

 ADMINISTRATOR GUIDE

Kiwi Syslog Server

Version 9.6

© 2017 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.

Table of Contents

About Kiwi Syslog Server	14
Get started with Kiwi Syslog Server	14
Learn more	14
Features in the free and licensed editions of Kiwi Syslog Server	15
Overview of licensed features	15
Detailed comparison of free and licensed features	15
Configure devices to send messages to Kiwi Syslog Server	18
Set display options	19
Rename console displays and change display options	19
Choose highlighting options and message font	19
Highlighting options	19
Message font	20
Add rules, filters, and actions	22
How rules, filters, and actions work	22
How rules are applied	23
Default rule	24
Next steps	24
Define rules	24
Add a filter	25
Filter messages based on priority	25
Filter messages based on IP address	26
Filter messages based on host name	28
Filter messages based on message text	29
Filter messages based on time of day	31
Trigger actions based on flags or counters	32

Filter messages based on input source	34
Regular expressions supported by Kiwi Syslog Server	35
Examples	37
Add an action	38
Add an action to display a message	38
Add an action to log messages to a file	39
Add an action to forward messages to another host	40
Add an action to play a sound	42
Add an action to run an external program	43
Add an action to send an email message	44
Add an action to send a syslog message	47
Add an action to log messages to a database	47
Prepare the database	48
Add the action	48
Add an action to log to the NT event log	50
Add an action to send an SNMP trap	51
Add an action to stop processing the message	53
Add an action to run a script	53
Script file caching	56
Triggering a script on a regular basis	56
Add an action to send a pager or SMS message via NotePager Pro	56
Add an action to log messages to Kiwi Server Web Access	57
Add an action to reset flags and counters	58
Add an action to log messages to Papertrail.com (a cloud-based server)	58
AutoSplit values in Kiwi Syslog Server	59
Message content or counters	66
All of the message	66
Date	66

Time	66
Facility	66
Level	67
Host address of sender	67
The message text	67
Alarm min msg threshold	67
Alarm max msg threshold	67
Alarm disk space threshold	67
Message count this hour	67
Message count last hour	68
Machine MAC address	68
Rule Name	68
Custom/Global/Statistics fields (Only in the registered version)	68
Test a filter or an action	69
Use the Test button on the filter or action setup dialog	69
Use the Kiwi SyslogGen utility	69
Rearrange rules, filters, actions, and schedules	69
Copy a filter or an action to a different rule	70
Import and export rules	70
Export a rule	71
Import a rule	71
Keyboard shortcuts for rules, filters, actions, and schedules	71
Scripting resources	73
Script examples	73
PIX message lookup	73
Run Script action setup	73
Rules setup	73
All the variables - (Info function)	75

Scripting custom statistics fields	76
Script variables	77
Common fields	77
Fields.VarFacility	77
Fields.VarLevel	77
Fields.VarInputSource	78
Fields.VarPeerAddress	78
Fields.VarPeerName	78
Fields.VarPeerDomain	78
Fields.VarCleanMessageText	79
Other fields	79
Fields.VarDate	79
Fields.VarTime	79
Fields.VarMilliseconds	79
Fields.VarSocketPeerAddress	79
Fields.VarPeerAddressHex	80
Fields.VarPeerPort	80
Fields.VarLocalAddress	80
Fields.VarLocalPort	80
Fields.VarPriority	81
Fields.VarRawMessageText	81
Custom fields	81
Fields.VarCustom01 to Fields.VarCustom16: Inter-script fields	81
Fields.VarGlobal01 to Fields.VarGlobal16: Custom script fields	81
Fields.VarGlobal01 to Fields.VarGlobal16: Control and timing fields	82
Script functions	82
Built-in functions of the "Fields" object	82
Fields.IsValidIPAddress(IPAddress as string) as Boolean	82

Fields.ConvertIPtoHex(IPAddress As String) As String	83
Fields.GetDailyStatistics() As String	83
Fields.ConvertPriorityToText(PriorityValue)	83
Fields.ActionPlaySound(SoundFilename As String, RepeatCount as Long)	84
Fields.ActionSendEmail(MailTo, MailFrom, MailSubject, MailMessage , [MailImportance] , [MailPriority] , [MailSensitivity])	84
Fields.ActionLogToFile(Filename, Data, [RotateLogFile] , [RotationType] , [NumLogFiles] , [Amount] , [Unit])	86
Fields.ActionSendSyslog(Hostname, Message, Port, Protocol)	88
Fields.ActionSpoofSyslog(AdapterAddress, SrcAddress, DstAddress, DstPort, Message)	89
Call Fields.ActionSpoofSyslog(AdapterAddress, SrcAddress, DstAddress, DstPort, Message)	90
Fields.ActionDeleteFile(Filename)	92
Fields.ActionDisplay(DisplayNumber, TabDelimitedMessage)	93
Fields.ActionLogToODBC(DSNString, TableName, InsertStatement, Timeout)	93
JScript escape characters	95
Scripting dictionaries	96
Built in functions of the "Dictionaries" object	96
StoreItem	96
AddItem	96
UpdateItem	97
RemoveItem	97
RemoveAll	97
Delete	97
DeleteAll	98
GetItemCount	98
GetItem	98
ItemExists	98
GetKeys	99
GetItems	99

Error Reference	99
Scripting tutorial	100
Task 1: Create the script action	100
Task 2: Create the actions	101
Task 3: Test the script	101
Task 4: Test the script with SyslogGen	102
Create scheduled tasks	103
Create a scheduled task to archive log files	103
Create a scheduled task to delete files	106
Create a scheduled task to run a program	107
Create a scheduled task to run a script	109
Set alarms	112
Log file and database formats	114
Log file formats available in Kiwi Syslog Server	114
Kiwi format ISO yyyy-mm-dd (Tab delimited)	114
Kiwi format ISO UTC yyyy-mm-dd (Tab delimited)	114
Kiwi format mm-dd-yyyy (Tab delimited)	114
Kiwi format dd-mm-yyyy (Tab delimited)	114
Kiwi format UTC mm-dd-yyyy (Tab delimited)	115
Kiwi format UTC dd-mm-yyyy (Tab delimited)	115
Comma Separated Values yyyy-mm-dd (CSV)	115
Comma Separated Values UTC yyyy-mm-dd (CSV)	115
BSD Unix syslog format	115
XML tagged format	115
RnRsoft ReportGen format	116
WebTrends format	116
Cisco PIX PFSS format (Raw logging)	116
3Com 3CDaemon format (BSD space delimited)	116

Raw - Message text only (no priority)	116
Sawmill format ISO yyyy-mm-dd (Tab delimited)	117
Create a custom log file format	117
Examples of fields and values	118
Database formats available in Kiwi Syslog Server	119
Default Microsoft Access database table design	119
Default Microsoft SQL and generic SQL database table design	120
Default MySQL database table design	120
Default Oracle database table design	120
Create a custom database format	120
Examples of data formats	123
DNS setup options	124
DNS resolution	124
DNS setup	126
DNS caching	128
Syslog message modifiers	132
Configure email options	134
Configure input options	137
Configure UDP input options	137
Configure TCP input options	139
Configure secure (TLS) TCP options	141
Configure SNMP trap input options	143
Enable keep-alive messages	147
Enable and configure keep-alive messages	147
How to use a keep-alive message in a script	148
Forwarding a keep-alive message to another host as a beacon	149
Enable IPv6 support	149
Enable a beep on every message	149

View syslog statistics	150
Protocols	153
The syslog protocol	153
Syslog Facilities	153
Syslog Levels	154
Syslog Priority values	155
Transport	156
Syslog RFC 3164 header format	156
The Kiwi Reliable Delivery Protocol (KRDP)	157
The problem	157
The solution	157
Unique message sequencing	157
Dealing with international characters	158
The KRDP message format	158
Message Types (MsgType)	158
Message format	158
Sequence of events	158
Rules	159
Message formats	159
KRDP error messages	160
Error and mail logs	162
The error log	162
The send mail log	162
Registry settings for Kiwi Syslog Server	163
Best practices	163
Available settings	163
DisplayColumnsEnabled	166
DisplayRowHeight	167

MailStatsDeliveryTime	167
ServiceStartTimeout	168
ServiceUpdateTimeout	168
NTServiceSocket	169
NTServiceDependencies	169
DebugStart	170
Command line value	170
Applies to	170
Effect	171
Files created	171
When to use	171
DNSSDisableWaitWhenBusy	171
DNSCacheMaxSize	172
DNSCacheFailedLookups	172
DNSSetupQueueBufferBurstCoefficient	173
DNSSetupQueueBufferClearRate	173
DNSSetupQueueLimit	174
DNSSetupDebugModeOn	174
MsgBufferSize	174
MailAdditionalSubjectText	175
MailAdditionalBodyText	176
MailMaxMessageSend	177
File write caching settings	178
FileWriteCacheEnabled	178
FileWriteCacheTimeout	179
FileWriteCacheEntries	179
FileWriteCacheMaxSizeKB	180
FileWriteCacheCleanup	180

FileWriteCacheFileLock	181
FileWriteCacheOpenFiles	181
LogFileDateSeparator	182
LogFileTimeSeparator	183
LogFileEncodingFormat	183
ScriptEditor	184
ScriptTimeout	185
DBCommandTimeout	186
ArchiveFileReplacementChr	186
ArchiveFileSeparator	187
UseOldArchiveNaming	187
ArchiveTempPath	188
EnableArchiveTempFile	188
ErrorLogFolder	189
MailLogFolder	189
KRDPACKTimer	190
KRDPCacheFolder	190
KRDPRxDebug	191
KRDPTxDebug	191
KRDPQueueSize	192
KRDPQueueMaxMBSize	192
KRDPAutoConnect	193
KRDPCConnectTime	193
KRDPSendSpeed	194
KRDPIidleTimeout	194
KRDPAAddSeqToMsgText	195
ProcessPriority	195

OriginalAddressStartTag and OriginalAddressEndTag	197
MaxRuleCount	198
DBLoggerCacheClearRate	198
DBLoggerCacheTimeout	199
DBLoggerCacheDisable	199
HostNosToDisplay	200
Command line arguments	201
Start-up Debug	201
Service - Install Service	201
Service - Uninstall Service	202

About Kiwi Syslog Server

Kiwi Syslog Server is a syslog server for the Windows platform. It receives syslog messages and SNMP traps from network devices such as routers, switches, and firewalls.

Kiwi Syslog Server includes many options for customization. For example, you can create rules to automatically respond to messages that meet the specified criteria, and you can set up schedules to automatically archive logs for regulatory compliance.

Get started with Kiwi Syslog Server

For information about downloading and installing Kiwi Syslog Server, including the system requirements and port requirements, see the [Kiwi Syslog Server Installation Guide](#).

i When you initially install Kiwi Syslog Server, all features are available during a 14-day trial period. When the trial period ends, you can continue to use the free edition without purchasing a license. Or you can enter a license key to access [features in the licensed edition](#).

To upgrade to the latest version, see the [Kiwi Syslog Server Upgrade Guide](#).

If you're new to Kiwi Syslog Server, see the [Kiwi Syslog Server Getting Started Guide](#). This guide walks you through examples of common configuration tasks.

i Not seeing messages? See the [troubleshooting tips](#) in the Getting Started Guide.

Learn more

See the following sections in this guide to learn more about:

- [Configuring devices](#) to send messages to Kiwi Syslog Server.
- [Adding rules, filters, and actions](#) to specify how Kiwi Syslog Server processes incoming messages.
- [Creating schedules](#) to archive messages and automatically clean out the archives after the required retaining period.
- Customizing your environment by choosing [message highlighting](#) and [console display options](#).
- Creating [scripts](#).
- [DNS setup options](#).

Features in the free and licensed editions of Kiwi Syslog Server





When you initially [install Kiwi Syslog Server](#), all features are available during a 14-day trial period. When the trial period ends, you can continue to use the free edition without purchasing a license. Or you can [enter a license key](#) to access features in the licensed edition.

Overview of licensed features

With the licensed edition of Kiwi Syslog Server, you can:

- Receive messages from an unlimited number of devices.
- To improve log organization, automatically split logs by device, functional role, or message contents.
- Implement your log retention policy with automatic archival and clean-up tasks.
- View messages from anywhere using Kiwi Syslog Web Access, a secure Web viewer.
- Apply message highlighting rules and DNS resolution of obscure IP addresses to help you quickly find the information you need.
- Forward messages to other syslog servers, databases (such as SQL Server), the Windows Event Log, SNMP, or other email addresses. You can configure Kiwi Syslog Server to act as a "syslog proxy" (spoof) and forward messages with original source information in the forwarded messages.
- Set up filters to react to specified message content, types of messages, messages sent at specified times, or a number of similar messages (such as five alerts in a row).
- Configure additional actions, including sending email notifications, playing sounds, running scripts, and running executables. Scripts and executables can be used to implement advanced filters and actions.

Detailed comparison of free and licensed features

	FREE EDITION	LICENSED EDITION
Collecting messages		
Maximum devices	5	Unlimited
Syslog (UDP and TCP)		
SNMP		
Message buffer	500	500,000

	FREE EDITION	LICENSED EDITION
Logging to disk		
Write logs to disk	✓	✓
Split by priority	✓	✓
Split by time of day	✓	✓
Split by IP or host name		✓
Split by network		✓
Split on message content		✓
Split by input source (UPD, TCP, or SNMP)		✓
Log file retention		
Unique log per day	✓	✓
Rotate on number of files		✓
Rotate on file size		✓
Rotate on file age		✓
Viewing messages		
Display windows	10	25
Statistics graphs	✓	✓
Custom font and color	✓	✓
Web-based displays		✓
Highlighting rules		✓
DNS resolution of IPs		✓
Forwarding messages		
To syslog (UDP or TCP)	✓	✓

	FREE EDITION	LICENSED EDITION
To database		✓
To Windows Event Log		✓
To SNMP		✓
To email		✓
As proxy (spoofed source)		✓
Filtering messages		
By time received	✓	✓
By priority	✓	✓
By host name or IP address of sending device		✓
By message text		✓
By input source		✓
By count of similar messages		✓
Reacting to messages		
High traffic alert	✓	✓
Send email		✓
Play sound		✓
Run script		✓
Run executable		✓
Configuring server and rules		
Tray icon status	✓	✓
GUI management application	✓	✓
Secure Web access		✓

Configure devices to send messages to Kiwi Syslog Server

To receive messages from a syslog-capable device, configure the device to send syslog messages to the appropriate port on the computer where Kiwi Syslog Server is installed.

Kiwi Syslog Server automatically listens for UDP messages on port 514. This is the default port for devices sending syslog messages as defined by the RFC standard 5426.

i You can configure Kiwi Syslog Server to [listen for UDP message on a different port](#). You can also enable Kiwi Syslog Server to listen for [TCP messages](#), [secure TCP messages](#), and [SNMP traps](#).

For information about configuring a specific device, see documentation from the device manufacturer. The Kiwi Syslog Server Getting Started Guide provides [an example of configuring a Cisco switch](#).

i Message logging must be enabled on the device. On many devices that generate syslog messages, logging is enabled by default.

If you have configured devices but Kiwi Syslog Server is not displaying messages, see the [troubleshooting tips](#) in the Getting Started Guide.

Set display options

You can rename and configure the console displays, and you can choose highlighting options for messages.

- [Rename console displays and change display options](#)
- [Choose message display options](#)

Rename console displays and change display options

Kiwi Syslog Server provides multiple displays which you can use to segment data. For example, you can create rules to log all messages to the default display but only high-priority messages to another display. You can give each display a more meaningful name, and specify other display options such as how many rows are shown.

1. Select File > Setup.
2. Click Display.
3. To rename a display:
 - a. Select the display under Modify display names.
 - b. Enter the new name in the box on the right.
 - c. Click Update.

The menu on the left is updated.

4. To change other display options, select or clear the associated check boxes.

 Except for display names, the changes you make affect all displays.


5. Click Apply to apply changes to the displays, and click OK to close the dialog box.

Choose highlighting options and message font

You can customize how messages are displayed in the console:

- Use [highlighting](#) to apply a set of display options to messages that meet the specified criteria.
- Change the [font, style, and color](#) of the message text.

HIGHLIGHTING OPTIONS

 This feature is available only in the registered version.

Use the highlighting options in Kiwi Syslog Server to specify a set of highlighting rules which will be applied to each message shown on the Kiwi Syslog Service Manager display. Highlighting rules are evaluated from the top-down, and any syslog messages that match a given rule will have the associated effects applied.

1. Select View > Highlighting options.
The Highlighting Options dialog box opens.
2. Select the following options and click OK.

Highlight Items	<p>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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>i That the first time you access the Highlighting 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.</p> </div>							
String to match	<p>The string pattern that will be searched for in the selected syslog message field.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Regular Expression</td> <td style="padding: 5px;">If checked, this option specifies if the string to match is a regular expression. See Regular Expressions.</td> </tr> <tr> <td style="padding: 5px;">Invert Match</td> <td style="padding: 5px;">If checked, this option specifies that the effect will be applied only if a match is NOT found.</td> </tr> <tr> <td style="padding: 5px;">Ignore Case</td> <td style="padding: 5px;">If checked, the search pattern (string to match) will be treated as case insensitive.</td> </tr> </table>		Regular Expression	If checked, this option specifies if the string to match is a regular expression. See Regular Expressions .	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.
Regular Expression	If checked, this option specifies if the string to match is a regular expression. See Regular Expressions .							
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	<p>Select the desired formatting and icons.</p> <p>A set of default icons is supplied. You can add additional icons 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 Server for the new icons to be displayed in this list.</p>							


MESSAGE FONT

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

1. Select View > Choose font.

The Font dialog opens.

2. Select the font options and click OK.

 If non ASCII characters appear in the display as blanks or square blocks, it means that the selected font doesn't contain the required Unicode character glyph. If you have Microsoft Office installed, Arial MS Unicode includes all Unicode glyphs.

Add rules, filters, and actions

Use rules, filters, and actions to specify how Kiwi Syslog Server processes the syslog messages it receives. See the following topics:

- [How rules, filters, and actions work](#)
- [Define rules](#)
- [Add a filter](#)
- [Add an action](#)
- [Test a filter or action](#)
- [Rearrange rules, filters, and actions](#)
- [Copy a filter or an action to a different rule](#)
- [Import and export rules](#)
- [Keyboard shortcuts for rules, filters, actions, and schedules](#)

How rules, filters, and actions work

Rules determine what actions Kiwi Syslog Server takes when it receives a message, and which messages trigger these actions. For example, you can create rules to:

- Log all messages to a file.
- Send an email if the message has a high priority level.
- Run a script if the message includes specific words or phrases.

Rules consist of the following elements:

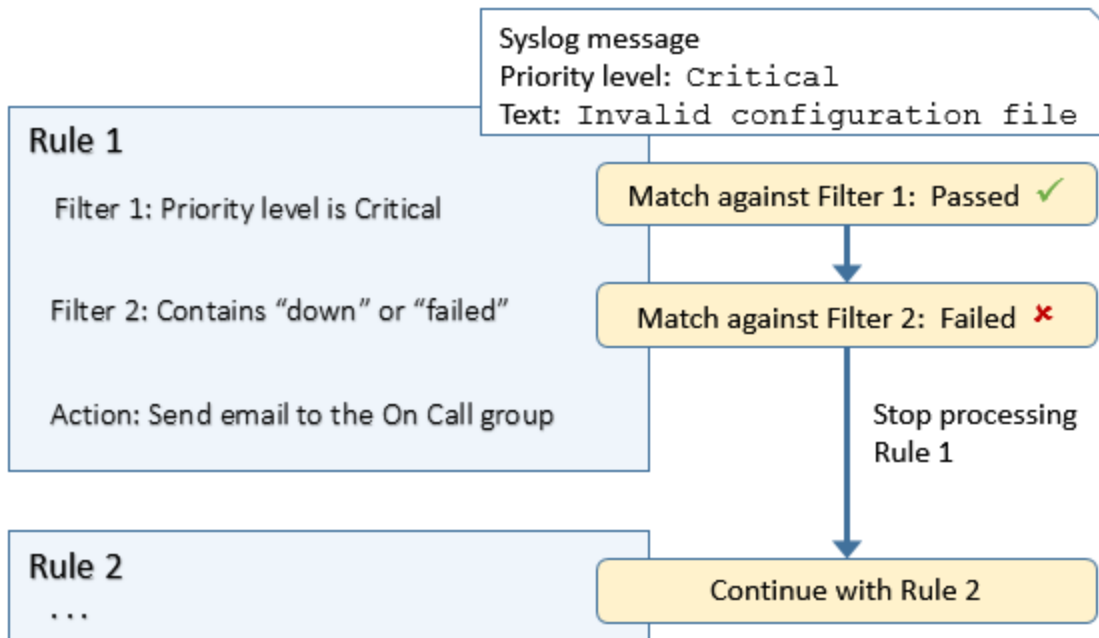
- **Filters** determine which messages trigger the actions. If a rule does not include any filters, all messages are acted on.
- **Actions** determine what happens when a message passes all of the filters.

You can define up to 100 rules. Each rule can include up to 100 filters and 100 actions.

HOW RULES ARE APPLIED

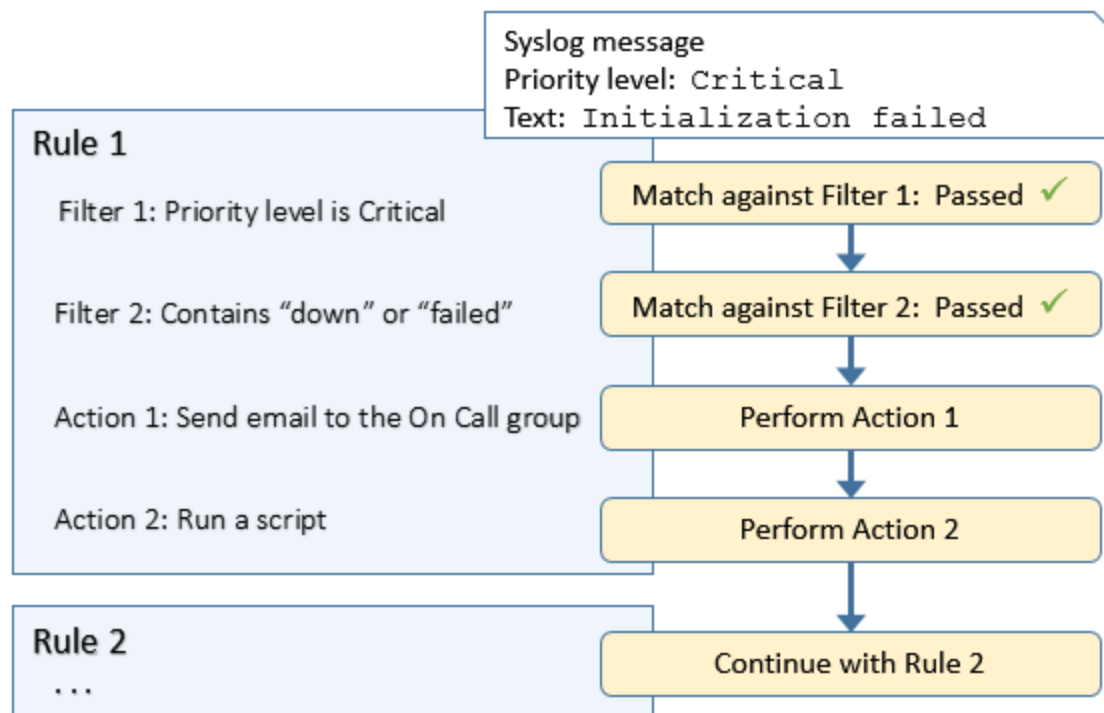
When a message is received, rules are applied to the message in order, starting with the rule at the top of the list. When a rule is applied to a message:

1. The message is matched against each filter in that rule, starting with the filter at the top of the list.
 - If the message passes a filter (all conditions in the filter return `TRUE`), it is matched against the next filter in that rule.
 - If the message does not pass a filter, processing stops for that rule and Kiwi Syslog Server applies the next rule.



- If the message passes all filters, each action is performed. Actions are performed in order, starting with the action at the top of the list.

When all actions within that rule have been performed, Kiwi Syslog Server applies the next rule.



DEFAULT RULE

When you install Kiwi Syslog Server, a rule named Default is created automatically. This rule applies two actions to all messages:

- Displays each message on the Kiwi Syslog Service Manager console.
- Logs each message to the `SyslogCatchAll.txt` file, which is located in the `\Logs` directory of the Kiwi Syslog Server installation folder.

NEXT STEPS

To define how Kiwi Syslog Server processes and responds to messages, complete the following tasks:

- [Define rules](#)
- Add [filters](#) to a rule
- Add [actions](#) to a rule
- [Rearrange rules, filters, and actions](#)
- [Copy a filter or an action to a different rule](#)

Define rules

Add [rules](#) to specify what actions Kiwi Syslog Server takes when a message meets the specified criteria.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
The Kiwi Syslog Server Setup dialog opens.
2. In the left pane, right-click Rules and choose Add rule.
A new rule is added to the tree.
3. Replace the default name with a descriptive name. (The name does not have to be unique.)
4. [Add one or more filters](#).
5. [Add one or more actions](#).
6. Click OK to save your changes.

Add a filter

Add one or more filters to each [rule](#) to determine which messages trigger the actions in the rule. Each rule can include up to 100 filters.

Filters are applied in order. The output from the first filter becomes the input for the next filter. You can [change the order](#) of the filters applied to a rule.

See the following topics for more information:

- [Filter messages based on priority](#)
- [Filter messages based on IP address](#)
- [Filter messages based on host name](#)
- [Filter messages based on message text](#)
- [Filter messages based on time of day](#)
- [Trigger actions based on flags or counters](#)
- [Filter messages based on input source](#)
- [Regular expressions supported by Kiwi Syslog Server](#)

FILTER MESSAGES BASED ON PRIORITY

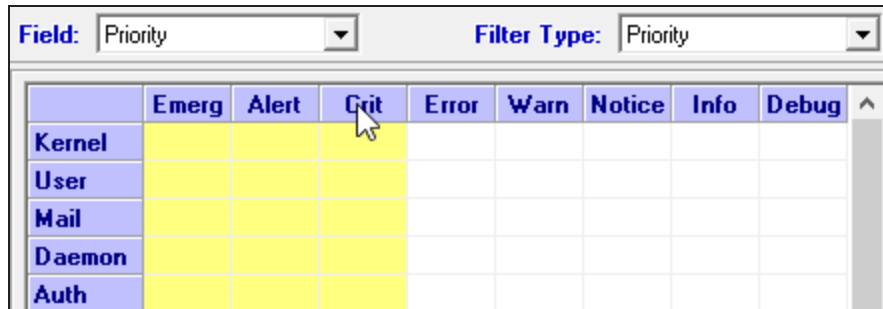
Each incoming message contains a priority value, which is made up of a facility and a level. Use the Priority filter to [trigger an action](#) when you receive messages with the selected priority. For example, you can create a rule that sends an email when you receive a message with a priority level of critical and higher.

 If a rule does not contain a Priority filter, all priorities are included.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) a new rule, or locate an existing rule.
3. Right-click the Filters node below the rule, and choose Add Filter.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. In the Field menu, select Priority.

6. Select one or more cells to specify the facility and level of messages to include:
 - Click and drag to select a block of cells.
 - Click a heading to select an entire column or row.
 - Click and drag across headings to select multiple columns or rows.

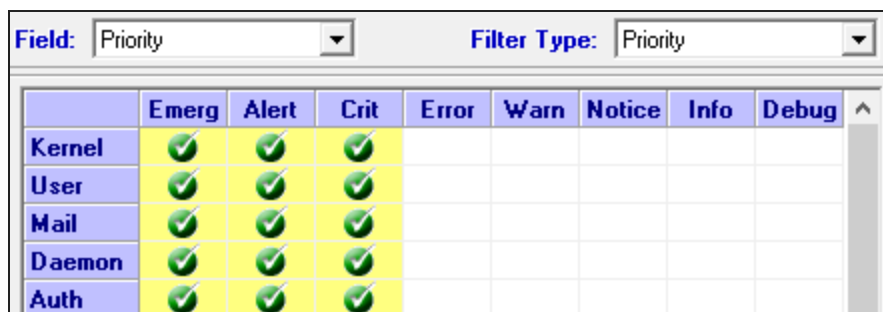
Selected cells are highlighted.



	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel								
User								
Mail								
Daemon								
Auth								

7. Right-click the highlighted area and select Toggle to On.

Green check marks indicate that the column cells are included.




	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel		✓	✓					
User		✓	✓					
Mail		✓	✓					
Daemon		✓	✓					
Auth		✓	✓					

8. (Optional) [Test the filter](#).
9. Click Apply to save the filter.

Only messages with the selected priorities trigger the [actions](#) in the associated rule.

FILTER MESSAGES BASED ON IP ADDRESS

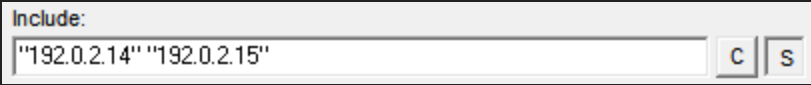

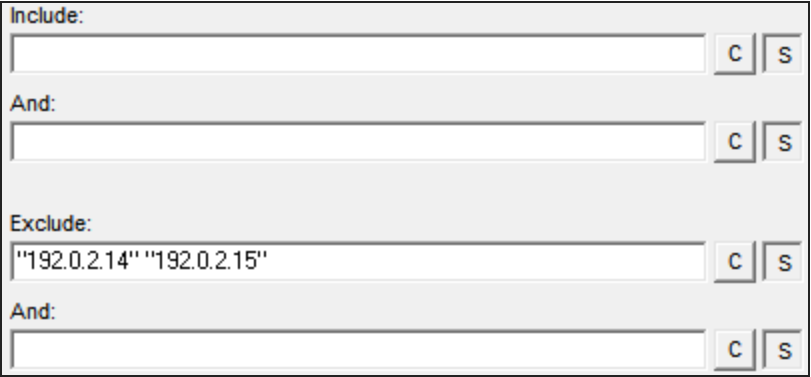
 This feature is available only in the licensed version.

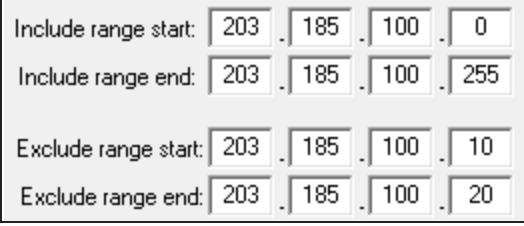
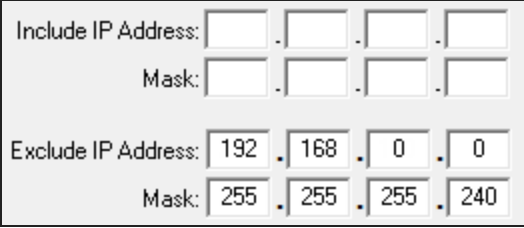
Use an IP address filter to include or exclude messages based on the IP address of the sending device. Only messages from included IP addresses [trigger the actions in the associated rule](#).

 If a rule does not contain an IP address filter, all IP addresses are included.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) a new rule, or locate an existing rule.
3. Right-click the Filters node below the rule, and choose Add Filter.

4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. In the Field menu, select IP address.
6. Select an option from the Filter Type menu, and specify one or more IP addresses.


Simple	<p>Enter one or more IP addresses to include. Enclose each IP address in quotes.</p> <p>There is an OR relationship between the IP addresses. Messages from any of the IP addresses are included.</p> <p>In the following example, a message is included if the IP address of the sending device is 192.0.2.14 or 192.0.2.15.</p> 
Complex	<p>Enter the IP addresses to include or to exclude. Enclose each IP address in quotes.</p> <p>There is an OR relationship between IP addresses on the same line. Messages are included or excluded if they are sent from any of the IP addresses on the line.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> For IP addresses, Complex filters are primarily used to exclude specific addresses. Do not use both the Include and Exclude sections. (If you include specific IP addresses, all others are automatically excluded.) Also, do not use the And lines.</p> </div> <p>In the following example, a message is excluded if the IP address of the sending device is 192.0.2.14 or 192.0.2.15.</p> 
RegExp	<p>Enter one or more regular expressions to specify the IP addresses to include or exclude.</p>
IPv4 Range	<p>Enter the range of IP addresses to include, exclude, or both.</p> <p>In the following example, a message is included if the sending device's IP address is between 192.0.2.0 and 192.0.2.24, but is not between 192.0.2.10 and 192.0.2.12.</p>

	 <p>Include range start: 203 . 185 . 100 . 0 Include range end: 203 . 185 . 100 . 255 Exclude range start: 203 . 185 . 100 . 10 Exclude range end: 203 . 185 . 100 . 20</p>
IPv4 Mask	<p>Specify a range of IP addresses to include or exclude based on mask matching. The IP address is logically AND'ed with the specified Mask and then compared with the IP address of the sending device. If the two addresses are on the same subnet, then the filter result is TRUE.</p> <p>In the following example, the message is excluded If the sending device's IP address is within the range of 192.168.0.0 to 192.168.0.15.</p>  <p>Include IP Address: [] . [] . [] . [] Mask: [] . [] . [] . [] Exclude IP Address: 192 . 168 . 0 . 0 Mask: 255 . 255 . 255 . 240</p>
IPv6 Range	<p>Enter the range of IP addresses to include, exclude, or both. (For a range example, see IPv4 Range.)</p>


7. (Optional) [Test the filter](#).
8. Click Apply to save the filter.

Only messages from included IP addresses trigger the [actions](#) in the associated rule.

FILTER MESSAGES BASED ON HOST NAME

 This feature is available only in the licensed version.

Use the Hostname filter to include or exclude messages based on the host name of the sending device. Only messages from included hosts [trigger the actions in the associated rule](#).

 If a rule does not contain a Hostname filter, all hosts are included.


1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) a new rule, or locate an existing rule.
3. Right-click the Filters node below the rule, and choose Add Filter.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. In the Field menu, select Hostname.
6. Select an option from the Filter Type menu, and specify one or more host names.

Simple	Enter one or more host names to include. Enclose each name in quotes. There is an OR relationship between the host names. Messages from any of these hosts are included.
Complex	Enter the host names to include or to exclude. Enclose each name in quotes. There is an OR relationship between host names on the same line. Messages are included or excluded if they are sent from any of the hosts on the line.
RegExp	Enter one or more regular expressions to specify the host names to include or exclude.

7. (Optional) [Test the filter](#).
8. Click Apply to save the filter.

Only messages from included hosts trigger the [actions](#) in the associated rule.


FILTER MESSAGES BASED ON MESSAGE TEXT

 This feature is available only in the licensed version.

Use the Message text filter to include or exclude messages based on the content of the message. Only included messages [trigger the actions in the associated rule](#). For example, you can create rules to send an email or run a script when a message contains specific text strings.

 If a rule does not contain a Message text filter, all messages are included.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) a new rule, or locate an existing rule.
3. Right-click the Filters node below the rule, and choose Add Filter.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. In the Field menu, select Message text.
6. Select an option from the Filter Type menu, and specify one or more text strings.

Simple	Enter one or more text strings, enclosed in quotes. There is an OR relationship between the strings. A message meets the filter criteria (returns TRUE) if it includes any of the strings.  • Select the C button to make the search case-sensitive.
--------	---



- Select the S button to perform a substring search (the default). A substring search returns TRUE if the text string appears anywhere in the message.

Deselect the S button to perform a whole string search. A whole string search returns TRUE only if the text string matches the entire message text.

Example: If the text string is "down" and the messages is `System down`, a substring search returns TRUE, but a whole string search does not.

In the following example, a message is included if it contains POP3 or SMTP or MAPI. The filter is not case-sensitive.

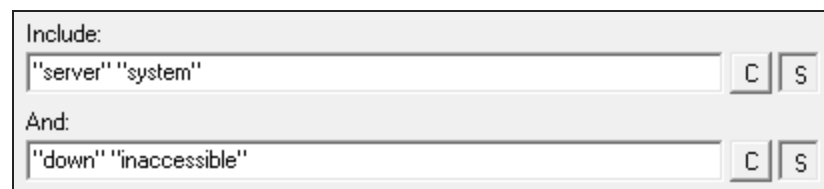


Include:
"POP3" "SMTP" MAPI [C] [S]

Complex Enter one or more text strings to include, exclude, or both. Enclose each string in quotes. There is an OR relationship between strings on the same line. Optionally, enter strings on the And line to include a Boolean AND operator.

Include The message is included if it contains any string on the Include line **and** any string on the And line.

In the following example, a message is included if it contains (`server` or `system`) and (`down` or `inaccessible`).

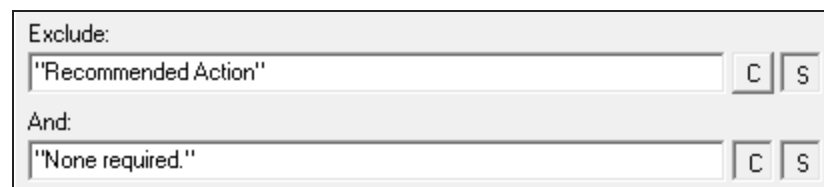


Include:
"server" "system" [C] [S]
And:
"down" "inaccessible" [C] [S]

The message "The system is down" is included, but not "The system is up."

Exclude The message is excluded if it contains any string on the Exclude line **and** any string on the And line.

In the following example, a message is excluded if it contains `recommended action` (not case-sensitive) and `None required.` (case sensitive).



Exclude:
"Recommended Action" [C] [S]
And:
"None required." [C] [S]

	<p>Both</p> <p>You can use both the Include and Exclude sections. In the following example, the message is included if it contains (server or system) and (down or inaccessible) but does not contain test.</p> <p>The message System down is included, but not the message Test system down.</p> <div data-bbox="480 415 1295 802" style="border: 1px solid gray; padding: 5px;"> <p>Include: <input style="width: 150px;" type="text" value="server"/> <input style="width: 150px;" type="text" value="system"/> <input type="button" value="C"/> <input type="button" value="S"/></p> <p>And: <input style="width: 150px;" type="text" value="down"/> <input style="width: 150px;" type="text" value="inaccessible"/> <input type="button" value="C"/> <input type="button" value="S"/></p> <p>Exclude: <input style="width: 150px;" type="text" value="test"/> <input type="button" value="C"/> <input type="button" value="S"/></p> <p>And: <input style="width: 150px;" type="text"/> <input type="button" value="C"/> <input type="button" value="S"/></p> </div>
RegExp	Enter one or more regular expressions to specify text strings to include or exclude.

7. (Optional) [Test the filter](#).

8. Click Apply to save the filter.

Only included messages trigger the [actions](#) in the associated rule.

FILTER MESSAGES BASED ON TIME OF DAY

Use the Time of day filter to include messages sent during specific times. For example, you can use this filter to stop processing messages sent during test or maintenance periods. Only messages sent during the specified times [trigger actions in the associated rule](#).

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) a new rule, or locate an existing rule.
3. Right-click the Filters node below the rule, and choose Add Filter.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. In the Field menu, select Time of day.

6. Select one or more cells to specify the times to include:
 - Click and drag to select a block of cells.
 - Click a heading to select an entire column or row.
 - Click and drag across headings to select multiple columns or rows.

 To exclude a time period, select that time period and click Inverse.

Selected cells are highlighted.

Field:	Time of day	Filter Type:	Time of day				
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00:00							
00:15							
00:30							
00:45							
01:00							

7. Right-click the highlighted area and select Toggle to On.


Green check marks indicate that the column cells are included.

Field:	Time of day	Filter Type:	Time of day				
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00:00		✓	✓	✓	✓	✓	
00:15		✓	✓	✓	✓	✓	
00:30		✓	✓	✓	✓	✓	
00:45		✓	✓	✓	✓	✓	
01:00		✓	✓	✓	✓	✓	

8. (Optional) [Test the filter](#).
9. Click Apply to save the filter.

Only messages received during the specified times trigger the [actions](#) in the associated rule.

TRIGGER ACTIONS BASED ON FLAGS OR COUNTERS

 This feature is available only in the licensed version.

Use Flags/Counters filters to trigger or suppress actions based on the number of times a filter returns TRUE during the specified interval. The following Flags/Counters filters are available:

- Use a **Time interval** filter to avoid triggering the same action multiple times during the specified interval.

Example: a rule sends an email alert when a message contains the text "link down." When a problem occurs, the link sometimes goes up and down many times a minute, and you receive an email alert for each "link down" message. To prevent this, you include a Time interval filter with a value of 5. Kiwi Syslog Server sends an email alert for the first "link down" message. Other "link down" messages during next five minutes do not trigger additional email alerts.


- Use a **Threshold** filter to be alerted if a message is sent more than a certain number of times during the specified interval.

Example: you occasionally receive a message containing the text "port scan detected," but you don't want to be alerted unless it occurs more than five times within a minute. That frequency would indicate that someone is persistently scanning your network.



You can also use this filter to watch for failed login attempts. If the text "login failed" occurs more than five times within 30 seconds, it could indicate a brute force login attempt.


- Use a **Timeout** filter to monitor syslog devices and send an alert when a device is unexpectedly quiet. This filter triggers an action when the filters that precede it in the rule are **not** met a minimum number of times per interval.

Example: your firewall normally generates at least 200 messages per hour. If the number of messages drops below 10 in an hour, this filter triggers an email alert.

 The internal counter or timer used by these filters can be reset with the action to [reset flags and counters](#).

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) a new rule, or locate an existing rule.
3. Right-click the Filters node below the rule, and choose Add Filter.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. In the Field menu, select Flags/Counters.
6. Select an option from the Filter Type menu.


Time interval	<p>Enter a time interval in minutes.</p> <p> A Time interval filter should be the last filter in a rule. You can reorder filters.</p>
Threshold	<ol style="list-style-type: none"> 1. Enter the threshold and interval (in seconds). 2. To have a separate count for messages from different IP addresses, select Maintain individual threshold counts. <p> A Threshold filter should be the last filter in a rule.</p>

Timeout	<p>To configure a Timeout filter:</p> <ol style="list-style-type: none">1. Add one or more filters before the Timeout filter to specify which messages to count. (For example, to watch for inactivity on the firewall, create a filter to include only messages from the firewall's IP address.)2. In the Timeout filter, enter the minimum number of times the message should be received.3. Enter the time interval in minutes.4. (Optional) To avoid triggering an alert at times when low activity is expected, add a Time of day filter to include only certain days and time periods. <div data-bbox="354 583 1513 688" style="border: 1px solid orange; background-color: #fff9c4; padding: 5px;"><p> Other than the optional Time of day filter, a timeout filter should be the last filter in a rule.</p></div> <p>When this filter returns TRUE, a message with the following format is passed to any actions in the rule:</p> <p>Priority: Local7.Debug (191) HostIP: 127.0.0.1 (localhost) MsgText: The rule '<i>ruleName</i>' has only been matched x times in y minutes. The threshold was set for z times.</p>
---------	--


7. (Optional) [Test the filter](#).
8. Click Apply to save the filter.

[Actions](#) in the associated rule are triggered when the specified threshold is exceeded (for Time interval and Threshold filters) or is not met (for Timeout filters).

FILTER MESSAGES BASED ON INPUT SOURCE

 This feature is available only in the licensed version.

Use the Input source filter to [trigger an action](#) only if the input source of the message matches one of the selected input sources (for example, only TCP messages).

 If there is no Input source filter in the rule, all input sources are included.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) a new rule, or locate an existing rule.
3. Right-click the Filters node below the rule, and choose Add Filter.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. In the Field menu, select Input source.
6. Select one or more input sources.

7. (Optional) [Test the filter](#).
8. Click Apply to save the filter.

[Actions](#) in the associated rule are triggered only by messages from the selected input source.

REGULAR EXPRESSIONS SUPPORTED BY KIWI SYSLOG SERVER

When you are adding a filter based on [IP address](#), [host name](#), or [message text](#), you can use the following regular expression characters and sequences to specify the filter values.

CHARACTER	DESCRIPTION
^	Looks only at the beginning of a string.
\$	Looks only at the end of a string.
.	Matches any character.
?	Matches when the previous character is repeated zero or one time. For example, 10? matches 1 and 10.
*	Matches when the previous character is repeated zero or more times. For example, 10* matches 1, 10, 100, 1000, and so on.
+	Matches when the previous character is repeated one or more times. For example, 10+ matches 10, 100, 1000, and so on.
\	Escapes the next character. When the next character is a special character (part of the syntax), use this to indicate that the character should be interpreted literally. For example, \. * \+ \\ matches . * + \.
	Separates alternatives. For example, z wood matches both z and wood. And (Hello Hi) world matches Hello world and Hi world.
{n}	Matches the preceding character exactly <i>n</i> times, where <i>n</i> is a non-negative integer. For example, o{2} does not match the o in Bob, but matches the first two o's in foood.
{n, }	Matches the preceding character at least <i>n</i> times. For example, o{2, } does not match the o in Bob, but matches all the o's in foood. o{1, } is equivalent to o+, and o{0, } is equivalent to o*.
{n, m}	Matches the preceding character at least <i>n</i> times but not more than <i>m</i> times.

CHARACTER	DESCRIPTION
	For example, <code>o{1,3}</code> matches the first three <code>o</code> 's in <code>fooooood</code> . <code>o{0,1}</code> is equivalent to <code>o?</code> .
<code>[]</code>	Matches any character enclosed within the brackets. For example, <code>[abc]</code> matches the <code>a</code> in <code>plain</code> .
<code>[^]</code>	Matches any character not enclosed within the brackets. For example, <code>[abc]</code> matches the <code>k</code> in <code>back</code> .
<code>[a-z]</code>	Matches any character in the specified range. For example, <code>[m-s]</code> matches any lowercase alphabetic character in the range <code>m</code> through <code>s</code> .
<code>[^a-z]</code>	Matches any character not in the specified range. For example, <code>[^m-s]</code> matches any character not in the range <code>m</code> through <code>s</code> .
<code>\b</code>	Matches a word boundary, that is, the position between a word and a space. For example, <code>er\b</code> matches the <code>er</code> in <code>never</code> but not the <code>er</code> in <code>verb</code> .
<code>\B</code>	Matches a non-word boundary. For example, <code>ear\B</code> matches the <code>ear</code> in <code>never early</code> .
<code>\d</code>	Matches a digit character. Equivalent to <code>[0-9]</code> .
<code>\D</code>	Matches a non-digit character. Equivalent to <code>[^0-9]</code> .
<code>\f</code>	Matches a form-feed character.
<code>\n</code>	Matches a newline character.
<code>\q</code>	Matches a quote character or ASCII value of 34.
<code>\r</code>	Matches a carriage return character.
<code>\s</code>	Matches any white space including space, tab, form-feed, etc. Equivalent to <code>[\f\n\r\t\v]</code> .
<code>\S</code>	Matches any nonwhite space character. Equivalent to <code>[^\f\n\r\t\v]</code> .
<code>\t</code>	Matches a tab character.
<code>\v</code>	Matches a vertical tab character.
<code>\w</code>	Matches any word character including underscore. Equivalent to <code>[A-Za-z0-9_]</code> .

CHARACTER	DESCRIPTION
<code>\W</code>	Matches any non-word character. Equivalent to <code>[^A-Za-z0-9_]</code> .
<code>(x)\n</code>	Matches consecutive identical characters or strings, where <i>x</i> is the character or string and <i>n</i> is the number of times it is repeated (not including the first occurrence). For example, <code>(.)\1</code> matches any two consecutive identical characters.
<code>\n</code>	Matches <i>n</i> , where <i>n</i> is an octal escape value. Octal escape values must be 1, 2, or 3 digits long. For example, <code>\11</code> and <code>\011</code> both match a tab character. <code>\0011</code> is the equivalent of <code>\001</code> and <code>1</code> . Octal escape values must not exceed 256. If they do, only the first two digits make up the expression. This allows ASCII codes to be used in regular expressions.
<code>\xn</code>	Matches <i>n</i> , where <i>n</i> is a hexadecimal escape value. Hexadecimal escape values must be exactly two digits long. For example, <code>\x41</code> matches <code>A</code> . <code>\x041</code> is equivalent to <code>\x04</code> and <code>1</code> . This allows ASCII codes to be used in regular expressions.

EXAMPLES

EXPRESSION	MATCHES
<code>^stuff</code>	Any string starting with <code>stuff</code>
<code>stuff\$</code>	Any string ending with <code>stuff</code>
<code>o.d</code>	<code>old</code> , <code>odd</code> , <code>ord</code> , etc.
<code>o[ld]d</code>	<code>old</code> or <code>odd</code> only
<code>o[^l]d</code>	<code>odd</code> , <code>ord</code> , but not <code>old</code>
<code>od?</code>	<code>o</code> or <code>od</code>
<code>od*</code>	<code>o</code> , <code>od</code> , or <code>odd</code>
<code>od+</code>	<code>od</code> , <code>odd</code> , etc.
<code>\.</code>	Decimal point (needs escape character)
<code>[A-Z][a-z]*</code>	Any uppercase word
<code>[0-9]+</code>	Any stream of digits
<code>[1-9]+[1-9]*</code>	Any stream of digits not starting with zero
<code>[+\-]?[0-9]*[\.]?[0-9]*</code>	Any number with optional sign and decimal point (needs two escape characters)

EXPRESSION	MATCHES
<code>dst=\qLOCAL MACHINE\q</code>	Any occurrence of <code>dst="LOCAL MACHINE"</code>
<code>dst=\x22LOCAL MACHINE\x22</code>	Any occurrence of <code>dst="LOCAL MACHINE"</code> , because Hex(22) = ASCII 34, or "
<code>(z w)oo</code>	zoo OR woo

Add an action

Actions are triggered when all the filters for a [rule](#) are evaluated as true. Multiple actions can be defined for each rule. You can define the following types of actions:


- [Add an action to display a message](#)
- [Add an action to log messages to a file](#)
- [Add an action to forward messages to another host](#)
- [Add an action to play a sound](#)
- [Add an action to run an external program](#)
- [Add an action to send an email message](#)
- [Add an action to send a syslog message](#)
- [Add an action to log messages to a database](#)
- [Add an action to log to the NT event log](#)
- [Add an action to send an SNMP trap](#)
- [Add an action to stop processing the message](#)
- [Add an action to run a script](#)
- [Add an action to send a pager or SMS message via NotePager Pro](#)
- [Add an action to log messages to Kiwi Server Web Access](#)
- [Add an action to reset flags and counters](#)
- [Add an action to log messages to Papertrail.com \(a cloud-based server\)](#)
- [AutoSplit values](#)
- [Message content or counters](#)

ADD AN ACTION TO DISPLAY A MESSAGE

You can add an [action](#) to display messages on one of the Kiwi Syslog Server display screens.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)

5. From the Action menu, select Display.
6. Select the display screen.

 You can [change the name](#) of a display screen.

7. (Optional) [Test the action](#).
8. Click Apply to save the action.

ADD AN ACTION TO LOG MESSAGES TO A FILE

You can add an [action](#) to log messages to a file in the file format you select.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Log to file.
6. Specify the following options:

Path and file name of log file	<p>Enter a path and file name, or browse to select a file. The default location is <code><installPath>\Logs\SyslogCatchAll-%DateISO.txt</code>.</p> <p>To split incoming messages into multiple files, insert an AutoSplit value in the path or file name.</p> <p>For example, the current date variable (<code>%DateISO</code>) is inserted at the end of the default file name. This appends the date to the end of the file name, so a new message log file is created for each day.</p> <p>To select a value:</p> <ol style="list-style-type: none"> 1. Place your cursor in the path or file name where you want to insert the AutoSplit value. 2. Click Insert AutoSplit value and select the value.
Log file format	<p>Specify the file format. You can select a standard format or create a custom format. Custom formats are listed at the end of the Log file format menu, after the standard and reserved formats.</p>

7. To automatically [rotate log files](#):
 - a. Select Enable Log File Rotation.
 - b. Specify the total number of log files in the rotation set.
 - c. Specify the rotation criteria:
 - To rotate files based on size, select Maximum log file size.
 - To rotate files based on age, select Maximum log file age.
8. (Optional) [Test the action](#).
9. Click Apply to save the action.

 You can use schedules to [automate log file archival and retention](#).

ADD AN ACTION TO FORWARD MESSAGES TO ANOTHER HOST

You can add an [action](#) to forward the received message to another syslog host using the specified syslog protocol.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Forward to another host.
6. Specify the remote host IP address or host name. To send messages to multiple hosts, separate each host name or IP address with a comma. For example:

`Myhost.com, SecondHost.net, 203.75.21.3, ABC:567:0:0:8888:9999:1111:0`

7. Specify the protocol.

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

8. Specify the port number. Recommended values are:
 - UDP: Port 514
 - TCP: Port 1468 or port 601
 - KRDP: Port 1468

9. Specify any of the following optional values.

New Facility	Forces outgoing messages to use a different facility. In most cases, accept the default value of - No change -.
New Level	Forces outgoing messages to use a different level. In most cases, accept the default value of - No change -.
KRDP connection identifier	<p>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.</p> <p>Examples are: Source:RemoteOffice1 or SyslogServer1</p> <p>The string of text used will uniquely identify the source of the connection to the destination syslog Server.</p> <p>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.</p> <p>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.</p> <p>Examples are: Source:RemoteOffice1-%MACAddress</p> <p>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.</p>
Send with RFC3164 header information	<p>Adds the standard RFC3164 header information to the outgoing message. The format is:</p> <p><Priority>Date Hostname PID Message text</p> <p>The Priority is a value between 0 and 191.</p> <p>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.</p>
Retain the original source address of the message	<p>Normally, the syslog protocol is unable to maintain the original sender's address when forwarding syslog messages. This is because the sender's address is taken from the received UDP or TCP packet.</p> <p>Kiwi Syslog solves this problem by placing a tag in the message text that contains the original sender's 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.</p>

	<p>These tags are inserted only if the "Retain the original source address of the message" option is selected.</p> <p>i If the "Spoof Network Packet" option is used, then the "Original Address=" tag will not be used. The Syslog packet will be forwarded to the destination address as though it has been sent from the originating IP address.</p>
Use a fixed source IP address	<p>Uses 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.</p> <p>i If the "Spoof Network Packet" option is used, then the "Original Address=" tag will not be used. The Syslog packet will be forwarded to the destination address as though it has been sent from the specified fixed IP address.</p>
Spoof Network Packet	<p>This option only applies to syslog messages forwarded via UDP protocol with IPv4 address only.</p> <p>The network packet is spoofed to appear as though the forwarded 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.</p> <p>i This feature is only available in the licensed version. It requires WinPcap 4.1+ installation.</p>

10. (Optional) [Test the action](#).
11. Click Apply to save the action.

ADD AN ACTION TO PLAY A SOUND

You can add an [action](#) to play a sound when a message matches the associated filters.

i This feature is available only in the licensed version.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Play a sound.

6. Specify which sound to play and how many times to play it.
7. (Optional) [Test the action](#).
8. Click Apply to save the action.

ADD AN ACTION TO RUN AN EXTERNAL PROGRAM


i This feature is available only in the licensed version.

You can add an [action](#) to run an external program. Details of the message and other Syslog statistics can be passed to the external program as command-line arguments.

i 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.


1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Run external program.
6. Specify the program file name.
7. Specify the command line options you would like to pass to the program in the Command line options field.
8. 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.
9. Specify the priority of the new process that will be created.

VALUE	PRIORITY LEVEL	DESCRIPTION
0	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.
1	BelowNormal	Indicates a process that has priority above Idle but below Normal.
2	Normal	(Default value.) Specify this class for a process with no special

VALUE	PRIORITY LEVEL	DESCRIPTION
		scheduling needs.
3	Above Normal	Indicates a process that has priority above Normal but below High.
4	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.
5	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.  Realtime priority can cause system lockups.


10. If the process has a user interface, specify the Window Mode.

This setting has no effect on processes that do not have a user interface. This setting is unavailable if you are running Syslog Server as a service.


 If you select Wait for program initialization to complete before continuing, Syslog will wait for the new process to complete its initialization. It does this by waiting until the new process signals that it is idle. This is a blocking operation. Kiwi Syslog will not process messages any further until it receives the 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 if you are interacting with the process at a later stage, and you want to be sure that the process has started.

11. (Optional) [Test the action](#).
12. Click Apply to save the action.

ADD AN ACTION TO SEND AN EMAIL MESSAGE

 This feature is available only in the licensed version.

You can add an [action](#) to send an email message to one or more recipients. Details from the syslog message and other syslog statistics can be included in the email subject line or the message body.

 Before Kiwi Syslog Server can send email, you must [configure email options](#).

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select E-mail message.


6. Specify the following options.

E-mail Recipients	Enter one or more email recipients. Separate multiple email addresses with commas.
E-mail From	Enter the From email address. If you are using secured email (SSL or TLS), the From email address entered here must match the From email address entered in E-mail setup options .
E-mail Subject	Specify the message subject. Only one line is allowed. Click Insert message content or counter to include a variable.
E-mail Message	<p>Specify the message body. Multiple lines are allowed. Click Insert message content or counter to include variables.</p> <p>If the message will be sent to a pager, you can leave the message blank because it will not be included.</p> <p>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.</p>
E-mail Delivery Options	Specify the Importance, Priority, or Sensitivity of messages sent by this action.
Expand <013><010> in message	<p>Select this option to expand any carriage return and line feed characters that have previously been replaced with <013> and <010>.</p> <p>If the Replace non printable characters with <ASCII value> option is selected in the Modifiers setup options, any CR and LF characters appearing in the syslog message are replaced. Expanding these characters again when the message is emailed can make the text more readable.</p>
Max subject length	Enter the maximum number of characters in the subject line, or leave blank to remove the limit.
Max message length	<p>Enter the maximum number of characters in the message body, or leave blank to remove the limit.</p> <p>If you used the variable %MsgText in the message body and a large syslog message arrives, it could be too large to send via email. Use this option to limit the message body length to ensure that the message can be sent.</p>

7. (Optional) [Test the action](#).

8. Click Apply to save the action.

ADD AN ACTION TO SEND A SYSLOG MESSAGE

 This feature is available only in the licensed version.


You can add an [action](#) to send a syslog message to one or more hosts. You can use this option to relay syslog messages to another host with extra information, or with your own text added to the message.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Send Syslog message.
6. Specify the following options.

IP address or hostname	Enter the IP address or host name of one or more hosts. Separate multiple entries with commas. IPv4 and IPv6 addresses are supported. For example: <code>Myhost.com, SecondHost.net, 203.75.21.3</code>
Syslog message text	Specify the message text. Click Insert message content or counter to include variables.
New Facility, New Level, and New Socket	To change the facility, level, or socket, enter the new values.

7. (Optional) [Test the action](#).
8. Click Apply to save the action.

ADD AN ACTION TO LOG MESSAGES TO A DATABASE

 This feature is available only in the licensed version.

You can add an [action](#) to log a syslog message to an ODBC database. By default, the Log to Database action logs the following message field values:

- Date
- Time
- Priority
- Host name
- Message text

i If you want to log different values, you can:

- [Create a custom database format](#). The custom format will be available for selection when you create a Log to Database action.
- Use [the Run script](#) action to parse the syslog message, assign values to custom fields, and log them to a database.
- Use the scripting function [ActionLogToODBC](#) to send SQL statements and raw data to a database connection.

PREPARE THE DATABASE

1. Create a database, or select an existing database that Kiwi Syslog Server can write to.

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

Some [example ODBC databases](#) are available for download from the SolarWinds Success Center. The ZIP file contains information and sample databases that you can use as a guide to help you set up ODBC logging on your own system.


2. Determine how you want to create the table that stores message values. The following options are available:

Automated option	When you add the action, click Create table. Kiwi Syslog Server creates a table containing the required columns.
Semi-automated option	When you add the action, click Show SQL commands. The SQL commands used to create the table are shown in a text editor. You can run these commands in your database application.
Manual option	If you choose to create the table manually before you add the action, use the table design for the selected database type . Be sure that the name, data type, and size of each column match the table design. If the sizes are too small, the data could be truncated when it is written to the database.


ADD THE ACTION

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Log to Database.
6. Specify the following options.

Data link connection string	<ol style="list-style-type: none"> 1. Press the Browse (...) button to create or edit Data link properties. The Data Link Properties dialog box opens. 2. On the Provider tab, select a database provider. 3. On the Connection tab, specify the source of the data by doing one of the following: <ul style="list-style-type: none"> • Select the data source name (DSN) of an available provider. The drop-down menu lists valid DSNs for providers that are predefined on your system. • Enter a custom connection string. 4. Click Test Connection to validate that the connection properties are correct. 5. Use the Advanced tab to view and set other initialization properties for your data. 6. Click OK.
Database Table name	<p>Enter the name of the database table where message values are logged. You can either:</p> <ul style="list-style-type: none"> • Enter an existing table name. The table must match the expected table design. To verify the table structure, click Query table to retrieve the last five rows of data. • Create a new table: <ol style="list-style-type: none"> 1. Specify the database type (below). 2. Enter a table name. 3. Click Create table. <p>Any existing table with that name is deleted and the contents are lost. The new table is created with the column names and data types for the database type you have selected.</p>
Database type/field format	<p>Choose from the list of default database types, or create your own format by clicking Edit custom format.</p>
Connection Inactivity timeout	<p>Specify 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 is closed. As soon as a new message arrives, the connection is reopened.</p>


	The default for this setting is 600 seconds (10 minutes). A value of 0 ensures that the connection will never time out. The maximum value is 86400 seconds (1 day).
Run debug command	<p>If there is a problem logging to the database, click this button and enter a SQL command to be executed on the database. If the command fails, the results field displays a detailed error message. By default, the current INSERT statement used for the selected database type is displayed in the query field. This statement can be modified to test particular variations of the statement.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> • You cannot use this option to query the database. For example, you cannot run a Select From statement and obtain results. Only error information is returned to the results field.</p> <p>• Use the Show SQL commands button to obtain the correct syntax to use in the debug test.</p> </div>
Database cleanup	<p>Select this option to clean up the database by deleting older messages.</p> <p>The cleanup operation is performed nightly. Click Cleanup now to perform the operation immediately.</p>

7. (Optional) [Test the action](#).
8. Click Apply to save the action.


 When you test logging messages from the Service Manager, the program runs as the current user (probably "Administrator"). When Kiwi Syslog Server actually logs messages to a database, the service runs as the "Local System" user by default.

If your test messages work but the messages are not being logged, try changing the service login ID to "Administrator" instead of "Local System." Use the Services applet under Control Panel. Also consider selecting the option that allows the program to interact with the desktop.

ADD AN ACTION TO LOG TO THE NT EVENT LOG

 This feature is available only in the licensed version.

You can add an [action](#) to log messages to the NT application event log.

 When you view the NT event log with the NT event log viewer, the log type is set to show System events by default. To show Application events, select the Application item in the Log menu of the NT Event viewer.


1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.

4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Log to NT event log.
6. Specify the following options.

Event log message type	Select the logging level to be used for messages logged to the NT event log by this action.
Insertion string options	<p>Select how messages are inserted into the Event Log:</p> <ul style="list-style-type: none"> • Single insertion string %1 is replaced with: Date - Tab - Time - Priority - Tab - Hostname - Tab - Message • 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

7. (Optional) [Test the action](#).
8. Click Apply to save the action.

ADD AN ACTION TO SEND AN SNMP TRAP

 This feature is available only in the licensed version.

You can add an [action](#) to send an SNMP trap to the specified host.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Send SNMP Trap.
6. Specify the following options.

Forward SNMP Trap without changing	Select this option to forward the original SNMP trap to destination host.
Destination host	Enter the IP address of the system that will be receiving the SNMP trap.
IPv6	Select IPv6 to send SNMP traps to an IPv6 address. To forward incoming IPv6 trap messages, select the IPv6 option.
Remote port	Enter the port to which the SNMP trap will be sent. The default is 162. If you change this setting, you will need to configure the receiving device to "listen" for SNMP traps on the same port number.
Message text	Enter the content of the SNMP trap to be forwarded. Click Insert message content or counters to insert content using variables.
Agent IP address	Enter 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" (that is, the address of the machine running the Kiwi Syslog Server).
Generic type	For version 1 traps, select the type of trap to be sent: <ul style="list-style-type: none">• 0 - Cold Start• 1 - Warm Start• 2 - Link Down• 3 - Link Up• 4 - Authentication Failure• 5 - EGP Neighbor Loss• 6 - Enterprise Specific
Enterprise OID	For version 1 traps, enter a dotted numerical value (1.3.6.1.x.x.x.x) that represents the MIB enterprise of the SNMP trap.

	<p>i Version 2 traps have the Enterprise value bound as the second variable in the message.</p> <p>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.</p>
Variable OID	Specify 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 is set to values such as "public", "private" or "monitor".
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).
Version	<p>Select the version used to send SNMP traps to another syslog server. If you select version 3, provide the User Name, Local Engine ID, Authentication Password, Encryption Password, Protocol, and Algorithm.</p> <p>Version type for SNMP traps (version 1, 2 or 3) should be selected to send the traps to another syslog server. For example, you leave the encryption password and algorithm, it acts as 'authentication only' security level.</p> <p>i To send version 3 traps, SNMP credentials are required on both the receiving and sending sides.</p>

7. (Optional) [Test the action](#).
8. Click Apply to save the action.

ADD AN ACTION TO STOP PROCESSING THE MESSAGE

You can add an [action](#) to stop processing a message. No further rules will be applied to the message, and therefore no further actions will be taken.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Stop processing message.
6. Click Apply to save the action.


ADD AN ACTION TO RUN A SCRIPT

You can add an [action](#) to run a script to filter or parse the current message.

i You can use the Run script action to run a parsing script that breaks the syslog message down into various sub-fields. The values can then be assigned to custom fields and 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. You must write a custom script to parse the message text and then place it in the custom database fields. Example parsing scripts can be found in the `\Scripts` subdirectory in the Kiwi Syslog Server installation directory.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Run Script.
6. Specify the following options.

Script file name	Enter the path and file name of an existing script file or of the file to be created.
Script description	Describe the purpose or function of the script.
Script language	<p>Select the scripting language.</p> <p>Windows Script provides script engines for the following languages, which have similar feature sets.</p> <ul style="list-style-type: none"> • VBScript: a variation of Visual Basic or VBA (Visual Basic for Applications) used in MS Word and Excel. • JScript: a variation of Java Script used in web pages. <p>Consider JScript if you are familiar with Java Script. Also, JScript is usually faster than VBScript at performing string manipulations.</p> <p>To use one of the following languages, you must install the Active Scripting engine for that language:</p> <ul style="list-style-type: none"> • PerlScript • Python • RubyScript
Edit script	<p>Click this button to open the script in a text editor. If the specified file does not exist, it is created.</p> <p>Modify the script and save your changes.</p> <p>Script file rules</p>

	<p>The script must always contain a function called <code>Main()</code>. 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 than 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.</p> <p>Each of the available script variables can be accessed from the Fields object.</p> <p>Example (VBScript):</p> <pre style="border: 1px solid black; padding: 10px;">Function Main() ' Your code goes here ' Set the return value Main = "OK" End Function</pre> <p>Additional information on scripting</p> <p>For examples, descriptions of variables and functions, dictionaries, and a tutorial, see Scripting resources. Sample scripts are located in the <code>\Scripts</code> subdirectory in the Kiwi Syslog Server installation directory.</p>
Field Read/Write permissions	<p>Select the groups of fields that Kiwi Syslog Server can access:</p> <ul style="list-style-type: none"> • When you grant read access to a group of fields, their values are copied into the script variables and are readable from within the script. • When you grant write access to a group of fields, their values are copied from the script variables and replace the equivalent program fields. <p>Each time a script runs, the available message fields are copied to the script variables and back again upon completion of the script. The copying takes time and uses CPU cycles. To improve script performance, SolarWinds recommends granting read and write access only to the variables used in the script.</p> <p> For more information about the fields in each group, see Script variables.</p>

7. (Optional) [Test the action](#).

Select if you want to see any changes that the script makes to the variables.

Kiwi Syslog Server attempts to run the specified script.

If an error occurs, a message displays the error description and the line number on which it occurred.

If you select the Show test results option and the script runs successfully, a dialog shows the variable values before and after the script ran. Use this to see what variable values the script changed.

8. Click Apply to save the action.


SCRIPT FILE CACHING

During normal operation, the script files are cached after they have been read from disk. This improves the program speed and prevents additional I/O. If you modify the script externally and save it back to disk, the changes do not take effect until the file is reloaded.

If you run Kiwi Syslog Server as an application, do either of the following to reload the file:

- Flush the cache. Choose File > Debug options > Clear the script file cache, or press Ctrl+F8 from the Service Manager console.
- Restart the application.

If you run Kiwi Syslog Server as a service, stop and restart the service to reload the file.


 When you test a script from the Kiwi Syslog Server Setup window, the script is not cached. Each script is freshly loaded before it is run.

TRIGGERING A SCRIPT ON A REGULAR BASIS

To trigger a script on a regular basis, you can:

- [Create a scheduled task to run a script](#)
- [Enable a keep-alive message](#), and add a Run Script action to run the script when the keep-alive message is received.

ADD AN ACTION TO SEND A PAGER OR SMS MESSAGE VIA NOTEPAGER PRO

 This feature is available only in the licensed version.

You can add an [action](#) to send a pager, SMS, or email message via the NotePagerPro application. Before you create this action, you must first purchase and install NotePager Pro. NotePager Pro is an inexpensive but powerful paging and SMS gateway application. Features 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

See the NotePager website to download the application.

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

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Send message via NotePager Pro.
6. Specify the following options.

Send page to	<p>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.</p> <p>You can choose either a single recipient or a group of recipients to send to. For example:</p> <p>Send to: Joe</p> <p>or</p> <p>Send To: All-Network-Staff</p>
Message from	<p>Enter any descriptive name. 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".</p>
Message	<p>Specify the message text. Click Insert message content or counter to include variables.</p>
Max message length	<p>Select this option 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 pager. Use this option to limit the message body length.</p> <p>If your pager is capable of receiving only numeric messages, you must 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.</p>

7. (Optional) [Test the action](#).
8. Click Apply to save the action.

ADD AN ACTION TO LOG MESSAGES TO KIWI SERVER WEB ACCESS

You can add an [action](#) to log messages to Kiwi Syslog Web Access, if it is installed.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Log to Kiwi Syslog Web Access.
6. (Optional) [Test the action](#).
7. Click Apply to save the action.

ADD AN ACTION TO RESET FLAGS AND COUNTERS

You can add an [action](#) to reset all of the internal counters used by the [Threshold, Timeout, and Time Interval filters](#) configured under all rules.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Reset Flags/Counters.
6. Click Apply to save the action.

ADD AN ACTION TO LOG MESSAGES TO PAPERTRAIL.COM (A CLOUD-BASED SERVER)

You can add an [action](#) to log messages to Papertrail, a cloud-based logging service. You can send logs from Kiwi Syslog Server (or any other servers or applications that can connect to the Internet). Then monitor, search, react to, and archive your messages on Papertrail.com.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. [Add](#) or locate the rule that the action applies to.
3. Right-click the Actions node below the rule, and choose Add Action.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. From the Action menu, select Log to Papertrail.com (cloud).

6. Specify the following options.

Papertrail Destination Hostname	Enter the location where logs are sent from a syslog server. The destination host is provided by Papertrail. For example: <code>logs2.papertrailapp.com</code>
Papertrail Destination Port	Papertrail provides specific port number while creating a login with Papertrail. Use the same port number to send the syslog messages. For example: <code>58612</code> For help in Papertrail, click here .

7. (Optional) [Test the action](#).

8. Click Apply to save the action.

AUTOSPLIT VALUES IN KIWI SYSLOG SERVER

When you [add an action](#) to log messages to a file, place an AutoSplit value in the path or file name to automatically split the log files. When a message is received, the variable is replaced with a value from the message.

AutoSplit values can be used anywhere within the path or log file name, as long as the result is a valid file name. Any number of AutoSplit values can be used within the path or file name.

If you are using the Run Script action, you can use any of the VarCustom or VarGlobal fields as an AutoSplit value. The following sections describe the available options.

Examples:

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

```
C:\Logs\MyLogFile%DateD2.txt
```

The %DateD2 is replaced by the current day of the month. On the 23rd of the month, the message is written to:

```
C:\Logs\MyLogFile23.txt
```

- To split the messages based on priority level and current date:

```
C:\Logs\%PriLevAA\MyLogFile-%DateISO.txt
```

On April 9, 2016, the path and file name look like this:

```
C:\Logs\Debug\MyLogFile-2016-04-09.txt
```

- To split the messages based on the sending host, and then by priority level:

C:\Logs\%HostName.%HostDomain\MyLogFile-%PriLevAA.txt

The path and file name look like this:

C:\Logs\myhost.mycompany.com\MyLogFile-Debug.txt

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	2017-10-15

Menu name	Year (YYYY)
Parameter	%DateY4
Explanation	4 digit year, always 4 characters in length
Example	2017

Menu name	Year (YY)
Parameter	%DateY2
Explanation	2 digit year, always 2 characters in length
Example	17

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.
.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.
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 (REGISTERED VERSION ONLY)

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

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

Menu name	IPv6 Address
Parameter	%IPv6Add6
Explanation	The IPv6 address of the device that sent the message. IPv6 address of the device is separated with ~ as special character is not accepted in file name.
Example	ABC~567~0~0~8888~9999~1111~0

HOST NAME VALUES (REGISTERED VERSION ONLY)

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 (REGISTERED VERSION ONLY)

WELF format is the WebTrends Extended Logging Format. This format is used by many firewalls such as GNATBox, SonicWall, CyberWallPlus, and NetScreen. Each field within the message text is prefixed with an identifying tag, such as `fw=` for the firewall name or `src=` for the source of the packet being logged.

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

INPUT SOURCE VALUES (REGISTERED VERSION ONLY)

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 (REGISTERED VERSION ONLY)

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	%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.

MESSAGE CONTENT OR COUNTERS

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.

To add a variable:

1. Position your cursor where you want to insert the variable.
2. Click Insert message content or counter.
3. Select a variable.

The following variables are available.

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.

DATE

Parameter: %MsgDate

Explanation: The date the message arrived in the format YYYY-MM-DD

Example: 2005-02-18

TIME

Parameter: %MsgTime

Explanation: The time the message arrived in the format HH:MM:SS

Example: 22:30:16

FACILITY

Parameter: %MsgFacility

Explanation: The facility of the message in text format.

Example: Local7, Mail

LEVEL

Parameter: %MsgLevel

Explanation: The level of the message in text format.

Example: Debug, Info

HOST ADDRESS OF SENDER

Parameter: %MsgHost

Explanation: The host IP address of the sending device.

Example: 192.168.1.1

THE MESSAGE TEXT

Parameter: %MsgText

Explanation: The message text part of the syslog message

Example: This is a test message

ALARM MIN MSG THRESHOLD

Parameter: %MsgAlarmMin

Explanation: The threshold level set for the minimum message count alarms

Example: 100 (messages per hour minimum)

ALARM MAX MSG THRESHOLD

Parameter: %MsgAlarmMax

Explanation: The threshold level set for the maximum message count alarms

Example: 5000 (messages per hour maximum)

ALARM DISK SPACE THRESHOLD

Parameter: %MsgAlarmDisk

Explanation: The threshold level set for the minimum disk space remaining in MB

Example: 90 (MB)

MESSAGE COUNT THIS HOUR

Parameter: %MsgThisHour

Explanation: The number of messages received so far this hour.

Example: 254

MESSAGE COUNT LAST HOUR

Parameter: %MsgLastHour

Explanation: The number of messages received in the last hour

Example: 254

MACHINE MAC ADDRESS

Parameter: %MACAddress

Explanation: The MAC address value of the first network adaptor found.

Example: AA-BB-CC-DD-EE-FF-00

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)

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.

VARGLOBAL01 TO VARGLOBAL16

Parameter: %VarGlobal01 to %VarGlobal16

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.

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.

Test a filter or an action

Before enabling a rule, test the filters or actions to make sure they work as intended.

USE THE TEST BUTTON ON THE FILTER OR ACTION SETUP DIALOG

When you add a [filter](#) or [action](#), you can use the Test button to test your configuration.

1. At the bottom of the action or filter setup dialog, click the Test Setup button.

The Test message dialog displays the values that are passed to the filter or action when you perform the test.

If necessary, change these inputs to match the values you are filtering for.

2. Click the Test button.

A green check mark next to the Test button indicates that the filter or action passed the test.

USE THE KIWI SYSLOGGEN UTILITY


You can also test filters and actions using Kiwi SyslogGen, a free utility that generates and sends syslog messages. You can specify message properties such as priority, message text, and sending IP address.

1. Go to www.kiwisyslog.com/downloads.aspx and download Kiwi SyslogGen.
2. Install Kiwi SyslogGen on the computer where Kiwi Syslog Server is installed.
3. Use Kiwi SyslogGen to generate messages that meet the filter criteria, and verify that the results are what you intended.

Rearrange rules, filters, actions, and schedules

[Rules are applied](#) in the order they are listed on the Kiwi Syslog Server Setup dialog. Within each rule, filters and actions are also applied in order. If multiple [scheduled tasks](#) are set to run at the same time, they run in the order that they are listed on the Setup dialog.

You can change the order of rules, filters, actions, or scheduled tasks.

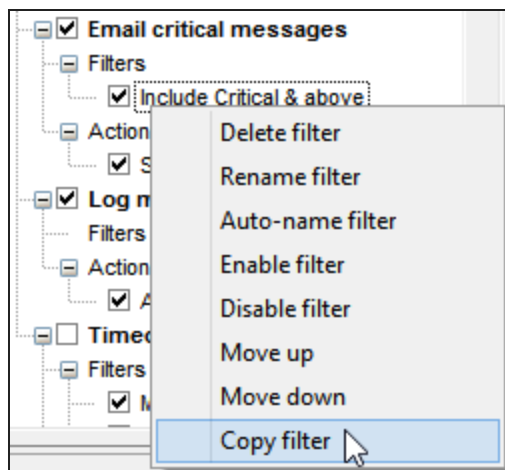
 You can also [copy a filter or an action to a different rule](#).

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. Right-click the rule, filter, action, or schedule.
3. Select Move up or Move down.

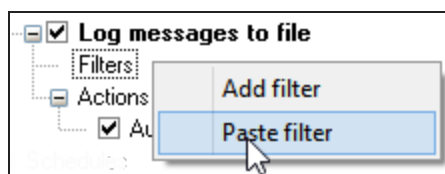
Copy a filter or an action to a different rule

To use the same filter or action in multiple [rules](#), you can create it for one rule and then copy it to a different rule.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. Right-click the filter or action.
3. Select Copy filter or Copy action.



4. Right-click the Filters or Actions section of a different rule.
5. Select Paste filter or Paste action.



Import and export rules

You can export a [rule](#) definition to a file to share with other Kiwi Syslog Server users. Other users can then import the rule definition to their servers.

EXPORT A RULE

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. Right-click the rule and choose Export rule.
3. Browse to the location where you want to save the rule and click Save.

The rule definition file is automatically given a .ksr extension, and the default file name is based on the rule name.

IMPORT A RULE

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. At the top of the left pane, right-click Rules and choose Import rule.
3. Browse to the file location, select the .ksr file, and click Open.

The imported rule is listed in the left pane at the bottom of the rules section. You can [move the rule](#) to a different position.

Keyboard shortcuts for rules, filters, actions, and schedules

When you are creating a [rule](#), [filter](#), [action](#), or [schedule](#) in Kiwi Syslog Server, the following keyboard shortcuts are available.

PRESS	TO
Delete	Delete the selected Rule, Filter, Action, or Archive schedule.
Insert	Add a new Rule, Filter, Action, or Archive schedule. (The selected item must be Rules, Filters, Actions, or Archiving.)
Ctrl-V	Paste the copied Rule, Filter, Action, or Archive schedule. (The selected item must be Rules, Filters, Actions, or Archiving.)
Ctrl-C	Copy the selected Rule, Filter, Action, or Archive schedule.
F2	Rename the selected Rule, Filter, Action, or Archive schedule.
F4	Auto-name the selected Filter, Action, or Archive schedule.
Home	Move the cursor to the top of the tree.
End	Move the cursor to the bottom of the tree.
Enter	Collapse or expand the tree at the currently selected position (same as double clicking with the mouse).
Space bar	Enable or Disable the selected Rule, Filter, Action, or Archive schedule.

PRESS	To
Shift + Up Arrow	Move the selected Rule, Filter, Action, or Archive schedule up one position.


Scripting resources

When you add an [action to run a script](#) or create a [scheduled task to run a script](#), use the following resources to help you write the script.

- [Script examples](#)
- [Scripting custom statistics fields](#)
- [Script variables](#)
- [Script functions](#)
- [JScript escape characters](#)
- [Scripting dictionaries](#)
- [Scripting tutorial](#)

Script examples

If you want to [add an action to run a script](#), use the examples in the following section to help you get started [writing scripts](#). The `\Scripts` folder in the Kiwi Syslog Server installation directory also includes sample scripts that show you how to play sounds, send e-mail, log to file, and other actions.

 If you have created a custom parsing script or something that would be useful to others, please [share it with the SolarWinds user community](#).

The following examples are provided:

- [PIX message lookup](#)
- [All the variables - \(Info function\)](#)

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 website.

RUN SCRIPT ACTION SETUP

Common fields: Read=yes

Custom fields: Write=yes

RULES SETUP

```
Rules setup
  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
```

```
Body: %MsgText
```

```
Explanation: %VarCustom01
```

```
Action to take: %VarCustom02
```

Rules

```
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
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. An IP packet was sent with
options. Because IP options are considered a security risk, the packet was
discarded."
            A = "A security breach was probably attempted. Check the local host 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

```

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.

 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
```

Scripting custom statistics fields

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.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Click Scripting.
3. Specify the name and initial value.

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](#).

4. Click Apply to save your changes.

The names and initial 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.

Script variables

The following variables are available for [scripts](#) used with Kiwi Syslog Server. Variables are passed to and from the script. Depending on the read/write permissions you set for the [action](#) or [scheduled task](#), the variables can be modified and returned for use in the syslog program.

The variables are passed via a globally accessible object named "Fields." To access a variable, simply prefix the word "Fields." to the variable 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	<p>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 contains the original sender's address.</p> <p>Case A: Firewall device (192.168.1.1) ---> First syslog collector (192.168.1.2) ---> This syslog collector (192.168.1.3).</p> <p>The field value would be 192.168.1.1.</p> <p>Case B: Firewall device (192.168.1.1) ---> This syslog collector (192.168.1.3).</p> <p>The field value would be 192.168.1.1.</p>
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 hostname. 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 (for example, header removed, DNS lookups, original address removed, and Cisco date removed).
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 bytes)
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)
---------	---

	<p>The field value would be 192.168.1.2.</p> <p>Case B: Firewall device (192.168.1.1) ---> This syslog collector (192.168.1.3)</p> <p>The field value would be 192.168.1.3.</p>
Type	String
Format	nnn.nnn.nnn.nnn (Values are not zero padded.)
Example	192.168.1.67

FIELDS.VARPEERADDRESSHEX

Details	<p>The IP address of the device that sent the message converted to an 8 digit hex value.</p> <p>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 must also make changes to the VarPeerAddressHex field.</p>
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

FIELDS.VARLOCALADDRESS

Details	The IP address that the message was sent to on this machine.
Type	String
Examples	127.0.0.1, 192.0.2.0

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

FIELDS.VARGLOBAL01 TO FIELDS.VARGLOBAL16: 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 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)

Script functions

When you are writing [scripts](#) for use with Kiwi Syslog Server, number of built in functions are available from the Fields object. To use a built in function, simply access the function name prefixed with the Fields object. Pass any parameters needed and the result is 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.

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:\Programfiles\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 receive 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

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

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

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 0 ' Use the standard syslog port
```

```
Protocol = ' 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 Address:- 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, whichever 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"

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 & vtab & MsgPriority & vtab & MsgHostAddress & vtab & 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:

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
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 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.

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

JScript escape characters

Use the following escape characters in JScript [scripts](#). 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\'.\"`

ESCAPE SEQUENCE	MEANING
\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.

Scripting dictionaries

When you are writing [scripts](#), the dictionaries collection allows for the creation of (named) dictionaries that store data key and item pairs. The data stored in these dictionaries is persistent, 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


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.

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

ADDITEM

 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.

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

UPDATEITEM

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.

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

REMOVEITEM

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.

Example: Call `Dictionaries.RemoveItem("MyDictionary", "MyKeyName")`

REMOVEALL

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
----------------	----------	----------------------------

Example: Call `Dictionaries.RemoveAll("MyDictionary")`

DELETE

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.
---------	----------	---

Example: `Call Dictionaries.RemoveItem("MyDictionary", "MyKeyName")`

DELETEALL

DeleteAll()

The **DeleteAll** method deletes all dictionaries.

Example: `Call Dictionaries.DeleteAll()`

GETITEMCOUNT

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.
----------------	----------	-----------------------------

Example: `ItemCount = Dictionaries.GetItemCount("MyDictionary")`

GETITEM

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.

Example: `MyItem = Dictionaries.GetItem("MyDictionary", "MyKeyName")`

ITEMEXISTS

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.

Example: `If Dictionaries.ItemExists("MyDictionary", "MyKeyName") Then`

...

`End If`

GETKEYS

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
---------	----------	----------------------------

```
Example: MyKeyArray = Dictionaries.GetKeys("MyDictionary")
For i = 0 to UBound(MyKeyArray)
ThisKey = MyKeyArray(i)
...
Next
```

GETITEMS

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
---------	----------	----------------------------

Example:

```
MyItemArray = Dictionaries.GetItems("MyDictionary")
For i = 0 to UBound(MyItemArray)
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

FUNCTION NAME	ERROR DESCRIPTION
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

Scripting tutorial

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 is available only in the registered version.

TASK 1: CREATE THE SCRIPT ACTION

1. Create a new rule called "Replace text" .
2. Add a new [Run Script action](#).
3. Set the script file name to: `ReplaceText.txt`.
4. Set the script description to: Replaces occurrences of "cat" with "dog". Set the script language to VBScript.
5. 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
6. 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.

7. Copy and paste the following script file into Notepad and then choose File > Save.

```
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
```

TASK 2: CREATE THE ACTIONS

1. Add a new Log to file action.
2. Set the file name to "MyCustomLog.txt" in the folder of your choice.
3. Leave the file format as default.
4. Click the action and then press F4 to auto name the action "Log to file".
5. Add a new Display action.
6. Leave the display number as default.
7. 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

TASK 3: TEST THE SCRIPT

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

Once the script runs, the results are 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".

TASK 4: TEST THE SCRIPT WITH SYSLOGGEN

1. 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.
2. Download SyslogGen from <http://www.kiwisyslog.com/downloads.aspx> Install it on the same machine as the Syslog Server
3. Set the send options to "send message once" Set the destination to localhost (127.0.0.1).
4. Set the message text to be: This is a test. The cat sat on the mat. Press the Send button

You should now see this message appear on the display "This is a test. The dog sat on the mat."

Create scheduled tasks

You can create up to 100 scheduled tasks in Kiwi Syslog Server. The following types of tasks are available:

- [Archive tasks](#) move or copy files to another location and (optionally) compress the files.
- [Clean-up tasks](#) delete files that meet the specified criteria (for example, files over a certain age).
- [Run Program tasks](#) run a Windows program.
- [Run Script tasks](#) run a script.

Each task can be triggered to run:

- On a schedule
- When the Kiwi Syslog Server application or service starts
- When the Kiwi Syslog Server application or service stops

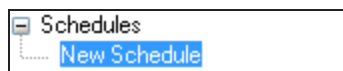
If multiple tasks are set to run at the same time, the tasks run in the order they are listed on the Setup dialog. You can [rearrange scheduled tasks](#).

Create a scheduled task to archive log files

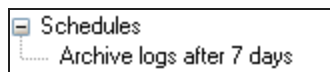
To save disk space, you can create a task to automatically archive log files that are no longer needed for troubleshooting (for example, log files that are more than a week old). The archive task includes options to move files to another location, compress them, encrypt them, and send notifications. You can schedule the task to run at regular intervals.

i You can also [create a scheduled task to remove archived files](#) after the retention period is over. For an example of creating archive and cleanup tasks, see [Create schedules to automate log archival and retention](#) in the Kiwi Syslog Server Getting Started Guide.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. In the left pane of the Setup dialog, right-click Schedules and select Add new schedule.



3. Replace the default name with a descriptive name (for example, Archive logs after 7 days).



4. As the Task Type, select Archive.

5. As the Task Trigger, specify when you want the archive task to run:

- To schedule the task, select On a schedule. Then specify the start date, frequency, end date, and any exceptions on the Schedule tab.
- To run the task each time you start or stop the Kiwi Syslog Server application or service, select On app/service startup or On app/service shutdown.

6. On the Source tab:

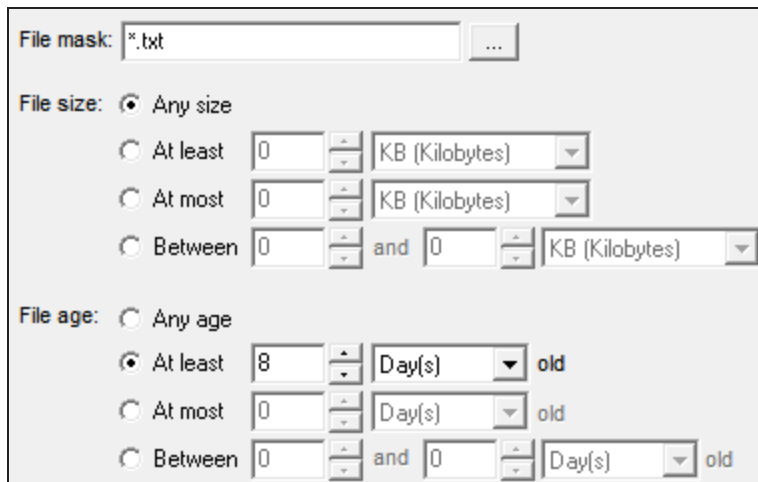
- a. Under Source location, specify the location of the files to archive.

By default, log files are stored in the following directory:

C:\Program Files (x86)\Syslogd\Logs\

- b. Under Source files, specify which files are archived.

The following example archives TXT files that are at least 8 days old.



The screenshot shows a configuration window for file selection. It includes a 'File mask' field with the value '*.txt'. Under 'File size', the 'Any size' radio button is selected. Under 'File age', the 'At least' radio button is selected with a value of 8 and the unit 'Day(s) old'.

7. On the Destination tab:

- a. Specify the destination folder.

Kiwi Syslog Server provides the following default folder for storing archived logs:

C:\Program Files (x86)\Syslogd\Dated Logs\

- b. Specify whether you want to move or copy the files.

- c. (Optional) Select options to create a dated root folder in the specified destination, and to add a date to each archived file name.

You can use the Adjust file/folder date(s) option to adjust each file or folder date to reflect the date of the logs, instead of the current date. For example, if you are archiving files that are a week old, you can shift the date back one week.

8. To compress the archived files, select the following options on the Archive Options tab:
- Select Zip files after moving/copying.
 - Select the compression level and method:


Compression level	<ul style="list-style-type: none"> None: does not compress the files. Low: takes the least amount of time to compress the data, but files are larger. Medium: provides the best balance between the time required to compress the data and the compression ratio. High: produces slightly smaller files but requires significantly longer compression times. This option is recommended only when space is limited and processing time is not important.
Compression method	<ul style="list-style-type: none"> Stored (None): does not compress the files. Deflate: provides the fastest compression. Deflate64: takes longer but provides better compression.

- (Optional) To encrypt the files, select Encrypt zip files, and specify the encryption properties.

Password	Enter a case-sensitive password of up to 79 characters. If the password is blank, the files are not encrypted.
Encryption type	WinZip AES provides stronger encryption than Compatible.
Encryption strength	If you selected WinZip AES, specify the size of the encryption key.

9. To run a program after the files are archived, select the following options on the Archive Options tab:
- Select the option to run a program after **each file** is archived or after **all files** are archived.
 - Specify the location of the executable file, and enter any command-line parameters to pass to the executable.
To include a file name, folder name, or current date in the command-line parameters, click Variable options and select the value to include.
 - To specify the maximum time to wait for the program to run, select Wait for program completion. Then enter the maximum number of seconds to wait.
Programs or processes that are still running after this period are terminated.


- To email or save the report generated each time the archive task runs, select one or more options on the Archive Notifications tab.

-  To email the report to multiple recipients, separate the list of email addresses by commas or semicolons.
- If you save the report to a file, insert date and time variables in the file name to ensure that it is unique. If the file name is not unique, Kiwi Syslog Server overwrites the existing file when it creates a new file.

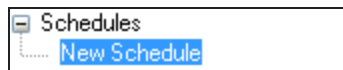
- Click Apply to save your changes.

Create a scheduled task to delete files

A clean-up task deletes files that match the specified criteria (including age, size, and file type). For example, you can create a clean-up task to remove archived log files after they have been retained for the required period. You can schedule the task to run at regular intervals.

-  You can also [create a scheduled task to archive log files](#) not needed for troubleshooting. For an example of creating archive and cleanup tasks, see [Create schedules to automate log archival and retention](#) in the Kiwi Syslog Server Getting Started Guide.

- From the Kiwi Syslog Service Manager, choose File > Setup.
- In the left pane of the Setup dialog, right-click Schedules and select Add new schedule.



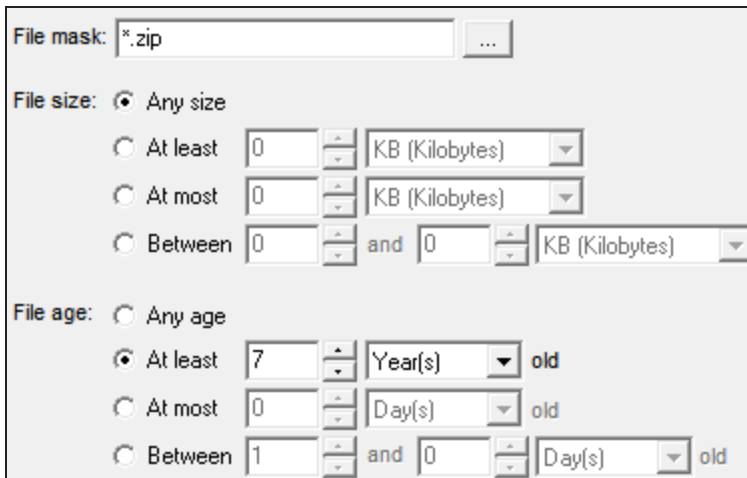
- Replace the default name with a descriptive name.
- As the Task Type, select Clean-up.
- As the Task Trigger, specify when you want the archive task to run:
 - To schedule the task, select On a schedule. Then specify the start date, frequency, end date, and any exceptions on the Schedule tab.
 - To run the task each time you start or stop the Kiwi Syslog Server application or service, select On app/service startup or On app/service shutdown.

6. On the Source tab:
 - a. Under Source location, specify the folder that contains the files to be deleted.

To delete files from subdirectories, select Include sub-folders.

- b. Under Source files, specify which files are deleted.

The following example deletes ZIP files that are at least 7 years old.



File mask: *.zip

File size: Any size

At least 0 KB (Kilobytes)

At most 0 KB (Kilobytes)

Between 0 and 0 KB (Kilobytes)

File age: Any age

At least 7 Year(s) old

At most 0 Day(s) old

Between 1 and 0 Day(s) old

7. To delete empty folders in the source location, click the Clean-up Options tab and select Remove empty folders.
8. To email or save the report generated each time the clean-up task runs, select one or more options on the Clean-up Notification tab.



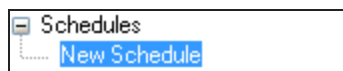
- To email the report to multiple recipients, separate the list of email addresses by commas or semicolons.
- If you save the report to a file, insert date and time variables in the file name to ensure that it is unique. If the file name is not unique, Kiwi Syslog Server overwrites the existing file when it creates a new file.

9. Click Apply to save your changes.

Create a scheduled task to run a program



Create a Run Program task to execute a Windows program, process, or batch file. You can schedule the task to run at regular intervals.

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. In the left pane of the Setup dialog, right-click Schedules and select Add new schedule.




3. Replace the default name with a descriptive name.

4. As the Task Type, select Run Program.
5. As the Task Trigger, specify when you want the archive task to run:
 - To schedule the task, select On a schedule. Then specify the start date, frequency, end date, and any exceptions on the Schedule tab.
 - To run the task each time you start or stop the Kiwi Syslog Server application or service, select On app/service startup or On app/service shutdown.
6. On the Program Options tab, complete the following fields:

Program file name	Specify the program to run.
Command line options	Enter any command-line parameters to be passed to the program.
Process priority	<p>Select the priority of the process created when the program runs. Select Normal (the default) for programs with no special scheduling needs.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p> Low priority processes run only when the system is idle. High and Realtime priority processes preempt the threads of lower level priorities. For more information on each priority level, see the ProcessPriority registry setting.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0; background-color: #fff9c4;"> <p> Realtime priority processes can cause system lockups.</p> </div>
Window mode	If the program has a user interface, select the Window mode.
Wait for program initialization to complete	<p>Select this option if you want Kiwi Syslog Server to suspend all processing until the program has started. Then enter the maximum time that Kiwi Syslog Server should wait.</p> <p>Use this setting if something interacts with the program after it starts and you want to be sure that the program has started before the interaction is triggered. To determine if the program has started, Kiwi Syslog Server monitors the process that is created when the program starts, and waits for that process to signal that it is idle.</p>

7. To email or save the report generated each time the clean-up task runs, select one or more options on the Run Program Notification tab.


 • To email the report to multiple recipients, separate the list of email addresses by commas or semicolons.

• If you save the report to a file, insert date and time variables in the file name to ensure that it is unique. If the file name is not unique, Kiwi Syslog Server overwrites the existing file when it creates a new file.

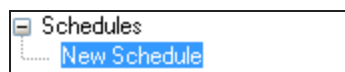
8. Click Apply to save your changes.

Create a scheduled task to run a script

Create a Run Script task to run a script. You can schedule the task to run at regular intervals.


 For information about writing scripts to use with Kiwi Syslog Server, see [Scripting resources](#).

1. From the Kiwi Syslog Service Manager, choose File > Setup.
2. In the left pane of the Setup dialog, right-click Schedules and select Add new schedule.



3. Replace the default name with a descriptive name.
4. As the Task Type, select Run Program.
5. As the Task Trigger, specify when you want the archive task to run:
 - To schedule the task, select On a schedule. Then specify the start date, frequency, end date, and any exceptions on the Schedule tab.
 - To run the task each time you start or stop the Kiwi Syslog Server application or service, select On app/service startup or On app/service shutdown.

6. On the Program Options tab, complete the following fields:

Script file name	Enter the path and file name of an existing script file or of the file to be created.
Script description	Describe the purpose or function of the script.
Script language	<p>Select the scripting language.</p> <p>Windows Script provides script engines for the following languages, which have similar feature sets.</p> <ul style="list-style-type: none">• VBScript: a variation of Visual Basic or VBA (Visual Basic for Applications) used in MS Word and Excel.• JScript: a variation of Java Script used in web pages. <p>Consider JScript if you are familiar with Java Script. Also, JScript is usually faster than VBScript at performing string manipulations.</p> <p>To use one of the following languages, you must install the Active Scripting engine for that language:</p> <ul style="list-style-type: none">• PerlScript• Python• RubyScript
Field Read/Write permissions	<p>Select the groups of fields that Kiwi Syslog Server can access:</p> <ul style="list-style-type: none">• When you grant read access to a group of fields, their values are copied into the script variables and are readable from within the script.• When you grant write access to a group of fields, their values are copied from the script variables and replace the equivalent program fields. <p>Each time a script runs, the available message fields are copied to the script variables and back again upon completion of the script. The copying takes time and uses CPU cycles. To improve script performance, SolarWinds recommends granting read and write access only to the variables used in the script.</p> <p> For more information about the fields in each group, see Script variables.</p>

7. To email or save the report generated each time the clean-up task runs, select one or more options on the Run Program Notification tab.



- To email the report to multiple recipients, separate the list of email addresses by commas or semicolons.
- If you save the report to a file, insert date and time variables in the file name to ensure that it is unique. If the file name is not unique, Kiwi Syslog Server overwrites the existing file when it creates a new file.

8. Click Apply to save your changes.

Set alarms



Use alarms to monitor network traffic, disk space, and the number of messages in the queue waiting to be processed. When an alarm is triggered, Kiwi Syslog Server alerts you by playing a sound, sending an email, or running a program.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Expand the Alarms node.
3. Click the type of alarm you want to enable.

Min message count	The alarm is triggered if Kiwi Syslog Server receives fewer than the specified number of messages per hour. This could indicate that messages are not being received.
Max message count	The alarm is triggered if Kiwi Syslog Server receives more than the specified number of messages per hour.
Disk space usage	The alarm is triggered if the amount of free disk space on the disk where Kiwi Syslog Server is installed drops below the specified threshold. You can also select options to close TCP connections or stop disk logging when free disk space is below the specified levels.
Message queue monitor	The alarm is triggered if: <ul style="list-style-type: none">• The syslog message queue overflows more than the specified number of times per hour.• More than the specified number of messages are in the queue waiting to be processed.

The configuration panel for the selected alarm opens.

4. Enter the alarm threshold.
5. Select the notification method.

Audible alarm	<p> This feature is available only in the licensed version.</p> <ul style="list-style-type: none"> • If you select Beep, the system beeps every second until the alarm is canceled. • If you select Play a sound file, the sound file is played every five seconds until the alarm is canceled. <p>To cancel an alarm, double-click the red alarm bell icon in the tool bar at the top of the Kiwi Syslog Service Manager window.</p>
Run program	<p> This feature is available only in the licensed version.</p> <p>Select the program file to run. You can pass information to the program using command line parameters and message content variables. Place quotation marks (") around file names or paths that contain spaces. For example:</p> <pre>Pager.exe "555-1234" ,"Syslog - Warning, lots of messages received, Max set at %MsgAlarmMax but received %MsgThisHour so far this hour."</pre> <p>Use the Test button to make sure the program runs as expected.</p>
Notify by e-mail	<p>An email is sent to the alarm message recipients specified in E-mail settings.</p> <p>The email message includes the alarm message, the threshold exceeded, and the current threshold value. For context, the last hour's statistics are also included.</p>

6. Click Apply to save your changes.

Log file and database formats

When you [add an action to log messages to a file](#), you can:

- Select an [existing log file format](#)
- [Create a custom log file format](#)

When you [add an action to log messages to a database](#), you can:

- Select an [existing database format](#)
- [Create a custom database format](#)

Log file formats available in Kiwi Syslog Server

When you [add an action to log messages to a file](#), you can choose any of the following standard log file formats.

 You can also [create a custom log file format](#).

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	2017-07-22 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	2017-07-22 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	07-22-2017 [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
Example	22-07-2017 [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	07-22-2017 [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	22-07-2017 [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	2017-07-22 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	2017-07-22 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>2017-07-23 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] 2017-07-23 [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 on their website.

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
Example	WTsyslog [2017-11-12 12:44:45 ip=192.168.168.1 pri=6] <134>id=firewall time="2017-11-15 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 on their website.

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	2017-07-22 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 on Sawmill website.

Create a custom log file format

When you add an [action to log messages to a file](#), you can specify the log file format. If you do not want to use the standard formats available, you can create your own custom file logging format.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Expand the Formatting node.
3. Right-click the Custom file formats node and choose Add new custom file format.

4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. Specify the following options:

Log file fields	<ol style="list-style-type: none"> 1. Select the fields that you want to include in the log file. (See the examples of fields and values below.) 2. Drag and drop the fields to specify the order in which the information is shown. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>i 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 <code>\Scripts</code> sub folder. If you select 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.</p> </div>
Date and Time formats	Select the date and time formats appropriate for your location.
Field delimiter	Select the character used to separate the fields. Tab characters are the most common delimiters used for syslog files.
Qualifier	Select an option if you want to enclose each field can be enclosed in quotes or tags. This option is useful when the delimiter is a comma.
Adjust time to UTC	Select this option to adjust the date and time stamps in your log files to be adjusted to UTC (GMT) time. The current time difference (in hours) between your system and UTC is shown in brackets.

6. Click Apply to save the format.

EXAMPLES OF FIELDS AND VALUES

The following table shows examples of fields and their values.


FIELD NAME	EXAMPLE
Date	28/01/2017
Time	16:12:54
Date-Time	28/01/2017 16:12:54
Milliseconds	123

FIELD NAME	EXAMPLE
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.

Database formats available in Kiwi Syslog Server

When you [add an action to log messages to a database](#), you can choose any of the following standard database formats:

- Microsoft Access
- Microsoft SQL
- MySQL
- Oracle

 You can also [create a custom database format](#).

The following sections describe the table columns used to store message field values. If you choose to create the table manually before you add a Log to Database action, use the table design for the selected database type.

DEFAULT MICROSOFT ACCESS DATABASE TABLE DESIGN

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

DEFAULT MICROSOFT SQL AND GENERIC SQL DATABASE TABLE DESIGN

FIELD	NAME	TYPE	SIZE
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	VarChar	30
Hostname	MSGHOSTNAME	VarChar	255
Message text	MSGTEXT	VarChar	1024

DEFAULT MYSQL DATABASE TABLE DESIGN

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



DEFAULT ORACLE DATABASE TABLE DESIGN

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

Create a custom database format

When you [add an action to log messages to a database](#), you must specify the database format. If you do not want to use the standard formats available, you can create your own custom database format.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Expand the Formatting node.
3. Right-click the Custom DB formats node and choose Add new custom DB Muformat.
4. Replace the default name with a descriptive name. (The name does not have to be unique.)
5. Specify the following options:

Type	Select your database type from the Type dropdown menu. If your database type is not included, select Unknown format.
Function	Drag and drop the gray Function cells to specify the order in which fields are created in the database table. This is also the order that data is inserted into the table.
Field name	<ol style="list-style-type: none"> 1. Select the fields to include as columns in the database table. <ul style="list-style-type: none">  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 <code>\Scripts</code> sub folder. If you select 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. 2. To edit a field name, double-click the name and replace it. <ul style="list-style-type: none">  The default 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.
Size	For each field, 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.
Type	Match each field type 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.
Format	<p>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.</p> <p>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.</p> <p>Leaving the format cell blank will leave the data unmodified and it will be added as it is received.</p>
Show SQL commands	<p>Click this button to 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.</p> <p>Example SQL commands:</p> <p>Database type: MySQL database</p> <p>Database name: New Format</p> <p>SQL command to create the table:</p> <pre>CREATE TABLE Syslogd (MsgDate DATE,MsgTime TIME,MsgPriority VARCHAR (30),MsgHostname VARCHAR (255),MsgText TEXT)</pre> <p>SQL INSERT command example:</p> <pre>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')</pre>

6. Click Apply to save the format.

EXAMPLES OF DATA FORMATS

FIELD NAME	TYPE	SIZE	DATA
MsgUnique	adInteger	4	1
MsgDate	adDBTimeStamp	16	28/01/2017
MsgTime	adDBTimeStamp	16	16:12:54
MsgDateTime	adDBTimeStamp	16	28/01/2017 16:12:54
MsgUTCDate	adDBTimeStamp	16	28/01/2017
MsgUTCTime	adDBTimeStamp	16	04:12:54
MsgUTCDateTime	adDBTimeStamp	16	28/01/2017 04:12:54
MsgTimeMS	adInteger	4	0
MsgPriorityNum	adInteger	4	191
MsgFacilityNum	adInteger	4	23
MsgLevelNum	adInteger	4	7
MsgPriority	adVarChar	30	Local7.Debug
MsgFacility	adVarChar	15	Local7
MsgLevel	adVarChar	15	Debug
MsgHostAddress	adVarChar	15	192.168.0.1
MsgHostname	adVarChar	255	host.company.com
MsgInputSource	adVarChar	10	UDP
MsgText	adLongVarChar	1024	This is a test message from KSS

DNS setup options


See the following topics to set DNS options:

- [DNS resolution](#)
- [DNS setup](#)
- [DNS caching](#)

DNS resolution

Complete the following steps to specify DNS resolution options.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Click DNS Resolution.
3. Specify the following options:

Resolve the address of the sending device	<p>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"</p> <p>The resolved host name is then used in the display and other actions.</p> <p>The Host name is also used for the "Hostname" type filter.</p> <p>If you like, the domain name section can be removed from the display by using the Remove the domain name option.</p>
Remove the domain name (show only the host name)	<p>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".</p> <p>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.</p> <p>This option also effects the host name field used for all the logging actions.</p>
Resolve IP addresses found within the syslog message text	<div data-bbox="358 1499 1513 1556" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">  This option is available only in the registered version. </div> <p>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 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.</p>

	<p>* 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.</p> <p>Examples:</p> <p>Test user connected to website <code>http://192.168.1.2/index.html. src=192.168.5.100 rxbytes=64</code></p> <p>With replace IP address with host name option, the message becomes...</p> <p>Test user connected to website <code>http://website.company.com/index.html. src=userpc.company.com rxbytes=64</code></p> <p>With place host name next to IP address option, the message becomes...</p> <p>Test user connected to website <code>http://192.168.1.2 (website.company.com) /index.html. src=192.168.5.100 (userpc.company.com) rxbytes=64</code></p> <p>The Remove the domain name option allows the stripping of the domain name portion from the resolved host name.</p> <p>To selectively keep or remove the domain name based on a filter match, check the If domain name contains check box.</p> <p>Place the domain name substrings to remove in quotes. To filter multiple domains, separate each quoted string with a space or comma.</p> <p><code>".companyabc.com", ".companyxyz.co.uk"</code></p> <p>An IP address resolved to <code>mypc.company.co.uk</code> will be changed to just <code>"mypc"</code>.</p> <p>Hostname tagging:</p> <p>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 <code>"hostname=["</code> and then have a <code>"] "</code> suffix. You can change the prefix and suffix characters to fit the format of your messages.</p> <p>A suggested tagging format for WELF format messages would be a prefix of resolved_host= and a suffix of a space character.</p>
DNS query timeout	<p>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.</p> <p>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.</p> <p>If your DNS server is local and you are only resolving internal addresses, you can safely reduce your timeout value down to 3 seconds.</p>

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.


4. Click Apply to save your changes.

DNS setup

To view or edit DNS setup information:

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Expand the DNS Resolution node.
3. Click DNS Setup.
4. Under Internal IP address - Name Resolution, specify the following options:

Internal IP address range(s)	<p>A list of masked IP addresses that identify your internal network address space.</p> <p>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.</p> <p>10.0.0.0 - 10.255.255.255 (10/8 prefix) 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)</p> <p>192.168.0.0 - 192.168.255.255 (192.168/16 prefix) 169.254.0.0 - 169.254.255.255 (link-local)</p> <p>Adding an internal IP address range:</p> <p>Enter the masked IP address in the text box directly underneath the "Internal IP address range" list, and click the "Add" button.</p> <p>IP addresses must be masked with an "x" character, the "x" signifying that any value within the range (0-255) is acceptable.</p> <p>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'.</p>
------------------------------	---

	<p> 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.</p>
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	<p>These entries determine which internal network address the DNS query will be sent to.</p> <p>By default these addresses are auto-detected by Kiwi Syslog Server, and depending on your network configuration may need to be altered.</p> <p>If the preferred DNS server is unavailable or cannot service the request, the same query will be asked of the alternate DNS server.</p> <p>If no alternate DNS server is available, then this address is to be left blank.</p>

5. Under External IP address - Name Resolution, specify the following options:

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	<p>These entries determine which external network address the DNS query will be sent to.</p> <p>By default these addresses are auto-detected by Kiwi Syslog Server, and depending on your network configuration may need to be altered.</p> <p>If the preferred DNS server is unavailable or cannot service the request, the same query will be asked of the alternate DNS server.</p> <p>If no alternate DNS server is available, then this address is to be left blank.</p>

6. Click Apply to save your changes.

DNS caching

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.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Expand the DNS Resolution node.
3. Click DNS Caching.

4. Under Entries in the cache:

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.

5. UnderCache 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.
Enable preemptive 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	<p>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.</p> <p>An example host file is included in the install folder. It is named "StaticHosts.txt".</p> <p>Example of a host file:</p>

```
# Static DNS host file
# Each entry must have 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 up to 63 characters
#
# Comments can be on a separate line and start with a #
#
# 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 recognized 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
```

6. Click Apply to save your changes.

Syslog message modifiers

When a 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.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Click Modifiers.
3. Specify the following options:

Replace non-printable characters with <ASCII value>	<p>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.</p> <p>For example, when a carriage return is received, it will be replaced with a <013> instead.</p>
Remove CR/LF from end of messages	<p>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.</p> <p>Check this box if you want to remove all trailing CR/LF characters from the messages.</p>
Remove imbedded date and time from Cisco messages	<p>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.</p> <p>This option works by looking for a particular Cisco message format. It will work with the following known Cisco date and time formats:</p> <ul style="list-style-type: none">• 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 50: *Mar 1 00:56:30.475: %SYS-5-CONFIG_I: Configured from console by console

	<ul style="list-style-type: none"> • 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 priority > 191 (use default priority)	<p>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.</p> <p>If this option is enabled, messages received with a priority higher than 191 will have their priorities set to the default priority setting.</p>
Allow messages with no priority (use default priority)	<p>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.</p> <p>A normal Syslog message has a priority code at the start of the message text. Example. <100>This is a test message</p> <p>The priority value should be between 0 and 191 for standard Unix priority codes</p>
Maximum message length (bytes)	<p>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.</p> <p>This limit allows the program to reject oversize messages sent by hackers or errors in transmission.</p> <p>Some Syslog Servers may crash when receiving large packets, this option limits the size of the packet that the program will accept and process.</p> <p>The Syslog RFC 3164 states that legal Syslog messages may not exceed 1024 bytes in length. (Not including packet headers)</p>

4. Click Apply to save your changes.


Configure email options

Before you [add an action to send email](#), specify the email format and configure other email options. For example, you can send alarm messages, send statistics, and enable logging.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Scroll down and click E-mail.
3. Specify the following options.

Email format	Choose HTML or Plain Text.
Security	<p>Select one of the following:</p> <ul style="list-style-type: none"> • None: This option can be used for sending email 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 syslog alarm messages to	<p>Select this option to send an email when an alarm threshold has been exceeded. The email can be sent securely.</p> <p>Enter the email address or addresses you want notified when an alarm is triggered. Email addresses must be separated by commas. For example:</p> <p><code>noc@company.com, helpdesk@company.com, pager123@company.com</code></p> <p>If the message is being sent to a paging service and there is a limited amount of display space, select Short alarm messages (for pagers). This option sends only the subject line, not the message body.</p>
Send syslog statistics to	<p>Select this option to email statistics for a selected interval. The message 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 and the facility and level.</p> <p>The message is best viewed in a fixed font such as Courier New so all the columns line up. This can be sent securely.</p> <p>Enter one or more recipients, separated by commas, and specify the interval:</p> <ul style="list-style-type: none"> • Hours: Hour interval can be in multiples of 24. Hour interval can accept values of 1, 2, 3, 4, 6, 8, and 12.

	<ul style="list-style-type: none"> • Days: Statistics are emailed out on midnight 00:00 based on the number of days set. • Weeks: By default, the statistics are emailed out on Sunday, for example, 00:00 based on the number of weeks set. • Months: By default, the statistics are emailed on the 1st of every month or for the number of months set. <p>Click More to set a maximum number of hosts to be displayed in the statistics email and in diagnostics.</p>
Hostname or IP address of SMTP mail server	<p>Enter the IP address or host name of your SMTP server. This can be your local server, or one provided by your ISP.</p> <p>The host name of the mail server is usually something like mail.company.com or smtp.company.com. Below are examples:</p> <ul style="list-style-type: none"> • Gmail - smtp.gmail.com • Yahoo - smtp.mail.yahoo.com • Hotmail - smtp.live.com
SMTP port	<p>If your SMTP server listens on a non-standard port, specify the alternate value here. Normally SMTP servers listen on port 25. Some companies change this value for security reasons. The value can be from 1 to 65535.</p> <p>The default port for SSL is 465 and for TLS is 587.</p>
Valid 'from' e-mail address on SMTP server	<p>SolarWinds recommends 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.</p> <p>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 email.</p> <p>Optionally, you can specify a friendlier name in brackets after the address. This will be shown as the From address in the mail client. For example:</p> <p><code>noc@company.com (Syslog Server)</code></p> <p>In the example above, the name "Syslog Server" will appear in the From field of the received message. Some SMTP servers might not support this format of from address.</p>
Timeout	<p>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. Valid values are from 1 second to 240 seconds.</p>

SMTP Username and Password	<p>Set these options only if your SMTP server requires authentication before accepting email. Most SMTP servers do not need these options set.</p> <p>To enable authentication, select the checkbox to the left and fill in your user name and password for the SMTP server. These values are supplied by your network administrator, SMTP server provider, or ISP.</p> <p>If you need to use the POP before SMTP option for authentication. SolarWinds recommends 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.</p>
Default E-mail Delivery Options	<p>Use this option to change the default importance, priority, and sensitivity flags of email messages sent by Kiwi Syslog Server.</p>
Keep a log file of e-mail activity	<p>If you intend to use the e-mail feature to notify you of alarms and statistics, select this option to keep a log of what messages have been sent and to whom. The log file is named <code>SendMailLog.txt</code> and is located in the Kiwi Syslog Server installation directory.</p> <ul style="list-style-type: none">• Click View log to open the log.• Click Delete log to delete the file and start a new log file.
Enable verbose logging	<p>Enable this option 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.)</p> <div data-bbox="386 1226 1513 1287" style="border: 1px solid #ccc; padding: 5px;"><p> This option can use a lot of disk space.</p></div>

4. Click Apply to save your changes.

Configure input options

Configure input options to enable Kiwi Syslog Server to listen on the port and for the protocol used by your network devices. You can also configure keep-alive messages and enable support for IPv6.


- [Configure UDP input options](#)
- [Configure TCP input options](#)
- [Configure secure \(TLS\) TCP options](#)
- [Configure SNMP trap input options](#)
- [Enable keep-alive messages](#)
- [Enable IPv6 support](#)
- [Enable a beep on every message](#)

Configure UDP input options

By default, Kiwi Syslog Server listens for UDP messages on port 514. You can configure UDP input options to change the port, bind to a specific interface, or specify a data encoding format.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Expand the Inputs node.
3. Click UDP.

4. Specify the following options:

Listen for UDP messages	This option is selected by default to enable Kiwi Syslog Server to receive UDP messages.															
UDP Port	<p>The default port for UDP Syslog messages is 514. If you want to listen on a different port for UDP messages, you can enter any port value from 1 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.</p> <p> Kiwi Syslog Server can listen for messages on only one UDP port.</p>															
Bind to address	<p>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.)</p> <p>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.</p>															
Data encoding	<p>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.</p> <p>Select a commonly used encoding format from the drop-down menu. Or, to select a different encoding, choose "Other-->" and then enter the code page number into the field on the right.</p> <p>The various code pages available on most Windows systems can be found on the Microsoft website. Here are some common code page numbers that can be used.</p> <table border="1"> <thead> <tr> <th>NAME</th> <th>CODE PAGE NUMBER</th> <th>DESCRIPTION</th> </tr> </thead> <tbody> <tr> <td>System</td> <td>1</td> <td>System Code Page</td> </tr> <tr> <td>ANSI</td> <td>0</td> <td>ANSI</td> </tr> <tr> <td>UTF-8</td> <td>65001 Format</td> <td>Unicode Transformation</td> </tr> <tr> <td>8Shift-JIS</td> <td>932</td> <td>Japanese</td> </tr> </tbody> </table>	NAME	CODE PAGE NUMBER	DESCRIPTION	System	1	System Code Page	ANSI	0	ANSI	UTF-8	65001 Format	Unicode Transformation	8Shift-JIS	932	Japanese
NAME	CODE PAGE NUMBER	DESCRIPTION														
System	1	System Code Page														
ANSI	0	ANSI														
UTF-8	65001 Format	Unicode Transformation														
8Shift-JIS	932	Japanese														

NAME	CODE PAGE NUMBER	DESCRIPTION
EUC-JP	51932	Japanese Extended Unix Code
BIG5	950	Traditional Chinese
Chinese	936	Simplified Chinese

i 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.

- Click Apply to save your changes.

Configure TCP input options


By default, Kiwi Syslog Server does **not** listen for TCP messages, because syslog messages are traditionally sent using UDP.

If any of your network devices send syslog messages using TCP, complete the following steps to enable Kiwi Syslog Server to listen for TCP messages.

- Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
- Expand the Inputs node.
- Click TCP.
- Specify the following options:

Listen for TCP Syslog messages	Select this option to enable Kiwi Syslog Server to receive TCP messages.
TCP Port	The default port for TCP syslog messages is 1468. If you want to listen on a different port for TCP messages, you can enter any port value from 1 to 65535. If you change the port from 1468, the device sending the syslog message must also be able to support the alternate port number.
Bind to address	By default, the TCP socket listens for messages on all connected interfaces. 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.

 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 Cisco website.


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.

Select a commonly used encoding format from the drop-down menu. Or, 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 on the Microsoft website. 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 Format	Unicode Transformation
8Shift-JIS	932	Japanese
EUC-JP	51932	Japanese Extended Unix Code
BIG5	950	Traditional Chinese
Chinese	936	Simplified Chinese

 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.

Message delimiters	<p>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.</p> <p>The kind of delimiter to use depends very much on the client or device which is sending Syslog over TCP.</p>
--------------------	---


5. Click Apply to save your changes.

Configure secure (TLS) TCP options

Some devices support sending secure syslog messages over the TCP channel with transport layer security (TLS). Kiwi Syslog Server supports Secure (TLS) Syslog (RFC 5425).

By default, Kiwi Syslog Server does **not** listen for TCP messages, because syslog messages are traditionally sent using UDP. If any of your network devices send syslog messages over the TCP channel with transport layer security (TLS), complete the following steps to enable Kiwi Syslog Server to listen for these messages.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Expand the Inputs node.
3. Click TCP.
4. Specify the following options:

Listen for secure (TLS) TCP Syslog messages	Select this option to enable Kiwi Syslog Server to receive secure TCP messages.
Certificates	<p>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.</p> <div data-bbox="367 1730 1511 1875" style="border: 1px solid #add8e6; padding: 5px;"> <p> Certificates that will be used by Kiwi Syslog Server have to be installed into the Local Machine certificate store. Use the Microsoft Management Console to install certificates.</p> </div>

	<p>What kind of certificate should be used and configuration of public key infrastructure (PKI) is device-specific. See the manufacturer documentation.</p>																								
TCP Port	<p>The default port for secure TCP syslog messages is 6514. If you want to listen on a different port for TCP messages, you can enter any port value from 1 to 65535. If you change the port from 6514, the device sending the syslog message must also be able to support the alternate port number.</p>																								
Bind to address	<p>By default, the TCP socket listens for messages on all connected interfaces. 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.)</p> <p>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.</p>																								
Data encoding	<p>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.</p> <p>Select a commonly used encoding format from the drop-down menu. Or, to select a different encoding, choose "Other-->" and then enter the code page number into the field on the right.</p> <p>The various code pages available on most Windows systems can be found on the Microsoft website. Here are some common code page numbers that can be used.</p> <table border="1"> <thead> <tr> <th>NAME</th> <th>CODE PAGE NUMBER</th> <th>DESCRIPTION</th> </tr> </thead> <tbody> <tr> <td>System</td> <td>1</td> <td>System Code Page</td> </tr> <tr> <td>ANSI</td> <td>0</td> <td>ANSI</td> </tr> <tr> <td>UTF-8</td> <td>65001 Format</td> <td>Unicode Transformation</td> </tr> <tr> <td>8Shift-JIS</td> <td>932</td> <td>Japanese</td> </tr> <tr> <td>EUC-JP</td> <td>51932</td> <td>Japanese Extended Unix Code</td> </tr> <tr> <td>BIG5</td> <td>950</td> <td>Traditional Chinese</td> </tr> <tr> <td>Chinese</td> <td>936</td> <td>Simplified Chinese</td> </tr> </tbody> </table>	NAME	CODE PAGE NUMBER	DESCRIPTION	System	1	System Code Page	ANSI	0	ANSI	UTF-8	65001 Format	Unicode Transformation	8Shift-JIS	932	Japanese	EUC-JP	51932	Japanese Extended Unix Code	BIG5	950	Traditional Chinese	Chinese	936	Simplified Chinese
NAME	CODE PAGE NUMBER	DESCRIPTION																							
System	1	System Code Page																							
ANSI	0	ANSI																							
UTF-8	65001 Format	Unicode Transformation																							
8Shift-JIS	932	Japanese																							
EUC-JP	51932	Japanese Extended Unix Code																							
BIG5	950	Traditional Chinese																							
Chinese	936	Simplified Chinese																							

	<p>i 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.</p>
Message delimiters	<p>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.</p> <p>The kind of delimiter to use depends very much on the client or device which is sending Syslog over TCP.</p> <p>i The RFC 5425 option is available for secure TCP messages. This delimiter conforms to the rule defined in RFC 5425. If you decide to look for this delimiter inside incoming message stream the search for this delimiter is performed before other delimiters are checked.</p>


5. Click Apply to save your changes.


Configure SNMP trap input options


Use the following options to enable Kiwi Syslog Server to listen for version 1, 2c, and 3 SNMP traps. The traps are decoded and then handled like syslog messages.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Expand the Inputs node.
3. Click SNMP.
4. Specify the following options:

Listen for SNMP Traps	Select this option to enable Kiwi Syslog Server to receive SNMP traps.
Add/Remove SNMP v3 Credentials	<p>SNMP v3 adds security and remote configuration enhancements. To process SNMP v3 traps, click this button and enter credential details:</p> <ul style="list-style-type: none"> • User name: User name that is specified in the device. It must be a unique value. • Authentication Password and Algorithm: Authentication from the valid source is focused using Authentication password and Algorithm which is ether MD5 or SHA.

	<ul style="list-style-type: none"> • Private Password and Algorithm: The data encryption for privacy is performed using the private password and algorithm which is either AES or DES/3DES. • Security Level: Security level follows any of the communication mechanism shown below: <ul style="list-style-type: none"> • No security: no authentication and no encryption for users. • Authentication only: authentication without any encryption of the data sent. • Authentication and Privacy: with authentication and encryption of data.
UDP Port	<p>Specify the UDP port that listens for SNMP traps. IPv4 Traps are usually sent to port 162 and IPv6 traps are sent to port 163. A value between 1 to 65535 can be entered here. If you choose a value other than 162 or 163, make sure the device sending the trap is also sending to the specified port.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> Port number shouldn't be the same for IPv4 and IPv6 in receiving SNMP traps.</p> </div>
Bind to address	<p>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.)</p> <p>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.</p>
Variable Binding	<p>SNMP traps can be bound into custom fields. Below are the SNMP fields that can be assigned to custom variables such as Custom1, Custom2... Custom16.</p> <p>For example:</p> <p>In the Send SNMP trap action, click Insert message content or counter to select custom variables.</p>
Specified fields	<p>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.</p>
Community	<p>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".</p>

	<p> SNMP Community strings are used only by devices which support SNMPv1 and SNMPv2 protocol. SNMPv3 uses username/password authentication, along with an encryption key.</p>
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 and 3 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 and 3.
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 an 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	<p>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 [].</p> <p>Here is an example of a message tagged with the fieldname=value option:</p>

	<pre>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</pre> <p> The values are only contained in quotes (") if they contain a space.</p>
Use LinkSys Display filter	<p>The LinkSys Display filter simply removes all PPP messages from being displayed. The PPP messages are still logged to file as normal.</p> <p>This feature is only useful if you are logging from a LinkSys network device.</p>
Perform MIB lookups	<p>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.</p> <p>The MIB database file is located in the InstallPath\MIBs folder in a file named: KiwiMIBDB.dat</p> <p>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.</p> <p>If you would like to add additional MIB lookup values, please contact SolarWinds Support. Send your zipped MIB files, and also include your Unknown_OID_list.txt file so we can ensure all the OIDs are referenced.</p> <p>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.</p>
Log failed lookups to debug file	<p>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.</p>
Show additional OID suffix info	<p>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.</p> <p>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.</p>

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.

5. Click Apply to save your changes.

Enable keep-alive messages

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.

For more information about using keep-alive messages, see [How to use a keep-alive message in a script](#) and [Forwarding a keep-alive message to another host as a beacon](#).

ENABLE AND CONFIGURE KEEP-ALIVE MESSAGES

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Expand the Inputs node.
3. Click Keep-alive.

4. Specify the following options:

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 255.255.255.255 for IPv4 and it supports IPv6 address as well. 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".

5. Click Apply to save your changes.

HOW TO USE A KEEP-ALIVE MESSAGE IN A SCRIPT

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 A KEEP-ALIVE MESSAGE 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.

Enable IPv6 support

If you want Kiwi Syslog Server to send and receive IPv6 messages, you must enable IPv6 support.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Click the Inputs node.
3. Select Enable IPv6 support .
4. Click Apply to save your changes.

Enable a beep on every message

If this option is enabled, Kiwi Syslog Server plays a beep when it receives 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.

i 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.

1. Choose File > Setup to open the Kiwi Syslog Server Setup dialog box.
2. Click the Inputs node.
3. Select Beep on every message received.
4. Click Apply to save your changes.

View syslog statistics

1. To view syslog statistics, select View > View Syslog Statistics.

The Syslog Statistics dialog opens.

Syslog Statistics are updated every 10 seconds. Press the Refresh button or F5 to cause the statistics to be recalculated and displayed immediately.

2. Click any of the following tabs.

1 Hour history	Displays a bar chart of the last 60 minutes 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.
24 Hour history	Displays a bar chart of the last 24 hours' 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.
Severity	<p>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.</p> <p>The message count and percentage of total traffic is shown in the table.</p> <p>Click on any header to sort the table by that column. Click again to reverse the sort order.</p>
Top 20 Hosts	<p>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.</p> <p>Click on any header to sort the table by that column. Click again to reverse the sort order.</p> <p>If a particular host is generating a lot of the traffic or the pattern changes, it could indicate a problem on that device.</p>
Counters	<p>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.</p> <p>Some counters show values for the interval period, and some are from the last 24-hour period (from the current time of display). Others show values since Midnight (0:00).</p>

The intervals start at 00 from the time the program starts rather than being related to the actual MM/DD/YYYY HH: MM:SS time. To see how long the program has been running, check the Program uptime counter, see the duration of the interval period, and check the start and end date & time.

Messages - Total:

This counter value shows the number of messages received since the program starts. To reset this value, you must restart the program or service.

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 - Last Interval (Hours/Days/Weeks/Months):

This counter value shows the numbers of messages received during the last interval period. The counter is reset once the statistics report is emailed out.

Messages - Since Midnight:

This counter value shows the number of messages received since midnight (00:00 - 23:59). This counter automatically resets at 00:00 every day.

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 reset to 0 each hour and will be incremented as each new message arrives.

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 - Average Last Interval (Hours/Days/Weeks/Months):

This counter value shows the average number of messages received per hour over the last interval period.

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 stats report have been emailed out. The stats are usually sent based on the interval set. The value being displayed is based on the interval duration.

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 stats report have been emailed out. The stats are usually sent based on the interval set. The value being displayed is based on the interval duration.

Errors - logged to disk:

This counter value shows the number of internal program errors that have been logged to disk. Errors are usually caused when the log file cannot be accessed or if an internal program error has occurred. If the value is not 0, 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.

Breakdown of messages by sending host in Stats:

The host table shows the breakdown of messages by sending the host. The message count per host and percentage of total traffic is show in the table.

Total number of hosts that can be listed depends on the total number set in **More options > Number of host**. Value should be within 1 to 999.

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 [Scripting custom statistics fields](#) to set the counter name and initial values

Protocols

For detailed information about syslog protocols, see the following topics:

- [The syslog protocol](#)
- [The Kiwi Reliable Delivery Protocol \(KRDP\)](#)

The syslog protocol

The following sections provide information about the syslog protocol:

- [Syslog Facilities](#)
- [Syslog Levels](#)
- [Syslog Priority values](#)
- [Transport](#)
- [Syslog RFC 3164 header format](#)

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.

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...

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.

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](#).

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. Check out their community discussion on Roxen website. For a comprehensive description of the syslog protocol, see Sans Institute website.

The Kiwi Reliable Delivery Protocol (KRDP)

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 acknowledgment 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 acknowledgment 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 reestablish 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)

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

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

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.

Error and mail logs

Kiwi Syslog Server automatically creates an error log that you can use for troubleshooting. You can also choose to log information about emails that Kiwi Syslog Server sends.

The error log

Kiwi Syslog Server writes to the error log if it has a problem writing messages to a log file or archiving log files. It also records any other error messages it encounters. If you are [troubleshooting](#) a problem, information in this log might help.

To open this log from the Kiwi Syslog Service Manager, select View > View error log file.

The log file location is `<installDir>\ErrorLog.txt`.

The send mail log

To log information about each email message that Kiwi Syslog Server sends, go to [E-mail settings](#), and select Keep a log file of e-mail activity.

If this option is selected, you can open the send mail log by selecting View > View e-mail log file.

When this option is selected, Kiwi Syslog Server emails an alarm notification or the daily statistics, it records information about the email in the email log file.

The log file location is `<installDir>\SendMailLog.txt`.

Registry settings for Kiwi Syslog Server

The registry values listed below can be used to affect the operation of Kiwi Syslog Server.

Best practices

Before you make changes to the registry:

- Back up the registry.
- Make sure that Kiwi Syslog Server is not running. If you are using the Service edition, stop the Syslogd service.

Use RegEdit to view and change registry values.

After you update registry values, restart Kiwi Syslog Server to ensure that your changes take effect.

Available settings

The following registry settings are available. Click any setting for details.

SETTING	SPECIFIES
DisplayColumnsEnabled	Which columns are shown on the Kiwi Syslog Service Manager display.
DisplayRowHeight	The row height (in pixels) on the Kiwi Syslog Service Manager display.
MailStatsDeliveryTime	What time the daily statistics email is sent.
ServiceStartTimeout	How long (in seconds) the Service Manager waits for a Service Start or Service Stop request to complete.
ServiceUpdateTimeout	How long (in seconds) the Service Manager waits for a Properties Update request to complete.
NTServiceSocket	The port used by the Manager part of Kiwi Syslog Server to connect to the Service.
NTServiceDependencies	Services that need to start before the Syslogd service.
DebugStart	Whether debug mode is enabled.
DNSDisableWaitWhenBusy	How full the input message buffer can get before disabling the DNS resolution waiting.
DNSCacheMaxSize	The size of the cache buffer.

SETTING	SPECIFIES
DNSCacheFailedLookups	Failed lookups to cache to Improve DNS name resolution performance.
DNSSetupQueueBufferBurstCoefficient	The number of DNS/NetBIOS requests that will be dequeued from the internal queue buffer at once.
DNSSetupQueueBufferClearRate	The rate at which the DNS/NetBIOS internal queue buffer is cleared.
DNSSetupQueueLimit	The DNS/NetBIOS internal queue buffer size.
DNSSetupDebugModeOn	Whether verbose debug mode is enabled.
MsgBufferSize	The maximum number of message buffer entries.
MailAdditionalSubjectText	A text string added to the beginning of the e-mail subject for daily statistics and alarm e-mails.
MailAdditionalBodyText	An additional line of text included in the daily statistics and alarm e-mails.
MailMaxMessageSend	The maximum number of email messages that are sent per minute.
File write caching settings	Values that enable and configure file write caching.
LogFileDateSeparator	The separation character used in dates.
LogFileTimeSeparator	The default separation character used in times.
LogFileEncodingFormat	The encoding format used to write messages to log files.
ScriptEditor	The script editor to be launched when you click the Edit Script button.
ScriptTimeout	The timeout value for scripts.
DBCommandTimeout	The timeout value for logging messages to a database.
ArchiveFileReplacementChr	The replacement character for invalid characters in dates that are not valid in file names.
ArchiveFileSeparator	The separator character placed between the existing file name and the current system date and time when files are archived.
UseOldArchiveNaming	The default Scheduled Archive Task archive naming convention for Single Zip Archives.

SETTING	SPECIFIES
ArchiveTempPath	The default temp folder used by Kiwi Syslog Server's archiver.
EnableArchiveTempFile	The default Scheduled Archive Task archiving behavior.
ErrorLogFolder	The location of the <code>errorlog.txt</code> file where operational errors are logged.
MailLogFolder	The location of the <code>SendMailLog.txt</code> file where mail activity is logged.
KRDPACKTimer	The interval of the TCP_ACK protocol's acknowledgment timer.
KRDPKeepAliveTimer	The interval between the sending of Keep Alive messages to of the connected sessions.
KRDPCacheFolder	The location of the disk cache files.
KRDP RxDebug	Whether the debug log file for KRDP receive events is enabled or disabled.
KRDP TxDebug	Whether the debug log file for KRDP send events is enabled or disabled.
KRDPQueueSize	The size of the message queues used to buffer the KRDP and TCP messages.
KRDPQueueMaxMBSize	The maximum size (in MB) of the memory queue.
KRDPAutoConnect	Whether the KRDP and TCP senders will try to automatically connect to the remote host.
KRDP SendSpeed	The maximum number of messages that can be sent per second.
KRDPIdleTimeout	The time the sending socket will remain connected after the last message has been sent.
KRDPAddSeqToMsgText	Whether the KRDP listener adds the received sequence number to the end of the message text.
ProcessPriority	The priority setting in Windows for the syslogd service.
OriginalAddressStartTag and OriginalAddressEndTag	The start and end tags for the original sender's address.
MaxRuleCount	The maximum number of rules.
DBLoggerCacheClearRate	The rate (in milliseconds) at which the Database Cache is

SETTING	SPECIFIES
	checked for SQL data to be executed.
DBLoggerCacheTimeout	The maximum age (in days) of an unchanged cache file.
DBLoggerCacheDisable	Whether the default database caching behavior is overridden.
HostNosToDisplay	The number of hosts to display in the statistics report.

DisplayColumnsEnabled

Use this [Kiwi Syslog Server registry setting](#) to specify which columns are shown on the Kiwi Syslog Service Manager display.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DisplayColumnsEnabled
Min value	0
Max value	31
Default value	31
Type	Decimal number from 0-31

By default, all the columns are shown. To display a different set of columns, enter the sum of the columns' decimal values.

BIT NUMBER	DECIMAL VALUE	COLUMN NAME
0	1	Date
1	2	Time
2	4	Priority
3	8	Hostname
4	16	Message

For example:

- To display all columns, set the value to 31.
- To display the Message (16) and Hostname (8) columns, set the value to 24 (16 + 8 = 24).
- To display the Message (16) and Time (2) columns, set the value to 18 (16 + 2 = 18).
- To display only the Message column, set the value to 16.

DisplayRowHeight

Use this [Kiwi Syslog Server registry setting](#) to specify the row height (in pixels) on the Kiwi Syslog Service Manager display.

i If the font is taller than the specified row height, the row is automatically resized to accommodate the text.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DisplayRowHeight
Min value	5
Max value	50
Default value	15
Type	Height of row in pixels

MailStatsDeliveryTime

Use this [Kiwi Syslog Server registry setting](#) to specify when the daily statistics email is sent.

By default, the statistics email is sent at midnight (00:00). To change the time, enter the new time using the 24 hour clock. For example, to specify 6 PM, enter 18:00.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	MailStatsDeliveryTime
Min value	00:00

Max value	23:59
Default value	00:00
Type	HH:MM

ServiceStartTimeout

Use this [Kiwi Syslog Server registry setting](#) to specify how long (in seconds) the Service Manager waits for a Service Start or Service Stop request to complete.

If you have more than 10 actions configured or are running on a computer with a CPU speed of less than 300 MHz, increase this value as needed.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	ServiceStartTimeout
Min value	1
Max value	120
Default value	30
Type	Seconds

ServiceUpdateTimeout

Use this [Kiwi Syslog Server registry setting](#) to specify how long (in seconds) the Service Manager waits 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 300 MHz, increase this value as needed.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	ServiceUpdateTimeout
Min value	1

Max value	120
Default value	5
Type	Seconds

NTServiceSocket

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.

Use this [Kiwi Syslog Server registry setting](#) to change the port value if some other process is also using this port.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	NTServiceSocket
Min value	1
Max value	65535
Default value	3300
Type	TCP port number

NTServiceDependencies

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 can modify this [Kiwi Syslog Server registry setting](#).

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	NTServiceDependencies

Default value	Blank
Type	Text string of service names. Delimited by semi-colons. For example: ServiceName1;ServiceName2;ServiceName3

To add service dependencies:

1. Uninstall the service from the Manage menu.
2. Run RegEdit.
3. Locate the section `HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties`.
4. Create the new string value of `NTServiceDependencies`.
5. Modify the value data to include the list of services that need to start first (for example, `LanmanWorkstation;TCPIP;WMI`).
6. 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.

DebugStart

Set this [Kiwi Syslog Server registry setting](#) value to "1" to enable debug for both the Service and Manager.

Section (32-bit Windows OS)	<code>HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Options</code>
Section (64-bit Windows OS)	<code>HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Options</code>
Value (STRING)	<code>DebugStart</code>
Enable Debug	1
Disable Debug	0
Type	String

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

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.

DNSDisableWaitWhenBusy

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.

Use this [Kiwi Syslog Server registry setting](#) 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 preemptive 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Min value	0
Max value	100

Default value	10
Type	Percentage

DNSSCacheMaxSize

Use this [Kiwi Syslog Server registry setting](#) to limit 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DNSSCacheMaxSize
Min value	50
Max value	1000000
Default value	20000
Type	Maximum number of cache entries

DNSSCacheFailedLookups

Use this [Kiwi Syslog Server registry setting](#) to Improve 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".

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	ServiceUpdateTimeout
Min value	0

Max value	1
Default value	
Type	1=Cache Failed DNS lookups, 0=Do not Cache Failed DNS lookups

DNSSetupQueueBufferBurstCoefficient

Use this [Kiwi Syslog Server registry setting](#) to specify the number of DNS/NetBIOS requests that will be dequeued from the internal queue buffer at once.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DNSSetupQueueBufferBurstCoefficient
Min value	1
Max value	50
Default value	10
Type	Numeric

DNSSetupQueueBufferClearRate

Use this [Kiwi Syslog Server registry setting](#) to specify the rate at which the DNS/NetBIOS internal queue buffer is cleared.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DNSSetupQueueBufferClearRate
Min value	1
Max value	100
Default value	10
Type	Numeric

DNSSetupQueueLimit

Use this [Kiwi Syslog Server registry setting](#) to specify the DNS/NetBIOS internal queue buffer size.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DNSSetupQueueLimit
Min value	100
Max value	30000
Default value	1000
Type	Numeric

DNSSetupDebugModeOn

Set this [Kiwi Syslog Server registry setting](#) to 1 to enable verbose debug mode, This mode uploads verbose DNS/NetBIOS requests and responses to {Program files}/Syslogd/DNSdebug.txt.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DNSSetupDebugModeOn
Min value	0
Max value	1
Default value	0
Type	DNS/NetBIOS verbose debug mode (1 is on, 0 is off)

MsgBufferSize

Use this [Kiwi Syslog Server registry setting](#) to specify the maximum number of message buffer entries.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
------------------------------------	---

Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	MsgBufferSize
Min value	100
Max value	10000000 (10 million)
Default value	500000
Type	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.

MailAdditionalSubjectText

Use this [Kiwi Syslog Server registry setting](#) 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	MailAdditionalSubjectText
Default value	Blank
Type	Text string

In the registry setting, 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.

 You can also [add additional body text](#).

MailAdditionalBodyText

Use this [Kiwi Syslog Server registry setting](#) to include an additional line of text 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	MailAdditionalBodyText
Default value	Blank
Type	Text string

In the registry setting, 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
```


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.

 You can also [add additional subject text](#).

MailMaxMessageSend

Use this [Kiwi Syslog Server registry setting](#) to specify the maximum number of email messages that are sent per minute. Any messages not sent will be requeued until the next email send a minute later.

Email 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.

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.

 Restart the service for any change in value to become active.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	MailMaxMessageSend
Min value	1
Max value	1000
Default value	50

Type	Message count
-------------	---------------

File write caching settings

Use the following [Kiwi Syslog Server registry settings](#) to enable and configure 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.

FILEWRITECACHEENABLED

Use this setting to enable or disable file write caching. 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	FileWriteCacheEnabled
Min value	0
Max value	1
Default value	1
Type	Enabled = 1, Disabled = 0

FILEWRITECACHETIMEOUT

Use this setting to specify the 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	FileWriteCacheTimeout
Min value	1
Max value	120
Default value	5
Type	Timeout in seconds

FILEWRITECACHEENTRIES

Use this setting to specify 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	FileWriteCacheEntries
Min value	10
Max value	100000
Default value	1000
Type	Maximum number of cache entries (messages)

FILEWRITECACHEMAXSIZEKB

Use this setting to specify 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	FileWriteCacheMaxSizeKB
Min value	1
Max value	2000
Default value	50
Type	Maximum size in KBytes for each cache

FILEWRITECACHECLEANUP

Use this setting to specify the 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\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

FILEWRITECACHEFILELOCK

Use this setting to enable or disable log file locking.

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 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	FileWriteCacheFileLock
Min value	0
Max value	1
Default value	0
Type	Enabled = 1, Disabled = 0

FILEWRITECACHEOPENFILES

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.

Use this value to set 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties

OS)	MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	FileWriteCacheOpenFiles
Min value	1
Max value	250
Default value	100
Type	Maximum number of open file handles

LogFileDateSeparator

Use this [Kiwi Syslog Server registry setting](#) to change the separation character used in dates.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\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)

A normal Kiwi ISO log file format message is formatted like this:

```
2004-05-27 10:58:22 Kernel.Warning 192.168.0.1 kernel: This is a test message
```

If you change 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
```

 You can also [change the time separator character](#).

LogFileTimeSeparator

Use this [Kiwi Syslog Server registry setting](#) to change the default separation character used in times.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\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)

The following is a default Kiwi ISO log file format message:

```
2004-05-27 10:58:22 Kernel.Warning 192.168.0.1 kernel: This is a test message
```

If you change 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
```

 You can also [change the date separator character](#).

LogFileEncodingFormat

Use this [Kiwi Syslog Server registry setting](#) to change the encoding format used to write messages to log files.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties

OS)	MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	LogFileEncodingFormat
Min value	1
Max value	120
Default value	5
Type	Seconds

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 are available on Microsoft website.

Here are some common code page numbers.

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

 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.

ScriptEditor

Use this [Kiwi Syslog Server registry setting](#) to choose and alternate script editor to be launched when you click the Edit Script button. By default, the scripts are edited with Notepad. This setting applies only to the Run Script action.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	ScriptEditor
Default value	Notepad.exe
Type	Path and file name of script editor application. For example: C:\Program Files (x86)\Notepad++\notepad++.exe

ScriptTimeout

Use this [Kiwi Syslog Server registry setting](#) to specify the timeout value for scripts.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\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)

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.

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).

DBCommandTimeout

Use this [Kiwi Syslog Server registry setting](#) to specify the timeout value for logging messages to a database.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DBCommandTimeout
Min value	1
Max value	120
Default value	5
Type	Seconds

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.

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).

ArchiveFileReplacementChr

Use this [Kiwi Syslog Server registry setting](#) to specify the replacement character for invalid characters in dates that are not valid in file names.

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, a 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	ArchiveFileReplacementChr
Default value	- (dash)
Type	Character, or string of characters

ArchiveFileSeparator

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 ("-"). Use this [Kiwi Syslog Server registry setting](#) to specify an alternative character.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	ArchiveFileSeparator
Default value	- (dash)
Type	Character, or string of characters

UseOldArchiveNaming

Use this [Kiwi Syslog Server registry setting](#) to override 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 convention present prior to version 8.3.x. Only archive tasks which zip to a single zip file are affected by this setting.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	UseOldArchiveNaming
Min value	0

Max value	1
Default value	0 (disabled)
Type	Number

ArchiveTempPath

Use this [Kiwi Syslog Server registry setting](#) to override the default temp folder used by Kiwi Syslog Server's archiver. By default, the Windows temp folder location is used (usually C:\Windows\Temp, or C:\Documents and Settings\\Local Settings\Temp).

 This setting takes effect only if the [EnableArchiveTempFile](#) has been enabled.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	ArchiveTempPath
Min value	0
Max value	1
Default value	0 (disabled)
Type	Number

EnableArchiveTempFile

Use this [Kiwi Syslog Server registry setting](#) to override the default Scheduled Archive Task archiving behavior.

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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties

Value (STRING)	EnableArchiveTempFile
Min value	0
Max value	1
Default value	0 (disabled)
Type	Number

ErrorLogFolder

Use this [Kiwi Syslog Server registry setting](#) to specify the location of the `errorlog.txt` file where operational errors are logged. By default, this file is located in the installation directory.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	ErrorLogFolder
Default value	Application installation path
Type	A path (for example, <code>C:\My Logs\</code>)

MailLogFolder

Use this [Kiwi Syslog Server registry setting](#) to specify the location of the `SendMailLog.txt` file where mail activity is logged. By default, this file is located in the installation directory.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	MailLogFolder
Default value	Application installation path
Type	A path (for example, <code>C:\My Logs\</code>)

KRDPACKTimer

Use this [Kiwi Syslog Server registry setting](#) to specify the interval of the TCP_ACK protocol's acknowledgment timer. By default, the protocol will acknowledge (ACK) the received packets after 200 milliseconds.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPACKTimer
Min value	10
Max value	65535
Default value	200
Type	Milliseconds

KRDPIKeepAliveTimer

Use this [Kiwi Syslog Server registry setting](#) to specify 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).

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPIKeepAliveTimer
Min value	1
Max value	65535
Default value	25
Type	ACK Timer intervals

KRDPCacheFolder

Use this [Kiwi Syslog Server registry setting](#) to specify the location of the disk cache files that might be created. Disk cache files are created only if the remote host is unavailable for some time and the memory cache has become full.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPCacheFolder
Default value	<InstallFolder>\Cache\
Type	Path to cache folder

KRDPRxDebug

Use this [Kiwi Syslog Server registry setting](#) to enable or disable 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 installation folder and named `KRDPRxDebug.txt`.

The KRDP listener is created by enabling the Inputs > TCP option.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPRxDebug
Min value	0
Max value	1
Default value	0
Type	Enable or disable

KRDPTxDebug

Use this [Kiwi Syslog Server registry setting](#) to enable or disable 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 installation folder and named `KRDPTxDebug.txt`.

The KRDP senders are created by using the Forward to another host actions.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPTxDebug
Min value	0
Max value	1
Default value	0
Type	Enable or disable

KRDPQueueSize

Use this [Kiwi Syslog Server registry setting](#) to specify 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPQueueSize
Min value	50
Max value	200000
Default value	10000
Type	Number of queued messages

KRDPQueueMaxMBSize

Use this [Kiwi Syslog Server registry setting](#) to specify the maximum size (in MB) of the memory queue.

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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\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

KRDPAutoConnect

Use this [Kiwi Syslog Server registry setting](#) to specify whether the KRDP and TCP senders will try to automatically connect to the remote host.

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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPAutoConnect
Min value	0
Max value	1
Default value	1
Type	Enable or disable

KRDPConnectTime

Use this [Kiwi Syslog Server registry setting](#) to specify the time between connection retries. When a connection cannot be made to the remote peer, a connection attempt will be made every KRDPConnectTime seconds.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
------------------------------------	---

Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPCoconnectTime
Min value	5
Max value	65535
Default value	5
Type	Seconds

KRDPSendSpeed

Use this [Kiwi Syslog Server registry setting](#) to specify 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.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPSendSpeed
Min value	10
Max value	10000
Default value	2000
Type	Messages per second send speed

KRDPIidleTimeout

Use this [Kiwi Syslog Server registry setting](#) to specify 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 KRDPIidleTimeout then the connection is closed.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties

OS)	MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPIIdleTimeout
Min value	0 (off)
Max value	65535
Default value	60
Type	Seconds

KRDPAddSeqToMsgText

Use this [Kiwi Syslog Server registry setting](#) to specify whether the KRDP listener adds the received sequence number to the end of the message text.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	KRDPAddSeqToMsgText
Min value	0
Max value	1
Default value	0
Type	Enable or disable

When this value is set to "1" the KRDP listener will add the received sequence number to the end of the 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.

For example:

```
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
```


ProcessPriority

Use this [Kiwi Syslog Server registry setting](#) to enable syslogd to modify its priority setting in Windows.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	ProcessPriority
Min value	0
Max value	5
Default value	0
Type	Syslog Process Priority

Acceptable values are listed below.

VALUE	PRIORITY LEVEL	DESCRIPTION
0	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.
1	Below Normal	Indicates a process that has priority above Idle but below Normal.
2	Normal	(Default value.) Specify this class for a process with no special scheduling needs.
3	Above Normal	Indicates a process that has priority above Normal but below High.
4	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.
5	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.

VALUE	PRIORITY LEVEL	DESCRIPTION
		 Realtime priority can cause system lockups.

OriginalAddressStartTag and OriginalAddressEndTag

Use the [Kiwi Syslog Server registry setting](#) OriginalAddressStartTag to override the default start tag for the sender's original address.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	OriginalAddressStartTag
Default value	Original Address=
Type	Original Address Start Tag

Use the OriginalAddressEndTag setting to override the default end tag for the sender's original address.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	OriginalAddressEndTag
Default value	(Space)
Type	Original Address End Tag

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

Kiwi Syslog solves this problem by placing a tag in the message text that contains the original sender's 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 "Forward to another host" action.

The two registry keys above allow you to override the default start and end tags with custom start and end tag values.

For example, when `nnn.nnn.nnn.nnn` is the originating IP address, the default originating address tags yield the following:

```
Original Address=nnn.nnn.nnn.nnn
```

If you change the start tag to `<ORIGIN>` and the end tag to `</ORIGIN>`, the result is:

```
<ORIGIN>nnn.nnn.nnn.nnn</ORIGIN>
```

MaxRuleCount

Use this [Kiwi Syslog Server registry setting](#) to specify the maximum number of rules allowed in Kiwi Syslog Server.

i Exceeding the maximum rule count of 100 is not recommended. Setting this value too high can adversely affect performance and increase memory consumption dramatically. SolarWinds recommends investigating alternative methods if you are approaching the rule count limit of 100. Using the autosplit feature of file logging is one potential solution.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Options
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Options
Value (STRING)	MaxRuleCount
Min value	10
Max value	999
Default value	100
Type	Maximum number of rules

DBLoggerCacheClearRate

Use this [Kiwi Syslog Server registry setting](#) to specify the rate (in milliseconds) at which the Database Cache is checked for SQL data to be executed.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties

Value (STRING)	DBLoggerCacheClearRate
Min value	10
Max value	1000
Default value	1000 (ms)
Type	Milliseconds

DBLoggerCacheTimeout

Use this [Kiwi Syslog Server registry setting](#) to specify the maximum age (in days) of an unchanged cache file. Any database cache file that is older than this will be deleted by the system.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DBLoggerCacheTimeout
Min value	1
Max value	30
Default value	3
Type	Number (days)

DBLoggerCacheDisable

Use this [Kiwi Syslog Server registry setting](#) to override the default database caching behavior.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Properties
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Properties
Value (STRING)	DBLoggerCacheDisable
Min value	0
Max value	1
Default value	0 (Enabled)

Type	Enabled or disabled
-------------	---------------------

HostNosToDisplay

Use this [Kiwi Syslog Server registry setting](#) to specify the number of hosts to display in the statistics report.

Section (32-bit Windows OS)	HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds\Syslogd\Options
Section (64-bit Windows OS)	HKEY_LOCAL_MACHINE\Software\WOW6432Node\SolarWinds\Syslogd\Options
Value (STRING)	HostNosToDisplay
Min value	25
Max value	999
Default value	No default value. If required, you must manually add this setting.
Type	Number

Command line arguments

The following command line parameters can be used when starting the syslog executable, `Syslogd.exe`, `Syslogd_Manager.exe`, or `Syslogd_Service.exe`. Parameters are not case sensitive. If you specify more than one parameter at a time, separate the values with a space.

Start-up Debug

This command creates a debug file that contains the results from the program start-up and socket initialization routines. The debug file is created in the installation directory, and the file name is based on the program file it was used with (as described below).

This debug file can help you troubleshoot the following issues:

- if the program does not appear to be receiving messages on the port specified by the [Inputs](#) setup option, check the start-up debug file to ensure that the sockets initialized correctly.
- If the program appears to crash on start-up, this option can help locate the problem.

i If you are running Kiwi Syslog Server as a service, the service can't be provided with a command line argument. Use the [DebugStart](#) registry entry to create this file.

Command line value	DEBUGSTART	
Applies to	Syslogd.exe, Syslogd_Service.exe, and Syslogd_Manager.exe	
Files created	When run with:	The file name is:
	Syslogd.exe	Syslogd_Startup.txt
	Syslogd_Service.exe	Syslogd_Service_Startup.txt
	Syslogd_Manager.exe	Syslogd_Manager_Startup.txt

Service - Install Service

This command attempts to install the Syslog Server as a service. A status message indicates whether the installation was successful.

Use this command if:

- Installing the service from the Manage menu of the Syslog Server Service Manager failed.
- You need to run the command from a batch file to automate the installation.

Command line value	-INSTALL
---------------------------	----------

Applies to	Syslogd_Service.exe
Silent option	Follow this command line value with <code>-silent</code> to prevent the status message from being displayed: <code>-install -silent</code>

Service - Uninstall Service

This command attempts to uninstall the Syslog Server as a service. A status message indicates whether the installation was successful.

Use this command if:

- Uninstalling the service from the Manage menu of the Syslog Server Service Manager failed.
- You need to run the command from a batch file to automate the process.

Be sure to stop the service before you uninstall it. To stop it from a command line, use the `net stop` command. For example:

```
net stop "Kiwi Syslog Server"
```

Command line value	-UNINSTALL
Applies to	Syslogd_Service.exe
Silent option	Follow this command line value with <code>-silent</code> to prevent the status message from being displayed: <code>-uninstall -silent</code>