RUT230 Events Log

 $\underline{\text{Main Page}} > \underline{\text{FOL Products}} > \underline{\text{RUT230}} > \underline{\text{RUT230 Manual}} > \underline{\text{RUT230 WebUI}} > \underline{\text{RUT230 Status section}} > \underline{\text{RUT230 Events}}$ Log

The information in this page is updated in accordance with the RUT2XX_R_00.01.14.1 firmware version.

Contents

- 1 Summary
- 2 All Events
- 3 System Events
- 4 Network Events
- <u>5 Events Reporting</u>
 - 5.1 Events Reporting Configuration
 - 5.1.1 Send SMS
 - 5.1.2 Send Email
 - 5.1.3 Event Types and Sub-types
 - 5.1.3.1 Config change
 - 5.1.3.2 New DHCP client
 - <u>5.1.3.3 Mobile Data</u>
 - <u>5.1.3.4 SMS</u>
 - 5.1.3.5 Signal Strength
 - <u>5.1.3.6 Reboot</u>
 - <u>5.1.3.7 SSH</u>
 - <u>5.1.3.8 WebUI</u>
 - 5.1.3.9 New WiFi client
 - 5.1.3.10 LAN Port State
 - <u>5.1.3.11 WAN Failover</u>
- 6 Reporting Configuration
 - 6.1 Events Log Report Configuration
 - <u>6.1.1 FTP</u>
 - 6.1.2 Email

Summary

In the **Events Log** window you can view records of events such as logins, reboots, resets, connections, configuration changes and more.

All Events

In this section you can view all occurred events.



System Events

In this section you can view all system events at once or filter it by choosing a type of events you want to see.



Network Events

In this section you can view all network events at once or filter it by choosing a type of events you want to see.



Events Reporting

The **Events Reporting** section gives you the ability to configure rules that will inform you via SMS or email when certain events occur on your router. These events can be almost anything – configuration changes, reboots, new connections, various status updates, etc.



Events Reporting Configuration

Events Reporting Configuration is used to create and customize Events Reporting Rules. Here you can specify any event type and subtype, chose whether you want to be informed by an SMS message or email, modify what kind of information you want receive should an event occur. To open this window, choose an Event type, Event subtype and Action and click the **Add** button. A new rule should appear in the Events Reporting Rules tab. Click the **Edit** button located next to that rule after which you will be redirected to that rule's configuration window.

Send SMS



FIELD NAME	VALUE	DESCRIPTION
Enable	yes no; Default: no	Toggles the rule ON or OFF
Event type	Config change New DHCP client Reboot SSH WebUI New WiFi client LAN port state WAN Failover Mobile data SMS Signal Strength; Default: Config change	The type of event that you wish to receive information about
Event subtype	Sample: After unexpected shut down	Specified event's sub-type. This field changes in accordance with Event type
Action	Send SMS Send email; Default: Send SMS	Action that is to be taken after the specified event occurs
Enable delivery retry	yes no; Default: yes	Toggles delivery retry On or OFF. If for some reason the message delivery is unsuccessful, the router initiates a retry if this field is enabled

Retry interval	1 min. 5 min. 10 min. 15 min. 30 min. 60 min.; Default 5 min.	Specifies when the router should try re-sending the message in case the first attempt was a failure
Retry count	2 3 4 5 6 7 8 9 10; Default: 2	Specifies the maximum number of failed attempts after which the router does not try to send the message anymore $$
Message text on Event	string; Default: Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;	Specifies the text that the message will contain
Get status after reboot	yes no; Default: no	Specifies whether the router should send an SMS message indicating the router's status after the reboot in addition to the original message
Status message after reboot	string; Default: Router name - %rn; WAN IP - %wi; Data Connection state - %cs; Connection type - %ct; Signal strength - %ss; New FW available - %fs;	Specifies the text that the status message will contain. This field becomes visible only if Get status after reboot is checked
Recipients	Single number User group; Default: Single number	Specifies the intended recipients. A guide on how to create a User group can be found in the SMS Utilities chapter, <u>User Groups</u> section
Recipient's phone number	phone number; Default: none	The intended recipient's phone number. To add more than one number, click the green plus symbol located to the right of this field. The phone number must be entered in the international format, but without dash symbols or spaces, e.g., +37061234567

Send Email



FIELD NAME	VALUE	DESCRIPTION
Enable	yes no; Default: no	Toggles the rule ON or OFF
Event type	Config change New DHCP client Reboot SSH WebUI New WiFi client LAN port state WAN Failover Mobile data SMS Signal Strength; Default: Config change	The type of event that you wish to receive information about
Event subtype	Sample: After unexpected shut down	Specified event's sub-type. This field changes in accordance with Event type
Action	Send SMS Send email; Default: Send SMS	Action that is to be taken after the specified event occurs
Enable delivery retry	yes no; Default: yes	Toggles delivery retry On or OFF. If for some reason the message delivery is unsuccessful, the router initiates a retry if this field is enabled
Retry interval	1 min. 5 min. 10 min. 15 min. 30 min. 60 min.; Default 5 min.	Specifies when the router should try re-sending the message in case the first attempt was a failure $$
Retry count	2 3 4 5 6 7 8 9 10; Default: 2	Specifies the maximum number of failed attempts after which the router does not try to send the message anymore ${\sf max}$
Subject	string; Default: none ; Character limit: 26	Specifies the subject of the email message
Message text on Event	string; Default: Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;	Specifies the text that the message will contain
Get status after reboot	yes no; Default: no	Specifies whether the router should send an SMS message indicating the router's status after the reboot in addition to the original message. If this is checked you will be prompted to enter the text that the status message should contain
SMTP server	ip host; Default: none	Sender's email service provider's SMTP server. If you don't know the SMTP server's address, you can easily look it up online since it is public information $\frac{1}{2}$
SMTP port	integer [065535]; Default: none	Sender's email service provider's SMTP port. If you don't know the SMTP server's port, you can easily look it up online since it is public information
Secure connection	yes no; Default: no	Toggles secure connection feature ON or OFF (use only if the email service provider's server supports SSL or TLS)
Username	string; Default: none	Sender's email account's login user name
Password	string; Default: none	Sender's email account's login password
Sender's email address	email; Default: none	The email address of the sender, i.e., the report message will be sent from this email. Make sure this is the same email that you provided login information to
Recipient's email address	email; Default: none	The intended recipient's email address. To add more than one email address, click the green \square plus symbol located to the right of this field
Send test mail	-	Sends a test mail using the information that you provided. Once you click this button, the router will login to the provided email account and send the specified message to the specified address(-es). You should always send a test mail before finishing the configuration to make sure that everything is in order

Event Types and Sub-types

The examples provided above are both concerning the **Reboot** Event type and **After unexpected shut down** sub-type. This section is an overview of all other Event type and sub-types.

Config change

OpenVPN Sends a report message when any OpenVPN configuration changes are applied. For example, whenever a new OpenVPN instance is created, a OpenVPN instance or and to hadde Reput on OpenVPN instance or open of the Sends or open or message when any SMS related configuration changes are applied. For example, whenever a new SMS Utilities rule is created changed. Mailtivan Sends a report message when may Mailtivan Sends a report message when any configuration changes to Periodic Reboot are applied. For example, whenever a new CRE Tunnel are enabled dissibility of the Sends a report message when any configuration changes to Periodic Reboot are applied. For example, whenever a new GRE Tunnel are applied Sends a report message when any configuration changes to Sends Report message when any configuration changes to Sends Report message when any configuration changes to Sends a report message when any configuration changes to Sends are applied. For example, whenever Ping Behoot gets enabled/dissibility for the sends a report message when any configuration changes to Sends are applied. For example, whenever Notice gets to have	ENEBT SUB-TYPE	DESCRIPTION
Syst Sends a report message when any SNS Trailer Loging is enabled-disabled, an OpenVTM instance get any pathod. For example, whenever a new SMS Littlities rule is created changed, changed are prott message when any SMS Trailer Loging is enabled-disabled or loging interval is changed. Multivan Sends a report message when achanges to WAN Backup configuration are applied. For example, whenever a switch from using Wired as main in to backup WAN occurs, Wireless is added as a Backup WAN, bellath monitor configurations are changed. Multivan Sends a report message when any RUT230, Mobile configuration changes are applied. For example, whenever a switch from using Wired as main in the backup WAN occurs, Wireless is added as a Backup WAN, bellath monitor configurations are changed. Sends a report message when any RUT230, Mobile configuration changes are applied. For example, whenever Service mode, APN, Connection type is changed, etc. Sends a report message when any configuration changes are applied. For example, whenever a new Events Reporting that created changed, decleded, and so in Ministry, data limit predict is changed, etc. Fernal Sends a report message when any configuration changes to Events. Reporting are applied. For example, whenever a new Events Reporting Rule created changed, decleded, and the All Sends are applied. For example, whenever a new GRE Tunnel instance is created, decleded, enabled/disabled, PERONE Rebot are applied. For example, whenever Ping Rehoot created, decleded, enabled/disabled, PERONE Rebot predicts and predicts. Pling reboot Sends a report message when any configuration changes to Rise Rebot are applied. For example, whenever Ping Rehoot pets enabled/disabled, PERONE Rebot predicts and predicts. Pring reboot Sends a report message when any configuration changes to Rise Rebot are applied. For example, whenever Whitelist is changed to bright be a logical products of the predicts of the predicts of the male disabled, PERONE Rebot products of the predicts of the predicts of the pre	All	Sends a report message when any type of configuration changes are applied
Mobile traffic Sends a ropott message when Analyse Tiffic Lograpi is enabled/disabled or logging interval is changed. Multiwan Sends a ropott message when analyse to WAN Backup configuration are applied. For example, whenever a switch from using Wired as man Y to backup WAN occurs, Wireless is dided on a Backup WAN. Health monitor configurations are changed. Mobile Sends a ropott message when any BUT239, Mobile configuration changes are applied. For example, whenever Service mode, APN, Connection type is changed, etc. Data limit Sends a ropott message when any Mobile bata Limit configuration changes are applied. For example, whenever new data limit is configured, data limit gest disabled-denabled on SINILAW. data limit period is changed, etc. Feents reporting Sends a ropott message when any configuration changes to Pental Reporting are applied. For example, whenever a new Events Reporting Rule created. Changed, delender, etc. Feriodic reboot Sends a ropott message when any configuration changes to Pental Reporting are applied. For example, whenever a new GRE Tunnel instance is created. Geleted, embled-disabled, Forcide Reboot are applied. For example, whenever a new GRE Tunnel instance is created. Geleted, embled-disabled, Forcide Reboot are applied. For example, whenever a new GRE Tunnel instance is created. Geleted, embled-disabled, Forcide Reboot are applied. For example, whenever a new GRE Tunnel instance is created. Geleted, embled-disabled, Forcide Reboot are applied. For example, whenever Ping Reboot pets enabled/disabled for them and Pis changed det. Auto update Sends a ropott message when any configuration changes to Alto update are applied. For example, whenever Ping Reboot pets enabled/disabled for but ping has changed det. PPTP Sends a ropott message when any configuration changes to Eliza Belecking are applied. For example, whenever Whitelist is changed to blackits vice versa, a new ontry is added to Blackits/Whitelist, etc. PPTP Sends a ropott message when any configuration change	OpenVPN	Sends a report message when any OpenVPN configuration changes are applied. For example, whenever a new OpenVPN instance is created, an OpenVPN instance gets disabled/enabled, an OpenVPN instance's protocol is changed from UDP to TCP or vice versa, etc.
Sends a report message when early configuration changes to WAN Backup configuration are applied. For example, whenever a switch from using Wired as main V beckup WAN Course. Writeds as added as a Backup WAN, Beath monitor configuration configuration configuration changes are applied. For example, whenever Service mode, APN, Connection type is changed, etc. Data limit Sends a report message when any Wahlie Data Limit configuration changes are applied. For example, whenever new data limit is configured, and interest of the stanges. The control of the stanges of the control of the cont	SMS	Sends a report message when any SMS related configuration changes are applied. For example, whenever a new <u>SMS Utilities</u> rule is created or changed, changes are made to <u>Auto Reply</u> or <u>Remote configurations</u> , etc.
to backup WAN occurs, Wireless is added as a Backup WAN, fiealth monitor configurations are changed, etc. Mobile Sends a report message when any RUT230, Mobile Configuration changes are applied. For example, whenever service mode, APN, Connection type is changed, etc. Periodic reboat Sends a report message when any Mobile Data Limit configuration changes are applied. For example, whenever new data limit is configured, data limit period is changed, etc. Feents reporting Sends a report message when any configuration changes to Periodic Reboot are applied. For example, whenever a new Events Reporting Rule created, changed, deleted, etc. Periodic reboot Sends a report message when any configuration changes to Periodic Reboot are applied. For example, whenever Periodic Reboot gets enabled/disabled, Periodic Reboot interval is changed, etc. GRE Tunnel Sends a report message when any configuration changes to Reporting are applied. For example, whenever a new GRE Tunnel instance is created, deleted, enabled/disabled, Local tunnel IP is changed, etc. Piling reboot Sends a report message when any configuration changes to Ring Reboot are applied. For example, whenever Ping Reboot gets enabled/disabled, best to ping lass changed, etc. Piling reboot Sends a report message when any configuration changes to Ring Reboot are applied. For example, whenever Ping Reboot gets enabled/disabled, best to ping lass changed, etc. PPTP Sends a report message when any configuration changes to Site Blocking are applied. For example, whenever Whitelist is changed to Blacking Vincery and the print of the	Mobile traffic	Sends a report message when Mobile Traffic Logging is enabled/disabled or logging interval is changed.
Data limit Sends a report message when any Mobile Data Limit configuration changes are applied. For example, whenever new data limit is configured, data limit gest disabled/enabled on SIMI/SIMA, data limit period is changed, etc. Events reporting Sends a report message when any configuration changes to Events Reporting are applied. For example, whenever a new Events Reporting Rule created, changed, deleted, etc. Sends a report message when any configuration changes to Periodic Reboot are applied. For example, whenever a new Events Reporting Rule created, deleted, enabled/disabled, Local tunned IP is changed, etc. GRE Tunnel Sends a report message when any configuration changes to SIRE Tunnel are applied. For example, whenever a new GRE Tunnel instance is created, deleted, enabled/disabled, Local tunnel IP is changed, etc. Fing reboot Sends a report message when any configuration changes to SIRE Blackling are applied. For example, whenever Ping Reboot gets enabled/disabled host to ping has changed, etc. Sends a report message when any configuration changes to Site Blackling are applied. For example, whenever Ping Reboot gets enabled/disabled vice versa, a new entry is added to Blacklist Withelist, etc. PPTP Sends a report message when any configuration changes to PIng Reboot are applied. For example, whenever a new PPTP instance was created, delete enabled/disabled, PPTP server address was changed, etc. Hotspot Sends a report message when any configuration changes to Instance are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Content blocker Content blocker Sends a report message when any configuration changes to Instance are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Praxy Based Content Blocker are applied. For example, whenever new DDNS ins	Multiwan	Sends a report message when changes to WAN <u>Backup</u> configuration are applied. For example, whenever a switch from using Wired as main WAN to backup WAN occurs, Wireless is added as a Backup WAN, Health monitor configurations are changed, etc.
data limit giest disabled(enabled on SIM1/SIM2, data limit period is changed, etc. Rends a report message when any configuration changes to Events Reporting are applied. For example, whenever a new Events Reporting Rule created, changed, deleted, etc. Rends a report message when any configuration changes to Periodic Reboot are applied. For example, whenever Periodic Reboot gets enabled/disabled, Periodic Reboot interval is changed, etc. GRE Tunnel Sends a report message when any configuration changes to Periodic Reboot are applied. For example, whenever a new GRE Tunnel instance is created, deleted, enabled/disabled, Local tunnel IP is changed, etc. Ping reboot Sends a report message when any configuration changes to Ping Reboot are applied. For example, whenever Ping Reboot gets enabled/disabled hot to ping his changed, etc. Sends a report message when any configuration changes to Site Blocking are applied. For example, whenever Whitelist is changed to Blacklist Whitelist, etc. PPTP Sends a report message when any configuration changes to Site Blocking are applied. For example, whenever Whitelist is changed to Blacklist Whitelist, etc. PPTP Sends a report message when any configuration changes to Site Blocking are applied. For example, whenever his publication and the send of the s	Mobile	Sends a report message when any <u>RUT230_Mobile</u> configuration changes are applied. For example, whenever Service mode, APN, Connection type is changed, etc.
created, changed, deleted, etc. Periodic reboot Sends a report message when any configuration changes to Periodic Reboot are applied. For example, whenever Periodic Reboot gets enabled/disabled, Periodic Reboot interval is changed, etc. GRE Tunnel Sends a report message when any configuration changes to GRE Tunnel are applied. For example, whenever a new GRE Tunnel instance is created, deleted, enabled/disabled, Local tunnel IP is changed, etc. Ping reboot Sends a report message when any configuration changes to Ping Reboot are applied. For example, whenever Ping Reboot gets enabled/disabled, Local tunnel IP is changed, etc. Auto update Sends a report message when any configuration changes to Ping Reboot are applied. For example, whenever Ping Reboot gets enabled/disabled, solvice versa, a new entry is added to Blacklist/Whitelist, etc. PPTP Sends a report message when any configuration changes to Ping are applied. For example, whenever histelist is changed to Blacklist whitelist, etc. PPTP Sends a report message when any configuration changes to Ping are applied. For example, whenever a new PPTP instance was created, delete enabled/disabled, PTTP server address was changed, etc. Hotspot Sends a report message when any configuration changes to Insput/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, on output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Insput/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, on output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Proxy Based Content Blocker are applied. For example, whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist/Whitelist, etc. Login page Sends a report message when any configuration changes to Droxy Based Content Blocker are applied. For example, whenever a new DDNS instance is create	Data limit	
enable/dusabled, Periodic Reboot interval is changed, etc. Firm and Sends a report message when any configuration changes to GRE Tunnel are applied. For example, whenever a new GRE Tunnel instance is created, deleted, enabled/disabled, Local tunnel P is changed, etc. Ping reboot Sends a report message when any configuration changes to Ping Reboot are applied. For example, whenever Ping Reboot gets enabled/disabled host to ping has changed, etc. Stet blocking Sends a report message when any configuration changes to Nuto update are applied. For example, whenever Whitelist is changed to Blacklist Whitelist, etc. PPTP Sends a report message when any configuration changes to PPTP are applied. For example, whenever Mittelist is changed to Blacklist Whitelist, etc. PPTP Sends a report message when any configuration changes to PPTP are applied. For example, whenever a new PPTP instance was created, delete enable/disabled, PPTP server address was changed, etc. Hotspot Sends a report message when any configuration changes to Diaput/Output are applied. For example, whenever Hotspot SSID was changed, Bedius server was changed, Hotspot was enabled/disabled, etc. Input/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ONOFF, etc. Content blocker Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ONOFF, etc. Login page Sends a report message when any Language Settlings are changed Profile Sends a report message when any Language Settlings are changed Profile Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created, changed, deleted, and the profile is added to addicable with the profile is added to addicable. For example, whenever new DDNS instance is created changed, deleted or edited Profile Sends a report message when any	Events reporting	Sends a report message when any configuration changes to Events Reporting are applied. For example, whenever a new Events Reporting Rule is created, changed, deleted, etc.
Pring reboot Sends a report message when any configuration changes to Pring Reboot are applied. For example, whenever Pring Reboot gets enabled/disable host to pring has changed, etc. Auto update Sends a report message when any configuration changes to Site Blocking are applied. For example, whenever Whitelist is changed to Blacklist vice versa, a new entry is added to Blacklist/Whitelist, etc. PPTP Sends a report message when any configuration changes to PPTP are applied. For example, whenever a new PPTP instance was created, delete enabled/disabled, PPTP server address was changed, etc. Hotspot Sends a report message when any configuration changes to BPTP are applied. For example, whenever new PPTP instance was created, delete enabled/disabled, PPTP server address was changed, etc. Hotspot Sends a report message when any configuration changes to Hotspot are applied. For example, whenever Hotspot SSID was changed, Radius server was changed, Bettopt was enabled/disabled, etc. Input/Output Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Perriodic Output Contre Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Proxy Based Content Blocker are applied. For example, whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist/Whitelist, etc. Login page Sends a report message when any Language Settings are changed Language Sends a report message when any endiguration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited DDNS Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever new DDNS instance is created changed, deleted, changed are made to SSH or WebUIA	Periodic reboot	
host to ping has changed, etc. Sends a report message when any configuration changes to Auto update are applied. For example, whenever Whitelist is changed to Blacklist Vice versa, a new entry is added to Blacklist Whitelist, etc. PPTP Sends a report message when any configuration changes to PPTP are applied. For example, whenever a new PPTP instance was created, delete enabled/disabled, PPTP server address was changed, etc. Bonds a report message when any configuration changes to BPTP are applied. For example, whenever a new PPTP instance was created, delete enabled/disabled, etc. Input/Output Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, and upto was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Proxy Based Content Blocker are applied. For example, whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist orWhitelist, etc. Login page Sends a report message when any Language Settings are changed Language Sends a report message when any Language Settings are changed Profile Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited Profile Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever are med DNS instance is created with the profile of the pr	GRE Tunnel	
Sends a report message when any configuration changes to Site Blocking are applied. For example, whenever Whitelist is changed to Blacklist/Whitelist, etc. PPTP Sends a report message when any configuration changes to PPTP are applied. For example, whenever a new PPTP instance was created, deleted enabled/disabled, PPTP server address was changed, etc. Sends a report message when any configuration changes to Hotspot are applied. For example, whenever Hotspot SSID was changed, Radius server was changed, Hotspot was enablet/disabled, etc. Input/Output Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Periodic Output Contre Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Proxy Based Content Blocker are applied. For example, whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist/Whitelist, etc. Login page Sends a report message when any Language Settings are changed Language Sends a report message when any Language Settings are changed Profile Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited Profile Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited Profile Sends a report message when any configuration changes to Dynamic DNS are applied. For example, sSH/HTTP/HTTPS remote or local access enabled/disabled, changes are made to SSH or WebUI Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCD address range is changed Wrapper of the server of the server of the server of the server of the school of th	Ping reboot	Sends a report message when any configuration changes to <u>Ping Reboot</u> are applied. For example, whenever Ping Reboot gets enabled/disabled, host to ping has changed, etc.
PPTP Sends a report message when any configuration changes to PPTP are applied. For example, whenever a new PPTP instance was created, delete enabled/disabled, PPTP server address was changed, telt. Hotspot Sends a report message when any configuration changes to Iotspot are applied. For example, whenever Hotspot SSID was changed, Radius server was changed, Hotspot was enabled/disabled, etc. Input/Output Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Sends a report message when any Language Settings are changed Language Sends a report message when any Language Settings are changed Language Sends a report message when any Language Settings are changed Profile Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited DDNS Sends a report message when any configuration changes to Insect of the profile in the profile is added or deleted or edited Access control Sends a report message when any configuration changes to Insect or example, a new IPsec instance is created, changed, deleted, access control are applied. For example, an ew IPsec instance is created, changed, deleted, access control are applied. For example, send in the profile in the profile is changed, deleted, and the profile in the prof	Auto update	Sends a report message when any configuration changes to Auto update are applied
enabled/disabled, PPTP server address was changed, etc. Hotspot Sends a report message when any configuration changes to Hotspot are applied. For example, whenever Hotspot SSID was changed, Radius server was changed, Hotspot was enabled/disabled, etc. Input/Output Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Proxy Based Content Blocker are applied. For example, whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist/Whitelist, etc. Login page Sends a report message when any Language Settings are changed Language Sends a report message when any Language Settings are changed Language Sends a report message when any Language Settings are changed Profile Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited DDNS Sends a report message when any configuration changes to Instance applied. For example, a new IPsec instance is created, changed, deleted, and clieded or edited Profile Sends a report message when any configuration changes to Access Control are applied. For example, shenever a new DDNS instance is created, changed, deleted, access control Profile Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, hanges are made to SSH Or WebDIT Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCD address range is changed, etc. SSH Sends a report message when any configuration changes to SSH are applied. For example, whenever Main WAN is changed, etc. Sends a report message when any configuration changes to SSH are applied. For example, whenever Main WAN is cha	Site blocking	Sends a report message when any configuration changes to Site Blocking are applied. For example, whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist/Whitelist, etc.
Input/Output Server was changed, Hotspot was enabled/disabled, etc. Input/Output Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Proxy Based Content Blocker are applied. For example, whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist/Whitelist, etc. Login page Sends a report message when any Language Settings are changed Language Sends a report message when any Language Settings are changed Profile Sends a report message when any Profile is added or deleted DDNS Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited Prece Sends a report message when any configuration changes to IPsec are applied. For example, a new IPsec instance is created, changed, deleted, and the sends a report message when any configuration changes to Description of the profile of the profile is deleted or edited Prece Sends a report message when any configuration changes to DHCP are applied. For example, a new IPsec instance is created, changed, deleted, and the profile is added or deleted. Prece Sends a report message when any configuration changes to DHCP are applied. For example, and IPSEC is enabled/disabled, changes are made to SSH or WebUI Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, VRRP IP address is changed, etc. SSH Sends a report message when any configuration changes to VRRP are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, whenever Main WAN is changed, etc.	PPTP	Sends a report message when any configuration changes to PPTP are applied. For example, whenever a new PPTP instance was created, deleted, enabled/disabled, PPTP server address was changed, etc.
Rule was created, changed, deleted, an output was turn ON/OFF, etc. Content blocker Sends a report message when any configuration changes to Proxy Based Content Blocker are applied. For example, whenever Whitelist is changed to Blacklist or vice versa, a new entry is added to Blacklist whitelist, etc. Login page Sends a report message when any Language Settings are changed Language Sends a report message when any Language Settings are changed Profile Sends a report message when a new Profile is added or deleted DDNS Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is create changed, deleted or edited Psec Sends a report message when any configuration changes to IPsec are applied. For example, a new IPsec instance is created, changed, deleted, Access control Sends a report message when any configuration changes to Access Control are applied. For example, SSH/HTTP/HTTPS remote or local access enabled/disabled, changes are made to SSH or WebUI Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCl address range is changed VRRP Sends a report message when any configuration changes to VRRP are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address range is changed, etc. SSH Sends a report message when any configuration changes to SSH are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, a rule is disabled/enabled, etc. Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a rule is disabled/enabled, etc. Sends a report message when any configuration changes to Firewall are applied. For example, whenever NTP	Hotspot	
Login page Sends a report message when any Language Settings are changed Profile Sends a report message when any Language Settings are changed Profile Sends a report message when any Language Settings are changed Profile Sends a report message when any Language Settings are changed DDNS Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is create changed, deleted or edited Profile Sends a report message when any configuration changes to IPsec are applied. For example, a new IPsec instance is created, changed, deleted, Access control Sends a report message when any configuration changes to IPsec are applied. For example, SSH/HTTP/HTTPS remote or local access enabled/disabled, changes are made to SSH or WebUI Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCl address range is changed VRRP Sends a report message when any configuration changes to VRRP are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address changed, etc. SSH Sends a report message when any configuration changes to VRRP are applied. For example, whenever Main WAN is changed, IAN IP address is changed, at WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, whenever Main WAN is changed, LAN IP address is changed, at WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, sibled, SSID is changed, etc. Sends a report message when any configuration changes to Wireless are applied. For example, a new Traffic rule is added, a rule is disabled/enabled, etc. Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc.	Input/Output	Sends a report message when any configuration changes to Input/Output are applied. For example, whenever a new Periodic Output Control Rule was created, changed, deleted, an output was turn ON/OFF, etc.
Sends a report message when any Language Settings are changed	Content blocker	
Profile Sends a report message when an new Profile is added or deleted DDNS Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited Psec Sends a report message when any configuration changes to Issec are applied. For example, a new Issec instance is created, changed, deleted, Access control Sends a report message when any configuration changes to Access Control are applied. For example, SSH/HTTP/HTTPS remote or local access enabled/disabled, changes are made to SSH or WebUI Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCI address range is changed VRRP Sends a report message when any configuration changes to VRRP are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address is changed, etc. SSH Sends a report message when any configuration changes to SSH are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. Sends a report message when any configuration changes to NTP are applied. For example, whenever a new L2TP instance was created, changed eleted, etc.	Login page	Sends a report message when any <u>Language Settings</u> are changed
Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created changed, deleted or edited Sends a report message when any configuration changes to IPsec are applied. For example, a new IPsec instance is created, changed, deleted, Access control Sends a report message when any configuration changes to Access Control are applied. For example, SSH/HTTP/HTTPS remote or local access enabled/disabled, changes are made to SSH or Web/II Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCI address range is changed VRRP Sends a report message when any configuration changes to VRRP are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address is changed, etc. SSH Sends a report message when any configuration changes to SSH are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. Sends a report message when any configuration changes to NTP are applied. For example, whenever a new L2TP instance was created, changed, etc. Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed, etc.	Language	Sends a report message when any Language Settings are changed
IPsec Sends a report message when any configuration changes to IPsec are applied. For example, a new IPsec instance is created, changed, deleted, Access control Sends a report message when any configuration changes to Access Control are applied. For example, SSH/HTTP/HTTPS remote or local access enabled/disabled, changes are made to SSH or WebUI Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCI address range is changed VRRP Sends a report message when any configuration changes to VRRP are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address is changed, etc. SSH Sends a report message when any configuration changes to SSH are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed etc.	Profile	Sends a report message when a new <u>Profile</u> is added or deleted
Sends a report message when any configuration changes to Access Control are applied. For example, SSH/HTTP/HTTPS remote or local access enabled/disabled, changes are made to SSH or WebUI Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCl address range is changed VRRP Sends a report message when any configuration changes to VRRP are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address is changed, etc. SSH Sends a report message when any configuration changes to SSH are applied Network Sends a report message when any Network related configuration changes are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed deleted, etc.	DDNS	Sends a report message when any configuration changes to Dynamic DNS are applied. For example, whenever a new DDNS instance is created, changed, deleted or edited
enabled/disabled, changes are made to SSH or WebUT Access Secure, etc. DHCP Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCl address range is changed VRRP Sends a report message when any configuration changes to VRRP are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address is changed, etc. SSH Sends a report message when any configuration changes to SSH are applied Network Sends a report message when any Network related configuration changes are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed eleted, etc.	IPsec	Sends a report message when any configuration changes to IPsec are applied. For example, a new IPsec instance is created, changed, deleted, etc
Address range is changed VRRP Sends a report message when any configuration changes to VRRP are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address is changed, etc. SSH Sends a report message when any configuration changes to SSH are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed eleted, etc.	Access control	Sends a report message when any configuration changes to Access Control are applied. For example, SSH/HTTP/HTTPS remote or local access is enabled/disabled, changes are made to SSH or WebUI Access Secure, etc.
is changed, etc. SSH Sends a report message when any configuration changes to SSH are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. L2TP Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed deleted, etc.	DHCP	Sends a report message when any configuration changes to DHCP are applied. For example, whenever DHCP Server is enabled/disabled, DHCP address range is changed
Network Sends a report message when any Network related configuration changes are applied. For example, whenever Main WAN is changed, LAN IP address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. L2TP Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed deleted, etc.	VRRP	Sends a report message when any configuration changes to <u>VRRP</u> are applied. For example, whenever VRRP is enabled/disabled, VRRP IP address is changed, etc.
address is changed, a WiFi Access Point is enabled/disabled, etc. Wireless Sends a report message when any configuration changes to Wireless are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. L2TP Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed deleted, etc.	SSH	Sends a report message when any configuration changes to SSH are applied
enabled/disabled, SSID is changed, etc. Firewall Sends a report message when any configuration changes to Firewall are applied. For example, a new Traffic rule is added, a new SNAT rule is added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. L2TP Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed deleted, etc.	Network	
added, a rule is disabled/enabled, etc. NTP Sends a report message when any configuration changes to NTP are applied. For example, whenever NTP is enabled/disabled, Time zone is changed, etc. L2TP Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changeleted, etc.	Wireless	Sends a report message when any configuration changes to <u>Wireless</u> are applied. For example, a new Wi-Fi Access point is created, deleted, enabled/disabled, SSID is changed, etc.
changed, etc. L2TP Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, chang deleted, etc.	Firewall	
deleted, etc.	NTP	
Other Sends a report message when any configuration changes other than the ones provided above are applied	L2TP	Sends a report message when any configuration changes to L2TP are applied. For example, whenever a new L2TP instance was created, changed, deleted, etc.
	Other	Sends a report message when any configuration changes other than the ones provided above are applied

New DHCP client

EVENT SUB-TYPE	DESCRIPTION	
All	Sends a report message when a new devices is connected to the router either via LAN or Wi-Fi	
Connected from WiFi	Sends a report message when a new device is connected to the router via Wi-Fi	

Mobile Data

EVENT SUB-TYPE	DESCRIPTION	
All	Sends a report message when mobile data connection status changes (from Connected to Disconnected or vice versa)	
Connected	Sends a report message when mobile data connection is achieved	
Disconnected	Sends a report message when mobile data connection is lost	

SMS

EVENT SUB-TYPE DESCRIPTION	SMS received	Sends a report message when the router receives a new SMS message
	EVENT SUB-TYPE	DESCRIPTION

Signal Strength

EVENT SUB-TYPE	DESCRIPTION
All	Sends a report message when the router's RSSI value leaves any one of the below specified ranges
-121 dBm -113 dBm	Sends a report message when the router's RSSI value leaves the -121 dBm to -113 dBm range
-113 dBm -98 dBm	Sends a report message when the router's RSSI value leaves the -113 dBm to -98 dBm range
-98 dBm -93 dBm	Sends a report message when the router's RSSI value leaves the -98 dBm to -93 dBm range
-93 dBm -75 dBm	Sends a report message when the router's RSSI value leaves the -93 dBm to -75 dBm range
-75 dBm -60 dBm	Sends a report message when the router's RSSI value leaves the -75 dBm to -60 dBm range
-60 dBm -50 dBm	Sends a report message when the router's RSSI value leaves the -60 dBm to -50 dBm range

Reboot

EVENT SUB-TYPE	DESCRIPTION	
All	Sends a report message when the router starts up after any type of reboot (except factory reset)	
After unexpected shutdown	Sends a report message when the router shuts down unexpectedly and starts back up again	
After FW upgrade	Sends a report message when the router initiates a Firmware upgrade (either from an uploaded FW file or from server)	
From WebUI	Sends a report message when the router starts up after a reboot command is initiated from the router's WebUI Administration->Reboot section	
From SMS	Sends a report message when the router starts up after a reboot command is initiated via SMS	
From Input/Output	Sends a report message when the router starts up after a reboot command is initiated via Input/Output	
From ping reboot	Sends a report message when the router starts up after a reboot command is initiated by the Ping Reboot function	
From periodic reboot	Sends a report message when the router starts up after a reboot command is initiated by the Periodic Reboot function	
From button	Sends a report message when the router starts up after being restarted by the press of the physical button located on the router	

SSH

EVENT SUB-TYPE	DESCRIPTION
All	Sends a report message when someone connects to the router via SSH (either successfully) or unsuccessfully)
Successful authentication	Sends a report message when someone successfully connects to the router via SSH
Unsuccessful authentication	Sends a report message when someone unsuccessfully tries to connect to the router via SSH

WebUI

EVENT SUB-TYPE	DESCRIPTION
All	Sends a report message when someone connects to the router via HTTP or HTTPS (either successfully or unsuccessfully)
Successful authentication	Sends a report message when someone successfully connects to the router via HTTP or HTTPS
Unsuccessful authentication	Sends a report message when someone unsuccessfully tries to connect to the router via HTTP or HTTPS

New WiFi client

EVENT SUB-TYPE	DESCRIPTION
All	Sends a report message when a device connects to or disconnects from the router's WLAN (Wireless Network or Wireless LAN)
Connected	Sends a report message when a device connects to the router's WLAN
Disconnected	Sends a report message when a device disconnects from the router's WLAN

LAN Port State

EVENT SUB-TYPE	DESCRIPTION	
All	Sends a report message when a device is either plugged in or unplugged from one of the router's LAN ports	
Unplugged	Sends a report message when a device is unplugged from one of the router's LAN ports	
Plugged in	Sends a report message when a device is plugged into one of the router's LAN ports	

WAN Failover

EVENT SUB-TYPE	DESCRIPTION	
All	Sends a report message when the router switches from using the Main WAN to using the Failover WAN and vice versa	
Switched to main	Sends a report message when the router switches from using the Main WAN to using the Failover WAN	
Switched to failover	Sends a report message when the router stops using the Failover WAN and start using the Main WAN	

Reporting Configuration

The **Reporting Configuration** section lets you create rules that transfer logs to email or FTP.



Events Log Report Configuration

Events Log Report Configuration provides you with the ability to change the configuration of periodic events reporting to email or FTP. You can access it by creating a rule and clicking the **Edit** button next to it, just like Event Reporting Configuration.

FTP



FIELD NAME	VALUE	DESCRIPTION
Enable	yes no; Default: no	Toggles the log file report rule ON or OFF
Events log	System Network All; Default: System	Specifies which log to transfer
Transfer type	Email FTP; Default: Email	Specifies whether to transfer the log(s) to FTP or Email
Compress file	yes no; Default: no	Compress events log file using gzip
Host	host ip; Default none	FTP server's IP address or hostname
User name	string; Default: none	Login user name used for authentication to the FTP server
Password	string; Default: none	Login password used for authentication to the FTP
Interval between reports	Week Month Year; Default: Week	Specifies how often the reports should be sent
Weekday Month day	weekday month day; Default: Sunday	Specifies the day of the month/week when the logging should take place. This field changes in accordance with Interval between reports

Email



FIELD NAME	VALUE	DESCRIPTION
Enable	yes no; Default: no	Toggles the log file report rule ON or OFF
Events log	System Network All; Default: System	Specifies which log to transfer
Transfer type	Email FTP; Default: Email	Specifies whether to transfer the log(s) to FTP or Email
Compress file	yes no; Default: no	Compress events log file using gzip
Subject	string; Default: none	Specifies the subject of the email log message
Message	string; Default: none	The text contained in the log email. This has nothing to do with the log itself, which will be sent as an attached file ${}^{\circ}$
SMTP server	ip host; Default: none	Sender's email service provider's SMTP server. If you don't know the SMTP server's address, you can easily look it up online since it is public information
SMTP server port	integer [065535]; Default: none	Sender's email service provider's SMTP server. If you don't know the SMTP server's address, you can easily look it up online since it is public information
Secure connection	yes no; Default: no	Toggles secure connection feature ON or OFF (use only if the email service provider's server supports SSL or TLS)
Username	string; Default: none	Sender's email account's login user name
Password	string; Default: none	Sender's email account's login password
Sender's email address	email; Default: none	The email address of the sender, i.e., the report message will be sent from this email. Make sure this is the same email that you provided login information to
Recipient's email address	email; Default: none	The intended recipient's email address. To add more than one email address, click the green → plus symbol located to the right of this field
Interval between reports	Week Month Year; Default: Week	Specifies how often the reports should be sent
Weekday Month day	weekday month day; Default: Sunday	Specifies the day of the month/week when the logging should take place. This field changes in accordance with Interval between reports
Hour	integer [124]; Default: 1	Specifies on the hour of the day when the logging should take place