Manual:System/Log

From MikroTik Wiki
< Manual:System

Contents

Applies to
RouterOS: v3, v4 +

Summary

RouterOS is capable of logging various system events and status information. Logs can be saved in routers memory (RAM), disk, file, sent by email or even sent to remote syslog server (RFC 3164).

Log messages

Sub-menu level: `/log`

All messages stored in routers local memory can be printed from `/log` menu. Each entry contains time and date when event occurred, topics that this message belongs to and message itself.

```
[admin@ZalaisKapots] /log> print
jan/02/1970 02:00:09 system,info router rebooted
sep/15 09:54:33 system,info,account user admin logged in from 10.1.101.212 via winbox
sep/15 12:33:18 system,info item added by admin
sep/15 12:34:26 system,info mangle rule added by admin
sep/15 12:34:29 system,info mangle rule moved by admin
sep/15 12:35:34 system,info mangle rule changed by admin
sep/15 12:42:14 system,info,account user admin logged in from 10.1.101.212 via telnet
sep/15 12:42:55 system,info,account user admin logged out from 10.1.101.212 via telnet
01:01:58 firewall,info input: in:ether1 out:(none), src-mac 00:21:29:6d:82:07, proto UDP,
                         10.1.101.1:520->10.1.101.255:520, len 452
```

If logs are printed at the same date when log entry was added, then only time will be shown. In example above you can see that second message was added on sep/15 current year (year is not added) and the last message was

added today so only the time is displayed.

Note: print command accepts several parameters that allows to detect new log entries, print only necessary messages and so on. For more information about parameters refer to scripting manual

For example following command will print all log messages where one of the topics is info and will detect new log entries until Ctrl+C is pressed

```
[admin@ZalaisKapots] /log > print follow where topics~".info"
12:52:24 script,info hello from script
-- Ctrl-C to quit.
```

If print is in follow mode you can hit 'space' on keyboard to insert separator:

```
[admin@ZalaisKapots] /log > print follow where topics~".info"
12:52:24 script,info hello from script

 = = =   = = =   = = =     = = =   = = =   = = =     = = =   = = =   = = =

-- Ctrl-C to quit.
```

Logging configuration

Sub-menu level: `/system logging`

Property	Description
`action` (*name*; Default: **memory**)	specifies one of the system default actions or user specified action listed in actions menu
`prefix` (*string*;	prefix added at the beginning of log

Default:)	messages
topics *(account, bfd, caps, ddns, dns, error, gsm, info, iscsi, l2tp, manager, ntp, packet, pppoe, radvd, rip, script, smb, sstp, system, timer, vrrp, web-proxy, async, bgp, certificate,*	log all messages that falls into specified topic or list of topics. '**!**' character can be used before topic to exclude messages falling under this topic. For example, we want to log NTP debug info without too much details: `/system logging add topics=ntp,debug,!packet`

debug, dude, event, hotspot, interface, isdn, ldp, mme, ospf, pim, pptp, raw, route, sertcp, snmp, state, telephony, upnp, warning, wireless, backup, calc, critical, dhcp, e-mail,	

firewall, igmp-proxy, ipsec, kvm, lte, mpls, ovpn, ppp, radius, read, rsvp, simulator, ssh, store, tftp, ups, watchdog, write; Default: **info**)	

Actions

Sub-menu level: `/system logging action`

Property	Description
`bsd-syslog` (*yes*/*no*;	whether to use

Default:)	bsd-syslog as defined in RFC 3164
`disk-file-count` (*integer [1..65535]*; Default: **2**)	specifies number of files used to store log messages, applicable only if action=disk
`disk-file-name` (*string*; Default: **log**)	name of the file used to store log messages, applicable only if action=disk
`disk-lines-per-file` (*integer [1..65535]*; Default: **100**)	specifies maximum size of file in lines, applicable only if action=disk
`disk-stop-on-full`	whether to stop

(*yes*/*no*; Default: **no**)	to save log messages to disk after the specified disk-lines-per-file and disk-file-count number is reached, applicable only if action=disk
`email-to` (*string*; Default:)	email address where logs are sent, applicable only if action=email
`memory-lines` (*integer [1..65535]*; Default: **100**)	number of records in local memory buffer, applicable only if

	action=memory
`memory-stop-on-full` (*yes*/*no*; Default: **no**)	whether to stop to save log messages in local buffer after the specified memory-lines number is reached
`name` (*string*; Default:)	name of an action
`remember` (*yes*/*no*; Default:)	whether to keep log messages, which have not yet been displayed in console, applicable if action=echo
`remote` (*IP/IPv6*	remote logging

Address[:Port]; Default: **0.0.0.0:514**)	server's IP/IPv6 address and UDP port, applicable if action=remote
`src-address` (*IP address*; Default: **0.0.0.0**)	source address used when sending packets to remote server
`syslog-facility` (*auth, authpriv, cron, daemon, ftp, kern, local0, local1, local2, local3, local4, local5, local6, local7, lpr, mail, news, ntp, syslog, user, uucp*; Default: **daemon**)	
`syslog-severity` (*alert, auto, critical,*	Severity level indicator defined in RFC 3164: ▪ Emergency: system is unusable ▪ Alert: action must be taken immediately

debug, emergency, error, info, notice, warning; Default: **auto**)	• Critical: critical conditions • Error: error conditions • Warning: warning conditions • Notice: normal but significant condition • Informational: informational messages • Debug: debug-level messages
`target` (*disk, echo, email, memory, remote*; Default: **memory**)	storage facility or target of log messages • disk - logs are saved to the hard drive more>> • echo - logs are displayed on the console screen • email - logs are sent by email • memory - logs are stored in local memory buffer • remote - logs are sent to remote host

Note: default actions can not be deleted or renamed.

Topics

Each log entry have topic which describes the origin of log message. There can be more than one topic assigned to log message. For example, OSPF debug logs have four different topics: route, ospf, debug and raw.

```
11:11:43 route,ospf,debug SEND: Hello Packet 10.255.255.1 -> 224.0.0.5 on lo0
11:11:43 route,ospf,debug,raw PACKET:
11:11:43 route,ospf,debug,raw     02 01 00 2C 0A FF FF 03 00 00 00 00 E7 9B 00 00
11:11:43 route,ospf,debug,raw     00 00 00 00 00 00 00 00 FF FF FF FF 00 0A 02 01
11:11:43 route,ospf,debug,raw     00 00 00 28 0A FF FF 01 00 00 00 00
```

List of Facility independent topics

Topic	Description
`critical`	Log entries marked as critical, these log

	entries are printed to console each time you log in.
`debug`	Debug log entries
`error`	Error messages
`info`	Informative log entry
`packet`	Log entry that shows contents from received/sent packet
`raw`	Log entry that shows raw contents of received/sent packet
`warning`	Warning message.

Topics used by various RouterOS facilities

Topic	Description
`account`	Log messages generated by accounting facility.
`async`	Log messages generated by asynchronous devices

`backup`	Log messages generated by backup creation facility.
`bfd`	Log messages generated by Manual:Routing/BFD protocol
`bgp`	Log messages generated by Manual:Routing/BGP protocol
`calc`	Routing calculation log messages.
`caps`	CAPsMAN wireless device management
`certificate`	Security certificate
`dns`	Name server lookup related information
`ddns`	Log messages generated by Manual:Tools/Dynamic

	DNS tool
`dude`	Messages related to the Dude server package Manual:The_Dude tool
`dhcp`	DHCP client, server and relay log messages
`e-mail`	Messages generated by Manual:Tools/email tool.
`event`	Log message generated at routing event. For example, new route have been installed in routing table.
`firewall`	Firewall log messages generated when **action=log** is set in firewall rule
`gsm`	Log messages generated by GSM devices

`hotspot`	Hotspot related log entries
`igmp-proxy`	IGMP Proxy related log entries
`ipsec`	IPSec log entries
`iscsi`	
`isdn`	
`interface`	
`kvm`	Messages related to the KVM virtual machine functionality
`l2tp`	Log entries generated by Manual:Interface/L2TP client and server
`lte`	Messasges related to the LTE/4G modem configuration
`ldp`	Manual:MPLS/LDP protocol related

	messages
`manager`	Manual:User_Manager log messages.
`mme`	MME routing protocol messages
`mpls`	MPLS messages
`ntp`	sNTP client generated log entries
`ospf`	Manual:Routing/OSPF routing protocol messages
`ovpn`	OpenVPN tunnel messages
`pim`	Multicast PIM-SM related messages
`ppp`	ppp facility messages
`pppoe`	PPPoE server/client related messages
`pptp`	

	PPTP server/client related messages
`radius`	Log entries generated by RADIUS Client
`radvd`	IPv6 radv deamon log messages.
`read`	SMS tool messages
`rip`	RIP routing protocol messages
`route`	Routing facility log entries
`rsvp`	Resource Reservation Protocol generated messages.
`script`	Log entries generated from scripts
`sertcp`	Log messages related to facility responsible for "/ports remote-access"

`simulator`	
`state`	DHCP Client and routing state messages.
`store`	Log entries generated by Store facility
`smb`	Messages related to the SMB file sharing system
`snmp`	Messages related to Simple network management protocol (SNMP) configuration
`system`	Generic system messages
`telephony`	*Obsolete! Previously used by the IP telephony package*
`tftp`	TFTP server generated messages
`timer`	Log messages that are related to timers used in RouterOS. For example bgp keepalive logs `12:41:40 route,bgp,debug,timer KeepaliveTimer expired`

	`12:41:40 route,bgp,debug,timer RemoteAddress=2001:470:1f09:131::`
`ups`	Messages generated by UPS monitoring tool
`vrrp`	Messages generated VRRP
`watchdog`	Watchdog generated log entries
`web-proxy`	Log messages generated by web proxy
`wireless`	M:Interface/Wireless log entries.
`write`	SMS tool messages.

Logging to file

To log everything to file, add new log action:

```
/system logging action add name=file target=disk disk-file-name=log
```

and then make everything log using this new action:

```
/system logging add action=file
```

You can log only errors there by issuing command:

```
/system logging add topics=error action=file
```

This will log into files **log.0.txt** and **log.1.txt**.

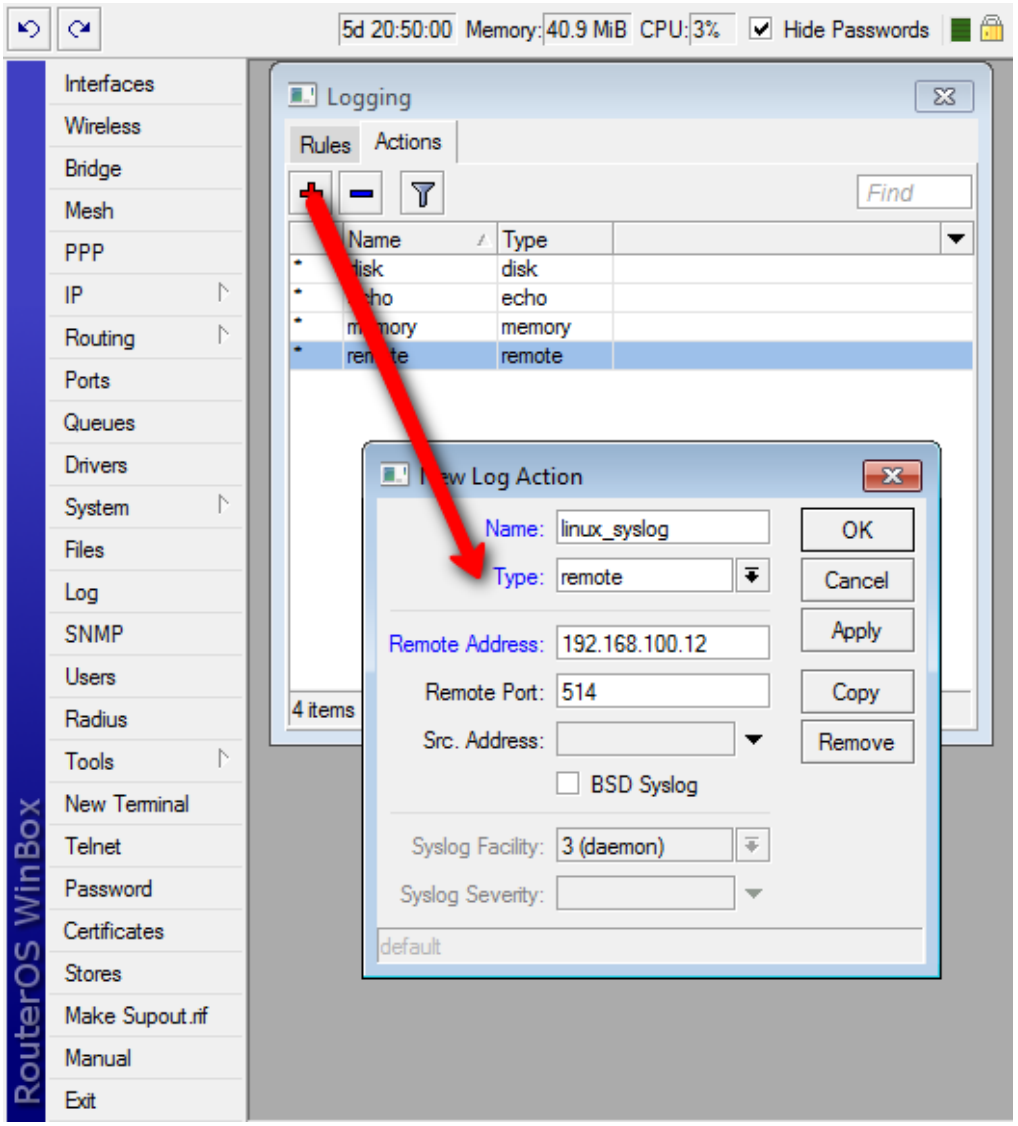
You can specify maximum size of file in lines by specifying *disk-lines-per-file*. **<file>.0.txt** is active file were new logs are going to be appended and once it size will reach maximum it will become **<file>.1.txt**, and new empty **<file>.0.txt** will be created.

You can log into USB flashes or into *MicroSD/CF* (on Routerboards) by specifying it's directory name before file name. For example, if you have accessible usb flash as **usb1** directory under */files*, you should issue following command:

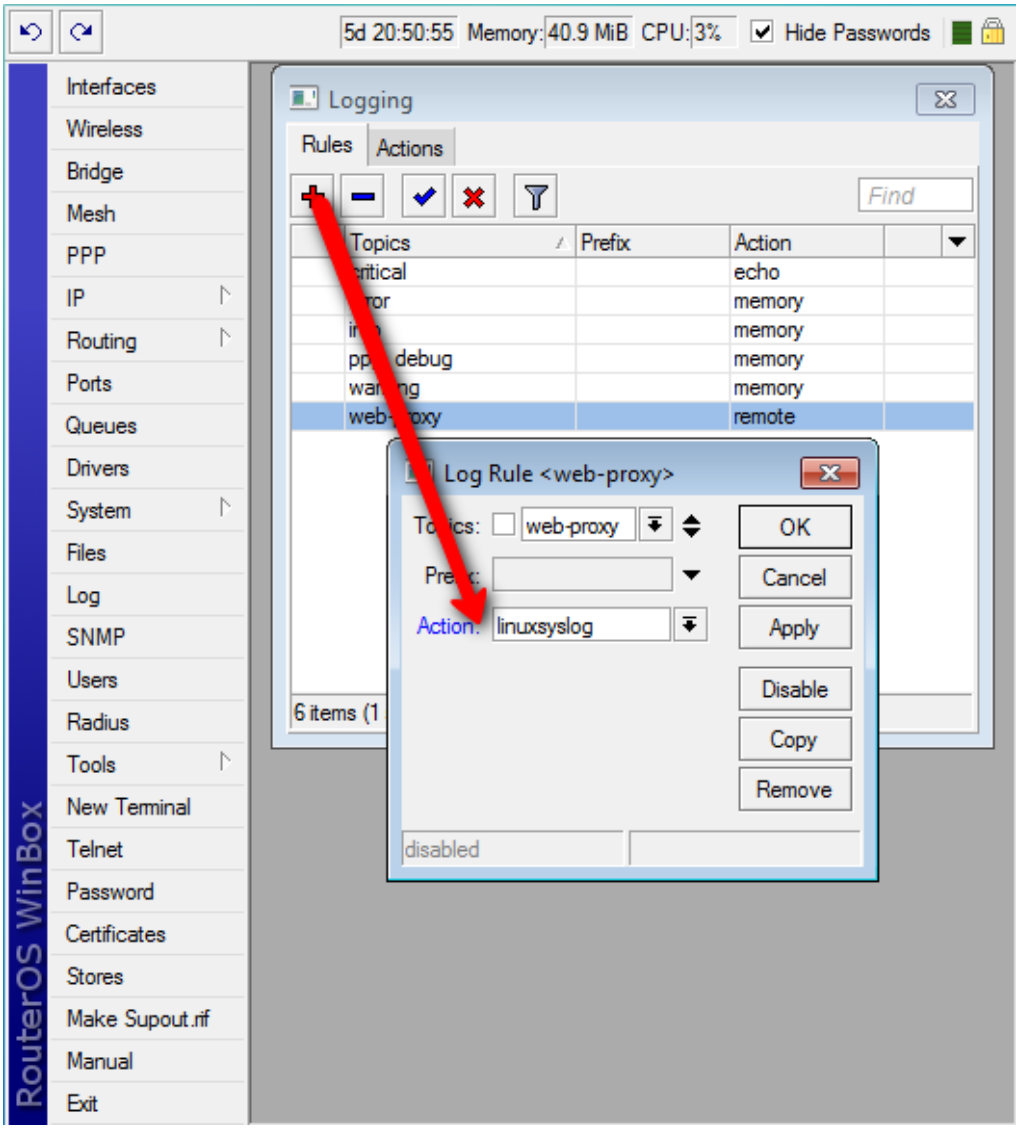
```
/system logging action add name=usb target=disk disk-file-name=usb1/log
```

Example:Webproxy logging

These two screenshots will show you how to configure the RouterOS logging facility to send Webrpoxy logs to a remote syslog server, in this example, located at 192.168.100.12. The syslog server can be any software that supports receiving syslogs, for example Kiwi syslog.

- 

Add a new logging action, with "remote" and the IP of the remote server. Call it whatever you like



Then add a new logging rule with the topic "webproxy" and then newly created action. Note that you must have webproxy running on this router already, for this to work. To test, you can temporary change the action to "memory" and see the "log" window if the webproxy visited websites are logged. If it works, change it back to your new remote action

Note: it's a good idea to add another topic in the same rule: ***!debug****. This would be to ensure you don't get any debug stuff, only the visited sites.*

- This page was last edited on 20 June 2017, at 08:43.