in the \Scripts sub folder.

Example of data format being logged:

```
Field name      Type            Size  Data
---------------+---------------+-----+----->
MsgUnique       adInteger          4 1
MsgDate         adDBTimeStamp     16 28/01/2005
MsgTime         adDBTimeStamp     16 16:12:54
MsgDateTime     adDBTimeStamp     16 28/01/2005 16:12:54
MsgUTCDate      adDBTimeStamp     16 28/01/2005
MsgUTCTime      adDBTimeStamp     16 04:12:54
MsgUTCDateTime  adDBTimeStamp     16 28/01/2005 04:12:54
MsgTimeMS       adInteger          4 0
MsgPriorityNum  adInteger          4 191
MsgFacilityNum  adInteger          4 23
MsgLevelNum     adInteger          4 7
MsgPriority     adVarWChar        30 Local7.Debug
MsgFacility     adVarWChar        15 Local7
MsgLevel        adVarWChar        15 Debug
MsgHostAddress  adVarWChar        15 192.168.0.1
MsgHostname     adVarWChar       255 host.company.com
MsgInputSource  adVarWChar        10 UDP
MsgText         adLongVarWChar  1024 This is a test message from Kiwi Syslog Server
```

Field format

©2014 SolarWinds, Inc.

The data format can be specified for each data field. In most cases no formatting is needed. For date and time fields, the database will accept data in many formats and convert it to its own internal format. When it is queried, the data may actually appear to be in a different format to which it was logged.

The HostAddress field formatting allows you to zero pad the address so that it appears with leading zeros. This ensures the address is always 15 bytes long and allows for easy sorting by IP address.

Leaving the format cell blank will leave the data unmodified and it will be added as it is received.

Show SQL commands button
Pressing this button will display a list of commands used to create and insert data into a table. You can use these commands to create your own table within your database application. A default table name of "Syslogd" is assumed when generating the commands.

Example of SQL commands:

```
Database type: MySQL database
Database name: New Format

SQL command to create the table:
CREATE TABLE Syslogd (MsgDate DATE,MsgTime TIME,MsgPriority VARCHAR(30),MsgHostname VARCHAR
(255),MsgText TEXT)

SQL INSERT command example:
INSERT INTO Syslogd (MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText) VALUES ('2005-01-
28','16:22:44','Local7.Debug','host.company.com','This is a test message from Kiwi Syslog
Server')
```

3.6 Setup - DNS Resolution

3.6.1 Resolve the address of the sending device

This converts the IP address of the sending device into a more meaningful host name. Instead of 203.50.23.4 you will see something like "sales-router.company.com"

The resolved host name is then used in the display and other actions.

The Host name is also used for the "Hostname" type filter.

If you like, the domain name section can be removed from the display by using the Remove the domain name option.

3.6.2 Remove the domain name (show only the host name)

If the Resolve the address of the sending device option is also checked, this option will remove the trailing domain name from the resolved host name. In this case, instead of "sales-router.company.com" you will see just "sales-router".

Enabling this option is useful when you only receive messages from a single domain or to reduce the amount of space used by the host name in the scrolling display.

This option also effects the host name field used for all the logging actions.

3.6.3 Resolve IP addresses found within the syslog message text

This feature is only available in the licensed version.

When you are logging data from web servers or firewalls etc, the message text may contain IP addresses. To turn these IP addresses into meaningful names and website addresses you need to enable this option. The

©2014 SolarWinds, Inc.

program will search through the message text and look for any IP address entries. You can also specify how the resolved name will be displayed. You may replace the IP address with the name or adding the name after the IP address in the message text.

* NetBIOS names can require more time to resolve than normal DNS entries. If you want to resolve NetBIOS names, increase the DNS timeout to 20 or 30 seconds.

Examples:

Test user connected to website http://192.168.1.2/index.html. src=192.168.5.100 rxbytes=64

With **replace IP address with host name** option, the message becomes...

Test user connected to website http://website.company.com/index.html. src=userpc.company.com rxbytes=64

With **place host name next to IP address** option, the message becomes...

Test user connected to website http://192.168.1.2 (website.company.com) /index.html. src=192.168.5.100 (userpc.company.com) rxbytes=64

The **Remove the domain name** option allows the stripping of the domain name portion from the resolved host name.

To selectively keep or remove the domain name based on a filter match, check the **If domain name contains** check box.

Place the domain name substrings to remove in quotes. To filter multiple domains, separate each quoted string with a space or comma.

".companyabc.com", ".companyxyz.co.uk"

An IP address resolved to mypc.company.co.uk will be changed to just "mypc".

Hostname tagging:
When you have selected the place host name next to IP address option, the hostname is normally tagged with brackets and a space character. The resolved host name can be tagged with any characters you like. For example, you might like to prefix the host name with "hostname=[" and then have a "] " suffix. You can change the prefix and suffix characters to fit the format of your messages.

A suggested tagging format for WELF format messages would be a prefix of **resolved_host=** and a suffix of a space character.

3.6.4 DNS query timeout

This option specifies the time to wait for the DNS server to respond to lookup queries. The default is 8 seconds. You may change this value if you are accessing a slow DNS server, or requests go through a slow network link.

This timeout value should only be increased if you are trying to resolve addresses via NetBOIS (Machine names of computers running Windows). Sometimes NetBOIS names can take up to 20 seconds to resolve via a unicast lookup request.

If your DNS server is local and you are only resolving internal addresses, you can safely reduce your timeout value down to 3 seconds.

If you increase the timeout value too much, you may find that the messages are being queued up waiting for the resolution to finish. In this case, when the queue reaches 1000 entries, messages will be dropped. The message buffer free space can be seen from the main syslog screen.

©2014 SolarWinds, Inc.

3.6.5 Setup - DNS Setup

3.6.5.1 Internal IP address - Name Resolution

Internal IP address range(s):

A list of masked IP addresses that identify your internal network address space.

The default entries in this list are standard internal (private) network address spaces, as identified in RFC1918/3330/3927. These include IANA reserved private internet address spaces, and the link-local address range.

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
169.254.0.0 - 169.254.255.255 (link-local)

Adding an internal IP address range:

Enter the masked IP address in the text box directly underneath the "Internal IP address range" list, and click the "Add" button.
IP addresses must be masked with an "x" character, the "x" signifying that any value within the range (0-255) is acceptable.

For example:

If you have an internal address space of '10.0.0.0' - '10.255.255.255', you should enter the masked IP address as '10.x.x.x'.

Important:
Syslog host IP addresses which match any of these address ranges will be resolved according to the options which are set for "Internal IP Address - Name Resolution" only. Those host IP addresses which do not match any of the internal address ranges will be resolved according to the options which are set for "External IP Address - Name Resolution". This distinction is important - the address range list essentially acts like a filter. The filter determining whether to try and resolve an IP address on an internal network using local DNS servers or NetBIOS, or whether to try and resolve the IP address with an external DNS server, etc. Ensuring that your internal address space is setup correctly can have a direct bearing on the turn-around times of each name resolution query.

Resolve internal addresses using NetBIOS:

If checked, Kiwi Syslog Server will attempt to resolve the internal IP address by sending a NetBIOS broadcast query to the local subnet.

Resolve internal addresses using DNS server:

If checked, Kiwi Syslog Server will attempt to resolve the internal IP address by sending a DNS query to a DNS server.

Preferred/Alternate internal DNS server addresses:

These entries determine which internal network address the DNS query will be sent to.
By default these addresses are auto-detected by Kiwi Syslog Server, and depending on your network configuration may need to be altered.

If the preferred DNS server is unavailable or cannot service the request, the same query will be asked of the alternate DNS server.
If no alternate DNS server is available, then this address is to be left blank.

©2014 SolarWinds, Inc.

3.6.5.2 External IP address - Name Resolution

Resolve external addresses using NetBIOS:

If checked, Kiwi Syslog Server will attempt to resolve the external IP address using NetBIOS.

Resolve external addresses using DNS server:

If checked, Kiwi Syslog Server will attempt to resolve the external IP address by sending a DNS query to a DNS server.

Preferred/Alternate external DNS server addresses:

These entries determine which external network address the DNS query will be sent to.
By default these addresses are auto-detected by Kiwi Syslog Server, and depending on your network configuration may need to be altered.

If the preferred DNS server is unavailable or cannot service the request, the same query will be asked of the alternate DNS server.
If no alternate DNS server is available, then this address is to be left blank.

3.6.6 Setup - DNS Cache

3.6.6.1 The local DNS cache

Every time an IP address to hostname resolution is needed, the DNS server is queried. This can be an extra overhead on the program, the network and the DNS server, especially if you receive lots of messages.

To reduce the DNS traffic and resolution time, a DNS cache is used. Once a hostname has been resolved the result is stored locally. The next time that address needs to be resolved, the result is taken from the cache instead of making another DNS request.

The registered version can hold up to 20,000 entries.

View button:
This dumps all the current cache entries into a file and then views the file with notepad. Information about the cache performance is also displayed.

Refresh button:
Counts the number of valid entries currently in the cache.

Clear button:
This will clear all the dynamic (learned from DNS lookups) entries. It won't clear the static entries that have been loaded from file.

Clear All button:
This will clear the entire DNS cache of all the entries (static and dynamic). A program restart is required to re-read the static entry file again.

3.6.6.2 Cache settings

Flush entries after X minutes:
This option allows old cached entries to be flushed from the cache after a specified time. By default a time to live of 1440 minutes (1 day) is used. After an entry has been in the cache for a day, it will be flushed from the cache and have to be re-learned via a lookup.

©2014 SolarWinds, Inc.

Enable pre-emptive lookup of IP addresses:
Instead of looking up each address sequentially, this option will extract the IP addresses from the message before it is added to the processing queue. The addresses will be asynchronously resolved and the results cached. When the message is processed seconds later, the results will already be available in the cache. The DNS resolution is done via a multi-threaded lookup system that can handle up to 100 simultaneous lookups. If you are receiving lots of messages and want to resolve IP addresses as they arrive, it is highly recommended that this option be enabled.

Pre-load the cache with static entries from a hosts file:
Enabling this option will cause the program to load a list of static host entries at start-up. The list must contain IP addresses and host names separated by a tab character. The addresses are loaded into the cache and marked as static, this means they will never expire and won't be flushed like the dynamically learned entries.

An example hosts file is included in the install folder. It is named "StaticHosts.txt"

Example of a host file:

```
# Static DNS host file
# Each entry must consist of an IP address, a tab, then a host name
# The IP address is in the format aaa.bbb.ccc.ddd
# The host name can be any text value that you like up to 63 characters in length
#
# Comments can be on a separate line and must start with a # character
#
# Example:
# 192.168.1.1     myhost.mycompany.com
#
# NOTE: The IP address and host name MUST be separated with a tab (ASCII chr 9)
#       Spaces will not be recognised as a valid separator


# Default value for localhost
127.0.0.1   localhost

# local machines
192.168.1.2 myfunny.valentine.com
192.168.1.5 flyme2.themoon.com
```

3.7 Setup - Modifiers

When the message arrives, various modifications can be made to the message to ensure that it fits within the specified bounds. The length of the message can be reduced, an invalid priority can be corrected and extra CR and LF characters can be removed.

3.7.1 Syslog message modifiers

Remove imbedded date and time from Cisco messages
When a Cisco device sends a Syslog message, it adds its own time stamp to the message. You may want to remove these extra time stamps to save space or make the logged files more readable.

This option works by looking for a particular Cisco message format. It will work with the following known Cisco date and time formats:

- Format for timestamp with timezone
  *47: *Mar 1 00:45:43 UTC: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console*
- Format for uptime
  49: 00:54:46: %SYS-5-CONFIG_I: Configured from console by console
- Format for timestamp localtime with msec

©2014 SolarWinds, Inc.

*50: *Mar 1 00:56:30.475: %SYS-5-CONFIG_I: Configured from console by console*

- Format for timestamp localtime with msec and timezone
  *51: *Mar 1 00:58:52.767 UTC: %SYS-5-CONFIG_I: Configured from console by console*

- Format for timestamp
  *53: *Mar 1 01:11:17: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console*

Allow messages with no priority (use default priority)
Some routers and hosts may send messages that contain no priority code in the message. In situations where this occurs you can apply a default priority to the message. Check this box and then set the **default priority** you want to use, from the drop down lists.

A normal Syslog message has a priority code at the start of the message text.
Example. <100>This is a test message
The priority value should be between 0 and 191 for standard Unix priority codes

Maximum message length (bytes)
This option allows you to limit the maximum message size of incoming messages. You may want to change this to a lower value than the default 4096 bytes if you are only expecting small messages.
This limit allows the program to reject oversize messages sent by hackers or errors in transmission.
Some Syslog Servers may crash when receiving large packets, this option limits the size of the packet that the program will accept and process.

The Syslog RFC 3164 states that legal Syslog messages may not exceed 1024 bytes in length. (Not including packet headers)

Allow messages with priority > 191 (use default priority)
Each Syslog message has a priority code at the beginning of the message. Normally with Unix systems and router devices, this priority code has a value between 0 and 191. Sometimes devices send messages with a priority code higher than 191. Even though the priority value can be higher than 191, there is no standard to define priority levels or facilities above 191.

If this option is enabled, messages received with a priority higher than 191 will have their priorities set to the default priority setting.

Remove CR/LF from end of messages
Some routers or hosts send messages with a CR/LF attached to the end of the message text. This will cause the log files to be double spaced.

Check this box if you want to remove all trailing CR/LF characters from the messages.

Replace non-printable characters with <ASCII value>
Some routers or hosts may send messages that contain control characters in the message text. For example, multi-line messages will contain carriage returns and line feeds. If you enable this option, instead of trying to display control characters, the equivalent ASCII value will be displayed.

E.g. When a carriage return is received, it will be replaced with a <013> instead.

3.8 Setup - Scripting

This option allows you to set the names and initial values of the custom statistics fields for use within the script files and statistics reports.

There are 16 custom statistics fields available for scripting use. These values are static and do not get erased with each new message like the other script fields do.

The custom statistics values can be viewed from the Statistics window under the Counters tab. The names for the fields that you have specified will be used in the statistics window and in the daily statistics e-mail report.

©2014 SolarWinds, Inc.

The initial values of the statistics counters can be set to any value you like. By default the values are all set to 0. If you want to create a decrementing counter then an initial value of 1000 for example can be set and then decremented by the run script actions.

The names and inital values are applied when the program starts. To force the program to reinitialize the fields with these values, use the **File | Debug options | Initialize custom statistics** menu, or press Ctrl-F9 from the main syslog window.

Click here for more information on scripting

3.9 Setup - Appearance

3.9.1 Wallpaper

Allows a background image to be set for the display. A paper-style image is provided as a sample.

3.10 Setup - E-mail options

3.10.1 E-mail setup options

Email format:
The format of the Email message can be set to HTML/Plain text for the email action, alarm via email and statistics via email.

Sending Email via secured channel:
Available options are,
- **None:** This option can be used for sending Emails via SMTP server through insecure channel.
- **SSL:** This option can be used for sending secured Emails via Email server which supports SSL (Secure Socket Layer), for example Gmail and Yahoo Email servers.
- **TLS:** This option can be used for sending secured Emails via Email server which supports TLS (Transport Layer Security), for example Webmail,POP,IMAP, and SMTP Email servers.

Send alarm messages via e-mail to:
Alarm messages will be sent via e-mail when an Alarm threshold has been exceeded. Can be sent securely. (The alarm thresholds can be set from the Alarms section.)

Enter the e-mail address or addresses you want notified when an alarm occurs. E-mail addresses must be separated by a comma.

E.g. noc@company.com,helpdesk@company.com,pager123@company.com

The checkbox on the left of the text is to enable or disable the sending of alarm e-mail.

Click here to see an example of the alarm message e-mail

Send daily statistics via e-mail to:
A daily statistics message is e-mailed out every night at midnight and contains information on log file size, disk space remaining on the archive drive, number of total messages and a breakdown of where the messages came from, on what facility and level.

The message is best viewed in a fixed font such as "Courier new" so all the columns line up. Can be sent securely

Click here to see an example of the daily statisics e-mail message

Short alarm messages (for pagers)
When this is enabled, only the subject line is used to send information. The message body part of the e-mail is

©2014 SolarWinds, Inc.

not used. This is useful when the message is being forwarded to a paging service and you only have a limited amount of display space.

Keep a log file of e-mail activity
If you intend to use the e-mail feature to notify you of alarms and statistics, then you may also want to keep a log of what messages have been sent and to whom.

This log file is named SendMailLog.txt and is located in the same directory that the program is installed in.

To view this file with notepad you can use the **View log** button.

To delete the file and start a new log file, you can use the **delete log** button

Enable verbose logging
This option is very useful if the mail is not being sent correctly. All the information being sent between the program and the mail server is logged to file (The message content is not shown).

Note: If there are a lot of messages being sent, be aware that this option can use a lot of disk space.

Hostname or IP address of SMTP mail server:
This is the IP address or host name of your SMTP server. This can be your local server, or one provided by your ISP.

The host name of the mail server is usually something like mail.company.com or smtp.company.com. Below are the few Email servers.

- Gmail - smtp.gmail.com
- Yahoo - smtp.mail.yahoo.com
- Hotmail - smtp.live.com

If you do not have a local SMTP server, we recommend you use something like Mail Direct which is available from: http://www.ocloudsoft.com

Valid 'from' e-mail address on SMTP server:
It is recommended that you use a valid reply address in this field. In case of a mail failure, the SMTP server will send the bounce message to this address.

Some SMTP servers require you to specify a domain name on the end, others do not.

The address you use here will be the name that appears in the 'message from' field on your received e-mail.

If you like, you can specify a more friendly name in brackets after the address. This will be shown as the From address in the mail client.

E.g. noc@company.com (Syslog Server)

In the example above, the name "Syslog Server" will appear in the From field of the received message. Some SMTP servers may not support this format of from address and you may have to use the e-mail address only.

SMTP port:
If your SMTP server listens on a non standard port, you may specify the alternate value here. Normally SMTP servers listen on port 25. Some companies change this value for security reasons. The value may be from 1 to 65535.
Default port for SSL is 465 and for TLS is 587.

Timeout:
The timeout value is how long the program waits for a response from the SMTP server before giving up. If your SMTP is via a dial-up link or very busy, you may want to increase this value from the default of 30 seconds. The value entered can be from 1 second to 240 seconds.

SMTP Username and Password:

©2014 SolarWinds, Inc.

These options only need to be set if your SMTP server requires authentication before accepting e-mail. Most SMTP servers do not need these options set.

To enable authentication, enable the checkbox to the left and fill in your username and password for the SMTP server. These values are supplied by your network administrator, SMTP server provider or ISP.

If you need to use the POP before SMTP option for authentication. It is recommended that you download a freeware POP mailbox checker and run this on your system as well. Have it check for new messages every 5 minutes which will then allow the SMTP mail to go through. The POP before SMTP authentication may be added to a future version.

Default E-mail Delivery Options
This option allows the default importance, priority and sensitivity flags of sent e-mail message to be specified. The e-mail recipients will recieve the messages with the various importance/priority/sensitivity levels set accordingly.
Importance: Unspecified (Default) / High / Normal / Low
Priority: Unspecified (Default) / Normal / Urgent / Non-Urgent
Sensitivity: Unspecified (Default) / Personal / Private / Confidential

3.10.2 An example Alarm message

```
Syslog Alarm: 2198 messages received this hour.
The current maximum threshold is set at 3 messages per hour.
This could indicate a problem, please check the log files and syslog statistics below.

///       Kiwi Syslog Server Statistics         ///
-------------------------------------------------
24 hour period ending on: Fri, 26 Jan 2005 15:39:16 +1200
Syslog Server started on: Wed, 17 Jan 2005 11:39:53
Syslog Server uptime:     9 days, 3 hours, 59 minutes
-------------------------------------------------

+ Messages received - Total:          361965
+ Messages received - Last 24 hours:  37964
+ Messages received - Since Midnight: 26530
+ Messages received - Last hour:      2821
+ Messages received - This hour:      2198
+ Messages per hour - Average:        1582

+ Messages forwarded:                 3063
+ Messages logged to disk:            26530

+ Errors - Logging to disk:           0
+ Errors - Invalid priority tag:      0
+ Errors - No priority tag:           0
+ Errors - Oversize message:          0

+ Disk space remaining on drive C:    59505 MB

-------------------------------------------------


  Breakdown of Syslog messages by sending host
+--------------------+------------+------------+
| Top 20 Hosts       |  Messages  | Percentage |
+--------------------+------------+------------+
| pix_firewall_inside|     26530  |    100.00% |
+--------------------+------------+------------+


    Breakdown of Syslog messages by severity
+--------------------+------------+------------+
| Message Level      |  Messages  | Percentage |
+--------------------+------------+------------+
| 0 - Emerg          |          0 |      0.00% |
| 1 - Alert          |          0 |      0.00% |
| 2 - Critical       |          0 |      0.00% |
| 3 - Error          |        123 |      0.46% |
| 4 - Warning        |          0 |      0.00% |
| 5 - Notice         |        715 |      2.70% |
```

©2014 SolarWinds, Inc.

```
| 6 - Info           |     25692  |     96.84% |
| 7 - Debug          |         0  |      0.00% |
+--------------------+------------+------------+


End of Report.
```

3.10.3 An example Statistics message

```
///       Kiwi Syslog Server Statistics         ///
-----------------------------------------------------
24 hour period ending on: Fri, 26 Jan 2005 00:00:01 +1200
Syslog Server started on: Wed, 17 Jan 2005 11:39:53
Syslog Server uptime:     8 days, 12 hours, 19 minutes
-----------------------------------------------------
+ Messages received - Total:          335435
+ Messages received - Last 24 hours:  35206
+ Messages received - Since Midnight: 35967
+ Messages received - Last hour:      1149
+ Messages received - This hour:      366
+ Messages per hour - Average:        1467
+ Messages forwarded:                 0
+ Messages logged to disk:            35967
+ Errors - Logging to disk:           0
+ Errors - Invalid priority tag:      0
+ Errors - No priority tag:           0
+ Errors - Oversize message:          0
+ Disk space remaining on drive C:    59573 MB
-----------------------------------------------------


  Breakdown of Syslog messages by sending host
+--------------------+------------+------------+
| Top 20 Hosts       |  Messages  | Percentage |
+--------------------+------------+------------+
| pix_firewall_inside|     35967  |    100.00% |
+--------------------+------------+------------+


    Breakdown of Syslog messages by severity
+--------------------+------------+------------+
| Message Level      |  Messages  | Percentage |
+--------------------+------------+------------+
| 0 - Emerg          |         0  |      0.00% |
| 1 - Alert          |         0  |      0.00% |
| 2 - Critical       |         0  |      0.00% |
| 3 - Error          |        69  |      0.19% |
| 4 - Warning        |         0  |      0.00% |
| 5 - Notice         |       731  |      2.03% |
| 6 - Info           |     35167  |     97.78% |
| 7 - Debug          |         0  |      0.00% |
+--------------------+------------+------------+


End of Report.
```

3.11 Setup - Alarm thresholds

3.11.1 Notify by Mail

If a Min or Max threshold is exceeded an e-mail message is sent to all the recipients in the "Alarm notification" list (set from the e-mail options)

The e-mail message states the alarm message, the threshold exceeded and the current threshold value etc.

The last hour's statistics are also included for more information.

©2014 SolarWinds, Inc.

Click here to see an example of the alarm message e-mail

3.11.2 Audible Alarm

This feature is only available in the licensed version.

If a Min or Max threshold is exceeded Syslog will beep once a second until the alarm is cancelled by double clicking the red flashing alarm bell icon in the status bar on the **Main Syslog Server** display.

If the ***Play sound file*** option is enabled then the specified sound file is played every 5 seconds until cancelled.

Double click the red flashing alarm bell icon to cancel any audible alarm.

3.11.3 Run Program

This feature is only available in the licensed version.

Runs an external program of your choice if a Min or Max threshold is exceeded.
It is possible to pass information to the program being run as command line parameters.

The insert message content section has more information on the command line replacement values available.

For example

Pager.exe "555-1234" ,"Syslog - Warning, lots of messages received, Max set at %MsgAlarmMax but received %MsgThisHour so far this hour."

Use the Test button to make sure the external program runs as you would expect.

Use quote (") marks around file names or paths that contain spaces.

3.12 Setup - Input options

3.12.1 Setup - Input options

The program is able to listen for syslog messages via UDP or TCP and can listen for version 1 or 2c SNMP traps.

By default, listening on UDP port 514 is enabled. This the most common method of syslog delivery.

Some firewalls (Cisco PIX) and other syslog Servers are able to send syslog messages via TCP. The Cisco PIX uses TCP port 1468 to send messages on. Listening on TCP is not enabled by default.

The reception and decoding of version 1 and 2c SNMP traps is supported, but not enabled by default. The normal SNMP trap listening port is UDP 162.

There are three separate listening sockets. UDP, TCP and SNMP.

Additionally, a keep alive message can be injected into the input stream to simulate traffic.

3.12.2 Inputs - UDP

Normally a Syslog Server listens on port 514 for UDP Syslog messages. If you want to listen on a different port for Syslog messages, you can enter any port value from 1 though to 65535. If you change the port from 514, the device sending the Syslog message must also be able to support the alternate port number.

If you would like to stop Syslog Server from listening for UDP Syslog messages, simply uncheck the **Listen for UDP Syslog messages** checkbox. This version of Kiwi Syslog Server can only listen for messages on a single

©2014 SolarWinds, Inc.

UDP port at once. Future versions will be able to listen to multiple UDP ports simultaneously.

Bind to Address:
By default, the UDP socket will listen for messages on all connected interfaces. If you want to limit the binding to a single specific interface, you can specify the IP address in the **Bind to address** field. Otherwise, leave this field blank. (If the **Bind to address** field is left blank, it will listen on all interfaces. This is the best option in most cases.)
For example, if you have two non routed interfaces on the computer, 192.168.1.1 and 192.168.2.1, then you can choose to bind to only the 192.168.1.1 interface. This will ignore any syslog messages sent to the other interface.

Data Encoding:
If you are receiving messages from systems that use different data encoding formats, you can specify the decoding method to apply to the incoming data. The default is to use the System code page.

The drop down list allows you to select some commonly used encoding formats. To select a different encoding, choose "Other-->" and then enter the code page number into the field on the right.

The various code pages available on most Windows systems can be found at:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/act/htm/actml_ref_scpg.asp

Here are some common code page numbers that can be used:

Name	Code Page Number	Description
System	1	System Code Page
ANSI	0	ANSI
UTF-8	65001	Unicode Transformation Format 8
Shift-JIS	932	Japanese
EUC-JP	51932	Japanese Extended Unix Code
BIG5	950	Traditional Chinese
Chinese	936	Simplified Chinese

Please note: If the number you specify is not a valid Code Page on your system, the incoming data will not be decoded correctly and will be dropped.

If in doubt, use UTF-8 encoding (65001) as it will handle all Unicode characters.

For more information on Unicode and UTF-8, please see:
http://en.wikipedia.org/wiki/UTF-8

3.12.3 Inputs - TCP

Syslog logging has been traditionally sent to port 514 using UDP.

UDP is a connectionless protocol, hence unreliability is inherent. There is no acknowledgement, error detection, sequencing or retransmission of missed packets when sending syslog messages over the UDP protocol.

Devices like the Cisco PIX implement the syslog protocol over a TCP transport. TCP is connection oriented. It relies on the destination host being there. The connection is built when the sending device is initialized, or prior to sending the first syslog message. It's slower to use TCP because of the initial time for the three-way handshake, and all packets get acknowledged by the server once they are received, and essentially before the next one can be sent. The TCP protocol offers reliability plus error correction; this is used to ensure messages are sent to the syslog server reliably.

See also, PIX Firewall Support and configuring the Cisco PIX

Bind to Address:
By default, the TCP socket will listen for messages on all connected interfaces. If you want to limit the binding to a single specific interface, you can specify the IP address in the Bind to address field. Otherwise, leave this field blank. (If the Bind to address field is left blank, it will listen on all interfaces. This is the best option in most cases.)
For example, if you have two non routed interfaces on the computer, 192.168.1.1 and 192.168.2.1, then you can choose to bind to only the 192.168.1.1 interface. This will ignore any syslog messages sent to the other

©2014 SolarWinds, Inc.

interface.

The Cisco PIX uses port 1468. Its default behavior is that if it cannot connect to the syslog server, it blocks all network traffic through it.

For more information on the Cisco Pix Firewall, please refer to: www.cisco.com/univercd/cc/td/doc/product/iaabu/pix

Data Encoding:
If you are receiving messages from systems that use different data encoding formats, you can specify the decoding method to apply to the incoming data. The default is to use the System code page.

The drop down list allows you to select some commonly used encoding formats. To select a different encoding, choose "Other-->" and then enter the code page number into the field on the right.

The various code pages available on most Windows systems can be found at:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/act/htm/actml_ref_scpg.asp

Here are some common code page numbers that can be used:

Name	Code Page Number	Description
System	1	System Code Page
ANSI	0	ANSI
UTF-8	65001	Unicode Transformation Format 8
Shift-JIS	932	Japanese
EUC-JP	51932	Japanese Extended Unix Code
BIG5	950	Traditional Chinese
Chinese	936	Simplified Chinese

Please note: If the number you specify is not a valid Code Page on your system, the incoming data will not be decoded correctly and will be dropped.

If in doubt, use UTF-8 encoding (65001) as it will handle all Unicode characters.

For more information on Unicode and UTF-8, please see:
http://en.wikipedia.org/wiki/UTF-8

Message Delimiters:
Because Syslog messages that are sent via TCP are not necessarily contained in a single TCP packet, Kiwi Syslog Server has a buffering facility which accumulates sequential TCP packets in an internally. Because of this, Kiwi Syslog Server needs to know how to identify separate Syslog messages in a single TCP stream. It does this through the use of message delimiters (or separators). Each delimiter signifying the character (or sequence of characters) that will be used to split the stream into individual Syslog messages.

The kind of delimiter to use depends very much on the client or device which is sending Syslog over TCP.

Possible delimiters are:

CRLF (ASCII 13, ASCII 10)
CR (ASCII 13)
LF (ASCII 10)
Null (ASCII 00)

3.12.4 Inputs - Secure (TLS) Syslog

Some devices available on the market, such as Cisco ASA-55XX, which support sending secure syslog messages over TCP channel with transport layer security (TLS). Kiwi Syslog Server starting from release 9.2 supports Secure (TLS) Syslog (RFC 5425).

Secure (TLS) Syslog is performed over TCP channel and thus most of the settings, available on "Input –Secure (TLS) Syslog" page, are the same as on the "Input – TCP" page. Only settings specific to Secure (TLS) Syslog

©2014 SolarWinds, Inc.

are described here.

Certificates:
TLS relies on certificate-based authentication. A proper certificate has to be selected from certificate store before any client will be able to successfully connect to Kiwi Syslog Server using TLS secured TCP channel. "Select Certificate" button allows the user to browse local certificate stores and pickup a suitable certificate. The selected certificate is used to prove identity of Kiwi Syslog Server to the client. The server itself does not check client certificate and accepts TLS connection from any client.

Note: Certificates which will be used by Kiwi Syslog Server have to be installed into the Local Machine certificate store.

To open this store the following procedure may be used:
Start -> Run -> [type] *mmc* [Enter] -> [Inside MMC Console] *File -> Add/Remove Snap-in… -> Add -> Certificate -> Add -> Computer account -> Next -> Local computer -> Finish -> Close -> OK*
Expend *Certificates (Local Computer)* and install certificate into *Personal*

What kind of certificate should be used and configuration of public key infrastructure (PKI) is device specific and manufacturer documentation should be consulted. Steps which may be used for Cisco ASA-5505 are given below on this page.

TCP Port:
By default the port allocated to Secure (TLS) Syslog is 6514 (RFC 5425).

Message Delimiters:
There is one more message delimiter type added for Secure (TLS) Syslog comparably to delimiters available on "Input – TCP" page. This delimiter conforms to the rule defined in RFC 5425. If the user decides to look for this delimiter inside incoming message stream the search for this delimiter is performed before other delimiters are checked.

Example: Configuring Cisco ASA-5505 for sending secure syslog to Kiwi Syslog Server and Cisco ASA-5505

1. Request certificate from Certification Authority (CA), e.g. Microsoft Certificate Service, specifying "Server Authentication Certificate" as certificate purpose.
2. When certificate is issued install it into *Local Machine* certificate store (see directions in ***Certificate*** section) of the machine where Kiwi Syslog Server is installed.
3. Load certificate into ASA-5505 (e.g. using terminal console access)
   a. Enter configuration mode
   b. Create trust point, e.g. naming it Syslog, and config it to accept certificate through terminal
      Tok-ASA5005(config)# **crypto ca trustpoint Syslog**
      Tok-ASA5005(config-ca-trustpoin)# **enrollment terminal**
   c. Authenticate trust point by downloading certificate
      Tok-ASA5005(config)# **crypto ca authenticate Syslog**
      (provide base64 certificate into terminal console and end it with "quit")
   d. Certificate loaded
4. Adjust ASA-5505 to send secure syslog
   Tok-ASA5005(config)# **logging enable**
   Tok-ASA5005(config)# **logging host [interface name] [ip] tcp/6514 secure**
   Tok-ASA5005(config)# **logging permit-hostdown**
5. Enable *Secure TCP* input in Kiwi Syslog Server and select certificate installed into *Local Machine* certificate store on step 2.

3.12.5 Inputs - SNMP

The program is able to listen for Version 1 and 2c SNMP traps. The traps can then be decoded and then handled like a regular syslog message.

Listen for SNMP traps:
By default this option is disabled. Check the box to enable listening for SNMP traps.

UDP port:
This is the UDP port to listen on for SNMP traps. Normally traps are sent to port 162. A value between 1 and 65535 can be entered. If you choose a value other than 162, make sure the device sending the trap is also sending to the specified port.

©2014 SolarWinds, Inc.

Bind to Address:
By default, the SNMP trap receiver will listen for messages on all connected interfaces. If you want to limit the binding to a single specific interface, you can specify the IP address in the **Bind to address** field. Otherwise, leave this field blank. (If the **Bind to address** field is left blank, it will listen on all interfaces. This is the best option in most cases.)
For example, if you have two non routed interfaces on the computer, 192.168.1.1 and 192.168.2.1, then you can choose to bind to only the 192.168.1.1 interface. This will ignore any syslog messages sent to the other interface.

Specified fields:
This option allows you to choose which SNMP fields are decoded and added to the incoming message. Check the box next to the field that you want enabled. You can change the order in which the message is decoded by clicking and dragging on the field name.

Community:
This is like a password that is included in the trap message. Normally this value is set to values such as "public", "private" or "monitor"

Enterprise:
This is a dotted numerical value (1.3.6.1.x.x.x.x) that represents the MIB enterprise of the SNMP trap. This field only applies for version 1 traps. Version 2 traps have the Enterprise value bound as the second variable in the message.

Uptime:
This is a value that represents the system uptime of the device sending the message. The value is in time ticks. The value resets to 0 when the device restarts. A low value would indicate that the device has been warm or cold started recently. This field only applies to version 1 traps. Version 2 traps have the system uptime value bound as the first variable in the message.

Agent address:
This represents the IP address of the sending device.

Trap type:
This check box represents three trap type fields. Generic Type and Specific Trap-Type and Specific Trap-Name. These fields only applies for version 1 traps. There are 6 defined Generic Type traps. If the Generic Type is set to 6 it indicates an Enterprise type trap. In this case the Specific Trap value needs to be considered.

Version:
This field indicates the version of the received trap. The program currently supports version 1 and 2c.

Message:
This field is made up of all the bound variables. Some traps may include more than a single variable binding. If the variable is a Octet String type, then it will be visible as plain text. Some variables represent counters or integer values. In this case, it is advisable to check the value against the MIB syntax for further explanation.

Syslog priority to use:
Each SNMP message that is received is converted internally into a standard syslog message. This allows you to filter the message like a standard syslog message. Because SNMP traps don't have a message facility and level, a default value must be applied. You can then use this value in the rule engine. For example, you might like to set all traps to be tagged as Local0.Debug. You can then create a priority filter to catch that facility and level and perform a specified action.

SNMP field tagging:
This drop down list allows you to specify how the decoded fields are converted into a message. By default, the "fieldname=value" option is used. This allows for easy parsing of the logs later. Other options are XML, comma delimited or delimited by [].

Here is an example of a message tagged with the fieldname=value option.

©2014 SolarWinds, Inc.

community=public enterprise=1.3.6.1.2.1.1.1 enterprise_mib_name=sysDescr uptime=15161 agent_ip=192.168.0.1 generic_num=6 specific_num=0 version=Ver1 generic_name="Enterprise specific" var_count=01 var01_oid=1.3.6.1.2.1.1.1 var01_value="This is a test message from Kiwi Syslog Server" var01_mib_name=sysDescr

Note the values are only contained in quotes ("") if they contain a space.

Use LinkSys Display filter:
The LinkSys Display filter simply removes all PPP messages from being displayed. The PPP messages are still logged to file as normal.
This feature is only useful if you are logging from a LinkSys network device.

Perform MIB lookups:
A well known list of object ID values and their text names have been included in a database that is included with the program. This will handle the most common traps from Cisco, 3Com, Allied Telesyn, SonicWall, Nokia, Checkpoint, BreezeCom, Nortel and SNMP MIB-II.

The MIB database file is located in the InstallPath\MIBs folder in a file named: KiwiMIBDB.dat
This database is a propriatry database file which has been compiled from over 60,000 MIB definitions. Since most MIB files only contain less than 5% of usable trap information, this pre-compiled method saves a huge amount of lookup time, disk space and hash table memory over using a standard MIB compiler/parser.

If you would like to add additional MIB lookup values, we are very happy to add them for you. Please send your zipped MIB files to KiwiSales@SolarWinds.com. We will compile a new database file for you and send you the update. Please also include your Unknown_OID_list.txt file so we can ensure all the OIDs are referenced.

When creating the MIB database, all the traps, notifications and referenced variables are parsed from the MIB files. Sometimes an object may not be referenced correctly and therefore won't be added. In this case, all we need to know is the OID value and we can ensure that it is included. See the next section for more information.

Log failed lookups to debug file:
If an OID value is unable to be located in the database, if you have the "log failed lookups" option checked, the OID value will be logged to a debug file. The file is located in InstallPath\MIBs and is named: Unknown_OID_list.txt. This file can be zipped up and sent to KiwiSales@SolarWinds.com so we can ensure that the next release of the database has these values listed.

Show additional OID suffix info:
Sometimes a device will send additional information encoded after the main OID number. This information can include things like the interface index, source and destination addresses and port numbers etc. This information can be shown as a suffix to the MIB name.

For example, a Cisco switch might send a "Link up" trap containing the variable: 1.3.6.1.2.1.2.2.1.2.3.
The last "3" of the OID refers to the interface index. The rest of the OID can be resolved to the MIB name of "ifDescr".

If the "Show additional OID suffix info" option is checked, then the MIB name displayed will contain the extra ".3" information. For example: ifDescr.3=SlowEthernet0/3. With the option unchecked, the display will look like: ifDescr=SlowEthernet0/3.

3.12.6 Beep on every message received

If this option is enabled, a beep will sound on the reception of any syslog message or SNMP trap. The beep will be heard even if a filter blocks the display or logging of the message. This option can be used for debugging to let you know that a message has been received.

* If you are hearing a beep on every message that comes in and this option isn't checked then there is a problem logging the messages to disk. Check the Error log for details of the problem. (From the View menu). If a message can't be written to the specified log file, a beep will sound to notify you of the problem.

©2014 SolarWinds, Inc.

3.12.7 Cisco PIX Firewall (TCP)

The Cisco PIX firewall offers secure connection oriented message logging using TCP instead of UDP. The default TCP port used for the PIX is port 1468. This port can be any value from 1 through to 65535. The Cisco PIX will also have to be configured to use the alternate port accordingly.

Because TCP is connection oriented, the logging device (Kiwi Syslog Server) can let the PIX know when it can no longer accept any more messages if the disk is full for example. To provide feedback to the PIX the Syslog Server simply closes the open connection to indicate that it can't accept any more messages. Kiwi Syslog Server will check the available disk space on the logging drive and if the percentage of space free falls below the threshold set, it will break the TCP connection to the PIX. **This will cause the PIX to stop passing any traffic** until Kiwi Syslog Server re-accepts the connection requests from the PIX. As soon as the percentage of free disk space rises above the threshold, Kiwi Syslog Server will accept log messages from the PIX and traffic will start flowing again.

Warning: If you enable disk space checking, and the disk space usage reaches the set threshold, all PIX traffic will stop. This means no Internet access for your users. Only enable this option if the log integrity is more important than your users having access to the Internet.

3.12.8 Inputs - Keep-alive

How keep alive messages work

Keep alive messages can be injected into the syslog input stream at a regular interval and used to trigger scripting actions or can serve as a method of stamping the log files at a regular interval.

The injected keep alive messages are treated as any other incoming message would be, and are processed by the rule engine. Depending on the rule set configured, the message may be written to disk, displayed or forwarded on to another syslog server.

When the keep alive message is forwarded on to another syslog server, it can act as a "I am still alive and well" message to tell the other server that everything is OK. On the remote server, a filter can be setup to detect missing keep alive messages and raise an alarm if necessary.

The injected message properties can be modified by specifying a Facility, Level, Host IP address and message text values.

The keep-alive message can be identified in a script by checking the varInputSource field value. A keep-alive message uses a value of "3".

Enable keep-alive messages:
By default this option is disabled. Check the box to enable the injection of keep-alive messages.

Frequency:
This sets how often the keep-alive messages are injected into the input stream. Every 60 seconds is the default value, but any value between 1 and 86400 seconds (1 day) can be entered.

Syslog facility:
This sets the facility of the keep-alive message. You can use a priority filter in the rule set to work with this facility only. Normally this option is set to a value of "Syslog" to indicate that it is the Syslog program generating the message.

Syslog level:
This sets the level of the keep-alive message. You can use a priority filter in the rule set to work with this facility/level combination only. Normally this option is set to a value of "Info" to indicate that it is an informational message.

From IP Address:
This sets the "From" IP address of the keep-alive message. This value can be from 1.1.1.1 to

©2014 SolarWinds, Inc.

255.255.255.255. It is recommended that a value of 127.0.0.1 be used as the default. The address specified can be filtered against by the rule set later.

Message text:
This is the message text that is used for the keep-alive message. It can be any message or text string that you like. By default the message reads "Keep-alive message".

How to use a keep alive message:

Scripting use.
Normally, the rules/filters/actions are only run when a message arrives and is processed by the rule engine. If you need to take action based on a time, then you can use the keep alive messages as a regular trigger of the rule engine.

```
Rules
 Rule: MyScript
  Filters
   Priority: Match Syslog.Info only
  Actions
   Action: Run script
   Action: Stop processing (Exits the rule engine here)
 Other Rules here...
```

The keep-alive message can be identified in a script by checking the varInputSource field value. A keep-alive message uses a value of "3".

Forwarding to another host as a beacon.
The keep alive messages can be forwarded to another host to tell it that "All is well".

```
Rules
 Rule: Send keep alive message
  Filters
   Priority: Match Syslog.Info only
  Actions
   Action: Forward to host (send to another host via a syslog message)
   Action: Stop processing (Exits the rule engine here)
 Other Rules here...
```

Because we are using the "Stop processing" action, the keep alive messages won't be seen by any other rules below this one. The priority filter will match the "Syslog.Info" priority, then the action will be taken (forward message) then the rule engine will discard the message and wait for the next one to arrive.

3.13 Setup - Display

3.13.1 Always on top

Ensures that Kiwi Syslog Server is always the top most window.

3.13.2 Rows of scrolling display

This sets the number of rows in the scrolling display.

Normally this is set to 40 rows (about a full screen worth of messages)

You can choose from 5 to 1000 rows.

Note – The higher number of scrolling display rows you choose the longer it will take to update the display. Every new message that is displayed causes the grid to shuffle all the displayed messages and drop off the last message. This shuffling uses CPU time, the more rows to shuffle, the more CPU time is consumed.

©2014 SolarWinds, Inc.

3.13.3 Minimize to System Tray on start-up

Check this option if you want Kiwi Syslog Server to minimize itself to the System Tray as soon as it starts.

This may be useful if you run Kiwi Syslog Server on Windows startup and want it to sit unobtrusively in the System Tray.

3.13.4 Use 3D titles

Uses 3D text (drop shadow) in the column headings for the main display and in headings of the Kiwi Syslog Server Setup window.

3.13.5 Use dd-mm-yyyy date format (non US format)

Normally Kiwi Syslog Server uses the US date format of mm-dd-yyyy

If you want to use the New Zealand (Kiwi), Australian, or European date format of dd-mm-yyyy then check this box.

The date format will apply only to the display. The date format of the log file is set by the chosen logging format.

3.13.6 Show messages per hour in title bar

This displays the number of messages received in an hour in the title bar, when it is active.

3.13.7 Blink System Tray Icon when receiving messages

A visual aid to show that messages are being received whilst minimized to the System Tray.

The icon alternates between blue and green on every received message

3.13.8 Word wrap

Wrap the message text for messages received which are longer than the Syslog window size, so that the content can be read without scrolling across.

3.13.9 Adjust column widths automatically

As messages arrive the column sizes are adjusted automatically to fit the text.

This adds to the readability of the text. If you need to see more of the message text you could lower the font size. To do this, use the **View | Choose font** menu option.

3.14 Enabling SSL

The steps to enable SSL are explained here in detail. After installation of Kiwi Web access, please

©2014 SolarWinds, Inc.

Create a Self-Signed Server Certificate and follow the below steps

1. Open UltiDev Web App Explorer.

2. Click to register new site or application with UltiDev Web Server.

3. Select the option ‘ASP.NET web Application’ and proceed.

4. Select the option ‘ASP.NET 2.0, 3.0 or 3.5’ and proceed.

5. Select the second option since we need to load ‘native 32 bit components’ and proceed.

6. Select the option .‘LOCAL SYSTEM’ and proceed.

7. Browse for default document.

8. Select Gateway.aspx file from \\SolarWinds\Kiwi Syslog Web Access\html in installed location.

9. Change the application name to ‘Syslogd’.

10. Remove the virtual directory default entry and make it as empty.

11. Remove the existing HTTP Listen Address for Kiwi Web Access.

12. Add HTPS/SSL Listen Address.

13. Select the created certificate .

14. Choose the port by .‘Find Free Port’ option or enter your own port and proceed.

15. Select the option ‘Anonymous’.

16. Click Finish.

17. Created host will be listed in the left side panel.

18. This can be clicking browse application tab.

19. Your host will be accessed with https.

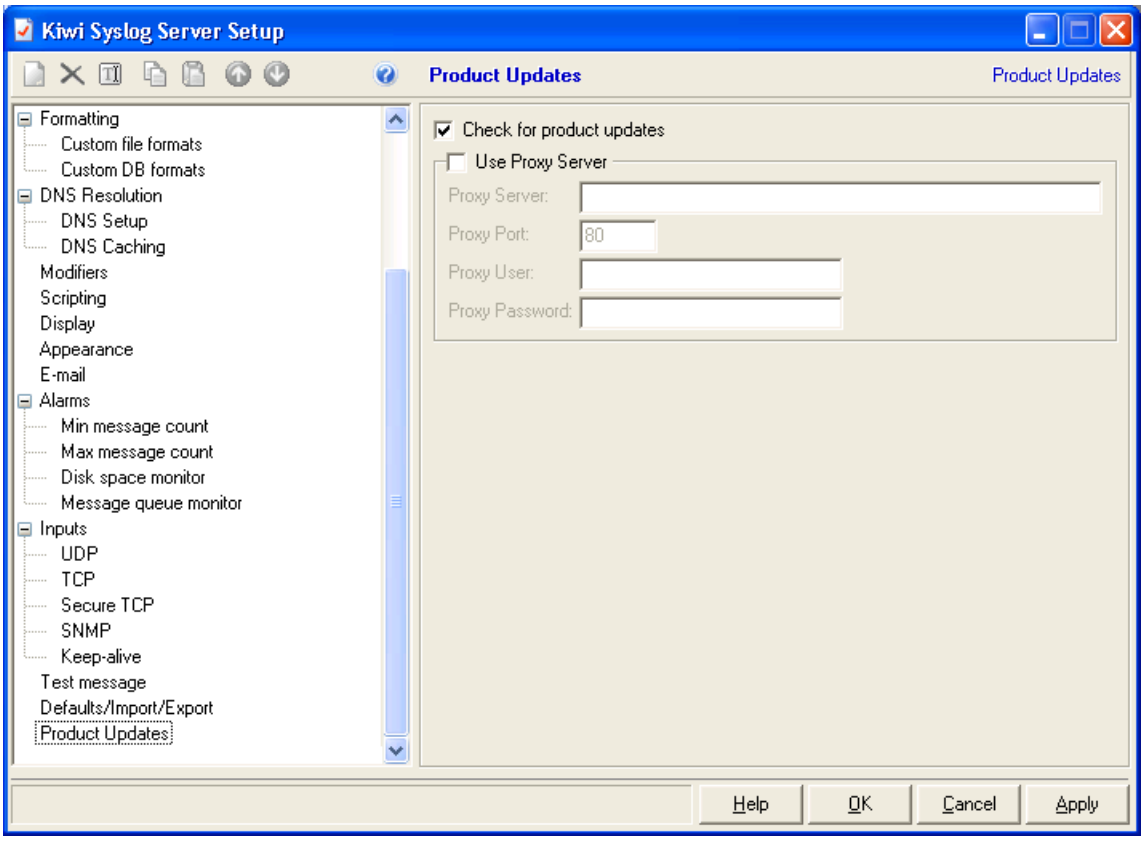
http://knowledgebase.solarwinds.com/kb/questions/4862/How+to+Enable+SSL+support+for+Kiwi+Web+Access

3.15 Setup - Product Updates

Kiwi Syslog Server will periodically communicate with the SolarWinds website, in order to obtain information related to available product updates.

In case if the Server falls behind a Proxy Server, the Proxy server settings should be configured by checking "Use Proxy Server" as given in the picture below:

©2014 SolarWinds, Inc.



This default behavior can be disabled, by unchecking the "Check for product updates" setting.

3.16 How the Test button works

When the "Test" button is pressed it passes a syslog message to your filter or action using the fields on the "Test Setup" page.

When testing a filter. If the values for the field that you are filtering against do not match then it will show a red cross beside the "Test" button.

To fix this you need to press the "Test Setup" button beside the "Test" button on the filter form. This will open up the "Test Message" form which shows you all the values that you are passing to the filter or action when you press the "Test" button.

To have the "Test" button show a green tick you will need to change whatever field that you are testing against to match what would cause the filter to become true. Just change the value in the matching fields input box on the "Test Message" page to match the value that you are filtering for. You should now be able to press the "Test" button and have it display a green tick.

When testing an action the fields on the "Test Message" page are sent to the action in the form of a syslog message. If the action is successful then you will receive a green tick. If the action failed for any reason you will receive a red cross.

For testing your filter and action setup we recommend that you download a copy of Kiwi SyslogGen from http://www.kiwisyslog.com/downloads. This program allows you to send test syslog messages to Kiwi Syslog Server
which is the ideal way to test your rules.

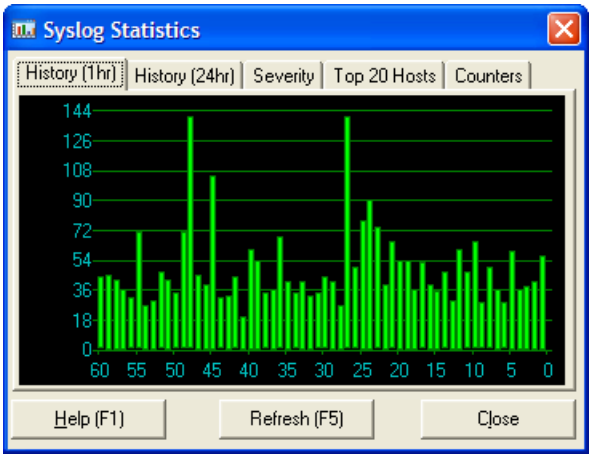
©2014 SolarWinds, Inc.

4 The Syslog statistics window

4.1 The Syslog statistics window

From the Kiwi Syslog Server main display, choose the **View | View Syslog Statistics** menu or press Ctrl-S.

This will present the Syslog Statistics window.



Syslog Statistics are updated every 10 seconds. Pressing the *Refresh* button or F5 will cause the statistics to be recalculated and displayed immediately.

4.2 1 Hour history

Displays a bar chart of the last 60 minutes worth of traffic. Each bar in the chart shows the number of messages received during that minute. The chart scrolls from right to left. The left side of the chart shows traffic an hour ago, the right most bar (0) indicates the current traffic.

4.3 24 Hour history

Displays a bar chart of the last 24 hours worth of traffic. Each bar in the chart shows the number of messages received during that hour. The chart scrolls from right to left. The left side of the chart shows traffic 24 hours ago, the right most bar (0) indicates the current traffic.

4.4 Severity

The Severity table shows the breakdown of messages by priority level. 0-Emergency has the highest severity all the way down to 7-Debug type messages which are used for troubleshooting.

The message count and percentage of total traffic is shown in the table.

Click on any header to sort the table by that column. Click again to reverse the sort order.

©2014 SolarWinds, Inc.

4.5 Top 20 Hosts

The hosts table shows the breakdown of messages by sending host. The message count per host and percentage of total traffic is shown in the table.

Click on any header to sort the table by that column. Click again to reverse the sort order.

If a particular host is generating a lot of the traffic or the pattern changes, it could indicate a problem on that device.

4.6 Counters

The counters show the traffic and error statistics for the program. The average messages counter can help you set maximum thresholds for alarm notification and to get a feel for the amount of syslog traffic being generated.

Some counters show values for the last 24 hour period (from the current time of display). Others show values since Midnight (0:00).

The hourly intervals start at 0 from the time the program started rather than being related to the actual HH:MM:SS time. To see how long the program has been running, check the Program uptime counter.

Messages - Total:
This counter value shows the number of messages received since the program was started. To reset this value, you must restart the program or service.

Messages - Last hour:
This counter value shows the number of messages received in the last full hour. The hours are counted from the time the program was started. If the program has been running less than 60 minutes, this value will be 0. Once an hour has completed, the value will contain the total number of messages received for the last hour. The value will remain constant until the next hour rolls over.

Messages - This hour:
This counter value shows the number of messages received since the last hour roll over. The hours are counted from the time the program was started. This value will be reset to 0 each hour and will be incremented as each new message arrives.

Messages - Last 24 hours:
This counter value shows the number of messages received during the last 24 hour period (from the current time of display). This value is a rolling count of the messages received in the last 23 hours, plus the messages received in the last hour. At the turn of each hour, the value will drop as the last 23 hours are shuffled. The value will then build again as more messages are received during the current hour. The value is represented by the formula: LastHours(1 to 23) + messages this hour.

Messages - Average:
This counter value shows the average number of messages received per hour over the last 24 hour period. At the turn of each hour, the value will be recalculated as the last 24 hours are shuffled. After the first hour has elapsed, the value is only updated once per hour.

Messages - Forwarded:
This counter value shows the number of messages that have been forwarded to other syslog collectors or relays using the "Forward message" action. This counter is reset immediately after the daily stats have been sent out. The daily stats are usually sent at midnight, so the value you see will be the count since midnight.

Messages - logged to disk:
This counter value shows the number of messages that have been logged to disk using the "Log to file" action. This counter is reset immediately after the daily stats have been sent out. The daily stats are usually sent at midnight, so the value you see will be the count since midnight.

Errors - logged to disk:
This counter value shows the number of internal program errors that have been logged to disk. Errors are

©2014 SolarWinds, Inc.

usually caused when the log file can not be accessed or if an internal program error has occurred. This counter is reset immediately after the daily stats have been sent out. The daily stats are usually sent at midnight, so the value you see will be the count since midnight. If the value is not 0, please check the error log (View | Error log menu) for more details on the error.

Disk space remaining:
This counter value shows the amount of disk space remaining in MB. The drive being watched can be set from the Alarms | Disk space monitor setup option. By default, drive C: is monitored.

CustomStats:
The custom statistics values can be viewed from the Counters tab. These values can be modified by using the "Run Script" action. These statistics counters can be used to count and display any values you like.

To set the counter name to something more meaningful, use the Scripting setup option to set the counter name and initial values.

5 Kiwi Syslog Server Service Edition

5.1 Kiwi Syslog Server Service requirements

Requirements for installing Kiwi Syslog Server as a Windows Service

Windows XP Professional, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 or Windows Server 2008 R2

Microsoft Internet Explorer Version 5.x or higher

Minimum of 256Mbytes RAM

Minimum screen resolution of 800 x 600 in 256 colors

5.2 Installing Kiwi Syslog Server as a Service

Care must be taken when installing Kiwi Syslog Server as an NT Service.

Before installing a new version, you must first ensure that any existing version of the service has been stopped and uninstalled.

To install, simply double click the installation .exe file to run the installation.

When the setup program is run, the Kiwi Syslog Server Service Manager is installed.

When the install is complete, run the program from the start menu and you will see the main syslog Server screen.

The **Manage** Menu is used to control the NT Service.

To install the service, use the **Manage | Install the Syslogd Service** menu.

A message will be displayed to indicate if the installation was successful or not.

If the install failed, it could be because there is already another version installed.

To install the service **manually** from the Start | Run menu or command line, you need to type…

C:\Program files\Syslogd\Syslogd_Service.exe –install

To uninstall the service manually use the –uninstall switch

C:\Program files\Syslogd\Syslogd_Service.exe –uninstall

©2014 SolarWinds, Inc.

Once the Service is installed, you need to start it.

The service will automatically start the next time NT is rebooted, but you can start it manually via the **Manage | Start the Syslogd service** menu. Alternatively you can press **Ctrl + F3**

To **start** the service manually from the command line, type the following…

C:\>net start "Kiwi Syslog Server"

The lines below should be displayed…
The Kiwi Syslog Server service is starting.
The Kiwi Syslog Server service was started successfully.

To **stop** the service manually from the command line, type the following…

C:\>net stop "Kiwi Syslog Server"

The lines below should be displayed…
The Kiwi Syslog Server service is stopping.
The Kiwi Syslog Server service was stopped successfully.

Note: it will take about 20 seconds for the Service to stop.

To control and configure NT services you can use the Services applet in the NT Control Panel.

Once the service is installed and started you can test its operation by getting the Service manager to 'Ping' the service.
To do this, use the **Manage | Ping the Syslogd service** menu.

To test that the Service is receiving Syslog messages, press the **Ctrl + T** key to send a test message to the localhost.

You should see a message appear on the display like this:

Kiwi Syslog Server - Test message number 0001

If no message is seen, make sure that there is an action for 'Display' by using the **File | Setup** menu option.

5.3 Managing the service edition

From the Kiwi Syslog Server Service Manager you can manage and control the Syslogd service.

Syslog service can be started by **Manage --> Start the Syslogd service** or by pressing **Ctrl+F1** key.

Syslog service can be stopped by **Manage --> Stop the Syslogd service** or by pressing **Ctrl+F2** key.

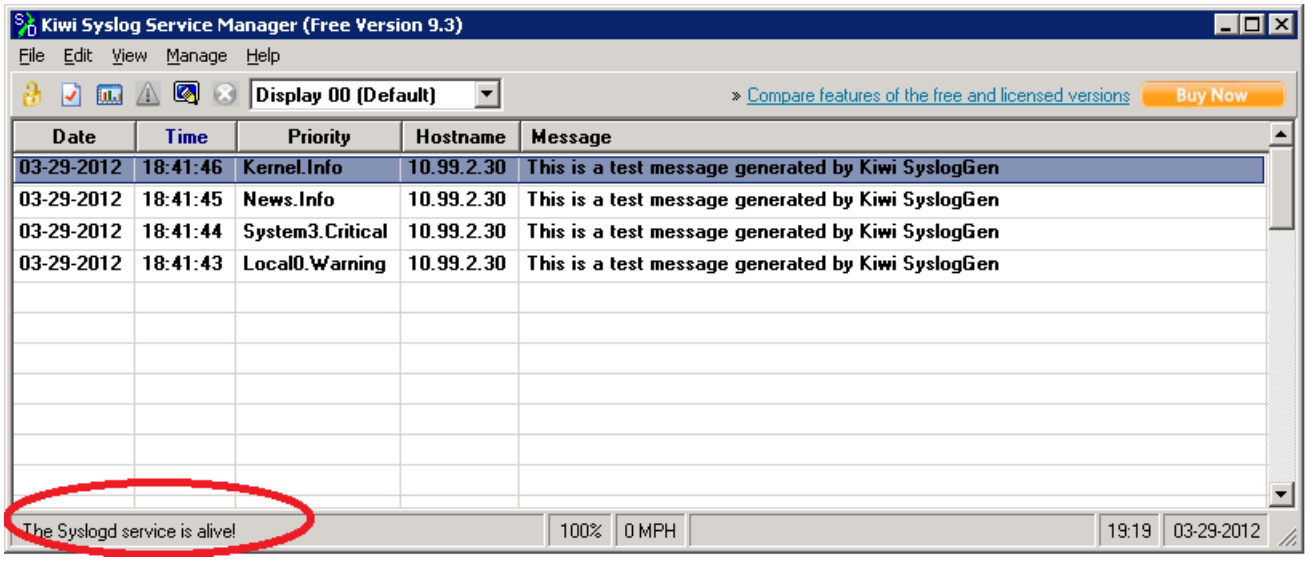
Syslog service can be pinged by **Manage --> Ping the Syslogd service** or by pressing **Ctrl+F3** key. The status is displayed in the status bar of the application window.

Syslog service status can be verified by **Manage --> Show the Syslogd service state** or by pressing **Ctrl+F4** key. The status is displayed in the status bar of the application window.

Syslog service version can be viewed by **Manage --> Debug --> Display the service version.** The version information is displayed in the status bar.

Diagnostic information can be viewed by **Manage --> Debug --> Get diagnostic information.** The information is loaded in notepad.

©2014 SolarWinds, Inc.



Enable Debug in Service mode

By default the debug mode is disabled. To enable it click **Manage --> Debug --> Enable Service Debug Mode**. When the debug mode is enabled, the syslog messages are logged in **<Program Files>\Syslogd\Syslogd-debug.txt** file.

Disable Debug in Service mode

To disable the debug mode, restart the service.

5.4 Troubleshooting the Service edition

What to check when things are not working -

1). Can you "**Ping**" the Service?
Use the **Manage | Ping Syslogd service** menu

2). Can you send a test message to yourself and receive it OK?
Press **Ctrl + T** from the Syslog Service Manager to send a test message to localhost.

3). Try sending messages from the local machine.

Download a copy of Kiwi Syslog Message Generator from: www.kiwisyslog.com.

5.5 Upgrading to a new version of Kiwi Syslog Server NT Service

5.5.1 Upgrading to a new version of Kiwi Syslog Server NT Service

When a new version of Kiwi Syslog Server is released it is a good idea to upgrade to ensure you get the latest features and bug fixes.

The latest version of Kiwi Syslog Server can always be obtained from www.kiwisyslog.com

It is important to remove the existing version before upgrading.

©2014 SolarWinds, Inc.

5.5.2 Steps to remove existing version

1). Using the Service Manager, stop the service
Use **Manage | Stop the Syslogd service** menu.

2). Using the Service Manager, uninstall the service
Use the **Manage | Uninstall the Syslogd service** menu.

3). Close the Service manager program.

4). Uninstall the application with the Windows **Control Panel | Add / Remove programs** applet.

5.5.3 Steps to installing the new version

1). Download the latest NT service version of Kiwi Syslog Server.

2). Install the new version

3). Run the Syslogd Service Manager from the Start menu
Start | Programs | Kiwi Syslog Server | Kiwi Syslog Server Service Manager

4). Choose yes or no to using the default "Action" settings.
Choose No if you want to keep your old settings.

5). Install the Syslogd Service.
Use the **Manage | Install the Syslogd service** menu.

6). Start the Syslogd Service.
Use the **Manage | Start the Syslogd service** menu.

7). Check the new installation by 'pinging' the service.
Use the **Manage | Ping the Syslog service** menu.

8). Check that messages can be received correctly. Press **Ctrl + T** to send a test message to localhost.

6 Configuring Syslog enabled devices

Guides for configuring network hardware to use syslog messaging are listed in this section.

If you know of other devices which can send Syslog messages, please provide details to http://www.kiwisyslog.com/support/ and we will be sure to add the information into the next release.

6.1 Configuring Log Forwarder to capture Windows Event logs

If you are wanting to collect information from Windows event logs, we recommend Kiwi Log Forwarder for Windows, which is freely available within your Kiwi Syslog download zip package.

You will need to ensure that the port you have Kiwi Syslog Server listening on (514) , is not being blocked by your Windows firewall.

If you have any issues receiving syslog messages, have a look at the following article in our Knowledge Base:
http://www.kiwisyslog.com/kb/info:-kiwi-syslog-Server-is-not-receiving-messages/

For more information: http://www.kiwicattools.com/downloads/logforwarder/LogForwarder.pdf

©2014 SolarWinds, Inc.

6.2 Configuring a 3Com NetServer

To enable the sending of Syslog messages from a NetServer 8 or NetServer 16…

Connect to the NetServer via Telnet or Console cable
Use the Add Syslog command with the following syntax…

ADD SYSLOG <IP Address> LOGLEVEL <*logging level*>

The IP address is the address of the PC running Kiwi Syslog Server

The ***Logging level*** can be any one of the following

COMMON
CRITICAL
DEBUG
UNUSUAL
VERBOSE

For example…
ADD SYSLOG 10.0.10.23 LOGLEVEL VERBOSE

To confirm the Syslog entry has been added use the **LIST SYSLOGS** command to show the entries.

The output should be something like…

```
Console Prompt>LIST SYSLOGS
SYSLOG SINKS
SysLog          Log Level Msg Count
192.168.203.203  COMMON    507
192.168.203.230  COMMON    4551
```

Remember to do a **SAVE ALL** command to store the new details to NVRAM.

6.3 Configuring a 3Com Total Control Chassis

To enable the sending of Syslog messages from a Total Control Chassis…

Connect to the HiPer Access Router Card (HiPer ARC) via Telnet or Console cable
Use the Add Syslog command with the following syntax…

ADD SYSLOG <IP Address> FACILITY <*Facility*> LOGLEVEL <*logging level*>

The IP address is the address of the PC running Kiwi Syslog Server

The ***Facility*** can be any one of the following…

LOG_AUTH
LOG_LOCAL0
LOG_LOCAL1
LOG_LOCAL2
LOG_LOCAL3
LOG_LOCAL4
LOG_LOCAL5
LOG_LOCAL6
LOG_LOCAL7

The ***Logging level*** can be any one of the following

COMMON
CRITICAL

©2014 SolarWinds, Inc.

UNUSUAL
VERBOSE

For example…
ADD SYSLOG 10.0.10.23 FACILITY LOG_LOCAL7 LOGLEVEL VERBOSE

To confirm the Syslog entry has been added use the **LIST SYSLOGS** command to show the entries.

The output should be something like…

```
Console Prompt>LIST SYSLOGS
SYSLOG SINKS
SysLog          Log Level Msg Count Facility
192.168.203.203  COMMON    507       LOG_LOCAL7
192.168.203.230  COMMON    4551       LOG_AUTH
```

Remember to do a **SAVE ALL** command to store the new details to NVRAM

6.4 Configuring an Alliant Cellular Gateway

Thanks to Mark Hamilton for this information.

For more information on the Alliant Cellular Gateway, please visit:
http://www.alliantnetworks.com/

Enabling and filtering SYSLOG messages

By default, the sending of SYSLOG messages is disabled. After the SYSLOG server is set up, you must enable SYSLOG messages. You may also want to set message filtering, which limits the type of messages that are logged.

You need the following information:
- The IP address of the SYSLOG server.
- The administrative password of the gateway. (The default password is: public)
- If you plan to use the Telnet CLI, the IP address of the gateway.
- If you plan to use the serial CLI, connect to the gateway with a serial cable.

Use the following procedure to enable and filter SYSLOG messages:
1. Access the CLI using Serial or Telnet
2. Enter the following commands:

```
CG> login <password>
CG# configure system
CG(sys)# configure syslog
CG(sys-sys)# set status on
```

3. To see the effect of this command, use the show log command to display the current SYSLOG configuration. The following is an example of show log output:

```
SYSLOG messages are enabled
First SYSLOG server's IP address: 10.0.1.2
Second SYSLOG server's IP address: 0.0.0.0
Severity threshold 6
CG(sys)#
```

4. It can be useful to filter out some messages based on their severity. The following example filters out all messages that are less severe than error, so that the log contains only error events (severity value of 3) and events more severe than error.

```
CG> login <password>
CG# configure system
Maintenance Onboard logging
CG(sys)# configure syslog
CG(sys-sys)# set status on
CG(sys-sys)# set severity 3
```

©2014 SolarWinds, Inc.

6.5 Configuring an Allied Telesyn router

Information kindly supplied by Taylor Wilkens from Allied Telesyn New Zealand.

You can create a log output definition which will send messages to a syslog Server. The command to create the output definition is:

```
create log output=1 destination=syslog server=address
```

where *address* is the IP address of the host running the Kiwi Syslog Server.

Having created this output definition, you must add filters to the definition to tell it what sort of log messages to send. For example, if you want to send messages that are generated by the IP traffic filters, the command would be:

```
add log output=1 type=IPFILT
```

Or, if you want to log the durations of all ISDN calls, the command would be:

```
add log output=1 mod=ICC type=CALL subtype=DOWN
```

To show all the events, use the filter:

```
add log output=1 filter=1 all
```

To log only interface events like the Frame going up/down and lmi states etc...

```
add log output=1 filter=1 type=vint
add log output=1 filter=1 type=dlink
```

For more information on the logging commands available, please visit:
http://www.alliedtelesyn.co.nz/documentation/arrouter/241/pdf/log.pdf

6.6 Configuring an Arris Cable Modem Termination System

Thank you to Dale Hutchinson for providing the following information...

Here are the console commands for using Kiwi Syslog Server with Arris CMTS1000 DOCSIS 1.0 Cable Modem Termination System and our CMTS1500 DOCSIS 1.1 Cable Modem Termination System -

```
manage
event-level
syslog-ip-addr xxx.xxx.xxx.xxx    //IP address of your Kiwi Syslog Server server
admin-status-of-throttle unconstrained
```

6.7 Configuring an Extreme Summit switch

Telnet to the switch or connect via the console and login as the administrator (admin) level user.

To add a syslog server entry to the config, use the following syntax:

Configure syslog add <IP address of syslog server> <Facility name>

E.g. Configure syslog add 192.168.1.1 local0

To delete a syslog server entry from the config, use the following syntax:

Configure syslog delete <IP address of syslog server> <Facility name>

©2014 SolarWinds, Inc.

E.g. Configure syslog delete 192.168.1.1 local0

To enable logging of the CLI configuration commands, use the following command.

enable cli-config-logging

6.8 Configuring a Barracuda Spam Firewall

This information is a summary from the Barracuda Spam Firewall documentation.

For more details:
http://www.barracudanetworks.com/ns/support/documentation.php

What is Barracuda Syslog and how to get it?
The Barracuda uses syslog messages as a means of logging what happens to each message as the Barracuda Spam Firewall processes the message. The syslog messages are sent to a text file on the Spam Firewall, as well as to a remote server configurable by the Barracuda administrator. With the syslog messages, the administrator can perform analysis for either reporting purposes, or for a better understanding of the message processing on the Barracuda Spam Firewall.

To enable syslog, navigate to Advanced->Syslog in the web GUI and enter the IP address of the syslog server you wish to direct the messages.

Note: There is a section for web GUI syslog notifications available on the same screen in the web GUI – that format is not covered in this document.

Syslog messages are sent UDP to the standard syslog port of 514. If there are any firewalls between the Barracuda and the server receiving the syslog messages, then be sure that port 514 is open on the firewalls. The syslog messages will arrive on the mail facility at the debug priority level. As the barracuda uses the syslog messages internally for its own message logging it is not possible to change the facility, or the priority level.

Barracuda Syslog Format

The Barracuda Spam Firewall will send syslog messages in the following format. Whenever an action is taken on a message it is logged with syslog. A message sent to multiple recipients will be logged separately for each recipient. Please be aware that the various syslog implementations may not display the messages in this exact format. However, the sections should still be present in the syslog lines. The following is the main part of the syslog line.

```
Timestamp Host Barracuda Process Client IP Message ID Start End Service Info
Sep 8 17:38:48 dev1 inbound/pass1[27564]: XX.XX.XX.XX 1126226282-27564-2-0 1126226286
1126226328 RECV [. . . . .]
```

6.9 Configuring a Bay Networks device

This information is copied from the Bay Networks web page at:

http://support.baynetworks.com/library/tpubs/html/switches/bstream/115412A/MARKER-2-455

Configuring Syslog on the Router
You can use Technician Interface commands to configure syslog on a router. You configure syslog as a sequence of *tasks,* where some tasks include one or more numbered *steps*.
The following is an overview of the tasks required to configure syslog on a router:
1. Using the console attached to the router, or using a TELNET connection to the router, open a Technician Interface session.
2. *Define a slot mask (a slot map) for loading Syslog on the router.*
3. *Create the syslog entity on the router.*
4. *Configure syslog global attributes.*
5. *Add a remote host to the syslog host table.*
6. *Add an entity filter to the syslog entity filter table.*

©2014 SolarWinds, Inc.

7. *Return to Task 5 to add another remote host or return to task 6 to add another entity filter for the remote host; otherwise go to Task 8.*
8. *Save to a file on an NVFS volume the syslog additions to your configuration.*
9. *Log out of the Technician Interface session.*
The paragraphs following in this section describe the syslog configuration sequence in greater detail (to the task *and* step level).
Following the configuration procedure, this chapter provides an example of syslog configuration, plus definitions of syslog attributes you use during configuration.

Task 1: Logging In to the Router's Technician Interface
For information on how to open a Technician Interface session with a Bay Networks router, refer to Chapter 1.

Task 2: Defining a Slot Mask for Syslog on the Router
Before creating the syslog entity on the router, define a slot mask for syslog. The slot mask identifies the slots on which the system will load and run the syslog entity. At the Technician Interface prompt, enter
$: set wfProtocols.wfSYSLLoad.0 0x7FFE0000;commit
This command enables syslog to run on all slots, regardless of router model.
Next, create the syslog entity on the router.

Task 3: Creating Syslog on the Router
Create the syslog entity in the router configuration, as follows:
set wfSyslog.wfSyslogDelete.0 **1;commit**
This also *enables* syslog on the router. (The system sets the attribute wfSyslogDisable, OID = 1.3.6.1.4.1.18.3.3.2.15.1.2, in the syslog base record to a value of 1.)
Next, configure the syslog global attributes.

Task 4: Configuring Syslog Global Attributes
Once you create and enable syslog on the router, you can accept the default values for the *wfSyslogMaxHosts* and *wfSyslogPollTimer* attributes, or you can configure a customized value for either attribute. If you want to accept default values for the syslog global attributes, go to Task 5; otherwise, perform the following steps:
1. Configure the maximum number of active hosts served by syslog on the router:
$: set wfSyslog.wfSyslogMaxHosts.0 *<1 - 10>;commit*
The default setting for **wfSyslogMaxHosts** is 5 hosts. You can add to the syslog host table more entries than the configured maximum, but syslog forwards messages only to the first "n" *active* hosts, where n = the current value of **wfSyslogMaxHosts**.
2. Configure the interval (in seconds) between syslog polling cycles on the router:
$: set wfSyslog.wfSyslogPollTimer.0 *<5 - 610000>;commit*
The default setting for **wfSyslogPollTimer** is 5 seconds.
Next, add a remote host to the syslog host table.

Task 5: Adding a Remote Host to the Syslog Host Table
You must define any remote hosts that you want to receive syslog (event) messages from routers in your network.
If this is the first host you are adding to the syslog host table, go to Step 1. Otherwise, you may want to first obtain a list of hosts already configured on the router. To list existing entries in the syslog host table, enter the following command at the Technician Interface prompt:
list -i wfSyslogHostEntry
The list includes the instance IDs (in this case, the IP addresses) of all remote hosts currently defined in the syslog host table.
1. Add a new host entry to the syslog host table, as follows:
$: set wfSyslogHostTable.wfSyslogHostDelete.<*host_IP_address*> *1*
$: commit
This entry informs syslog of a remote host at the destination IP address that you specified.
If you want to accept the default settings for host attributes **wfSyslogHostLogFacility** (184 = Local7) and **wfSyslogHostTimeSeqEnable**
(2 = disabled), go to Task 6. Otherwise, continue with Step 2 to configure a customized setting for either attribute.
2. **To define the UNIX system facility you want to receive syslog messages** from the router, enter the following:
$: set wfSyslogHostTable.wfSyslogHostLogFacility.<*host_IP_address*> <*128*|*136*|*144*|*152*|*160*|*168*|*176*|*184*> ;commit

128 = local0 160 = local4
136 = local1 168 = local5
144 = local2 176 = local6
152 = local3 184 = local7

©2014 SolarWinds, Inc.

3. **To optionally enable syslog message time sequencing** for the remote host, enter the following:
$: set wfSyslogHostTable.wfSyslogHostTImeSeqEnable.
<host_IP_address> 1;commit

Note: Only hosts represented by entries that are ENABLED (wfSyslogHostDisable =*1*) and have an operational state of ACTIVE (wfSyslogHostOperState = *1*) receive messages from syslog on the router.
Next, add an entity filter for the host entry you just added.

Task 6: Adding an Entity Filter for a Remote Host
Once you define a host in the syslog host table, add (define) an entity-specific message filter for the host.
If this is not the first filter for a given entity and remote host pair, first obtain a list of filter instances, as follows:
list -i wfSyslogEntFltrEntry
From the resulting list of instance IDs (of the form <*host_IP_address*>.<*entity_code*>.<*filter_index*>), determine the next <*filter_index*> number available to assign to a new filter, for a given <*host_IP_address*>.<*entity_code*> pair. The number you assign to the new filter will have a value of +1 higher than the highest <*filter_index*> in the list.
Now proceed to Step 1.
1. Create a new filter for the desired entity and remote host pair by first creating an entry in the syslog entity filter table, as follows:
$: set WfSyslogEntityFilterTable.WfSyslogEntFltrDelete. *<host_IP_address>.<entity_code>.<filter_index> 1;commit*
<*host_IP_address*> is the IP address of the desired remote host (a management workstation).
<*entity_code*> identifies the software entity for which you want syslog to forward event messages to the remote host at the <*host_IP_address*>.
<*filter_index*> is the next available index number you can assign to a filter for the desired entity and remote host pair.
2. After you create an entity filter for a specific host, define

- An event number (or range) and a slot number (or range)

or:

- A severity mask and a slot number (or range)

Note: The filter remains inactive until you define the event and slot number(s), or the severity mask and slot number(s).
Set entity filter attributes, as follows:
a. **To define by event number(s)** the event messages you want syslog to select and forward to a specific remote host:
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtLowBnd.
<host_IP_address>.<entity_code>.<filter_index> <0 - 255>
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtUppBnd.
<host_IP_address>.<entity_code>.<filter_index> <0 - 255>
$: commit
If you do not want to define filtering by event number(s), accept the default values for event number lower bound (0) and upper bound (255). (Go to Step 2b.) Accepting these default values causes syslog to use only the severity and slot mask criteria for selecting and forwarding messages.
b. Define a severity mask *only* if you did not already define an event number (or event number range). If you defined an event number or number range, syslog ignores any severity mask for this filter.
To define by severity levels the event messages you want syslog to select and forward to a specific remote host, enter the following:
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrSevMask.
<host_IP_address>.<entity_code>.<filter_index> "<fwitd>"
$: commit
c. **To also define by slot number(s)** the event messages you want syslog to select and forward to a specific remote host, enter the following:
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotLowBnd.
<host_IP_address>.<entity_code>.<filter_index> <0 - 14>
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotLowUpp.
<host_IP_address>.<entity_code>.<filter_index> <0 - 14>
$: commit

Note: Although the valid range for the slot lower and upper boundaries is 0 to 14, specify only values within the range of actual slot numbers for the model of router you are configuring. Otherwise, the filter will not transition to an active state.
3. **Define how router event message severity levels and UNIX system error levels map to one another.**
In most cases, you accept the default mapping and go to Task 7. Otherwise, continue with the following

©2014 SolarWinds, Inc.

instructions to customize the message mapping.
Enter at the Technician Interface prompt the command line(s) appropriate for the message mapping(s) you want to change:
a. Change router FAULT message mapping, as follows:
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrFaultMap.
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
The default value of *wfSyslogEntFltrFaultMap* is 3, mapping router FAULT level messages to UNIX system level CRIT messages.
b. Change router WARNING message mapping, as follows:
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrWarningMap.
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
The default value of *wfSyslogEntFltrWarningMap* is 5, mapping router WARNING level messages to UNIX system level WARNING messages.
Example:
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrWarningMap 5
The example command maps each Warning level router event message to a Warning level UNIX system error message
c. Change router INFO message mapping, as follows:
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrInfoMap.
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
The default value of *wfSyslogEntFltrInfoMap* is 7, mapping router INFO level messages to UNIX system level INFO messages.
d. Change router TRACE message mapping, as follows:
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrTraceMap.
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
The default value of *wfSyslogEntFltrTraceMap* is 3, mapping router TRACE level messages to UNIX system level CRIT messages.
e. Change router DEBUG message mapping, as follows:
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrDebugMap.
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
The default value of *wfSyslogEntFltrDebugMap* is 8, mapping router DEBUG level messages to UNIX system level DEBUG messages.

Task 7: Adding More Hosts or Entity Filters
You can add more hosts or entity filters to your syslog configuration, as follows:
1. If you have finished adding entity filters for this remote host, and you do not want to add another remote host at this time, go to Task 8. Otherwise, continue with Step 2.
2. **If you want to add another entity filter for the same remote host**, return to "Task 6: Adding an Entity Filter for a Remote Host." Otherwise, continue with Step 3.
3. If you want to add another remote host to receive syslog messages from the router, return to "Task 5: Adding a Remote Host to the Syslog Host Table."

Task 8: Saving Your Syslog Configuration on the Router
Save to a file on an NVFS volume the syslog additions to your configuration, as follows:
save config *<vol>:<filename>*

Task 9. Log Out of the Technician Interface
Enter at the Technician Interface command line interface the following command:
$: logout

6.10 Configuring a Bintech access router

Thanks to Torsten Richter for providing this information.

More information available from: http://www.bintec.net/en/index.php

Command Line Interface configuration:

- Telnet to the router
- goal - (input / action)
- switch off the time-out for this session - (type "t 0")
- open setup - (type "setup")
- choose - (select "SYSTEM")
- choose - (select "External System Logging")

©2014 SolarWinds, Inc.

- choose - (select "ADD")
- field: Log Host - (enter the Kiwi Syslog machine [IP or Hostname])
- field: Level - (select with space tab)
- field: facility - (select with space tab)
- field: Type - (select with space tab)
- field: Timestamp - (select with space tab)
- save - (save)
- exit to setup tool/system - (exit)
- exit to setup tool - (save)
- save and exit - (select "Save as boot configuration and exit")

6.11 Configuring a BuffaloTech AirStation Router

This information was obtained from the Buffalo AirStation user manual.

For more information, please refer to the on-line manuals at:
http://www.buffalotech.com/wireless/support/downloads.php?type=manuals

Configuration guide:

- Install the AirStation setup software "AirNavigator" from the CD that comes with the device.
- Connect to the AirStation you want to manage.
- From the left hand menu list, choose the "Management" item.
- From the tree list, click the "Syslog Transmitting" item.
- Select "Use" to enable the sending of syslog messages.
- Enter the IP address of the machine running Kiwi Syslog Server.
- Select Error and/or Notify to specify the level of the messages to be logged to the remote syslog Server.
- From the Log information item, select the specific reports to be sent to the syslog Server.

6.12 Configuring a Checkpoint FW-1 firewall

This information is from a post on the LogAnalysis forum.

http://lists.jammed.com/loganalysis/2001/09/0006.html

This applies to the UNIX version of Firewall-1.

You can use the Checkpoint command $FWDIR/bin/fw log -f to convert from the Checkpoint proprietary log format to plain text, and then the UNIX "logger" utility to get the plain text into syslog. However, be aware that the "fw log -f" converts *everything* in the network connections log to text -- so every time you stop and restart the firewall, you will blat out everything in the connections log back into syslog. We recommend to our customers that they perform a log rotation on the network connection logs every time they restart the system - that way there are no duplicates.

Also, there's a lot of valuable information about the health of the firewall that doesn't show up in either the network connection logs or the standard host OS syslog, especially if you use the GUI for firewall management (this includes things like administrators logging into and out of the GUI, and pushing new policies to the firewalls). If you want to capture that info in your central log server, you need to do the "logger" trick described above with the file $FWDIR/log/cpmgmt.aud.

6.13 Configuring a Cisco 3000 series VPN concentrator

The Cisco VPN 3000 Series concentrators support the sending of Syslog message and SNMP traps. Kiwi Syslog Server can receive either form of messaging.

Information on the setup procedures can be found on the Cisco web site at the address below...

Cisco VPN setup information

©2014 SolarWinds, Inc.

6.14 Configuring a Cisco Catalyst switch

This will work on the Cisco **Catalyst switches that use the 'set' command type CLI**. This includes the old 2900 series or 5000 series switches.

Telnet to the switch or connect via the console and enter into enable mode.

Enter the following commands from the enable prompt on the switch.

Set logging enable

Set logging level all 7 default (this will set all facilities with a level of debug)

Set logging [IP Address or Hostname of machine running Kiwi Syslog Server]

For the new **Catalyst switches that use the IOS type CLI** use the following commands.

Logging on

logging trap warnings (or whatever level you want)
Logging Facility Local7 (or any other facility you want to allocate for this router.)
Logging <IP Address or Hostname of machine running Kiwi Syslog Server>

More logging information for the Catalyst 6000 can be found at:
www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_5/cnfg_gd/logging.htm

And also at:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_system_message_guide_chapter09186a008007e784.html

6.15 Configuring a Cisco PIX

To enable the sending of Syslog messages from a Cisco PIX Firewall...

Visit the Cisco web site at:
www.cisco.com/warp/public/110/pixsyslog.html

Information on the PIX log messages can be found at:

www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/63syslog/pixemsgs.htm

www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/syslog/pixemsgs.htm

or: www.cisco.com/cgi-bin/Support/Errordecoder/home.pl

or: www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm

Notes:

If you choose to send syslog messages from the PIX using the TCP protocol, you may want to also add the following command:

```
logging permit-hostdown
```

This will stop the PIX from not forwarding traffic if the syslog server becomes unavailable for some reason. Without this command the PIX will stop forwarding any traffic as soon as the syslog server TCP connection can not be established.

©2014 SolarWinds, Inc.

More information on TCP inputs and configuring a PIX for use with Kiwi Syslog.

Information on sending SNMP traps or Syslog messages from your PIX via a secure VPN tunnel can be found at:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a0080094469.shtml

6.16 Configuring a Cisco Router

Telnet to the router or connect via the console and enter into enable mode.

Enter the following commands from the enable prompt on the router.

Config term

Logging on

Logging Facility Local7 (or any other facility you want to allocate for this router.)

Logging [IP Address or Hostname of machine running Kiwi Syslog Server]

End

Another useful command is **logging source-interface** which first appeared in IOS v11.2. According to Cisco, a syslog message contains the IP address of the interface it uses to leave the router. The logging source-interface command specifies that syslog packets contain the IP address of a particular interface, regardless of which interface the packet uses to exit the router.

* The logging source-interface command MUST be used on some versions of IOS due to a bug. If the command is not used the Syslog messages sent have an invalid UDP checksum and are dropped by Winsock before the Kiwi Syslog Server gets to see them.

More information on Cisco logging commands can be found on the Cisco web site at:
www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/cs/csprtf/csprtf4/cstroubl.htm

6.17 Configuring a Cisco Wireless device (Aironet)

Telnet to the wireless access point or connect via the console and enter into enable mode.

Enter the following commands from the enable prompt on the device.

Config terminal

Logging on

Logging Facility Local7 (or any other facility you want to allocate for this device.)

Logging [IP Address or Hostname of machine running Kiwi Syslog Server]

End

Another useful command is **logging source-interface** which first appeared in IOS v11.2. According to Cisco, a syslog message contains the IP address of the interface it uses to leave the device. The logging source-interface command specifies that syslog packets contain the IP address of a particular interface, regardless of which interface the packet uses to exit the device.

* The logging source-interface command MUST be used on some versions of IOS due to a bug. If the command is not used the Syslog messages sent have an invalid UDP checksum and are dropped by Winsock before the Kiwi Syslog Server gets to see them.

©2014 SolarWinds, Inc.

More information on Cisco logging commands can be found on the Cisco web site at:
http://www.cisco.com/en/US/products/hw/wireless/ps5279/products_configuration_guide_chapter09186a0080184b04.html#42426

6.18 Configuring a D-Link DFL-700 firewall

Thanks to Geir Aasmoe for providing this information.

For more information please visit: http://support.dlink.com/products/view.asp?productid=DFL%2D700

How to configure your DFL-700 to send syslog messages:

1). Your firewall must be installed and working.
2). Open a web browser to the configuration panel (http://192.168.1.1) and click on the "System" tab from the top navigation bar.
3). Select "Logging" from the left side navigation bar.
4). Check the Syslog check box
5). In the box named "Syslog Server 1", enter the IP address of the computer you have installed Kiwi Syslog Server on.
6). Choose a Syslog facility to use. (Local0 to Local7 is recommended)

6.19 Configuring a DLink DL-840V router

This information has been obtained from the www.dshield.org setup guide.

For more information please visit: http://www.dshield.org/clients/dlinkhelp

1). Your router must be installed and working.
2). Go into the configuration panel (http://192.168.0.1) and click on the "Advanced Settings" tab from the top navigation bar.
3). Select "Administration Settings" from the left side navigation bar.
4). Under 'SYSTEM Log' click on "Enable System Log Function" and enter the IP address of the computer you have installed Kiwi Syslog Server on.

6.20 Configuring a FortiGate Anti-Virus Firewall

This information is a summary from the FortiGate 60 configuration manual.

For more details:
http://docs.forticare.com/fgt/admin/01-28008-0002-20050909_FortiGate-60_Administration_Guide.pdf

You can configure the FortiGate unit from the CLI or web interface to send logs to a remote computer running a syslog server.

Command syntax pattern

```
config log syslogd setting
  set <keyword> <variable>

config log syslogd setting
  unset <keyword>

get log syslogd setting

show log syslogd setting
```

Note: The only command keyword for syslog setting that is not represented in the web based manager is the

©2014 SolarWinds, Inc.

facility keyword.

Examples:

This example shows how to enable logging to a remote syslog server, configure an IP address and port for the server, and set the facility type to user.

```
config log syslogd setting
  set status enable
  set server 220.210.200.190
  set port 514
  set facility user
end
```

This example shows how to display the log setting for logging to a remote syslog server.

```
get log syslogd setting
```

This example shows how to display the configuration for logging to a remote syslog server.

```
show log syslogd setting
```

If the show command returns you to the prompt, the settings are at default.

More information on configuring FortiGate devices running FortiOS V 2.8 can be found here: http://kc.forticare.com/default.asp?id=1580&Lang=1&SID=

6.21 Configuring a FREESCO router/firewall

Information kindly provided by Bill Hely.

Freesco (http://www.freesco.org) is an excellent and well supported single-floppy Linux Firewall/Router O/S that will run on any hardware from a 386sx and up (486 or newer recommended), with 8Mb RAM minimum. Optional HDD installation allows the use of large packages and add-ons, of which there are many available. Freesco is syslog-enabled and requires only one minor file edit to work with the Kiwi Syslog Server.

- Login at the Freesco PC as root
- At the [Linux] prompt, type: edit /boot/etc/syslog.cfg

(The existing syslog.cfg file will be displayed. Note that in this file a TAB is represented as a vertical bar that looks like an upper-case "I" for India.)

- At the very bottom of the existing file, on a line by itself, add the entry: *.*[press the TAB key] @192.168.1.20

(Where the IP address is that of the Windows computer running the Kiwi Syslog Server. Note the "@" symbol immediately preceding the IP address.)

- Press the Enter key to ensure there is a blank line at the very bottom of the file.
- Press Alt-S to save the modified file, then Alt-X to exit the editor.
- Pressing F1 will list other available command keys.
- Restart the Freesco computer to put the changes into effect.

6.22 Configuring a HP JetDirect Printer

The syslog configuration for a HP JetDirect can be set by using the HP JetAdmin program or by using the built-in web interface.

To connect via the web interface, type http://print_server_address:8000 into your web browser.

- Click on the HP logo that appears to enter the main menu
- Choose the printer you want to configure from the list of available devices
- Click on the Configuration link
- Click on the Network link from the left hand menu
- Locate the System Log Server field on the page
- Enter the address of the machine running Kiwi Syslog Server

©2014 SolarWinds, Inc.

- Press the Apply button

6.23 Configuring a Intertex ADSL router

Copied from the online IG Manual ADSL router pages.

Export System Log to external Syslog Server

The syslog client in this product can send contents of its system and the security log to any RFC 3164 compliant syslog server running on a connected computer.
To be able to use the syslog, you need to have a syslog server running on your computer.

To start syslog:

1. Start your web browser and surf to the Internet Gate web pages. (Default IP address: 192.168.0.1.)
2. Log in.
3. Click **Administration** .
4. Enter the IP address of the computer the Kiwi Syslog Server is running on in the **Syslog server** field.
5. Click **Save** .

Now all new events logged on the system log will also be sent to the Kiwi Syslog Server server you have specified.

6.24 Configuring a Linksys firewall

Linksys routers send messages via SNMP so you will need to enable Kiwi Syslog Server to listen for SNMP traps on port 162.

- From the main Kiwi Syslog Server window, select the **File | Setup** menu option
- Locate the **Inputs | SNMP** option on the Kiwi Syslog Server Setup window.
- Check the option "**Listen for SNMP traps**". (The port will be set to 162 by default).

You may also want to check the "**Use Linksys Display Filter...**". This will remove all the PPP and PPPoe messages from the display but not from the log files. This can be quite useful as Linksys firewalls tend to send a lot of these messages.

Please restart the system after making these changes to ensure that Kiwi Syslog Server has been updated correctly.

The LinkSys messages are just text strings encoded into SNMP traps. Although MIB lookups can be done on the OID values, most of the useful information is already included in the text strings.

6.25 Configuring a Linksys wireless VPN router

The new Linksys Wireless-G VPN broadband router is now able to send syslog messages. Previous Linksys firmware used to send alerts via SNMP traps. For information on configuring the SNMP traps, please see the Linksys firewall setup.

- Use a web browser to login to your Linksys router
- Click on the Administration tab
- Click on the Log sub-tab
- Locate the Syslog notification section
- Set the option to Enabled
- Enter a unique Device name to identify the log message, or leave the option set to "Linksys"
- Enter the IP address of the machine running Kiwi Syslog Server (for example: 192.168.1.100)
- Set the types of syslog message you would like sent. Informational is the default. For all messages, set the priority to debug.

©2014 SolarWinds, Inc.

- Under the Alert Log section, check the boxes relating to the alerts you would like to be notified about
- Under the General Log section, check the boxes relating to the messages you would like to be notified about
- To save the changes, click the Save Settings link at the bottom of the page.
-

6.26 Configuring a Lucent router

Ethernet -> Mod Config --> Log...

Syslog=Yes
Log Host=10.23.45.111
Log Facility=Local5

To configure the MAX to send messages to a Syslog Server, open the Log submenu of the Ethernet Profile (Mod Config menu). Then, follow these steps:

Set Syslog to Yes.

If the host is not on the subnet as the MAX, specify the IP address of the host running Kiwi Syslog Server.

The MAX must have a route to that host via RIP or a static route.

See Table 12-3. "System configuration and administration parameters."
"Location Parameters via RIP or a static route."
See Chapter 10. "Configuring the MAX as an IP Router."

Note: Do not configure the MAX to send reports to a Syslog host that can only be reached by a dial-up connection. Doing so will cause the MAX to redial the log host for every logged action, including hang ups.

The Log Facility parameter is used to flag messages from the MAX. After you set a log facility number, you need to configure Kiwi Syslog Server to write all messages containing that facility number to a particular log file (That will be the MAX log file).

Use the Actions tab to set a log file for each facility (or use all.debug to catch all facilities)

For more details on these parameters, see the MAX Reference Guide or visit the Lucent website

6.27 Configuring a Meinberg time server

Thanks to Heiko Gerstung from Meinberg Funkuhren for providing this information.

More information available from: http://www.meinberg.de/english/products/time-server.htm

Meinberg LANTIME timeservers

http://www.meinberg.de/english/products/time-server.htm

Meinberg Linux-based timeservers can be configured to forward their locally created syslog entries to a max. of two remote syslog servers (e.g. Windows-based PCs or servers running Kiwi Syslog Server). This can be setup in the web-administration-interface of the systems like this:

- Log on to the web-interface of your LANTIME
- On the main page, choose "Ethernet"
- Fill in the hostname and/or IP address of your system running Kiwi Syslog Server in the field "Syslog Server 1". (If you operate another syslog server, you can add a second syslog receiver by using the "Syslog Server 2" field)
- Click on "Save Settings" to permanently store this configuration, you will see almost immediately that the first syslog messages are received by Kiwi Syslog Server

An online demo of the web-based configuration interface can be found here:

©2014 SolarWinds, Inc.

http://www.meinberg.de/cgi-bin/main.cgi

(This demo skips the logon process, you are directly starting on the main page mentioned above)

Meinberg GPS receivers equipped with the LAN-XPT module

http://www.meinberg.de/english/products/lanxpt.htm

A number of the Meinberg GPS radio clocks, mostly the GPS167 series (see http://www.meinberg.de/english/products/gps167.htm), can be equipped with an additional network management module, allowing the user to query the status values of the GPS radio clock by using SNMP. Additionally, these modules can send syslog messages to one syslog server and SNMP traps to a max. of three SNMP trap receivers.

In order to configure such a module, you need to:
- logon to the module via Telnet to port 9999

```
*** Meinberg XPT Setup V1.5 ***
MAC address 00204A82B8B8
Software version V0160 (050127) CPK_580_XPTEX
[] XPT Password:********
```

- In the Setup menu, choose option 4 (syslog configuration) by entering a "4" followed by RETURN.

```
Change Setup:
  1 Network configuration
  2 Clock port configuration
  3 SNMP configuration
  4 SYSLOG configuration
  7 factory defaults
  8 exit without save (no reboot)
  9 save and exit

 90 Change password
                          Your choice ?
```

- Answer "Y" (=yes) to the "Use SYSLOG logging?" question

Enter the IP number of the system running Kiwi Syslog Server as it is described in the manual of the radio clock:

```
******** SYSLOG Configuration ********
Use SYSLOG logging?  (Y) ? Y

  Enter IP address for SYSLOG server:(172) .(016) .(003) .(042)
```

Save the settings by entering "9" followed by RETURN, the module (not the whole radio clock) will reboot and starts sending its status messages to the Syslog server

Meinberg Redundant GPS radio clocks
(equipped with the SCU-XPT network management module)

http://www.meinberg.de/english/products/scu_xpt.htm

The SCU-XPT module is used in redundant GPS radio clock systems, where two GPS radio clocks are running and the SCU-XPT module switches the source for the output signals depending on the status of the two clocks. This unit is very similar to the LAN-XPT module in terms of Syslog and SNMP Trap features and procedures, you can use the LAN-XPT configuration description for this product without any changes.

6.28 Configuring a Netgear / ZyXEL RT311/RT314

This info is taken from the unofficial Netgear support page.

www.netgear.org

©2014 SolarWinds, Inc.

The syslog configuration is not available from the web interface and can only be done from the telnet command line interface.

```
Menu 24.3.2 - System Maintenance - UNIX Syslog

Syslog:
Active= Yes
Syslog IP Address= xxx.xxx.xxx.xxx <---- ip address of the syslog
Log Facility= Local 1 <------ Make sure you set it as the same group in your syslog
Types:
CDR= Yes
Packet triggered= Yes
Filter log= Yes
PPP log= Yes
```

6.29 Configuring a Netgear ADSL Firewall Router DG834

More info available at: http://www.netgear.com/products/details/DG834.php

To configure syslog message sending:
- Login to the Netgear router via the web interface
- Under SECURITY in the left hand frame, select Security logs.
- On the Security logs screen, under the Syslog section, check the "Send to this syslog server IP addres" option
- In the field for "Send syslog to this address", put the IP address of the system running your Kiwi Syslog Server.
- Optionally you can check the log items you would like your device to send from the "Include in Log" section above

6.30 Configuring a Netgear FVS318 VPN Firewall

Thanks to Paul Bohn from Mount Sterling Ohio for this information.

More info available at: http://www.netgear.com/products/details/FVS318.php

PREREQUISITE FIRMWARE LEVEL: NETGEAR FVS318 FIRMWARE 1.01j beta dated 7 August 2002 or later.

To configure syslog message sending:
- Sign onto the Netgear router
- Under SECURITY in the left hand frame, select Security logs.
- On the Security logs screen, check the box for SYSLOG
- In the field for "Send syslog to this address", put the IP address of the system running your Kiwi Syslog Server.

6.31 Configuring a Netgear RP114 Router

This info is taken from the Netgear RP114 documentation file.

More info available at: www.netgear.com

The syslog configuration is not available from the web interface and can only be done from the telnet command line interface.

Syslog can be configured in Menu 24.3.2 - System Maintenance - UNIX Syslog. Menu 24.3.2 configures the router to send UNIX system logs to another machine. You must configure the parameters to activate syslog.

Field: Active
Command: Press the space bar to toggle between yes and no.

©2014 SolarWinds, Inc.

Description: The syslog option is turned on or off.

Field: Syslog IP Address
Command: Enter the address in dotted-decimal notation such as a.b.c.d where a, b, c and d are numbers between 0 and 255.
Description: This field is the IP address location to send your syslog.

Field: Log Facility
Command: Enter a Facility value
Description: Seven different local options can be selected. The log facility allows the message to be logged to different files in the server.

Field: Types: CDR, Packet triggered, Filter log, PPP log
Command: For each type, press the space bar to toggle between yes and no.
Description: Enable logging for: Call detail record (CDR), Packet trigger, Filter event (match or not match), PPP event.

To configure the router for logging with the syslogd program on a local host:

1. Go to Menu 24.3.2 - System Maintenance - UNIX Syslog.

2. Set Active to Yes.

3. In the Syslog IP Address field, enter the IP address of the syslogd host PC.

4. Select a number for Log Facility.

5. Select the type of activity that you would like to log.

You can enable the router to send the following types of syslog messages:
- Call detail record (CDR)
- Packet trigger
- Filter event log
- PPP event log

6. Save this menu.

6.32 Configuring a NetScreen firewall

Thanks to George McCashin for providing this information.

Web based configuration:

1). Log on to the web interface as an "admin" user
2). Go to Configuration->Report Settings->Syslog
3). Click on 'Enable Syslog'
4). If you want all traffic logged also click on 'Include Traffic Log' as well
5). Enter the log host address and port (Address of Kiwi Syslog Server and UDP port 514)

Additional note provided by Kevin Branch:

This will log all traffic coming through all types of Netscreen policies (permit/deny/tunnel), as well as log traffic permitted by default (if the Netscreen is set to permit sessions that are not specifically denied).

The "Log Packets Terminated to Self" option has nothing to do with sessions across the Netscreen, but rather logs sessions to the Netscreen itself (which should only be Netscreen management traffic, but will also show up probes from the Internet)

Alternatively, you can configure the NetScreen from the CLI.

Command Line Interface configuration:

©2014 SolarWinds, Inc.

The specific commands required to set up a Syslog server are listed below:

```
set syslog config ip_address security_facility
local_facility
set syslog enable
set syslog traffic
set log module system level level destination syslog
```

Note: The set syslog config command requires that you define the security facility and local facility. See the syslog command in the NetScreen CLI Reference Guide for a complete list of options for security_facility and local_facility.

Note: You must enter the set log command once for each message level. The options for level are listed below:

```
emergency
alert
critical
error
warning
notification
information
```

6.33 Configuring a Nortel Networks router

Thanks to Flavio Ramos for this information.

From the Bay Command Console (BCC), type the following commands:

```
stack# syslog
  syslog
     log-poll-timer 10
  log-host address <IP Address of PC running Kiwi Syslog Server>
  filter name WILDCARD entity all
     severity-mask {fault warning}
     slot-lower-bound 1
     slot-upper-bound 14
   back
  back
back
```

6.34 Configuring the Pack X IDScenter

IDScenter is a configuration and management tool for Snort IDS on Windows platforms.

It can be downloaded from:

http://www.packx.net/packx/html/en/index-en.htm

Alerts can be sent to Kiwi Syslog Server by using an output plugin.

Configuration:

From the IDScenter main window, choose the IDS Rules tab on the left hand side.
Press the Output plugins icon on the left hand side
You will now see a list of all the configured output plugins.

To add a new plugin, press the -> **Add** button and choose "**Syslog Alert Plugin**" from the popup menu.

A configuration display for this plugin will appear in the lower part of the window.

©2014 SolarWinds, Inc.

Select the facility and priority (level) that you want to have the alert messages sent on.

Facility: LOG_LOCAL7
Priority: LOG_ALERT

Then check all the error conditions that you want to be notified about.

LOG_CONS, LOG_PERROR, LOG_NDELAY, LOG_PID

Then press the **Add** button on the lower right hand side. Your syslog alert output plugin should now appear in the top list.

6.35 Configuring a SnapGear SOHO+

Using a web browser, connect to the SOHO+ management console.

On the left hand side, under the **SYSTEM** section, click on the **Advanced** link.

Under the **System Log** section, click on the **System Log** link.

Enter the IP address or host name of the machine running Kiwi Syslog Server into the **Address of remote machine** field.

To enable the sending of messages, tick the **Enable remote logging** checkbox.

Press the **Submit** button to apply the changes.

Now all new events logged on the system log will also be sent to the Kiwi Syslog Server server you have specified.

6.36 Configuring a SonicWall firewall

SonicWALL firewall appliances support the sending of syslog messages a remote syslog Server. Up to two servers can be configured.

To configure, use a web browser to connect to the SonicWALL management interface, then login with your user name and password.

From the left hand side menu, click the **Log button**.

A tabbed window will appear in the main display.

Click the **Log Settings tab.**

Under the **Sending the Log** heading, enter the IP address of the machine running the Kiwi Syslog Server into the field named: Syslog Server 1. If you are listening on a port other than 514, enter the value in the field named: Syslog server port 1.

Under the **Automation** heading, set the **Syslog Format** to Webtrends.

Under the **Categories** heading, Log subheading, check all the types of events that you would like to receive syslog messages for.

Press the **update** button.

A reboot of the SonicWALL may be required for the new settings to take effect.

We recommend RnRSoft ReportGen for SonicWALL to produce reports on the SonicWALL syslog messages. A

©2014 SolarWinds, Inc.

trial version can be downloaded from www.reportgen.com

6.37 Configuring a Symantec Firewall/VPN 200

Thanks to David Masilotti for providing this information.

Using a web browser, connect to the management console.

On the left hand side, under the **Advanced** section, click on the **Log Settings** link.

Enter the IP address or host name of the machine running Kiwi Syslog Server into the **Syslog Server** field.

To enable the sending of different message types, tick the check boxes labelled: **System**, **Debug**, **Blocked**, **Dropped** and **Attack** as required. Try enabling all the message types to start with and then uncheck them if there is too much information being logged.

Press the **Save** button to apply the changes.

Now all new events logged on the system log will also be sent to the Kiwi Syslog Server server you have specified.

6.38 Configuring a Unix machine

Thanks go to Antonino Iannella for supplying the following information.

With a Unix host, you will need super user privileges to modify the files -

/etc/syslog.conf
/etc/hosts

And to restart (HUP) the Syslog Server on the Unix box.

Use vi or any text file editor of your choice to modify the /etc/hosts file first.

A sample hosts file

```
#
# Internet host table
#
127.0.0.1         localhost
192.168.230.23    loghost
```

```
This allows you to use the hostname loghost to direct your messages to.
The IP address used for loghost should be the address of the Windows or NT box you are running
Kiwi Syslog Server on.

Now use vi or any text file editor of your choice to modify the /etc/syslog.conf file.

A sample syslog.conf file

# Syslog configuration file.
#
*.err;kern.notice;auth.notice             /dev/console
*.err;kern.debug;daemon.notice;mail.crit  /var/adm/messages

*.alert;kern.err;daemon.err               operator
*.alert                                   root

*.emerg                                   @loghost
mail.debug                                @loghost
```

©2014 SolarWinds, Inc.

You will notice that all facilities with a level of **emerg** will be forwarded to the loghost (defined in the hosts file) and any mail alerts with a level of **debug** will also be forwarded.

The general idea is **Facility.Level <TAB> @loghost**

Save this file after editing and restart the Syslog Server on the Unix box for it to take effect. Find the syslog Server process ID, and send it a SIGHUP signal. Test that the syslog server is writing messages using the **logger** command, such as **logger –p user.emerg Unix test message**.

If in doubt resort to 'man syslogd'.

6.39 Configuring a VegaStream Telephony Gateway

This information is taken from the VegaStream Technical Documentation

The original document can be found at:
http://www.vegaassist.com/documentation/3-Technical%20Documentation/IN_21-Syslog_01.pdf

Configuring Syslog on a Vega

Vega gateways support four types of Syslog information:

1. Log data (equivalent to log display on)
2. Billing / CDR data (equivalent to bill display on)
3. Console audit (a log of all serial, web, and telnet commands for all consoles)
4. Debug information (equivalent to debug on)

Vega gateways support up to 5 Syslog sessions; each Syslog session can be configured to send one or more of these sets of information.

The Syslog data that the Vega sends is always UDP.

To configure Syslog sessions, on the web browser select Logging on the left hand menu, then SYSLOG in the SYSLOG Configuration section.

From the list of syslog servers, choose Add, Delete or Modify.

The Name field is for self-documentation purposes, Host is the IP address of the Syslog server to send the messages to.

Port is the UDP port number to send the messages to (Normally port 514).

Logging, Billing, Console and Debug define the types of information to send to this server.

The changes made can be activated by selecting Apply Changes button after the Submit button.

Note: Syslog can produce a significant amount of data traffic, especially if multiple syslog logging options are selected and multiple syslog destinations are chosen – this can affect LAN bandwidth and gateway performance.

6.40 Configuring a Watchguard Firebox to work with DShield

More information can be found at:

http://live.dshield.org/clients/watchguard_kiwi_setup.php

©2014 SolarWinds, Inc.

6.41 Configuring a WatchGuard SOHO firewall

This info is taken from the WatchGuard Knowledgebase.

The SOHO has the ability to send its logs over the network to a syslog server with firmware 2.4.0 and above. Syslog is the common service in use for capturing log data from Solaris, SCO Unix, BSD, Linux, and other *nix-style operating systems. Because the syslog functionality of the SOHO runs simultaneously to the standard logging, it can be a good backup logging method.

There are a few limitations with the syslog service however. The syslog service transmits its data over the network using port 514 UDP packets. Thus, accurate delivery of the log data is not verified by the SOHO or the syslog host. The data is also unencrypted, as per the syslog specification.

Configuration is straightforward. We will step through it here:

SOHO syslog configuration
Open the configuration interface of the SOHO.
Click **System Administration**.
Click **Syslog Logging**.
Click the **Enable Syslog output** checkbox.
Enter the IP address of the host running Kiwi Syslog Server.
Syslog has no provision for encrypting the log data. Never configure syslog logging to send the data to or through a potentially hostile network!
Click **Submit**.

Your SOHO will now reboot.

6.42 Configuring a W-Linx MB Broadband router

This information was provided by Philipp Beckers.

For more information please visit: http://www.w-linx.com.tw/products/multifunction/soho_mate.htm

1. Use a web browser to connect to the W-Linx box, (http://192.168.1.254) and login as admin
2. Click on "Advanced Setting" and then on System Log
3. Enter in the Field "IP Adress for Syslog" the (static) IP of your PC running Kiwi Syslog Server
4. Now make sure that the checkbox "enable" is checked and click to save
5. Reboot the router and now you can use syslog

6.43 Configuring a ZyXEL ZyWALL 10

Thanks to Killian McCourt for this info.

www.netgear.org

The syslog configuration is not available from the web interface and can only be done from the telnet command line interface or via the console port.

```
Menu 24.3.2 - System Maintenance - UNIX Syslog

Syslog:
Active= Yes
Syslog IP Address= xxx.xxx.xxx.xxx (IP address of the syslog)
Log Facility= Local 1 (Send messages with a facility of Local1)

Types:
CDR= No
Packet triggered= No
```

©2014 SolarWinds, Inc.

```
Filter log= No
PPP log= No
Firewall log= Yes
VPN log= No
```

This setup is very similar to the Netgear/Zyxel RT311/RT314 devices

7 Configuring SNMP Trap generating devices

Guides for configuring network hardware that can generate SNMP traps are listed in this section.

If you know of other devices which can send SNMP traps, please provide details to http://www.kiwisyslog.com/support/ and we will be sure to add the information into the next release.

7.1 Configuring Cisco IOS SNMP Trap support

Cisco devices that run the standard IOS Software (routers, Asynchronous Transfer Mode (ATM) switches and Remote Access Servers) of Cisco can generate many SNMP traps.

Information on Cisco IOS SNMP traps supported and how to configure them is available at:

http://www.cisco.com/warp/public/477/SNMP/snmp_traps.html

8 The Syslog Server error and e-mail logs

8.1 The error log

If Kiwi Syslog Server is unable to write a message to a log file or has a problem archiving the log files an error will be logged in the error log text file.

The file name is: InstallPath\Errorlog.txt

Any other errors that are encountered by Kiwi Syslog Server are also recorded in this file.

8.2 To view the error log file

From the **Main Syslog Server** display…

Choose the **View | View Error log file** menu option or press **Ctrl+R**.

This will open the error log text file with notepad if there have been errors logged.

8.3 The SMTP mail log

Every time an alarm notification is mailed out or the daily statistics are sent the e-mail details are logged in the send mail log file.

The file name is: InstallPath\SendMailLog.txt

©2014 SolarWinds, Inc.

8.4 To view the e-mail log file

From the Main Syslog Server display…

Choose the **View | View e-mail log file** menu option or press **Ctrl+M**.

This will open the SendMailLog text file with notepad if there has been any mail activity logged.

9 The Syslog Protocol

9.1 Syslog Facilities

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 messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
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.

©2014 SolarWinds, Inc.

9.2 Syslog Levels

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 or Informational level for normal messages.

A detailed explanation of the severity Levels:

DEBUG:
Info useful to developers for debugging the app, not useful during operations

INFORMATIONAL:
Normal operational messages - may be harvested for reporting, measuring throughput, etc - no action required

NOTICE:
Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required

WARNING:
Warning messages - not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time

ERROR:
Non-urgent failures - these should be relayed to developers or admins; each item must be resolved within a given time

ALERT:
Should be corrected immediately - notify staff who can fix the problem - example is loss of backup ISP connection

CRITICAL:
Should be corrected immediately, but indicates failure in a primary system - fix CRITICAL problems before ALERT - example is loss of primary ISP connection

EMERGENCY:
A "panic" condition - notify all tech staff on call? (earthquake? tornado?) - affects multiple apps/servers/sites...

©2014 SolarWinds, Inc.

9.3 Syslog Priority values

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.

9.4 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

Ports used by Kiwi Syslog Server are documented here.

9.5 Syslog RFC 3164 header format

The HEADER part contains a timestamp and an indication of the hostname 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 hostname, as it knows itself. If it does not have a hostname, 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 freeform 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 BSD Syslog protocol is discussed in RFC 3164.
http://community.roxen.com/developers/idocs/rfc/rfc3164.html

For a comprehensive description of the syslog protocol, see:
http://www.sans.org/infosecFAQ/unix/syslog.htm

©2014 SolarWinds, Inc.

9.6 The Kiwi Reliable Delivery Protocol (KRDP)

Background:

The Kiwi Reliable Delivery Protocol was designed to solve the problem of losing data when a TCP connection is broken due to a network failure.

KRDP uses the TCP protocol as the underlying transport. This ensures that each packet sent is sequenced and acknowledged when received. The TCP protocol on the receiving system handles the packet order and ensures that any missing packets are resent.

The problem:

TCP works well as a reliable transport when the connection can be opened and closed cleanly. During a TCP close handshake, any outstanding packets are usually received and acknowledged before the connection is closed.

However, if a break in the network occurs during message sending, the sender will continue to send packets until the TCP window size is reached. When no acknowledgement is received after a timeout period, the Winsock stack will fire a timeout event. When this happens, it is not possible to know exactly which message (or part message) was last received and acknowledged by the remote end. Any data that was sitting in the Winsock stack's buffer will be lost. Depending on the TCP window size and the speed of the data being sent, this could be hundreds of lost messages.

The solution:

KRDP works by adding another acknowledgement and sequencing layer over the top of the TCP transport. KRDP wraps each syslog message with a header which contains a unique sequence number. The KRDP sender keeps a local copy of each message it has sent. The KRDP receiver periodically acknowledges receipt of the last KRDP wrapped syslog message it has received. The KRDP sender can then remove all locally stored messages up to the last acknowledged sequence number. When the connection is broken and re-established, the receiver informs the sender which messages need to be resent.

Each KRDP sender is identified with a unique connection name. This allows the sender and receiver to re-establish the same session and sequence numbers, even if the IP address or sending port of the sender has been changed due to DHCP etc.

Unique message sequencing:

Each KRDP message is identified with a unique sequence number. The sequence starts at 1 and increments in steps of 1 up to 2147483647 (2 billion), then wraps around to 1 again. The message number 0 is used to indicate that the system does not know the last sequence number and that it has had to assume a fresh start. If this occurs, both the sender and receiver will log an error to note the lost messages.

Dealing with international characters:

Unicode allows the mapping of all international character sets into a known byte sequence. The mapping of non US-ASCII characters requires the use of more than a single byte per character. The most commonly used way of sending these multi-byte characters over TCP is to use UTF-8 encoding. The KRDP sender will encode the syslog messages as UTF-8 and the KRDP receiver will decode them back to Unicode again.

The KRDP message format:

Sender (S)
Receiver (R)

Message Types (MsgType):

©2014 SolarWinds, Inc.

00 = SenderID
01 = ReceiverResponse
02 = Sequenced message
03 = Message acknowledgement
04 = Receiver KeepAlive
99 = Error message

Message format:

KRDP AA 0000000000 Message<CR>

KRDP = Unique tag
Space (ASCII 32)
AA = Msg type (as above)
Space (ASCII 32)
0000000000 = Sequence number 0 to 2147483647
Space (ASCII 32)
Message = UTF-8 encoded message text
<CR> = Carriage return character ASCII 13 to indicate end of message stream

Sequence of events:

S connects via TCP
S sends first ID packet (MsgType 00)
R responds with ReceiverResponse message (MsgType 01)
S sends sequenced messages (MsgType 02)

Rules:

1. If the first message R receives is not a ID message (MsgType 00), R disconnects. (Any data received is ignored).
2. If R does not receive ID message after 60 seconds, R disconnects.
3. After S sends the ID message, S will wait up to 60 seconds for a ReceiverResponse message. If there is no response, S will disconnect session.
4. R sends ACK messages to S with the next expected message sequence
5. ACK messages are sent no more frequently than once every 200ms

Message formats:

MsgType 00 (Version and SenderID)
KRDP 00 PV UniqueKey<CR>
The unique key identifies the channel and is used to synchronise the message numbers
PV = Protocol Version to use. 01 = KRDP Reliable/Acknowledged
Unique key format is free form.
An example would be: "IP=192.168.1.1, Host=myhost.com, ID=Instance1"
Or, just: "Instance1"
Since the receiver might already have an "Instance1" name from another source, the first UniqueKey would be better. Use as much information to uniquely describe the source of the messages

MsgType 01 (ReceiverResponse message)
KRDP 01 0000000000 Listener ID<CR>
Message number is 10 digit number 0000000000 to 2147483647

MsgType 02 (Sender Message content)
KRDP 02 0000000000 Message content<CR>
Message number is 10 digit number 0000000000 to 2147483647

MsgType 03 (Receiver ACK)
KRDP 03 0000000000 ACK<CR>
Message number is 10 digit number 0000000000 to 2147483647
Message number indicates the next sequence number it expects to receive
ACK messages are sent at a maximum rate of once every 200ms

MsgType 04 (Keep alive)
KRDP 04 0000000000 KeepAlive<CR>
Message number is 10 digit number 0000000000 to 2147483647

©2014 SolarWinds, Inc.

Message number = Next expected message number
If being sent by Sender, MsgSeq should be set to 0
If being sent by Receiver, MsgSeq should be set to next expected message number

MsgType 99 (Error)
KRDP 99 0000000000 0000 Error message here<CR>
Message number is 10 digit number 0000000000 to 2147483647
Message number indicates which message caused the error if any. Set to zero (0) if not related to a message number
0000 = Error number (0000 to 9999)
Error message can be any text

9.6.1 KRDP Error Messages

Error 1000 - Unable to decode the following message: <Invalid message appears here>
A message was received that wasn't encoded correctly or corrupted. The message content appears for debugging purposes.

Error 1001 - Sender is unable to supply message number: <NextMsgSeq>. Starting again from 0. Sender ID: <UniqueSenderID>
Expecting a sequence > 0, but sender unable to supply message, must start at 0 again. The receiver will now re-sync with the sender.

Error 1002 - Missed message number: <NextMsgSeq>. Received: <ActualMsgSeq> on ID: <UniqueSenderID>
The expected message number was not received from the sender. The receiver will now re-sync with the sender.

Error 1003 - Received unexpected message data. Message ignored. Sender ID: <UniqueSenderID>
Message data arrived while the receiver was not expecting it. This data is ignored.

Error 1004 - First message did not contain Sender ID. Connection closed.
The first message received after connection was established did not contain the Sender ID. The receiver has closed the connection.

Error 1005 - Unable to send Expected message number reply. Connection closed.
The receiver was unable to send a reply message over the established connection. The receiver has closed the connection.

Error 1006 - Unable to send error message.
The receiver was unable to send an error message over the established connection.

Error 1007 - Unable to send KeepAlive message. Connection closed.
The receiver was unable to send a KeepAlive message over the established connection. The receiver has closed the connection.

Error 1008 - Unable to send KeepAlive to connection: <UniqueSenderID>
The receiver was unable to send a KeepAlive message over the established connection.

Error 1009 - Unable to send ACK to connection: <UniqueSenderID>
The receiver was unable to send an ACK message over the established connection.

Error 1099 - <Error message content from sender>
The sender can notify the receiver of an error by using the 1099 error type. The message content is from the sender.

Error 1010 - Unexpected message received. Type: <MsgType>. Message content: <Message Content>
An unexpected message type was received. The message content appears for debugging purposes.

©2014 SolarWinds, Inc.

10 Troubleshooting

10.1 Troubleshooting

If no messages are being displayed to the screen or being logged:

- Check network connectivity by pinging from the sending device to the Syslog Server machine
- Check only one instance of Kiwi Syslog Server is running (Ctrl-Shift-Esc to get the task-list)
- Disable any personal firewall software such as ZoneAlarm or BlackIce
- Check DNS resolution is working as expected by pinging a hostname from the Command Prompt
- Check that there is a "Display" action setup for the facility and level you are expecting to receive messages on.
- Send a test message to yourself by pressing **Ctrl+T**
- Download a copy of the Free Syslog Server Message Generator (SyslogGen) from: www.kiwisyslog.com/downloads
- Install SyslogGen and set it to send a message every second to the address 127.0.0.1 (local host).
- If you see messages appearing, the problem is with the router, switch or Unix box sending the Syslog messages.
- Try sending messages with SyslogGen from another machine to the host running the Syslog Server
- The device that is sending messages to you may not be including a priority code in its message. You can set a default priority to use from the **Modifiers** option of the Kiwi Syslog Server Setup window. To open the setup window use the **File | Setup** menu option from the main Kiwi Syslog Server window.
- If you are running a Cisco router and are not receiving messages, use the Logging source-interface command to specify an interface to log from. There is a bug in the Cisco IOS that causes invalid UDP checksums unless this command is specified.

If the Kiwi Syslog Server still fails to display messages:

- Restart the computer (power off as well if possible)
- Disable the DNS settings so that no IP address resolution is performed
- Disable the e-mail settings by un-checking the Alarm and Statistics notification options
- From the **Defaults/Import/Export** option, press the **Load default Rules and Settings** button. Then press OK to accept the changes.
- Check the Kiwi Syslog Server errorlog file to see if this contains any information that may be of assistance. This file is called "ErrorLog.txt" and is located in the installation directory.
-
- If you find a message in the errorlog file stating that Kiwi Syslog Server is unable to bind to a particular port then you will need to close down the application that is using that port before restarting Kiwi Syslog Server again. Further information on this can be found in the FAQ section on our website: http://www.kiwisyslog.com/support.

If the program still fails to display messages:

If the problem still exists after following the instructions above, then please use the http://www.kiwisyslog.com/support to receive further assistance.

Please provide as much technical detail as possible. This makes the remote troubleshooting a lot easier.

10.2 Running on Windows XP SP2 or Windows 2003 Server SP1

When Windows XP Service Pack 2 or Windows 2003 Server Service Pack 1 is installed it turns on the Windows Firewall by default. This causes any traffic that is being sent to Kiwi Syslog Server to be blocked.

To fix the problem, you will need to create an "Exception" in the Windows Firewall setup.

To do this follow the steps provided below...

- Open Windows Firewall from the Windows Control Panel
- Select the "Exceptions" Tab

©2014 SolarWinds, Inc.

- Press the "Add Port" button
- Specify a Name, Port number and select whether or not is it TCP or UDP.
  (By default, Kiwi Syslog Server uses UDP port 514.)

If you have setup Kiwi Syslog Server to listen on other ports you will also need to create exceptions for each of these ports. For example, if you are listening for SNMP traps then you will need to create a exception that allows UDP port 162.

If the problem still exists after following the instructions above, then please use the http://www.kiwisyslog.com/support to receive further assistance.

See also: Troubleshooting

11 Advanced Information

11.1 Registry settings for Kiwi Syslog Server

The following registry values will affect the operation of Kiwi Syslog Server.

Ensure that Kiwi Syslog Server is not running before making changes to the registry. If you are running the Service edition, use the Manage menu from the Service Manager to stop the service first.

Use RegEdit to access and modify the values.

Once changes have been made, Kiwi Syslog Server can be restarted and will read the new settings.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.1 Display - Enabled columns

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DisplayColumnsEnabled

Min value: 0
Max value: 31
Default value: 31
Type: Decimal number from 0-31

This value specifies the display columns to show on the scrolling display. Normally all the columns are shown. By adjusting the number, you can enable or disable the display column.

Each column is represented by a binary bit value being set to 0 or 1.

Bit number	Decimal value	Column name
0	1	Date
1	2	Time
2	4	Priority
3	8	Hostname

©2014 SolarWinds, Inc.

4 16 Message text

To show all columns set the value to 31.

To show the Message text (16) and the Hostname (8) columns, set the value to 24 (16 + 8 = 24).

To show the Message text (16) and Time (2) columns, set the value to 18 (16 + 2 = 18).

To show just the Message text column, set the value to 16.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.2 Display - Default row height

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DisplayRowHeight

Min value: 5
Max value: 50
Default value: 15
Type: Height of row in pixels

This value specifies the default row height for the scrolling display. If the font to be displayed is taller than the specified row height, the row will automatically resize to accomodate the text.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.3 Statistics mail delivery time

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): MailStatsDeliveryTime

Min value: 00:00
Max value: 23:59

©2014 SolarWinds, Inc.

Default value: 00:00
Type: HH:MM

This time value specifies when the daily statistics e-mail is to be sent out. By default the statistics mail is sent at midnight (00:00). You may want to receive the mail at a different time of day instead. To have the statistics mail sent at 6p.m. set the value to 18:00.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.4 Service - Start/Stop Timeout

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): ServiceStartTimeout

Min value: 1
Max value: 120
Default value: 30
Type: Seconds

This value specifies how long the Service Manager will wait for a "Service Start" or "Service Stop" request to complete. If you have more than 10 actions configured or are running on a machine with a CPU speed of less than 300MHz, increase this value accordingly.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.5 Service - Properties Update Timeout

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): ServiceUpdateTimeout

Min value: 1
Max value: 120
Default value: 5
Type: Seconds

©2014 SolarWinds, Inc.

This value specifies how long the Service Manager will wait for a "Properties Update" request to complete. If you have more than 10 actions configured or are running on a machine with a CPU speed of less than 300MHz, increase this value accordingly.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.6 Service - Inter-App communication port

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): NTServiceSocket

Min value: 1
Max value: 65535
Default value: 3300
Type: TCP port number

The Manager part of Kiwi Syslog Server connects to the Service via TCP port 3300. This allows the two applications to communicate. The Service passes messages to be displayed, alarms and statistic information to the Manager so it can be viewed as it arrives. The port value can be changed if some other process is also using this port.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.7 Service - Dependencies

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): NTServiceDependencies

Default value: Blank
Type: Text string of service names. Delimited by semi-colons.

E.g. ServiceName1;ServiceName2;ServiceName3

©2014 SolarWinds, Inc.

Service Dependencies

Under most operating systems, the service will start without problems. On some Windows Server systems, the service may have to wait for some other system services starting before it can start. Otherwise you will see the error message "One or more system services failed to start" on the console after a reboot.

To ensure that the required services have started before Kiwi Syslog Server is started, you will need to modify the above registry setting.

How to add service dependencies

- Uninstall the service from the Manage menu
- Run RegEdit
- Locate the section "HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties"
- Create the new string value of "NTServiceDependencies"
- Modify the value data to include the list of services that need to start first
- E.g. "LanmanWorkstation;TCPIP;WMI" (without the quotes)
- Install the service from the Manage menu

The example above will ensure that the Workstation, WMI (Windows Management Interface) and TCP/IP stack services are running before trying to start the Kiwi Syslog Server Service.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.8 Service - Debug start-up

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Options

Value (STRING): DebugStart

Enable Debug: 1
Disable Debug: 0
Type: String

Setting this string value to "1" will enable debug for both the Service and Manager.

Command line value: DEBUGSTART

Applies to: Syslogd.exe, Syslogd_Service.exe & Syslogd_Manager.exe

Effect:
When the program is run with this registry value set to "1", a debug file is created in the install directory. The file name will depend on the executable name (see below). The debug file will contain the results from the program start-up and socket initialization routines.

Files created:
SyslogNormal = Syslogd_Startup.txt
SyslogService = Syslogd_Service_Startup.txt
SyslogManager = Syslogd_Manager_Startup.txt

©2014 SolarWinds, Inc.

When to use:
If the program does not appear to be receiving messages on the port specified on the "Inputs" setup option, check the start-up debug file to ensure the sockets initialized correctly.

If the program appears to crash on start-up, this option can help locate the problem.

For command line options, see: Start-up Debug

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.9 DNS - Disable wait when busy

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DNSDisableWaitWhenBusy

Min value: 0
Max value: 100
Default value: 10
Type: Percentage

Disable wait when busy:

Normally, if an IP address is not found in the DNS cache, the program will wait for a set period of time for the IP address to finish resolving. Under heavy load this delay can fill the message input buffer until it overflows and drops new messages.

This option allows you to specify how full the input message buffer can get before disabling the DNS resolution waiting. By default, when the input buffer reaches more than 10% of capacity, the Syslog Server will stop waiting for the IP addresses to be resolved.

If you have pre-emptive lookup enabled, the IP addresses will still be resolved in the background and results placed in the cache. This option just disables the "DNS timeout" waiting period while the buffer is under load. This frees the program up so that it can process the buffered messages without waiting for resolutions to occur.

When the input buffer level drops below the set value, the normal resolution waiting timeouts will be re-enabled.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

©2014 SolarWinds, Inc.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.10 DNS - Max cache size

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DNSCacheMaxSize

Registered mode:
Min value: 50
Max value: 1000000
Default value: 20000
Type: Maximum number of cache entries

Maximum number of cache entries:
This limits the size of the cache buffer to conserve memory. The registered version will allow 1,000,000 entries. Set this value to the number of IP addresses you are expecting to have to cache.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.11 DNS - Cache Failed Lookups

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DNSCacheFailedLookups

Min value: 0
Max value: 1
Default value: 1
Type: 1=Cache Failed DNS lookups, 0=Do not Cache Failed DNS lookups

DNSCacheFailedLookups
Improves DNS name resolution performance by caching failed lookups. In the event that a DNS server responds with a valid response, but where the response does not include a resolved name, Kiwi Syslog Server will cache that response to avoid repeated queries to the DNS server. This situation can occur when querying a DNS server for the name of and IP address that the DNS server itself does not know. Instead of timing out, the DNS server sends a valid response of "NAME NOT FOUND". This is the sort of response that is cached, which avoids repeated queries to the DNS server for a name that will not be found. Failed lookups will be flushed from the cache at the frequency defined in "**Flush entries after X minutes".**

Running Kiwi Syslog Server on a native 64-bit machine?

©2014 SolarWinds, Inc.

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.12 DNS Setup - DNS/NetBIOS queue buffer burst coefficient

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DNSSetupQueueBufferBurstCoefficient

Min value: 1
Max value: 50
Default value: 10
Type: The number of DNS/NetBIOS requests that will be dequeued from the internal queue buffer at once.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.13 DNS Setup - DNS/NetBIOS queue buffer clear rate

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DNSSetupQueueBufferClearRate

Min value: 1
Max value: 100
Default value: 10
Type: The rate at which the DNS/NetBIOS internal queue buffer is cleared

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all

©2014 SolarWinds, Inc.

registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to:
HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...

11.1.14 DNS Setup - DNS/NetBIOS queue limit

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DNSSetupQueueLimit

Min value: 100
Max value: 30000
Default value: 1000
Type: The DNS/NetBIOS internal queue buffer size

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to:
HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...

11.1.15 DNS Setup - Debug Mode

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DNSSetupDebugModeOn

Min value: 0
Max value: 1
Default value: 0
Type: DNS/NetBIOS verbose debug mode (on/off)

If set (1) then verbose DNS/NetBIOS requests and responses will be unloaded to {Program files}/Syslogd/DNS-debug.txt

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to:
HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...

©2014 SolarWinds, Inc.

11.1.16 Message buffer size

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): MsgBufferSize

Registered mode:
Min value: 100
Max value: 10000000 (10 million)
Default value: 500000
Type: Maximum number of message buffer entries

Maximum number of message buffer entries:
As messages are received via the inputs (UDP, TCP, SNMP, Keep Alive), the messages are placed in an internal queue. The messages are then taken from the queue and processed in the order they arrived (FIFO). If a burst of messages arrive while the processing engine is busy, the messages are queued. This ensures messages are not lost under times of heavy load.

Each message that is queued uses a small amount of memory. In most situations, buffering up to 500,000 messages is sufficient. You may want to increase the buffer size in situations where messages are arriving in large bursts. The buffering will smooth the message flow and allow the processing engine to catch up when it can.

Messages are stored in Unicode which uses 2 bytes for each character. Therefore, if each message is 100 characters, it will occupy 200 bytes of memory. Messages can vary in size based on their content. 500,000 messages of 100 characters each will use 100,000,000 bytes (~100 MB) of memory. If each message was 200 characters long, it would use ~200 MB of memory. Memory is only used when the messages are being queued. Under normal traffic loads, the processing engine will be able to keep up with message flow and no messages will need to be queued.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.17 E-mail - Additional subject text

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): MailAdditionalSubjectText

Default value: Blank
Type: Text string

Additional text message to add to the beginning of the e-mail subject:

Allows you to add a text string to the beginning of the e-mail subject for daily statistics and alarm e-mails. If you are receiving daily statistics or alarm e-mails from many syslog Servers, it can be useful to include a way of identifying which syslog Server the e-mail came from.

©2014 SolarWinds, Inc.

Simply add a line of text that best describes the name or location of the syslog Server. The text will be added to the beginning of the e-mail subject.

For example:

A normal max message alarm e-mail subject line looks like this:

```
Syslog Alarm: 16000 messages received this hour.
```

If you set the **MailAdditionalSubjectText** setting to "[London]", the alarm subject e-mail will look like this:

```
[London] Syslog Alarm: 16000 messages received this hour.
```

A space is automatically added after the text to separate it from the existing subject text.

See also. E-mail additional body text

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.18 E-mail - Additional body text

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): MailAdditionalBodyText

Default value: Blank
Type: Text string

Additional text message to add to the e-mail body:

This setting specifies an additional line of text that can be included in the daily statistics and alarm e-mails. If you are receiving daily statistics or alarm e-mails from many syslog Servers, it can be useful to include a way of identifying which syslog Server the e-mail came from.

Simply add a line of text that best describes the name or location of the syslog Server. The text will be added to the beginning of the e-mail body.

For example:

A normal statistics e-mail looks like this:

```
///       Kiwi Syslog Server Statistics         ///
--------------------------------------------------
24 hour period ending on: Fri, 06 Feb 2004 13:04:55 +1300
Syslog Server started on: Fri, 06 Feb 2004 13:03:54
Syslog Server uptime:     24 hours, 0 minutes
--------------------------------------------------

+ Messages received - Total:          20000
+ Messages received - Last 24 hours:  20000
```

©2014 SolarWinds, Inc.

If you set the **MailAdditionalBodyText** setting to "London - Firewall Monitoring Syslog Server", the daily statistics e-mail will look like this:

```
London - Firewall Monitoring Syslog Server

///       Kiwi Syslog Server Statistics         ///
-------------------------------------------------
24 hour period ending on: Fri, 06 Feb 2004 13:04:55 +1300
Syslog Server started on: Fri, 06 Feb 2004 13:03:54
Syslog Server uptime:     24 hours, 0 minutes
-------------------------------------------------

+ Messages received - Total:          20000
+ Messages received - Last 24 hours:  20000
```

An additional CRLF is added before and after the text for better visibility.

See also. E-mail additional subject text

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.19 E-mail - Limiting the messages sent

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): MailMaxMessageSend

Min value: 1
Max value: 1000
Default value: 50
Type: Message count

E-mail messages are queued internally for up to a minute and then sent in bulk. This means only a single connection to the SMTP server is required. Each message is sent separately, and then the connection to the server is closed.

The MailMaxMessageSend value specifies the maximum number of messages that are sent per minute. Any messages not sent will be re-queued until the next e-mail send a minute later.

This option can be useful when a lot of e-mail messages are being sent via an SMS gateway which has a limit on message sending. It can also reduce the load on a mail server and spread the message load out over a few sending intervals.

Note: Restart the service for any change in value to become active.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit

©2014 SolarWinds, Inc.

emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.20 File write caching

File write caching considerably improves the performance of the "Log to file" action under heavy message load.

When enabled, the "Log to File" action will cache the output data for X seconds or X messages before writing to the log file. The data is cached in memory until the log file is updated in bulk. This is more efficient than writing a single message to a file as it arrives.

There is a separate memory cache for each output file. In most cases there is only a single output file, but if AutoSplit or filters are used to split the messages into separate files, there could be additional active output files.

When an output file cache is not being used X seconds, the cache is destroyed to save resources.

When the program shuts down, all the caches are written to the appropriate files so that no data is lost.

Enable File write caching

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): FileWriteCacheEnabled

Min value: 0
Max value: 1
Default value: 1
Type: Enabled = 1, Disabled = 0

When enabled, the "Log to File" action will cache the output data for X seconds or X messages before writing to the log file. The data is cached in memory and the log file is updated in bulk. This is more efficient than writing a single message to a file as it arrives.

Cache timeout

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): FileWriteCacheTimeout

Min value: 1
Max value: 120
Default value: 5
Type: Timeout in seconds

After the timeout period the contents of the cache are written to disk. The timer is started when the first message arrives in the cache. If the cache is not full and has not been flushed before the timeout period has expired, the cache will be flushed automatically. This value sets the maximum time that the cache will hold a message before writing it to disk. The less frequently the disk is written to, the more efficient the file logging process becomes.

Maximum number of Cache entries

©2014 SolarWinds, Inc.

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): FileWriteCacheEntries

Min value: 10
Max value: 100,000
Default value: 1000
Type: Maximum number of cache entries (messages)

Sets the maximum number of messages to be cached for each output file before being written to file.

Messages are added to the cache until the maximum is reached or the timeout period elapses. The less frequently the disk is written to, the more efficient the file logging process becomes. The messages are stored in memory in UNICODE which requires two bytes for each character in the message. For example, a 100 character message requires 200 bytes of memory for storage.

Maximum memory size per cache

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): FileWriteCacheMaxSizeKB

Min value: 1
Max value: 2,000
Default value: 50
Type: Maximum size in KBytes for each cache

Sets the maximum cache size in KBytes. When the cache exceeds this size, it is written to file.

Messages are added to the cache until the maximum memory size is reached or the timeout period elapses. The less frequently the disk is written to, the more efficient the file logging process becomes. The messages are stored in memory in UNICODE which requires two bytes for each character in the message. For example, a 100 character message requires 200 bytes of memory for storage. If you experience any "Out of Memory" errors, lower this value or disable the file write caching.

Cache cleanup time

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): FileWriteCacheCleanup

Min value: 10
Max value: 1440
Default value: 10
Type: Time (in minutes) that a cache can inactive before being destroyed

When a cache becomes inactive and is not receiving any further messages, the cleanup process will destroy the cache to free up resources. No data is lost because the cleanup process only destroys inactive caches that have already been written to file.

Log file locking

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): FileWriteCacheFileLock

Min value: 0
Max value: 1
Default value: 0
Type: Enabled = 1, Disabled = 0

For efficiency and security reasons, the log files can be held open in "append shared" mode. This improves efficiency by not having to open and close the file with each write. While the file is held open, not other

©2014 SolarWinds, Inc.

application can modify or delete the contents. Only new entries can be added to the file. The files can be opened for viewing, but not for modification.

If you are receiving high syslog message traffic, enable this option to improve performance. The only drawback is that the file may not immediately show the new log entries. The OS will cache the data until the internal buffers are full then it will write the buffers to file. Under heavy load, this happens immediately, but when traffic is low, it can take a while for the buffers to fill and the data to be written. The log file is automatically updated and closed when the cache has been inactive for **FileWriteCacheCleanup** minutes.

Maximum number of open log files

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): FileWriteCacheOpenFiles
Min value: 1
Max value: 250
Default value: 100
Type: Maximum number of open file handles

When **FileWriteCacheFileLock** is set to 1 (enabled), each log file is held open in "append shared" mode. The program can only open a maximum of 255 files at once. This value sets the maximum number of concurrently open files. Once this limit is reached, the **FileWriteCacheFileLock** value for the current cache is disabled. Log files will then be opened and closed with each cache write. If the Log to File action uses the AutoSplit syntax to create separate files for each logging host, it is possible that more than 255 files could be opened at once (assuming more than 255 actively sending hosts). A value of 100 files is recommended to keep system resource usage to a reasonable level.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.21 File logging - Date separator character

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): LogFileDateSeparator

Default value: "-" (dash)
Type: Character, or string of characters

Normally the current date is represented in the YYYY-MM-DD format using a dash (-) as the separation character. You can change the separation character to any character you like. For example, some countries use a forward slash (/) as a date separator.

Be aware that changing the date separator may make the log files unreadable by some log file parsers and reporters. Reporting software may be looking for the dash (-) characters and may get confused when they are not present.

This setting applies only to the following formats:
- Kiwi format ISO yyyy-mm-dd (Tab delimited)
- Kiwi format ISO UTC yyyy-mm-dd (Tab delimited)

©2014 SolarWinds, Inc.

Example usage:

Normal Kiwi ISO log file format message:

2004-05-27 10:58:22 Kernel.Warning 192.168.0.1 kernel: This is a test message

Changing the separator character to forward slash (/), the message would become:

2004/05/27 10:58:22 Kernel.Warning 192.168.0.1 kernel: This is a test message

See also, changing the time separator character

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.22 File logging - Time separator character

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): LogFileTimeSeparator

Default value: ":" (colon)
Type: Character, or string of characters

Normally the current time is represented in the HH:MM:SS format using a colon (:) as the separation character. You can change the separation character to any character you like. For example, some countries use a dot (.) as the time separator.

Be aware that changing the time separator may make the log files unreadable by some log file parsers and reporters. Reporting software may be looking for the colon (:) characters and may get confused when they are not present.

This setting applies only to the following formats:
- Kiwi format ISO yyyy-mm-dd (Tab delimited)
- Kiwi format ISO UTC yyyy-mm-dd (Tab delimited)

Example usage:

Normal Kiwi ISO log file format message:

2004-05-27 10:58:22 Kernel.Warning 192.168.0.1 kernel: This is a test message

Changing the time separator character to dot (.), the message would become:

2004-05-27 10.58.22 Kernel.Warning 192.168.0.1 kernel: This is a test message

See also, changing the date separator character

©2014 SolarWinds, Inc.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.23 File logging - Encoding format

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): LogFileEncodingFormat

Min value: 0
Max value: 65535
Default value: 1 (System)
Type: Code page number

Normally the messages are written to the log files using the default encoding format (code page) of the system. If you are receiving messages from systems that use different default code pages, the best solution is to send/receive the messages using UTF-8 encoding. Kiwi Syslog Server can be set to convert the received messages into Unicode internally. When writing Unicode messages to a log file, it is recommended that you use UTF-8 (code page 65001) encoding. UTF-8 can represent all of the Unicode character set.

The various code pages available on most Windows systems can be found at:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/act/htm/actml_ref_scpg.asp

Here are some common code page numbers that can be used:

Name	Code Page Number	Description
System	1	System Code Page
ANSI	0	ANSI
UTF-8	65001	Unicode Transformation Format 8
Shift-JIS	932	Japanese
EUC-JP	51932	Japanese Extended Unix Code
BIG5	950	Traditional Chinese
Chinese	936	Simplified Chinese

Please note: If the number you specify is not a valid Code Page on your system, no data will be written to the file.

If in doubt, use UTF-8 encoding (65001) as it will handle all Unicode characters.

For more information on Unicode and UTF-8, please see:
http://en.wikipedia.org/wiki/UTF-8

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

©2014 SolarWinds, Inc.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.24 Script Editor

This setting allows you to choose and alternate script editor to be launched when the "Edit Script" button is pressed. By default, the scripts are edited with Notepad. This setting only applies to the "Run Script" action setup page.

Script Editor

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): ScriptEditor

Default value: Notepad.exe
Type: Path and file name of script editor application

E.g. "C:\Program files\MetaPad\MetaPad.exe"

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.25 Script Timeout

Some scripts may take longer to run than others. If your script causes a timeout error, you may want to extend the timeout value for running the script. Because the scripts are processed in real time, a script that takes a long time to run may cause message loss or delay the processing of other messages in the queue. If you have a complex or long running script, it is recommended that you run it as a post process. To do this, use the Windows Scripting Host to run your script against the log file that Kiwi Syslog Server creates. Try to avoid using long running scripts in real time.

Script Timeout

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): ScriptTimeout

Min value: 0 (No timeout - not recommended)
Max value: 60000
Default value: 10000
Type: Timeout in milliseconds (10000 = 10 seconds)

By default, the script can run for a maximum of 10 seconds before returning a timeout condition. If your scripts need more time to process the data in real-time, you can extend the timeout up to a maximum of 60 seconds. Setting the timeout value to 0 will cause the script to never timeout (this setting is not recommended as it can cause the program to fail if a script gets into an infinite loop).

©2014 SolarWinds, Inc.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.26 Database Command Timeout

The "Log to Database" action uses ADO to insert records into the specified database. By default ADO database commands will timeout after 30 seconds if the database is busy or does not respond.

If you see ADO command timeout errors in the error log, you may want to extend the timeout value. Because the database records are inserted in real time, a long timeout may cause message loss or delay the processing of other messages in the queue. Only extend this timeout if you are experiencing timeout errors.

Database Command Timeout

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DBCommandTimeout

Min value: 0 (No timeout - not recommended)
Max value: 120
Default value: 30
Type: Timeout in seconds

By default, the database insert command will wait up to 30 seconds before returning a timeout condition. If your database is slow and needs more time to process the data in real-time, you can extend the timeout up to a maximum of 120 seconds. Setting the timeout value to 0 will cause the command to never timeout (this setting is not recommended as it can cause the program to fail if the database does not respond).

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.27 Archiving - Replacement character

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): ArchiveFileReplacementChr

©2014 SolarWinds, Inc.

Default value: "-" (dash)
Type: Character, or string of characters

The archiving process uses the current system date and time to create dated files or dated folders for the archived log files.

Because the date format is user selectable, it may contain characters that are not valid in file names. The archiving process will create a valid file or folder name by replacing invalid values such as "&*+=:;,/\|?<>" with a valid character such as "-".

For example, if the system date and time is "2004/12/25 12:45:00", the archiving process will convert the name to "2004-12-25 12-45-00". This string will be used as a folder or file name for archiving purposes. Instead of using the "-" character, an different character can be chosen. Be aware that if any illegal character is used, it may cause the archiving process to create incorrect files or folders.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.28 Archiving - Separation character

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): ArchiveFileSeparator

Default value: "-" (dash)
Type: Character, or string of characters

When an archiving schedule is setup for "Use dated file names", a separator is placed between the existing file name and the current system date and time. Normally this character is a dash ("-"). By modifying this registry setting, an alternative character can be used instead.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

©2014 SolarWinds, Inc.

11.1.29 Archiving - Use Old Archive Naming Convention

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): UseOldArchiveNaming

Min value: 0
Max value: 1
Default value: 0 (disabled)
Type: Number

This setting overrides the default Scheduled Archive Task archive naming convention for Single Zip Archives. Setting this to (1) triggers Kiwi Syslog Server to use the Archive naming convertion present prior to version 8.3.x.
Only archive tasks which zip to a single zip file are affected by this setting.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.30 Archiving - Archive Temp Path

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): ArchiveTempPath

Default value: (nothing)
Type: String

This setting overrides the default temp folder used by Kiwi Syslog Server's archiver.

By default, the Windows temp folder location is assumed. (Usually C:\Windows\Temp, or C:\Documents and Settings\<Username>\Local Settings\Temp).

Please Note: This setting only takes effect if the Archive Temp File has been enabled (see EnableArchiveTempFile).

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to:

©2014 SolarWinds, Inc.

HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...

11.1.31 Archiving - Enable Temp File

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): EnableArchiveTempFile

Min value: 0
Max value: 1
Default value: 0 (disabled)
Type: Number

This setting overrides the default Scheduled Archive Task archiving behaviour.

If set (to 1) then Kiwi Syslog Server will use Temporary files when creating Archives. A temporary file is useful when writing to zip files located on write-once media (CD-WORM) or across a network because the zip file is created in the temporary file (usually on a local drive) and written to the destination drive or network location only when the zipping operation is complete.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to:
HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...

11.1.32 Error Log Folder

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): ErrorLogFolder

Default value: Application install path
Type: A folder path ("C:\My Logs\")

The errorlog.txt file is where any operational errors are logged. Normally this file is located in the application install path. By setting this value to an alternative path, the errorlog.txt file will be written there instead.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to:
HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...

©2014 SolarWinds, Inc.

11.1.33 Mail Log Folder

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): MailLogFolder

Default value: Application install path
Type: A folder path ("C:\My Mail Logs\")

The SendMailLog.txt file is where any mail activity is logged. Normally this file is located in the application install path. By setting this value to an alternative path, the SendMailLog.txt file will be written there instead.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.34 KRDP - ACK timer

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPACKTimer

Min value: 10
Max value: 65535
Default value: 200
Type: Milliseconds

This determines the interval of the TCP_ACK protocol's acknowledgement timer. By default, the protocol will acknowledge (ACK) the received packets after 200 milliseconds.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

©2014 SolarWinds, Inc.

11.1.35 KRDP - Keep Alive timer

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPKeepAliveTimer

Min value: 1
Max value: 65535
Default value: 25
Type: ACK Timer intervals

This determines the interval between the sending of Keep Alive messages to of the connected sessions. This counter is a multiple of the KRDPACKTimer. For example: If KRDPACKTimer is set to 200ms and you want a keep alive time of 5 seconds, you will need to set the value to 25. (25 x 200ms = 5 seconds).

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.36 KRDP - Disk cache folder

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPCacheFolder

Default value: InstallFolder\Cache\
Type: Path to cache folder

This determines the location of the disk cache files that might be created. Disk cache files are only created if the remote host is unavailable for some time and the memory cache has become full.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.37 KRDP - Rx Debug

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

©2014 SolarWinds, Inc.

Value (STRING): KRDPRxDebug

Min value: 0
Max value: 1
Default value: 0
Type: Enable/Disable

This option enables or disables the debug log file for KRDP receive events. This is all the events relating to the KRDP TCP listener. The log file is created in the install folder and named: "KRDPRxDebug.txt".

The KRDP listener is created by enabling the "Inputs | TCP" option.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.38 KRDP - Tx Debug

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPTxDebug

Min value: 0
Max value: 1
Default value: 0
Type: Enable/Disable

This option enables or disables the debug log file for KRDP send events. This is all the events relating to the KRDP senders. The log file is created in the install folder and named: "KRDPTxDebug.txt".

The KRDP senders are created by using the "Forward to another host" actions.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.39 KRDP - Queue size

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

©2014 SolarWinds, Inc.

Value (STRING): KRDPQueueSize

Min value: 50
Max value: 200000
Default value: 10000
Type: Queued messages

This determines the size of the message queues used to buffer the KRDP and TCP messages. If the memory queue becomes full, the queue is written to a cache file.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.40 KRDP - Queue Max MB Size

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPQueueMaxMBSize

Min value: 1
Max value: 100
Default value: 20
Type: Maximum size (in MB) of memory queue and cache file

As each buffered message is added to the memory queue the total size of the memory queue is monitored. When the total size of the queue exceeds the KRDPQueueMaxMBSize setting, the queue is written to a cache file. This ensures that if the messages are larger than normal, the system memory is not exhausted.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.41 KRDP - AutoConnect

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPAutoConnect

Min value: 0

©2014 SolarWinds, Inc.

Max value: 1
Default value: 1
Type: Enable or disable

When this value is set to "1" the KRDP and TCP senders will try to automatically connect to the remote host. If this value is set to "0" then a connection will only occur if there are messages queued to be sent.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.42 KRDP - Connect time

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPConnectTime

Min value: 5
Max value: 65535
Default value: 5
Type: Seconds

Sets the time between connection retries. When a connection can't be made to the remote peer, a connection attempt will be made every KRDPConnectTime seconds.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.43 KRDP - Send speed

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPSendSpeed

Min value: 10
Max value: 10000
Default value: 2000
Type: Messages per second send speed

©2014 SolarWinds, Inc.

Sets the maximum number of messages that can be sent per second. This allows the messages to be sent to the remote peer at a maximum speed and avoids overloading the receiver or network link.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.44 KRDP - IdleTimeout

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPIdleTimeout

Min value: 0 (off)
Max value: 65535
Default value: 60
Type: Seconds

Sets the time the sending socket will remain connected after the last message has been sent. Because TCP has an overhead when connecting and disconnecting, the TCP connection will remain open for a time to allow any further messages to be sent without triggering a new connection. The idle timer starts as soon as a message has been sent. If no further messages have been sent in the time specified by KRDPIdleTimeout then the connection is closed.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.45 KRDP - Add SeqNum

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): KRDPAddSeqToMsgText

Min value: 0
Max value: 1
Default value: 0
Type: Enable/Disable

When this value is set to "1" the KRDP listener will add the received sequence number to the end of the

©2014 SolarWinds, Inc.

message text. Each sequence number is unique per connection ID and will range from 0 to 2147483647.

The tag added will look like: " KRDP_Seq=1234".

E.g.

The quick brown fox jumped over the lazy dogs back KRDP_Seq=5742
The quick brown fox jumped over the lazy dogs back KRDP_Seq=5743
The quick brown fox jumped over the lazy dogs back KRDP_Seq=5744
The quick brown fox jumped over the lazy dogs back KRDP_Seq=5745

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.46 Syslogd Process Priority

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): ProcessPriority

Min value: 0
Max value: 3
Default value: 0
Type: Syslog Process Priority

This registry setting (if present) enables syslogd to modify it's priority setting in Windows.

Acceptable values are:
0 - LOW_PRIORITY
1 - BELOW_NORMAL_PRIORITY
2 - NORMAL_PRIORITY (default)
3 - ABOVE_NORMAL_PRIORITY
4 - HIGH_PRIORITY
5 - REALTIME_PRIORITY (Caution: REALTIME priority can cause system lockups)

AboveNormal
Indicates a process that has priority above Normal but below High.

BelowNormal
Indicates a process that has priority above Idle but below Normal.

High
Specify this class for a process that performs time-critical tasks that must be executed immediately. The threads of the process preempt the threads of normal or idle priority class processes. An example is the Task List, which must respond quickly when called by the user, regardless of the load on the operating system. Use extreme care when using the high-priority class, because a high-priority class application can use nearly all available CPU time.

Low
Specify this class for a process whose threads run only when the system is idle. The threads of the process are preempted by the threads of any process running in a higher priority class. An example is a screen saver. The idle-priority class is inherited by child processes.

©2014 SolarWinds, Inc.

Normal
Specify this class for a process with no special scheduling needs.

RealTime
Specify this class for a process that has the highest possible priority. The threads of the process preempt the threads of all other processes, including operating system processes performing important tasks. For example, a real-time process that executes for more than a very brief interval can cause disk caches not to flush or cause the mouse to be unresponsive.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.47 Originating Address - Custom Start and End tags

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): OriginalAddressStartTag

Default value: "Orignial Address="
Type: Original Address Start Tag

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): OriginalAddressEndTag

Default value: " " (Space)
Type: Original Address End Tag

Normally, the syslog protocol is unable to maintain the original senders address when forwarding/relaying syslog messages. This is because the senders address is taken from the received UDP or TCP packet.

The way Kiwi Syslog gets around this problem is to place a tag in the message text that contains the original senders address. By default, the tag looks like Original Address=192.168.1.1. That is, the "Original Address=" tag, followed by the IP address, followed by a " " (space) delimiter or tag.

These tags are only inserted if the "Retain the original source address of the message" option is checked in the "Foward to another host" action.
See - Action - Forward to another host

The two registry keys above allow for the default start and end tags to be overidden with custom start and end tag values.

For example:

The default originating address tags:
OriginalAddressStartTag = "Orginial Address="
OriginalAddressEndTag = " " (Space)
- Which yields "Original Address=nnn.nnn.nnn.nnn ", where nnn.nnn.nnn.nnn is the originating IP address.

New (custom) originating address tags:
OriginalAddressStartTag = "<ORIGIN>"

©2014 SolarWinds, Inc.

OriginalAddressEndTag = "</ORIGIN>"
-Yields "<ORIGIN>nnn.nnn.nnn.nnn</ORIGIN>", where nnn.nnn.nnn.nnn is the originating IP address.

New (custom) originating address tags:
OriginalAddressStartTag = "F="
OriginalAddressEndTag = " "
-Yields "F=nnn.nnn.nnn.nnn ", where nnn.nnn.nnn.nnn is the originating IP address.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.48 Rules - Maximum Rule Count

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Options

Value (STRING): MaxRuleCount

Min value: 10
Max value: 999
Default value: 100
Type: The Maximum number of rules allowable in Kiwi Syslog Server

Note:
Exceeding the maximum rule count of 100 is not recommended. Setting this value too high can adversely affect Kiwi Syslog Servers' performance and increase memory consumption dramatically. SolarWinds recommend persuing alternative methods if you are approaching the rule count limit of 100. Utilising the autosplit feature of file logging is one potential solution: for more information see AutoSplit values.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.49 Database Logger - Cache Clear Rate

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DBLoggerCacheClearRate

Min value: 10
Max value: 1000

©2014 SolarWinds, Inc.

Default value: 1000 (ms)
Type: Number

This is the rate (in milliseconds) at which the Database Cache is checked for SQL-data to be executed.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.50 Database Logger - Cache Timeout

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DBLoggerCacheTimeout

Min value: 1
Max value: 30
Default value: 3 (days)
Type: Number

This is the maximum age of an unchanged cache file (in days). Any database cache file that is older than this will be deleted by the system.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.51 Database Logger - Disable Database Cache

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties

Value (STRING): DBLoggerCacheDisable

Min value: 0
Max value: 1
Default value: 0 (enabled)
Type: Number

©2014 SolarWinds, Inc.

This setting overrides the default database caching behaviour.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.1.52 Statistics Report – No of Hosts to Show

Section: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\options\

Value (STRING): HostNosToDisplay

Min value : 25
Max value : 999
Default value : No default value – If required Customer needs to manually insert
Type: Height of row in pixels

This value specifies the no of hosts to display in statistics report. By default there will not be any entry. If required customer needs to manually insert.

Running Kiwi Syslog Server on a native 64-bit machine?

On 64-bit Windows installations, Kiwi Syslog Server runs in WOW (Windows on Windows) 32-bit emulated mode. In WOW mode, the SolarWinds registry hive resides in: HKEY_LOCAL_MACHINE\Software\WOW6432Node, not in HKEY_LOCAL_MACHINE\Software as it does on a native 32-bit Windows environment.

If you are running Kiwi Syslog Server on a native 64-bit windows machine, please re-map all registry settings from HKEY_LOCAL_MACHINE\Software\SolarWinds\... to: **HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\...**

11.2 Command-line arguments

The following command line parameters can be used when starting the syslog executable, **Syslogd.exe or Syslogd_Manager.exe, or Syslogd_Service.exe**. Parameters are not case sensitive. If specifying more than one parameter at a time, separate the values with a space.

11.2.1 Start-up Debug

Command line value: DEBUGSTART

Applies to: Syslogd.exe, Syslogd_Service.exe & Syslogd_Manager.exe

©2014 SolarWinds, Inc.

Effect:
When the program is run with this command line value, a debug file is created in the install directory. The file name will depend on the executable name (see below). The debug file will contain the results from the program start-up and socket initialization routines.

Files created:
SyslogNormal = Syslogd_Startup.txt
SyslogService = Syslogd_Service_Startup.txt
SyslogManager = Syslogd_Manager_Startup.txt

When to use:
If the program does not appear to be receiving messages on the port specified on the "Inputs" setup option, check the start-up debug file to ensure the sockets initialized correctly.

If the program appears to crash on start-up, this option can help locate the problem.

Debugging the Service Edition.

Since the service can't be provided with a command line argument, a registry entry can be set instead.

See Registry settings: Service - Debug start-up

11.2.2 Service - Install Service

Command line value: -INSTALL

Applies to: Syslogd_Service.exe

Effect:
Will try to install the Syslog Server as a Service. A message box will appear to indicate success or failure.

When to use:
Use if an install fails from the Manage menu of the Syslog Server Service Manager. Or from a batch file if automation of the Service installation is required.

Silent option:
Follow this command line value with -silent to disable the message box from being displayed

E.g. -install -silent

11.2.3 Service - Uninstall Service

Command line value: -UNINSTALL

Applies to: Syslogd_Service.exe

Effect:
Will try to uninstall the Syslog Server as a Service. A message box will appear to indicate success or failure.

When to use:
Use if an uninstall fails from the Manage menu of the Syslog Server Service Manager. Or from a batch file if automation of the Service installation/uninstallation is required.

Ensure the Service is stopped first before uninstalling.

©2014 SolarWinds, Inc.

This can be done from the command line with "net stop" command.
E.g. net stop "Kiwi Syslog Server"

Silent option:
Follow this command line value with -silent to disable the message box from being displayed

E.g. -uninstall -silent

11.3 Automating the installation of Kiwi Syslog Server

It is possible to automate the installation and startup of Kiwi Syslog Server without the need for any human interaction.

To install and start Kiwi Syslog Server as a standard interactive application you will need to create a batch file that contains the following information;

"AppPath\Kiwi_Syslogd_X.X.X.setup.exe" /S INSTALL=APP /D=InstallPath

To install and start Kiwi Syslog Server as a Windows NT service you will need to create a batch file that contains the following information;

"AppPath\Kiwi_Syslogd_X.X.X.setup.exe" /S INSTALL=SERVICE /D=InstallPath

To apply a license key via the installer, simply pass the license details as follows:

"AppPath\Kiwi_Syslogd_X.X.X.setup.exe" REGKEY="Name|Company|E-mail|Serial|Key"

This will attempt to automatically license the software after installation is complete.

You can combine the ALL the switches together however you need to insure that you have the /D switch as the last argument.

"AppPath\Kiwi_Syslogd_X.X.X.setup.exe" REGKEY="..." /S INSTALL=SERVICE /D=InstallPath

It is also possible to have Kiwi Syslog Server automatically use predefined configuration settings and have these loaded the first time that the application or service is run.

For further information relating to this please have a look at the following link;
Configuring settings automatically via an ini file.

* AppPath refers to the actual path of the installation package (Kiwi_Syslogd_X.X.X.setup.exe) is currently located
* Double quotes are required where shown if there are spaces in AppPath e.g. "C:\Program Files\"

11.4 Using an INI file to automatically configure the settings

Normally the program settings are read from the registry when the program starts. If you want to modify the settings remotely, you can place an special INI file in the install folder and it will be used to load the settings from. This INI file can be copied to the folder from a remote machine if you want. The next time the program starts, it will read the settings from the INI file and write them into the registry for next time. The special INI file will then be deleted to indicate that the settings have been read. To stop the INI file from being deleted, simply enable the Read Only file attribute for that file.

©2014 SolarWinds, Inc.

On start-up the program looks for a file named "LoadNewSettings.ini" in the install folder. (Normally C:\Program files\Syslogd). If found, the settings are read from the INI file and placed in the registry under the normal Syslogd registry key: HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd
The file is then deleted so that it won't be loaded again. The program then reads the settings from the registry and starts as normal. The settings found in the INI file will have overwritten any existing registry settings.

The INI file can be any valid Kiwi Syslog Server INI file. To export settings use the File | Export menu or the Defaults/Import/Export option from the setup screen.

The INI file is not meant to be modified by hand because it contains many encoded settings for the rules, actions and filters. However, if you need to modify the settings manually to change drive letters (D: to C: for example), this can be done with search and replace in notepad. Do not try to change any encoded strings as it may cause unexpected results when the program tries to read the INI file back in.

If in doubt, contact http://www.kiwisyslog.com/support/ for assistance.

11.5 Ports used by Kiwi Syslog Server

Kiwi Syslog Server uses the following ports:

UDP Input - UDP 0.0.0.0:514 (default) (plus one Ephemeral port)
TCP Input - TCP 0.0.0.0:1468 (default)
SNMP Input - UDP 0.0.0.0:162 (default)
Secure TCP Input - TCP 0.0.0.0:6514 (default)

Syslog Service <-> Syslog Manager internal comms port - TCP 0.0.0.0:3300 (plus one Ephemeral port).

Web Access - TCP 0.0.0.0:8088 (default)

***Note**: Versions of Kiwi Syslog Server prior to 9.2.1 were installed with the Ultidev Cassini Web Server Explorer, which used an additional port TCP 0.0.0.0:7756. Cassini Web Server Explorer (and this port) are no longer used.*

12 Other Kiwi Software

12.1 Kiwi CatTools

Kiwi CatTools is an application that provides automated device configuration management on routers, switches and firewalls.

Support is provided for Cisco / 3Com / Extreme / Foundry / HP / Netscreen / Multicom devices and more.

Some of the many tasks Kiwi CatTools perform to make your life easier are:

- Perform configuration backups and have any differences instantly e-mailed to you.
- Issue commands via Telnet or SSH to many devices at once.
- Change the configuration at scheduled times.
- Change all your network device passwords in one go.

This configuration management tool is also fully scriptable, has a built-in TFTP server, supports SSH, Telnet and more.

To download or find our more information about the Kiwi CatTools please visit the Solarwinds website

12.2 Kiwi SyslogGen

A Syslog Message Generator for Windows 95/98/ME/NT4/2K/XP

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

©2014 SolarWinds, Inc.

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

Features:
- 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
- Randomly corrupted packets can be generated to test the robustness of the receiving Syslog 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.

To download or find our more information about the Kiwi SyslogGen please visit the SolarWinds website

12.3 Kiwi Logfile Viewer

Kiwi Logfile viewer is a Freeware application for XP and 2003

Its purpose is to display tab delimited log files created by Kiwi Syslog Server in an easy to read manner.

Features include:

- Column re-ordering via drag and drop
- Output to tab delimited file format
- Output to comma delimited file format
- Output to HTML table suitable for a browser.
- Read from a tab delimited file
- Read from a comma delimited file
- Command line options and switches
- Ability to use standard Syslog field titles in header
- Ability to set default behavior

To download or find our more information about the Kiwi Logfile Viewer please visit the SolarWinds website

12.4 Kiwi Secure Tunnel

Kiwi Secure Tunnel is a freeware Windows Secure Tunnel Service for use with Kiwi Syslog Server (or compatible). It receives, compresses, encrypts and securely transports, syslog messages from distributed network devices to Kiwi Syslog Server.

Kiwi Secure Tunnel is provided only as a Service Edition that runs on Windows XP or Windows 2003. The Kiwi Secure Tunnel Manager program provides the interface to configure and manage the Windows NT service.

The Kiwi Secure Tunnel is made up of a client and a server.

The Tunnel Client gathers messages from one or more devices on a network and forwards the messages across a secure link to the Tunnel Server.

The Server then forwards the messages on to one or more Syslog Servers.

Kiwi Secure Tunnel also has the ability to monitor the contents of selected files and send data from these files as syslog messages to Kiwi Syslog Server using the Secure Tunnel.

To download or find our more information about the Kiwi Secure Tunnel please visit the SolarWinds website

12.5 Kiwi Harvester

Kiwi Harvester is a free application that listens for data via the computer's serial interface and converts the data received into standard syslog messages. The messages are then forwarded via the UDP protocol to a

©2014 SolarWinds, Inc.

central logging server such as Kiwi Syslog Server.

The Kiwi Harvester allows you to integrate non-ethernet enabled devices into your central logging system. Such devices include: PBX call logging systems, main frame computers, remote sensing devices and router console ports.

Kiwi Harvester is installed as a Windows service on Windows XP and Windows 2003.

The application has a small footprint and is easily and quickly configured via an ini text file.

The purpose of the Kiwi Harvester is to enable non-ethernet and non syslog capable devices to send their notification messages to a central logging server such as Kiwi Syslog Server.

Typical uses might include:

- Forwarding of router console messages for out of band notification.
- Forwarding of PBX call records for billing purposes.
- Forwarding of messages from a remote sensing device or PLC device.
- Out of band messaging for a secure firewall. (Redirect the logging output to the serial port)
- Capturing of redirected printer output. (Printer port set to Com1)

To download or find our more information about the Kiwi Harvester please visit the SolarWinds website

©2014 SolarWinds, Inc.