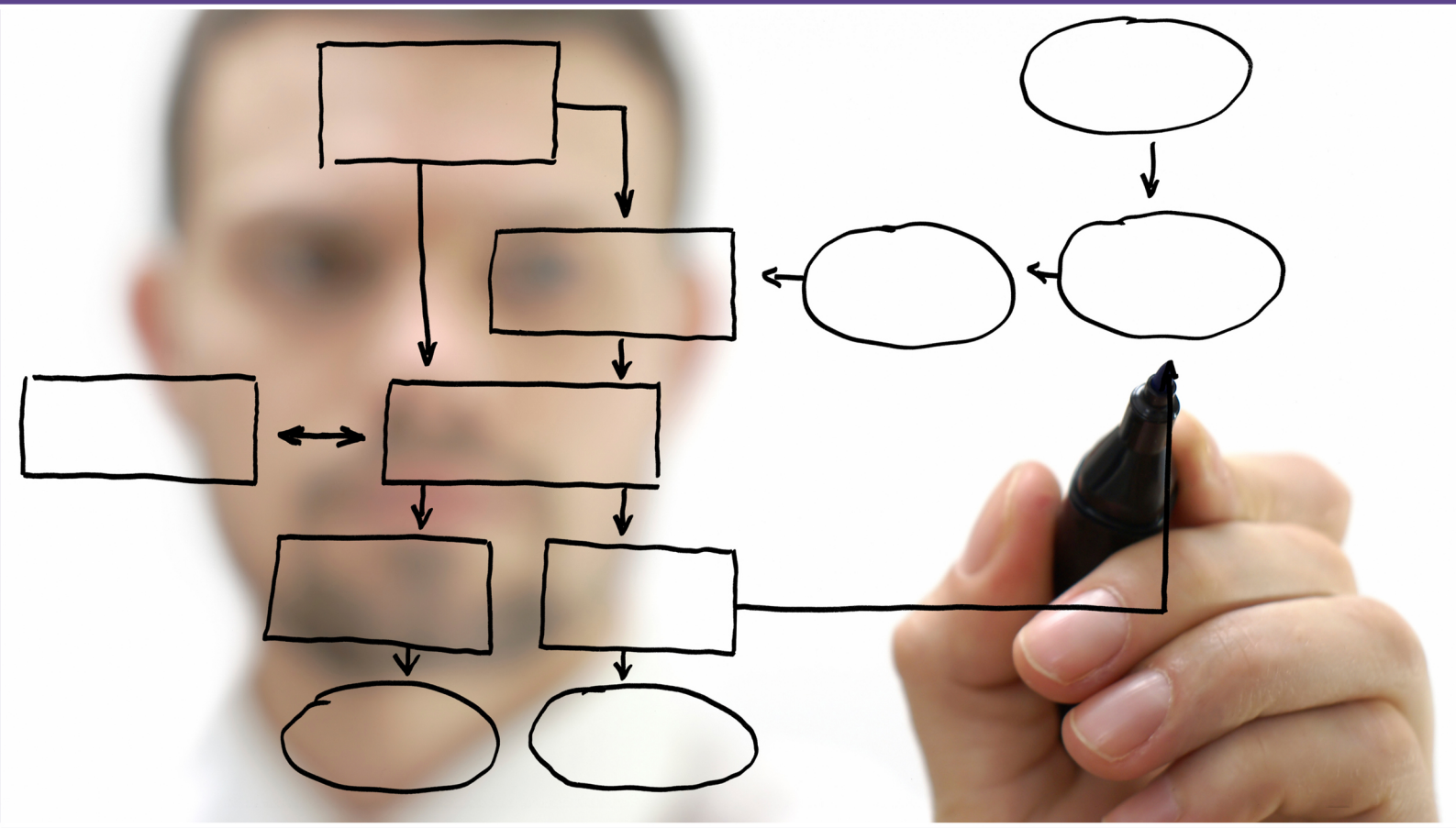
OpenRG Configuration Entries Guide

Version 4.11



JUNGO
Smarter Gateway

OpenRG Configuration Entries Guide

Version 4.11

Jungo Software Technologies Ltd.

OpenRG Configuration Entries Guide: Version 4.11

This document is available for download at: *http://www.jungo.com/openrg/documentation.html, version 4.11*

Revision: 4113-20090401-174730

Table of Contents

1. Overview 1
    1.1. Entry Fields 1
    1.2. Conventions 1
    1.3. Entry Types 1
2. Administrator 3
    2.1. User 4
    2.2. Remote Management 8
    2.3. Group 9
    2.4. Timezone 10
    2.5. Daylight Saving 10
    2.6. Time of Day 12
    2.7. Telnets 13
    2.8. HTTP Server 14
    2.9. Support Cost Reduction 15
3. Bluetooth 16
4. Certificates 18
5. Disk 20
6. DNS 23
7. Domain Routing 25
8. DSL Home 26
    8.1. General 26
    8.2. Periodic Inform 32
    8.3. Download 33
    8.4. Attribute 34
9. Dynamic DNS 35
10. File Server 39
11. File System Backup 43
    11.1. General 43
    11.2. Full 44
    11.3. Incremental 45
12. Firewall 47
    12.1. General 48
    12.2. Reserved Ports 48
    12.3. Rule 49
        12.3.1. General 49
        12.3.2. Special Applications 52
        12.3.3. Local Server 53
    12.4. Log 54
    12.5. Protect 59
    12.6. Policy 60
    12.7. Interception 79
13. FTP Server 82
14. Hybrid Bridge 85
15. Internet Protocol Security (IPSec) 87
    15.1. General 88
    15.2. Block IP 88

15.3. RSA 89
15.4. Log 91
15.4.1. Internet Key Exchange Log 91
15.4.2. IPSec Log 93
16. IPv6 97
17. Jungo.net 98
18. Kerberos 100
19. Layer 2 Tunneling Protocol (L2TP) Server 101
19.1. General 102
19.2. Remote 102
19.3. Authentication 103
19.4. Encryption 104
19.5. IPSec 105
20. Multicast Groups 106
21. Mail 108
21.1. Email Notification 108
21.2. Email Client 109
21.3. Mail Server 111
21.3.1. Mail Transfer Agent 111
21.3.2. POP3 113
21.3.3. Internet Message Access Protocol 114
21.3.4. Internet Message Access Protocol over SSL 114
22. Manufacturer 115
23. Network Connections 119
23.1. General 120
23.1.1. Static 127
23.1.2. Fallback 128
23.1.3. Dynamically Obtained Information 128
23.1.4. Additional IP addresses 129
23.1.5. Statistics 130
23.2. Enslaved Devices 130
23.3. DNS 133
23.4. Dynamic Host Configuration Protocol (DHCP) Relay 133
23.5. Dynamic Host Configuration Protocol (DHCP) Server 134
23.5.1. General Entries 135
23.5.2. Lease 138
23.6. Asynchronous Transfer Mode (ATM) 143
23.7. Digital Subscriber Line (DSL) 146
23.8. Point-to-Point Protocol (PPP) 146
23.8.1. Authentication 146
23.8.2. Encryption 148
23.8.3. Compression 149
23.8.4. Connection 149
23.8.5. PPPoE 150
23.8.6. Layer 2 and Point-to-Point Tunneling Protocols 151
23.9. Internet Protocol Security (IPSec) 151
23.9.1. General 151
23.9.2. Remote 153

23.9.3. Local 155
23.9.4. Protect 156
23.9.5. Manual 157
23.9.6. Automatic 160
23.9.7. Phase 1 161
23.9.8. Phase 2 165
23.9.9. Dead Peer Detection 167
23.10. IPv6 168
23.11. RADIUS 169
23.12. Web Authentication 170
23.13. Wireless Local Area Network (WLAN) 171
23.13.1. General 171
23.13.2. Key 173
23.13.3. Repeater 174
23.14. Wireless LAN Access Point 175
23.15. Wi-Fi Protected Access (WPA) 182
23.16. Routing Information Protocol (RIP) 187
23.17. Quality of Service (QoS) 188
23.17.1. Shaping 188
23.17.2. Traffic Class 190
23.17.3. VLAN to DSCP 192
23.18. Route 193
24. Network Objects 195
25. Point-to-Point Protocol over Ethernet (PPPoE) Relay 198
26. Point-to-Point Tunneling Protocol (PPTP) Server 199
26.1. General 199
26.2. Remote 200
26.3. Authentication 200
26.4. Encryption 202
27. Print Server 203
28. Quality of Service (QoS) 206
29. RADIUS Client 212
30. RADIUS Server 214
31. Remote Update 216
32. Routing 219
32.1. Routes 219
32.2. Routing Information Protocol (RIP) 221
32.3. Border Gateway Protocol (BGP) 221
32.4. Open Shortest Path First (OSPF) 222
32.5. Zebra 222
33. Secure Shell 224
34. Secure Socket Layer Virtual Private Network 227
35. Services 233
36. Simple Network Management Protocol (SNMP) 237
36.1. General Entries 237
36.2. Community MIB 241
36.3. View-Based Access Control Model MIB 244
36.3.1. Context Table 244

36.3.2. Security to Group Table 245
36.3.3. Access Table 246
36.3.4. View Tree Table 248
36.4. Notification MIB 250
36.4.1. Notify Table 250
36.4.2. Filter Profile Table 252
36.4.3. Filter Table 253
36.5. Target MIB 255
36.5.1. Target Address Table 255
36.5.2. Target Parameters Table 258
36.6. USM MIB 260
37. Support Cost Reduction 265
38. System 266
39. System Log 272
40. Time Enabling Rules 274
41. Transparent Proxy 276
42. Antivirus 280
43. Universal Plug and Play (UPnP) 281
44. Voice over Asynchronous Transfer Mode (VoATM) 285
45. Voice over IP (VoIp) 286
45.1. General 287
45.2. Codec 288
45.3. Signalling 290
45.3.1. General 290
45.3.2. MGCP Call Agent 290
45.3.3. SIP 290
45.3.4. H323 292
45.3.5. MGCP Media Gateway 295
45.4. IP Phone 297
45.5. Line 298
45.5.1. General 298
45.5.2. Proxy 306
45.5.3. Outbound Proxy 308
45.6. Phonebook 309
45.7. Audio 310
45.7.1. General 310
45.7.2. Echo Cancellation 310
45.7.3. DSP 312
45.7.4. Call Waiting 313
45.7.5. FXS Ports 314
45.7.6. Jitter 316
45.7.7. Caller ID 318
45.8. MSS Clamping 320
45.9. Trunk 320
45.10. Trunk Group 326
45.11. Voice Mail 327
45.12. Music on Hold 327
45.13. Call Park 328

45.14. Extension 329
45.15. Auto Attendant 334
45.16. Dial Plan 337
45.17. Day Mode Schedule 338
45.18. Hunt Group 339
45.19. Feature Codes 342
46. Web-Based Management (WBM) 343
47. Web Filtering 349
48. Web Server 352
48.1. General 352
48.2. HTTP Server 353
48.3. User Directory 354
48.4. Virtual Host 354
49. Licensing Acknowledgement and Source Code Offering 356
50. Contact Jungo 357

1

Overview

1.1 Entry Fields

Each entry includes the following fields:

- Name - the entry name
- Description - the description of the entry
- Relevance - other components to which the entry is relavant
- Type - the type of the entry
- Default - the default value of the entry, if exists

1.2 Conventions

MGT Any type of management task - e.g. Web-Based Management (WBM), Simple Network Management Protocol (SNMP).

% Numerical index. Certain entries can have a number of similar entities beneath them, each with a unique index, starting with zero, e.g. **admin/user/0/full_name** is the fullname of **user(0)** and **admin/user/8/full_name** is the fullname of **user(8)**.

1.3 Entry Types

Each entry may be of the C types listed below (denoted '`<type>`') or of type `text[l]`.

<type> A C type

- **integer**
- **boolean** – Either **True=1** or **False=0** (int)
- **time_t** – Saved as an integer
- **enums** – Include all the enum values
- **string** – Usually includes all the possible string values
- **port** – An integer 0-65535
- **binary**

`text[length]` – general text with specified length

- **ip** Internet Protocol (IP) address/netmask represented as text, e.g. `"122.45.22.89"` or `"255.255.255.0"` (text[MAX_IP_SIZE=16])
- **ipv6** IPv6 address represented as text, e.g. `"2002:C0A8:5BBA:1:204B:69FF:FE81:E63E"` (text[MAX_IPV6_SIZE=40])
- **date** Formatted date and time, e.g. `"Wed Apr 10 16:26:42 2002"` (text[25])
- **mac** Hardware MAC address, e.g. `"01:23:45:67:89:AB"` (text[MAX_MAC_SIZE=18])
- **host** Fully Qualified Domain Name (FQDN) representing the host (see RFC-1034), e.g. `"http://www.jungo.com"` (text[MAX_DOMAIN_NAME_LEN=255])
- **email** A legitimate email address (text[MAX_EMAIL_LEN=320])
- **netobj** Network Object. Can be in one of the following forms:
  - Foreign key to Network Objects table e.g. `"net_obj/3"` , where '3' is the key of the specified Network Object.
  - In-line Network Object e.g. `"item/0/hostname/lou.home"` , where lou.home is the desired host name.

2

Administrator

- User -- the entries for each user, including the user identification details, permissions, mailbox settings, etc. (refer to Section 2.1).
- Group -- the entries for each group of users (refer to Section 2.3).
- Timezone -- the timezone entries (refer to Section 2.4).
- Daylight Saving -- all daylight saving-related entries (refer to Section 2.5).
- Time of Day -- all the Time of Day related entries (refer to Section 2.6).
- Telnets -- the primary, secondary and Secure Socket Layer (SSL) Telnet server entries (refer to Section 2.7).
- HTTP Server -- the primary, secondary, primary over SSL and secondary over SSL HTTP server entries (refer to Section 2.8).
- Support Cost Reduction -- settings related to the specified feature. Section 2.9

2.1 User

admin/user/%/full_name

Description Keeps the full name of the OpenRG user. The default value is only for the first user of OpenRG, a new user you add will not have a default full name.

Relevant to General

Type text[MAX_FULLNAME_LEN=128]

Default Value Administrator

admin/user/%/password

Description The password used to log into OpenRG. The default value is only for the first user of OpenRG, a new user you add will not have a default password. This entry is encrypted.

Relevant to General

Type text[MAX_PASSWORD_LEN=64]

Default Value admin

admin/user/%/username

Description The user-name used to log into OpenRG. The default value is only for the first user of OpenRG, a new user you add will not have a default user name.

Relevant to General

Type text[MAX_USERNAME_LEN=64]

Default Value admin

admin/user/%/email

Description Keeps the email address of the OpenRG user. This field is required if you wish to receive email notifications.

Relevant to General

Type email

Default Value

admin/user/%/group

Description Identification (ID) of primary group of the user. This group is used as the owning group of files and directories created by this user.

Relevant to File Server, Print Server

Type integer

Default Value

admin/user/%/restricted

Description Determines if a user is a restricted user, having a restricted access to OpenRG's configuration options.

Relevant to WBM

Type boolean

Default Value True=1

admin/user/%/directory

Description Enables a user home directory and creates it if it does not exist.

Relevant to File Server

Type boolean

Default Value False=0

admin/user/%/permissions/mgt

Description Access permissions to Web-Based Management (WBM) and other management applications, such as CLI (Telnet). The default value is only for the first user of OpenRG. A new user you add will not have access permissions by default.

Relevant to Login

Type boolean

Default Value True=1

admin/user/%/permissions/vpns

Description Access permissions as a client to Point-to-Point and Layer 2 Tunneling Protocols (PPTP and L2TP) servers.

Relevant to PPTPS

Type boolean

Default Value False=0

admin/user/%/permissions/fs

Description Permissions for Microsoft File and Printer sharing access. Access level must be defined separately per file server share. The default value is only for the first user of OpenRG. A new user you add will not have access permissions by default.

Relevant to Microsoft File and Printer Sharing Access

Type boolean

Default Value True=1

admin/user/%/permissions/ftp

Description Access permissions to login to File Transfer Protocol (FTP) server.

Relevant to FTP

Type boolean

Default Value False=0

admin/user/%/permissions/mails

Description Access permissions to login to Mail server.

Relevant to Mail Server

Type boolean

Default Value False=0

admin/user/%/mailbox/enabled

Description Enable a user's mailbox to receive email from the Mail Server after creating it if it does not exist.

Relevant to Mail Server

Type boolean

Default Value False=0

admin/user/%/mailbox/quota

Description Quota of a mailbox in Megabytes. The default value is taken from the mail server default quota (see entry email/mta/quota on page 111).

Relevant to Mail Server

Type integer

Default Value 30

admin/user/%/mailbox/aliases

Description List of aliases for the mailbox. Each user can have aliases (other names) that he can link to his mailbox using this entry. Aliases are separated by a comma (','), a semicolon (';') or a space.

Relevant to Mail Server

Type text

Default Value

admin/user/%/notify_level/0

Description Email notification level for system messages. In order to receive email notification for the system messages as defined here, you must also specify the email address of the user (see entry admin/user/%/email on page 4) and the outgoing mail server details (see entry email/smtp/server on page 109).

Relevant to Email Notification

Type enum INFO = 2,
WARN = 3,
ERR = 4,
NONE = 0xf

Default Value NONE

admin/user/%/notify_level/1

Description Email notification level for security messages. In order to receive email notification for the security messages as defined here, you must also specify the email address of the user (see entry admin/user/%/email on page 4) and the outgoing mail server details (see entry email/smtp/server on page 109).

Relevant to Email Notification

Type enum INFO = 2,
WARN = 3,
ERR = 4,
NONE = 0xf

Default Value NONE

admin/user/%/8021x_eap_method

Description Extensible Authentication Protocol Over LAN (EAPOL) method for 802.1x authentication.

Relevant to 8021x Authentication

Type one string of:
"none" (EMI_NONE),
"radius" (EMI_RADIUS),
"md5" (EMI_MD5),
"tls" (EMI_TLS),
"ttls" (EMI_TTLS)

Default Value

2.2 Remote Management

admin/rmt_mng/ports/%/enabled

Description Indicates whether remote management listens to its ports. Index 0 is for a regular remote management port, 1 is for an SSL remote management port and 2 is for a loopback port.

Relevant to Remote management, WBM

Type boolean

Default Value False=0

admin/rmt_mng/ports/%/port

Description Remote management port. Index 0 for a regular remote management port, 1 is for SSL remote management port, and 2 if for loopback port.

Relevant to Remote management, WBM

Type unsigned integer

Default Value

admin/rmt_mng/ports/%/remote_access

Description Indicates whether remote management ports are accessible from the WAN. Index 0 is for a regular remote management port, 1 is for an SSL remote management port and 2 is for a loopback port.

Relevant to Remote management, WBM

Type boolean

Default Value

2.3 Group

admin/group/%/name

Description Name of the users group. The default value is only for the first group. A new group you add will not have access permissions by default.

Relevant to File Server

Type text[MAX_USERNAME_LEN=64]

Default Value Users

admin/group/%/description

Description Description of the group

Relevant to File Server

Type text[MAX_DESCR_LEN]=64

Default Value

admin/group/%/user/%

Description User ID of members of this group.

Relevant to File Server

Type integer

Default Value

2.4 Timezone

admin/tz_offset

Description Time zone offset in minutes past Greenwich Mean Time (GMT). This entry is ignored if the **timezone** entry is specified.

Relevant to General

Type integer

Default Value 0

admin/timezone

Description Linux style time zone name. If you prefer to enter your time zone as an offset in minutes past GMT, do so in **tz_offset** and leave this entry empty.

Relevant to General

Type text[MAX_LINE_SIZE=1024]

Default Value GMT

2.5 Daylight Saving

admin/daylight_saving/from

Description Daylight saving starting date.

Relevant to General

Type text[6] - "day;month"

Default Value 28;2

admin/daylight_saving/to

Description Daylight saving end date.

Relevant to General

Type text[6] - "day;month"

Default Value 28;9

admin/daylight_saving/start/hour

Description Daylight saving starting hour.

Relevant to General

Type integer

Default Value 0

admin/daylight_saving/start/min

Description Daylight saving starting minute.

Relevant to General

Type integer

Default Value 0

admin/daylight_saving/end/hour

Description Daylight saving end hour.

Relevant to General

Type integer

Default Value 1

admin/daylight_saving/end/min

Description Daylight saving end minute.

Relevant to General

Type integer

Default Value 0

admin/daylight_saving/offset

Description Offset of the daylight saving in minutes past your local time.

Relevant to General

Type integer

Default Value 60

admin/daylight_saving/enabled

Description Toggle daylight saving option.

Relevant to General

Type boolean

Default Value False=0

2.6 Time of Day

admin/tod/enabled

Description Toggle Automatic Time Update option.

Relevant to General

Type boolean

Default Value True=1

admin/tod/server/%/name

Description IP or hostname of Time Of Day (TOD) server. The default value is only for the first server. A new server you add will not have an IP or hostname of TOD server by default. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to General

Type host or ip

Default Value ntp.jungo.com

admin/tod/protocol

Description TOD protocol.

Relevant to General

Type one string of:
"time" (TOD_P_TIME),
"sntp" (TOD_P_SNTP)

Default Value "sntp"

admin/tod/update_period

Description Number of seconds between time updates from the TOD server.

Relevant to General

Type integer (greater than 0)

Default Value 24

admin/sntp/server/enabled

Description Enable SNTP Server.

Relevant to sntp server

Type boolean

Default Value True

2.7 Telnets

admin/telnets/ports/%/port

Description Port numbers of Telnet servers. The Telnet server indexes can be 0, 1 or 2, representing primary, secondary and Secure Socket Layer (SSL) respectively.

Relevant to General

Type integer (1-65535)

Default Value Port 23, 8023 and 992 for index 0, 1 and 2 respectively

admin/telnets/ports/%/ssl_mode

Description Indicates if the server is over SSL, and if it is, how to authenticate the client. The Telnet server indexes can be 0, 1 or 2, representing primary, secondary and SSL respectively.

Relevant to General

Type one string of:
"none" (MGT_SRV_SSL_NONE),
"no_verify" (MGT_SRV_SSL_NO_PEER_VERIFY),
"verify" (MGT_SRV_SSL_VERIFY_PEER),
"verify_fail_no_cert" (MGT_SRV_SSL_VERIFY_FAIL_IF_NO_PEER_CERT)

Default Value "none" for index 0 and 1, "no_verify" for index 2

admin/telnets/ports/%/remote_access

Description Indicates if the server can be accessed from WAN. The Telnet server indexes can be 0, 1 or 2, representing primary, secondary and SSL respectively.

Relevant to General

Type boolean

Default Value False=0

2.8 HTTP Server

admin/https/ports/%/port

Description Port number of Hypertext Transfer Protocol (HTTP) server. The HTTP server indexes can be 0, 1, 2 or 3, representing primary, secondary, primary over SSL and secondary over SSL respectively.

Relevant to General

Type integer (1-65535)

Default Value Port 80, 8080, 443 and 8443 for index 0, 1, 2 and 3 respectively

admin/https/ports/%/ssl_mode

Description Indicates if this server is over SSL, and if it is, how to authenticate the client. The HTTP server indexes can be 0, 1, 2 or 3, representing primary, secondary, primary over SSL and secondary over SSL respectively.

Relevant to General

Type one string of:
"none" (MGT_SRV_SSL_NONE),
"no_verify" (MGT_SRV_SSL_NO_PEER_VERIFY),
"verify" (MGT_SRV_SSL_VERIFY_PEER),
"verify_fail_no_cert" (MGT_SRV_SSL_VERIFY_FAIL_IF_NO_PEER_CERT)

Default Value "none" for index 0 and 1, "no_verify" for index 2 and 3

admin/https/ports/%/remote_access

Description Indicates if the server can be accessed from WAN. The HTTP server indexes can be 0, 1, 2 or 3, representing primary, secondary, primary over SSL and secondary over SSL respectively.

Relevant to General

Type boolean

Default Value False=0

admin/https/connect_inactivity_timeout

Description The idle timeout until the http task closes the CONNECT tunnel.

Relevant to SSL VPN

Type integer

Default Value 600

2.9 Support Cost Reduction

admin/scr/enabled

Description Indicates whether the entire Support Cost Reduction feature is globally enabled. All depending features would be enabled/disabled accordingly.

Relevant to Support Cost Reduction, WBM

Type boolean

Default Value True=1

3

Bluetooth

Yet another method to connect to OpenRG's LAN is by Bluetooth, an open specification for wireless, short-range transmission between PCs, mobile phones and other portable devices. When connected to OpenRG via Bluetooth, users can benefit from standard network connectivity, limited only by the capabilities of their connected devices. OpenRG utilizes the Bluetooth Network Encapsulation Protocol (BNEP), used by the Bluetooth Personal Area Network (PAN) profile. This layer encapsulates packets from various networking protocols, which are transported directly over the Logical Link Control and Adaptation Protocol (L2CAP) layer.

bluetooth/security/auth_level **Description** Bluetooth security/authentication level. **Relevant to** Bluetooth **Type** one string of: "none" (BT_AUTH_NONE), "auth" (BT_AUTH_ON), "encrypt" (BT_AUTH_ENCRYPT) **Default Value**
bluetooth/security/pin **Description** Bluetooth Private Identification Number (PIN). **Relevant to** Bluetooth **Type** string **Default Value**

bluetooth/mac

Description Bluetooth device MAC address. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to Bluetooth

Type mac

Default Value

bluetooth/name

Description Bluetooth device name, derived from the Bluetooth device MAC address (**bluetooth/mac**).

Relevant to Bluetooth

Type string

Default Value

4

Certificates

Public-key cryptography uses a pair of keys: a public key and a corresponding private key. These keys can play opposite roles, either encrypting or decrypting data. Your public key is made known to the world, while your private key is kept secret. The public and private keys are mathematically associated; however it is computationally infeasible to deduce the private key from the public key. Anyone who has the public key can encrypt information that can only be decrypted with the matching private key. Similarly, the person with the private key can encrypt information that can only be decrypted with the matching public key.

Technically, both public and private keys are large numbers that work with cryptographic algorithms to produce encrypted material. The primary benefit of public-key cryptography is that it allows people who have no preexisting security arrangement to authenticate each other and exchange messages securely. OpenRG makes use of public-key cryptography to encrypt and authenticate keys for the encryption of Wireless and VPN data communication, the Web Based Management (WBM) utility, and secured telnet.

cert/%/cert

Description Certificate data. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to IPSec, WBM, MGT, HTTPS, 802.1x

Type binary

Default Value

cert/%/owner

Description This entry indicates whether the certificate is for identifying yourself as OpenRG (X509_OPENRG) or for confirmation of identification (X509_CA). In most cases you will need to change your given certificate owner to X509_OPENRG.

Relevant to IPSec, WBM, MGT, HTTPS, 802.1x

Type enum x509_cert_owner_t
X509_OPENRG = 1,
X509_CA = 2

Default Value X509_OPENRG = 1

cert/%/private

Description Certificate's private key. Exists for owner X509_OPENRG only.

Relevant to IPSec, WBM, MGT, HTTPS, 802.1x

Type binary

Default Value

cert/%/request

Description Certificate's request. Details are sent via a request in order to receive a signed certificate.

Relevant to IPSec, WBM, MGT, HTTPS, 802.1x

Type binary

Default Value

cert/%/name

Description Certificate name. Exists for owner X509_OPENRG only. Used for OpenRG's certificate identication. It is the same as field 'CN=OR_<name>' in the certificate data if the field exists. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to IPSec, WBM, MGT, HTTPS, 802.1x

Type text[MAX_X509_NAME_LEN=64]

Default Value

5

Disk

Disk Management is the feature that controls USB, FireWire and IDE storage devices, such as disk-on-keys, USB disks and regular IDE disks. It provides the ability to configure disks: mount, partition, format and check, and also build raid0, raid1 and raid5 disk arrays.

disk/enabled **Description** Indicates whether disk management is enabled. **Relevant to** Disk Management **Type** boolean **Default Value** True=1
disk/storage_auto **Description** Indicates whether system/storage_path (aka System Storage Area) should be automatically detected or defined by user. **Relevant to** Disk Management **Type** boolean **Default Value** True=1

disk/system_path

Description Path of the system partition.

Relevant to Disk Management

Type text[18]

Default Value

disk/user_path

Description Path of the user partition.

Relevant to Disk Management

Type text[100]

Default Value

disk/device/%/path

Description Store the last assigned path to a partition on a removable device. Each partition is identified by a signature in the following format: <vendor>:<model>:<revision>:<serial number>:<partition start>:<size>.

Relevant to Disk Management

Type text[18]

Default Value

disk/raid/%/name

Description RAID device name.

Relevant to Disk Management

Type text[18]

Default Value

disk/raid/%/enabled

Description Indicates whether RAID device is enabled.

Relevant to Disk Management

Type boolean

Default Value

disk/raid/%/level

Description RAID level.

Relevant to Disk Management

Type one string of:
"raid0" (RAID_LEVEL_0),
"raid1" (RAID_LEVEL_1),
"raid5" (RAID_LEVEL_5)

Default Value

disk/raid/%/uuid

Description 128-bit Universally Unique Identifier. If does not exist, it indicates that the array was never initialized.

Relevant to Disk Management

Type text[UUID_LEN=36] (32 hex digits + 4 ':')

Default Value NULL

disk/raid/%/path

Description Name of mount point for the device.

Relevant to Disk Management

Type text[18]

Default Value

disk/raid/%/dev/%/name

Description Name of device in RAID array.

Relevant to Disk Management

Type text[18]

Default Value

6

DNS

dns/entry/%/ip **Description** Manually entered DNS IP address. **Relevant to** General, DNS **Type** ip **Default Value**
dns/entry/%/hostname **Description** Manually entered DNS hostname. **Relevant to** General, DNS **Type** host **Default Value**
dns/domainname **Description** OpenRG domain name (automatic name completion). When a DHCP lease is given to a client the domain name is also given. **Relevant to** DHCPS, General **Type** host **Default Value** home

dns/hostname

Description OpenRG name.

Relevant to General

Type host

Default Value openrg

7

Domain Routing

domain_routing/enabled

Description Is domain routing enabled. If this option is enabled, the route is decided on according to the DNS resolve.

Relevant to DNS, WBM

Type boolean

Default Value False=0

8

DSL Home

8.1 General

cwmp/enabled **Description** Indicates whether TR-069 (DSLHome CPE WAN Management Protocol (CWMP)) is enabled. **Relevant to** DSLHome **Type** boolean **Default Value** True=0
cwmp/acs_url **Description** Auto Configuration Server (ACS) (TR-069 server) URL. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide. **Relevant to** DSLHome **Type** text[MAX_DOMAIN_NAME_LEN=255] **Default Value**

cwmp/username

Description Username used to authenticate OpenRG when connecting to ACS. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DSLHome

Type text

Default Value

cwmp/password

Description Password used to authenticate OpenRG when connecting to ACS. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DSLHome

Type text

Default Value

cwmp/conn_req_username

Description Username used to authenticate the ACS making a Connection Request to OpenRG. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DSLHome

Type text

Default Value

cwmp/conn_req_password

Description Password used to authenticate the ACS making a Connection Request to OpenRG. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DSLHome

Type text

Default Value

cwmp/conn_req_realm

Description HTTP Realm used in ACS authentication when making a Connection Request to OpenRG. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DSLHome

Type text

Default Value

cwmp/provisioning_code

Description String used in Inform message as DSLHome InternetGatewayDevice.DeviceInfo.ProvisioningCode. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DSLHome

Type text

Default Value

cwmp/last_bootstrap_url

Description URL which last successful BOOTSTRAP Inform was sent to

Relevant to DSLHome

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

cwmp/parameter_key

Description ParameterKey argument which was received in latest SetParameterValues, AddObject or DeleteObject Remote Procedure Calls (RPCs).

Relevant to DSLHome

Type text

Default Value

cwmp/command_key

Description CommandKey argument which was received in latest Reboot, ScheduledInform or Upload RPCs. Cleared after being used in the Inform message. This entry is for internal use.

Relevant to DSLHome

Type text

Default Value

cwmp/ip_ping_diagnostics/diagnostics_state

Description The state of the ping diagnostics. Can be either Completed, None, Requested or Error_CannonResolveHostName

Relevant to DSLHome

Type enum CWMP_PING_DIAG_STATE_NONE
CWMP_PING_DIAG_STATE_REQUESTED
CWMP_PING_DIAG_STATE_COMPLETE
CWMP_PING_DIAG_STATE_ERROR
CWMP_PING_DIAG_STATE_RUNNING

Default Value CWMP_PING_DIAG_STATE_NONE

cwmp/ip_ping_diagnostics/params/interface

Description The interface (in cwmp parameter format) from which the ping test will be performed.

Relevant to DSLHome

Type text

Default Value

cwmp/ip_ping_diagnostics/params/number_of_repetitions

Description The number of times the ping test will be performed.

Relevant to DSLHome

Type unsigned integer

Default Value

cwmp/ip_ping_diagnostics/params/data_block_size

Description The amount of bytes that will be send in each ping test.

Relevant to DSLHome

Type 1-65535

Default Value

cwmp/ip_ping_diagnostics/params/host

Description The host name or IP that ping packets will be send to.

Relevant to DSLHome

Type text

Default Value

cwmp/ip_ping_diagnostics/params/timeout

Description The time interval between every two ping tests, in milliseconds.

Relevant to DSLHome

Type unsigned integer

Default Value

cwmp/ip_ping_diagnostics/params/dscp

Description The DiffServ codepoint to be used for the test packets.

Relevant to DSLHome

Type 0-64

Default Value

cwmp/ip_ping_diagnostics/result/success_count

Description The number of successful pings in the most recent ping test.

Relevant to DSLHome

Type unsigned integer

Default Value

cwmp/ip_ping_diagnostics/result/failure_count

Description The number of failed pings in the most recent ping test.

Relevant to DSLHome

Type unsigned integer

Default Value

cwmp/ip_ping_diagnostics/result/average_reponse_time

Description The average response time in milliseconds over all repetitions with succesfull resonses of the most recent ping test.

Relevant to DSLHome

Type unsigned integer

Default Value

cwmp/ip_ping_diagnostics/result/minimum_reponse_time

Description The minimum response time in milliseconds over all repetitions with succesfull resonses of the most recent ping test.

Relevant to DSLHome

Type unsigned integer

Default Value

cwmp/ip_ping_diagnostics/result/maximum_reponse_time

Description The maximum response time in milliseconds over all repetitions with succesfull resonses of the most recent ping test.

Relevant to DSLHome

Type unsigned integer

Default Value

cwmp/next_boot_events/%/code

Description For internal use of TR-069 implementation: pending Inform event code.

Relevant to DSLHome

Type unsigned integer

Default Value

cwmp/next_boot_events/%/key

Description For internal use of TR-069 implementation: CommandKey to be send with the event.

Relevant to DSLHome

Type string

Default Value

cwmp/next_boot_events/%/sent

Description For internal use of TR-069 implementation: whether this event was already send and now is waiting for acknoledgement.

Relevant to DSLHome

Type boolean

Default Value

8.2 Periodic Inform

cwmp/periodic_inform/enabled

Description Indicates whether periodic inform is enabled.

Relevant to DSLHome

Type boolean

Default Value False=0

cwmp/periodic_inform/interval

Description Duration, in seconds, between periodic Inform messages. Relevant only when **cwmp/periodic_inform/enabled** is true.

Relevant to DSLHome

Type unsigned integer

Default Value

cwmp/periodic_inform/time

Description If not zero and periodic inform is enabled - OpenRG should issue Inform message at that time plus or minus an integer multiple of **periodic_inform/interval**. Relevant only when **cwmp/periodic_inform/enabled** is true.

Relevant to DSLHome

Type time_t

Default Value

8.3 Download

cwmp/download/%/command_key

Description CommandKey argument which was received in latest Download RPC. Cleared after being used in the Inform message. This entry is for internal use.

Relevant to DSLHome

Type text

Default Value

cwmp/download/%/start_time

Description Time when download started.

Relevant to DSLHome

Type time_t

Default Value

cwmp/download/%/complete_time

Description Time when download finished.

Relevant to DSLHome

Type time_t

Default Value

8.4 Attribute

cwmp/attribute/<modified_parameter_name>/notification

Description Notification assigned for parameter. If the notification is not "off", you can either assign "active" notification, where you initiate communication with ACS to update the parameter, or "passive" notification, where you notify about the updated parameter the next time there is communication with ACS. <modified_parameter_name> is the parameter name, where each '.' is replaced with '/'.

Relevant to DSLHome

Type one string of:
"off" (CWMP_NOTIFICATION_OFF),
"passive" (CWMP_NOTIFICATION_PASSIVE),
"active" (CWMP_NOTIFICATION_ACTIVE)

Default Value

cwmp/attribute/<modified_parameter_name>/acs_only_access

Description AccessList assigned for parameter. If set - only ACS is allowed to change the parameter value. <modified_parameter_name> is the parameter name, where each '.' is replaced with '/'.

Relevant to DSLHome

Type boolean

Default Value False=0

cwmp/attribute/<modified_parameter_name>/notified_value

Description String representation of last value which was sent to ACS in the last successfull Inform. <modified_parameter_name> is the parameter name, where each '.' is replaced with '/'.

Relevant to DSLHome

Type text

Default Value

9

Dynamic DNS

The Dynamic DNS (DDNS) service enables you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessible from various locations on the Internet. Typically, when you connect to the Internet, your service provider assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, whilst maintaining a constant domain name. When using the DDNS service, each time the IP address provided by your ISP changes, the DNS database will change accordingly to reflect the change. In this way, even though your IP address will change often, your domain name will remain constant and accessible.

ddns/host/%/hostname **Description** Host name of the device to be updated to Dynamic DNS provider. **Relevant to** Dynamic DNS **Type** text[MAX_DOMAIN_NAME_LEN=255] **Default Value**
ddns/host/%/device **Description** Name of device to be updated. Same as **dev/<name>**. **Relevant to** Dynamic DNS **Type** text **Default Value**

ddns/host/%/username

Description Username to login to Dynamic DNS service.

Relevant to Dynamic DNS

Type text[MAX_USERNAME_LEN=100]

Default Value

ddns/host/%/password

Description Password to login to Dynamic DNS service. This entry is obscured.

Relevant to Dynamic DNS

Type text[MAX_PASSWORD_LEN=100]

Default Value

ddns/host/%/status

Description Current Dynamic DNS update status.

Relevant to DNS

Type one string of:
"updated" (MT_DDNS_UPDATED),
"not_updated" (MT_DDNS_NOT_UPDATED),
"error" (MT_DDNS_ERROR)

Default Value

ddns/host/%/last_ip

Description Last IP address updated to provider. This entry is read only.

Relevant to Dynamic DNS

Type ip

Default Value

ddns/host/%/last_update

Description Time of last update to provider (in seconds from epoch). This entry is read only.

Relevant to Dynamic DNS

Type integer

Default Value

ddns/host/%/provider/name

Description The name of Dynamic DNS provider.

Relevant to Dynamic DNS

Type text[MAX_FULLNAME_LEN=128]

Default Value

ddns/host/%/provider/offline

Description Provider specific parameter. Indicates whether Dynamic DNS host is set to offline. When false, the DNS host is set online. The exact behaviour of this parameter is provider dependent. Please refer to your provider's documentation.

Relevant to Dynamic DNS

Type boolean

Default Value False=0

ddns/host/%/provider/wildcard

Description Provider specific parameter. Indicates whether Dynamic DNS host is set to offline. When false, the DNS. Indicates whether the hostname wildcard is enabled. When enabled, this option allows *.yourhost.dyndns.org to point to yourhost.dyndns.org. The exact behaviour of this parameter is provider dependent. Please refer to your provider's documentation.

Relevant to Dynamic DNS

Type boolean

Default Value False=0

ddns/host/%/provider/mx

Description Provider specific parameter. The server to which mail for the updated domain should be sent. The exact behaviour of this parameter is provider dependent. Please refer to your provider's documentation.

Relevant to Dynamic DNS

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

ddns/host/%/provider/backup_mx

Description Provider specific parameter. Indicates whether the backup mail exchanger is enabled. If enabled, this option provides a secondary mail server to hold your e-mail for you should your main e-mail server go offline for any reason. The exact behaviour of this parameter is provider dependent. Please refer to your provider's documentation.

Relevant to Dynamic DNS

Type boolean

Default Value False=0

ddns/host/%/provider/response

Description The Dynamic DNS's response to the last Dynamic DNS request. The response depends on the provider.

Relevant to Dynamic DNS

Type text[]

Default Value

10

File Server

OpenRG can operate as a disk manager for storage devices connected via USB. Your home-network's LAN devices can share this storage device as a mapped network drive, and exchange information without directly accessing each other.

fs/enabled **Description** Indicates whether the file server is enabled. **Relevant to** File Server **Type** boolean **Default Value** True=1
fs/workgroup **Description** NetBIOS Workgroup Name. **Relevant to** FileServer **Type** text[MAX_DOMAIN_NAME_LEN=255] **Default Value** HOME

fs/codepage

Description Client codepage. This entry specifies the character encoding table to be used when reading files using the file server. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to FileServer

Type integer

Default Value 437

fs/auto_share/enabled

Description Indicates whether the automatic sharing feature is enabled.

Relevant to File Server

Type boolean

Default Value True=1

fs/auto_share/guest_access

Description Indicates the guest access mode of the automatic sharing feature.

Relevant to File Server

Type One string of:
"disabled" (FS_GUEST_ACCESS_DISABLED),
"rw" (FS_GUEST_ACCESS_RO),
"ro" (FS_GUEST_ACCESS_RW)

Default Value ro

fs/share/%/name

Description Share name needed for file sharing on Windows PCs.

Relevant to File Server

Type text[FSRV_MAX_SHARE_NAME_LEN=sizeof("_dev_sdz99")]

Default Value

fs/share/%/path

Description Share path starting at OpenRG root mount point(/mnt/fs).

Relevant to File Server

Type text

Default Value

fs/share/%/comment

Description Text seen next to a share when a client queries the server.

Relevant to File Server

Type text

Default Value

fs/share/%/permissions/%/id

Description The ID of a user or a group with access to this share. The type entry specifies whether it is a group or a user. The ID is the index of the user or group you used in **admin/user/%/** and **admin/group/%/**.

Relevant to File Server

Type integer

Default Value

fs/share/%/permissions/%/type

Description Specifies whether a group or a user has access to this share. The user or group ID is specified in the id entry.

Relevant to File Server

Type one string of:
"user" (ACCESS_OBJ_USER),
"group" (ACCESS_OBJ_GROUP)

Default Value

fs/share/%/permissions/%/access_level

Description Access level of the user or group with access to this share. The possible levels are admin, read-write or read only.

Relevant to File Server

Type one string of:
"admin" (ACCESS_ADMIN),
"rw" (ACCESS_RW),
"ro" (ACCESS_RO)

Default Value

11

File System Backup

11.1 General

backup/%/source **Description** Specifies the subdirectory to backup. **Relevant to** Backup System **Type** text[MAX_PATH_LEN=100] **Default Value**
backup/%/destination **Description** Specifies the location of the archive directory, under /mnt/fs/, where the chosen subdirectory will be backed up. **Relevant to** Backup System **Type** text[MAX_PATH_LEN=100] **Default Value**

11.2 Full

backup/%/full/type

Description How often to perform full backups.

Relevant to Backup System

Type one string of:
"disabled" (BACKUP_FREQ_DISABLED),
"daily" (BACKUP_FREQ_DAILY),
"weekly" (BACKUP_FREQ_WEEKLY),
"monthly" (BACKUP_FREQ_MONTHLY)

Default Value "disabled"

backup/%/full/day

Description Specifies the day of the month or the week to perform a full backup. For weekly backup, specify 0 (Sunday) to 6 (Saturday).

Relevant to Backup System

Type integer

Default Value

backup/%/full/hour

Description Specifies the hour to perform a full backup.

Relevant to Backup System

Type integer

Default Value

backup/%/full/last_time

Description Specifies the time that this backup was last performed (seconds since 1970).

Relevant to Backup System

Type time_t

Default Value

backup/%/full/location

Description Specifies the path of the last backup file, (under /mnt/fs).

Relevant to Backup System

Type text[MAX_PATH_LEN=100]

Default Value

11.3 Incremental

backup/%/incr/type

Description How often to perform incremental backups.

Relevant to Backup System

Type one string of:
"disabled" (BACKUP_FREQ_DISABLED),
"daily" (BACKUP_FREQ_DAILY),
"weekly" (BACKUP_FREQ_WEEKLY),
"monthly" (BACKUP_FREQ_MONTHLY)

Default Value "disabled"

backup/%/incr/day

Description Specifies the day of the month or the week to perform an incremental backup. For weekly backup, specify 0 (Sunday) to 6 (Saturday).

Relevant to Backup System

Type integer

Default Value

backup/%/incr/hour

Description Specifies the hour to perform an incremental backup.

Relevant to Backup System

Type integer

Default Value

backup/%/incr/last_time

Description Specifies the time that this backup was last performed (seconds since 1970).

Relevant to Backup System

Type time_t

Default Value

backup/%/incr/location

Description Specifies the path of the last backup file, (under /mnt/fs).

Relevant to Backup System

Type text[MAX_PATH_LEN=100]

Default Value

12

Firewall

After the security level is set, the firewall regulates the flow of data between the home network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through OpenRG) or rejected (barred from passing through OpenRG), according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing home users access to the Internet services that they require.

The firewall rules specify what types of services available on the Internet may be accessed from the home network and what types of services available in the home network may be accessed from the Internet. Each request for a service that the firewall receives, whether originating from the Internet or from a computer in the home network, is checked against the set of firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, then all subsequent data associated with this request (a "session") will also be allowed to pass, regardless of its direction.

- General -- general firewall entries (refer to Section 12.1).
- Reserved Ports -- reserved ports settings (refer to Section 12.2).
- Rule -- firewall rules entries for all rule types: parental control, remote access, access control, local server, special applications, DMZ host and transparent proxy (refer to Section 12.3).
- Log -- firewall log settings (refer to Section 12.4).
- Protect -- protection settings, such as SYN, UDP and ICMP flood protection and WinNuke protection (refer to Section 12.5).
- Policy -- filtering policies entries (refer to Section 12.6).
- Interception -- generic redirector entries (refer to Section 12.7).

12.1 General

fw/enabled

Description Indicates whether the firewall is enabled.

Relevant to WBM, fw_config

Type boolean

Default Value True=1

fw/filter/enabled

Description Indicates whether the firewall filtering operations are enabled.

Relevant to fw_config

Type boolean

Default Value True=1

fw/nat_ip_pool

Description Contains the pool of IPs, used by the firewall for static NAT/NAPT.

Relevant to Firewall

Type netobj

Default Value

12.2 Reserved Ports

Reserved Ports are used by OpenRG tasks and should not be used in the Network Address and Port Translation (NAPT) port pool.

fw/reserved_ports/%/protocol

Description Reserved port protocol type.

Relevant to Firewall

Type text[32] - "UDP";"TCP"

Default Value

fw/reserved_ports/%/port **Description** Reserved port number. **Relevant to** Firewall **Type** unsigned short **Default Value**
fw/reserved_ports/%/description **Description** Reserved port description. **Relevant to** Firewall **Type** string **Default Value**

12.3 Rule

12.3.1 General

In the following set of entries, the `<type>` must be one of the following rule types, represented as the corresponding string:

- Parental control – **prntl_ctrl**
- Remote access – **remote_access**
- Local Server – **loc_srv**
- Special applications – **special_apps**
- DMZ host – **dmz_host**
- Transparent proxy – **trans_proxy**

fw/rule/<type>/%/src/%/net_obj **Description** Reference to a global network object. Mutually exclusive with **fw/rule/<type>/%/src/%**. The network object entries are described in Chapter 24. **Relevant to** MGT, fw_config **Type** netobj **Default Value**

fw/rule/<type>/%/src/%

Description An inline source network object for generic firewall rule. Mutually exclusive with **fw/rule/<type>/%/src/%/net_obj**. The structure of an inline network object is identical to that of a global network object, and its entries are described in Chapter 24.

Relevant to MGT, fw_config

Type netobj

Default Value

fw/rule/<type>/%/dst

Description Destination network object for generic firewall rule. The network object entries are described in Chapter 24.

Relevant to MGT, fw_config

Type netobj

Default Value

fw/rule/<type>/%/rdir

Description Redirection network object for local server NAT rule. The network object entries are described in Chapter 24.

Relevant to MGT, fw_config

Type netobj

Default Value

fw/rule/<type>/%/services/%/service_id

Description Reference to a global service object (port and protocol data). Mutually exclusive with **fw/rule/<type>/%/services/%**. The service object entries are described in Chapter 35.

Relevant to MGT, fw_config

Type integer

Default Value

fw/rule/<type>/%/services/%

Description An inline service object (port and protocol data). Mutually exclusive with **fw/rule/<type>/%/services/%/service_id**. The structure of an inline service object is identical to that of a global service object, and its entries are described in Chapter 35.

Relevant to MGT, fw_config

Type service

Default Value

fw/rule/<type>/%/mac

Description The MAC address of the LAN client that added this rule.

Relevant to UPnP

Type mac

Default Value

fw/rule/<type>/%/enabled

Description Indicates whether the generic firewall rule is enabled.

Relevant to MGT, fw_config

Type boolean

Default Value

fw/rule/<type>/%/action

Description Generic firewall rule action for the packet.

Relevant to MGT, fw_config

Type one string of:
"drop" (FW_ACTION_DROP),
"accept" (FW_ACTION_ACCEPT),
"accept_stateless" (FW_ACTION_ACCEPT_STATELESS),
"nat" (FW_ACTION_NAT),
"napt" (FW_ACTION_NAPT),
"reject" (FW_ACTION_REJECT),
"redirect" (FW_ACTION_REDIRECT),
"call" (FW_ACTION_CALL),
"qos" (FW_ACTION_QOS)

Default Value

fw/rule/<type>/%/context

Description Generic firewall rule context for the packet that can be passed to the ALG. This entry is currently used only for Surf Control.

Relevant to MGT, fw_config

Type integer

Default Value

fw/rule/<type>/%/time_rule/%/time_rule_id

Description Reference to a global set of time enabling rules. Mutually exclusive with **fw/rule/<type>/%/time_rule**. The time rules object entries are described in Chapter 40.

Relevant to Firewall

Type integer

Default Value

fw/rule/<type>/%/time_rule

Description An inline time rule object (see entry /time_rule/% on page 275). Mutually exclusive with **fw/rule/<type>/%/time_rule/%/time_rule_id**. The structure of an inline time rule object is identical to that of a global time rule object, and its entries are described in Chapter 40.

Relevant to Firewall

Type time_set

Default Value

12.3.2 Special Applications

fw/rule/special_apps/%/connection_single

Description When set, allows only one returning data connection, otherwise enables multiple returning data connections.

Relevant to ipnat

Type boolean

Default Value

fw/rule/special_apps/%/open_wild

Description Indicates whether a state is opened with a wildcard IP for other IP addresses.

Relevant to ipnat

Type boolean

Default Value

fw/rule/special_apps/%/open_age

Description The state age in seconds.

Relevant to ipnat

Type integer

Default Value

12.3.3 Local Server

fw/rule/loc_srv/%/rule_owner

Description Description of the entity to which this rule applies.

Relevant to Firewall

Type enum service_src_t
LS_SRC_NO_OWNER = 0,
LS_SRC_WBM = 1,
LS_SRC_UPNP = 2,
LS_SRC_VOIP = 3,
LS_SRC_ALG = 4

Default Value

fw/rule/loc_srv/%/fwd_from

Description First port in forwarded port range for local server with port forwarding.

Relevant to Firewall

Type port

Default Value

fw/rule/loc_srv/%/fwd_to

Description Last port in forwarded port range for local server with port forwarding.

Relevant to Firewall

Type port

Default Value

12.4 Log

The 'Firewall Log' screen displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate through an administrative interface (WBM or Telnet terminal), firewall configuration and system start-up.

fw/log/spoofed

Description Indicates whether the firewall log records blocked spoofed connection trials.

Relevant to WBM, fw_config

Type boolean

Default Value False=0

fw/log/synflood

Description Indicates whether the firewall log records SYN flood attacks.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/udpflood

Description Indicates whether the firewall log records User Datagram Protocol (UDP) flood attacks.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/icmpflood

Description Indicates whether the firewall log records ICMP flood attacks.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/icmpreplay

Description Indicates whether the firewall log records ICMP error replay attacks.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/winnuke

Description Indicates whether the firewall log records WinNuke attacks.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/badfrag

Description Indicates whether the firewall log records fragmentation attacks.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/icmp_redirect

Description Indicates whether the firewall log records blocked ICMP redirect packets.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/icmp_multicast

Description Indicates whether the firewall log records blocked ICMP multicast packets.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/illegal_ops

Description Indicates whether the firewall log records blocked illegal options packets.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/broadcast

Description Indicates whether the firewall log records blocked broadcast packets.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/echo_chargen

Description Indicates whether the firewall log records echo chargen attacks.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/frag

Description Indicates whether the firewall log records dropped fragments.

Relevant to fw_config

Type boolean

Default Value False=0

fw/log/conn_blocked

Description Indicates whether the firewall log records blocked connection trials.

Relevant to WBM, fw_config

Type boolean

Default Value False=0

fw/log/accepted_wan_in

Description Indicates whether the firewall log records accepted packets/connections from the WAN to the LAN.

Relevant to WBM, fw_config

Type boolean

Default Value

fw/log/accepted_lan_out

Description Indicates whether the firewall log records accepted packets/connections from the LAN to the WAN.

Relevant to WBM, fw_config

Type boolean

Default Value

fw/log/remote_admin

Description Indicates whether the firewall log records remote-administration connection attempts.

Relevant to WBM, fw_config

Type boolean

Default Value

fw/log/conn_state

Description Indicates whether the firewall log records changes in connection states -- open/hooked/closed.

Relevant to WBM, fw_config

Type boolean

Default Value False=0

fw/log/wbm_blocked

Description Indicates whether the firewall log records blocked WBM login trials.

Relevant to WBM, fw_config

Type boolean

Default Value

fw/log/wbm_accepted

Description Indicates whether the firewall log records successful WBM login trials.

Relevant to WBM, fw_config

Type boolean

Default Value

fw/log/telnet_blocked

Description Indicates whether the firewall log records blocked Telnet login trials.

Relevant to WBM, fw_config

Type boolean

Default Value

fw/log/telnet_accepted

Description Indicates whether the firewall log records successful Telnet login trials.

Relevant to WBM, fw_config

Type boolean

Default Value

fw/log/conn_internal

Description Indicates whether the firewall log records internal log messages.

Relevant to WBM, fw_config

Type boolean

Default Value

12.5 Protect

fw/protect/synflood/enabled

Description Indicates whether the firewall SYN flood protection is enabled.

Relevant to Firewall

Type boolean

Default Value True=1

fw/protect/synflood/rate_limit

Description The rate limit (connections per second) for SYN flood protection.

Relevant to Firewall

Type integer

Default Value 30

fw/protect/udpflood/enabled

Description Indicates whethet the firewall UDP flood protection is enabled.

Relevant to Firewall

Type boolean

Default Value True=1

fw/protect/udpflood/rate_limit

Description The rate limit (connections per second) for UDP flood protection.

Relevant to Firewall

Type integer

Default Value 30

fw/protect/icmpflood/enabled

Description Indicates whether the firewall ICMP flood protection is enabled.

Relevant to Firewall

Type boolean

Default Value True=1

fw/protect/icmpflood/rate_limit

Description The rate limit (connections per second) for ICMP flood protection.

Relevant to Firewall

Type integer

Default Value 30

fw/protect/winnuke

Description Indicates whether the firewall WinNuke protection is enabled.

Relevant to fw_config

Type boolean

Default Value False=0

fw/protect/auth_reject/enabled

Description Indicates whether sending rejects on Ident/Auth (port 113) requests is enabled.

Relevant to fw_config

Type boolean

Default Value False=0

fw/protect/allow_rg_remote_administration_only

Description Indicates whether to block all non-remote adminstration to LAN, if the firewall on the LAN is enabled.

Relevant to Firewall

Type boolean

Default Value

12.6 Policy

fw/policy/ip_frags

Description Indicates whether to accept fragmented packets.

Relevant to WBM, fw_config

Type boolean

Default Value

fw/policy/acpt_output

Description Indicates whether to allow outbound packets as the default.

Relevant to WBM, fw_config

Type boolean

Default Value True=1

fw/policy/acpt_input

Description Indicates whether to allow inbound packets as the default.

Relevant to WBM, fw_config

Type boolean

Default Value

The following entries are for the advanced firewall:

fw/policy/active

Description The name of the active policy.

Relevant to Firewall

Type string

Default Value default

fw/policy/%/name

Description The name of the policy corresponding to the index.

Relevant to Firewall

Type text[GROUP_SIZE]

Default Value

fw/policy/%/description

Description The description of the policy corresponding to the index.

Relevant to Firewall

Type text

Default Value

fw/policy/%/chain/%/name

Description The internal name of the chain corresponding to the policy index.

Relevant to Firewall

Type text[GROUP_SIZE]

Default Value

fw/policy/%/chain/%/description

Description Readable description of the chain corresponding to the policy index.

Relevant to Firewall

Type text[GROUP_SIZE]

Default Value

fw/policy/%/chain/%/type

Description The type of the chain, used for WBM categorization/ordering of display.

Relevant to WBM

Type enum fw_chain_type_t
CHAIN_PRE = 1,
CHAIN_DEV = 2,
CHAIN_POST = 3,
CHAIN_SYSTEM = 4,
CHAIN_ROOT = 5,
CHAIN_NAT_NAPT = 6

Default Value

fw/policy/%/chain/%/activate/if

Description The interface on which to force the firewall.

Relevant to Firewall

Type text[IFNAME_SIZE]

Default Value

fw/policy/%/chain/%/activate/wildcard_if

Description The interfaces that matches the wildcard group, on which to force the firewall.

Relevant to Firewall

Type enum wildcard_if_t
WC_IF_REGULAR = 0,
WC_IF_CH_WAN = 1,
WC_IF_CH_AGGR_LAN = 2,
WC_IF_ALL = 3,
WC_IF_LAN = 4,
WC_IF_WAN = 5,
WC_IF_DMZ = 6,
WC_IF_WAN_ACCESS_DEV = 7

Default Value WC_IF_REGULAR

fw/policy/%/chain/%/dev

Description Device to which this chain is associated. Only for CHAIN_DEV chains.

Relevant to WBM

Type text[IFNAME_SIZE]

Default Value

fw/policy/%/chain/%/output

Description Indicates whether the chain is for output or input rules.

Relevant to WBM

Type boolean

Default Value

fw/policy/%/chain/%/all_packets

Description Indicates that this chain works on all packets (whether on on connection or not)

Relevant to WBM

Type boolean

Default Value

fw/policy/%/chain/%/rule/%/enabled

Description Indicates whether the specified rule in the chain is enabled.

Relevant to Firewall

Type boolean

Default Value

fw/policy/%/chain/%/rule/%/rule_id

Description The ID of the rule, which is displayed at the WBM. Stays with the rule even if its order is changed.

Relevant to Firewall

Type integer

Default Value

fw/policy/%/chain/%/rule/%/description

Description Description of the specified rule.

Relevant to SSI

Type text

Default Value

fw/policy/%/chain/%/rule/%/match/if

Description The interface, if exists, through which the matching packet is sent/received.

Relevant to Firewall

Type text[IFNAME_SIZE]

Default Value

fw/policy/%/chain/%/rule/%/match/wildcard_if

Description The interface type, if any, through which the packet matching the rule is sent/ received. The interface type belongs to the wild card group.

Relevant to Firewall

Type enum wildcard_if_t
WC_IF_REGULAR = 0,
WC_IF_ALL = 3,
WC_IF_LAN = 4,
WC_IF_WAN = 5,
WC_IF_DMZ = 6,
WC_IF_WAN_ONLY_DEV = 7

Default Value WC_IF_REGULAR

fw/policy/%/chain/%/rule/%/match/if_list/<if_entry>

Description Interface list, through which the packet matching the rule is sent/received.
Each interface entry may specify a specific interface name or a wildcard group optionally with a specified attribute. Wildcard group has the following format: <wildcard_name>[,<flags>...].
<wildcard_name> is one of the following string:
"regular" (= WC_IF_REGULAR),
"ch_wan" (= WC_IF_CH_WAN),
"ch_aggr_lan" (= WC_IF_CH_AGGR_LAN),
"all_devices" (= WC_IF_ALL),
"all_lan" (= WC_IF_LAN),
"all_wan" (= WC_IF_WAN),
"all_dmz" (= WC_IF_DMZ),
"wan_only_dev" (= WC_IF_WAN_ONLY_DEV).
<flags> is one of the following string:
"wireless" (= WC_IF_FLAG_WIRELESS),
"non_wireless" (= WC_IF_FLAG_NON_WIRELESS),
"web_auth" (= WC_IF_FLAG_WEB_AUTH),
"non_web_auth" (= WC_IF_FLAG_NON_WEB_AUTH),
"nz" (= WC_IF_FLAG_NZ),
"non_nz" (= WC_IF_FLAG_NON_NZ),
"has_ip" (= WC_IF_FLAG_HAS_IP),
"has_no_ip" (= WC_IF_FLAG_HAS_NO_IP).

Relevant to Firewall

Type string

Default Value

fw/policy/%/chain/%/rule/%/match/mac_src

Description The source MAC address, if any, of the packet matching the rule.

Relevant to Firewall

Type mac

Default Value

fw/policy/%/chain/%/rule/%/match/mac_dst

Description The destination MAC address, if any, of the packet matching the rule.

Relevant to Firewall

Type mac

Default Value

fw/policy/%/chain/%/rule/%/match/mac_protocol

Description The next protocl field of the MAC header, if any, of the packet matching the rule.

Relevant to Firewall

Type mac

Default Value

fw/policy/%/chain/%/rule/%/match/wildcard_ip_src

Description The source IP address type with which the packet's IP is matched. The IP address type is predefined by the wild card group.

Relevant to Firewall

Type enum wildcard_ip_t
WC_IP_REGULAR = 0,
WC_IP_MAIN_WAN = 1,
WC_IP_LAN = 2,
WC_IP_FIRST_LAN = 3,
WC_IP_OPENRG_IP = 7

Default Value WC_IP_REGULAR

fw/policy/%/chain/%/rule/%/match/ip_src_start

Description Start of source IP address range with which the packet's IP is matched. If a single IP is specified, then the start and end of the IP range will have the same value. If 'Any Address' is specified, the start value will be represented as 0.0.0.0 and the end value will be represented as 255.255.255.255.

Relevant to Firewall

Type ip

Default Value

fw/policy/%/chain/%/rule/%/match/ip_src_end

Description End of source IP address range with which the packet's IP is matched.

Relevant to Firewall

Type ip

Default Value

fw/policy/%/chain/%/rule/%/match/wildcard_ip_dst

Description The destination IP address type with which the packet's IP is matched. The IP address type is predefined by the wild card group.

Relevant to Firewall

Type enum wildcard_ip_t
WC_IP_REGULAR = 0,
WC_IP_MAIN_WAN = 1,
WC_IP_LAN = 2,
WC_IP_FIRST_LAN = 3,
WC_IP_OPENRG_IP = 7

Default Value WC_IP_REGULAR

fw/policy/%/chain/%/rule/%/match/ip_dst_start

Description Start of destination IP address range with which the packet's IP is matched.

Relevant to Firewall

Type ip

Default Value

fw/policy/%/chain/%/rule/%/match/ip_dst_end

Description End of destination IP address range with which the packet's IP is matched.

Relevant to Firewall

Type ip

Default Value

fw/policy/%/chain/%/rule/%/match/host_src

Description Source host name of the packet matching the rule.

Relevant to Firewall

Type string

Default Value

fw/policy/%/chain/%/rule/%/match/host_dst

Description Destination host name of the packet matching the rule.

Relevant to Firewall

Type string

Default Value

fw/policy/%/chain/%/rule/%/match/addr_in_list/dir

Description Determines whether source or destination is checked in this match rule.

Relevant to Firewall

Type one string of:
"src" (ADDR_LIST_DIR_SRC),
"dst" (ADDR_LIST_DIR_DST)

Default Value

fw/policy/%/chain/%/rule/%/match/addr_in_list/type

Description Determines whether the list contains MAC addresses, IP addresses or host anmes.

Relevant to Firewall

Type one string of:
"ip" (ADDR_LIST_TYPE_IP),
"mac" (ADDR_LIST_TYPE_MAC),
"host" (ADDR_LIST_TYPE_HOST)

Default Value

fw/policy/%/chain/%/rule/%/match/addr_in_list/is_ram

Description If not zero then the list should be read from rg_conf_ram, otherwise from rg_conf.

Relevant to Firewall

Type boolean

Default Value

fw/policy/%/chain/%/rule/%/match/addr_in_list/list

Description rg_conf or rg_conf_ram path of the address list.

Relevant to Firewall

Type string

Default Value

fw/policy/%/chain/%/rule/%/match/addr_in_list/index

Description Relevant for hostname list. If exists then the list is an indexed list with child elements with this name (e.g. /jnet/web_server/0/<index>/<hostname1>, /jnet/web_server/1/<index>/<hostname2> ...), otherwise the list is unindexed (e.g. /jnet/web_server/<hostname1>, /jnet/web_server/<hostname2> ...).

Relevant to Firewall

Type string

Default Value

fw/policy/%/chain/%/rule/%/match/ip_option

Description IP option, if exists, with which to match packets.

Relevant to Firewall

Type Flags:
FW_IP_OPT_LSRR 1$<<$0 (Loose Source Routing)
FW_IP_OPT_SSRR 1$<<$1 (String Source Routing)
FW_IP_OPT_RR 1$<<$2 (Record Route)
FW_IP_OPT_TIMESTAMP 1$<<$3 (Timestamp)
FW_IP_OPT_SEC 1$<<$4 (Security)

Default Value

fw/policy/%/chain/%/rule/%/match/services/%/service_id

Description Reference to a global service object (port and protocol data) with which to match packets. Mutually exclusive with **fw/policy/%/chain/%/rule/%/match/services/%**. The service object entries are described in Chapter 35. Only for TCP, UDP and ICMP.

Relevant to Firewall

Type integer

Default Value

fw/policy/%/chain/%/rule/%/match/services/%

Description An inline service object (port and protocol data) with which to match packets. Mutually exclusive with **fw/policy/%/chain/%/rule/%/match/services/%/service_id**. The structure of an inline service object is identical to that of a global service object, and its entries are described in Chapter 35.

Relevant to Firewall

Type service

Default Value

fw/policy/%/chain/%/rule/%/match/tcp_flags_value

Description Value of the TCP flags against which to match the packet, together with the mask of the TCP flags, described in the following entry.

Relevant to Firewall

Type text[FLAG_NUM]

Default Value

fw/policy/%/chain/%/rule/%/match/tcp_flags_mask

Description Mask of the TCP flags against which to match the packet, together with the value of the TCP flags, described in the previous entry.

Relevant to Firewall

Type text[FLAG_NUM]

Default Value

fw/policy/%/chain/%/rule/%/match/dscp/value

Description Value of DSCP to match against.

Relevant to Firewall

Type integer

Default Value

fw/policy/%/chain/%/rule/%/match/dscp/mask

Description Mask for DSCP value to match against.

Relevant to Firewall

Type integer

Default Value

fw/policy/%/chain/%/rule/%/match/priority

Description Packet priority value to match against.

Relevant to Firewall

Type integer

Default Value

fw/policy/%/chain/%/rule/match/length/type

Description Match packets with either entire packet or data section length

Relevant to QoS

Type one string of:
"packet" (PKT_MATCH_LENGTH_PACKET),
"data" (PKT_MATCH_LENGTH_DATA)

Default Value

fw/policy/%/chain/%/rule/match/length/from

Description Match packets with length between from and to

Relevant to QoS

Type 0 - 65535

Default Value

fw/policy/%/chain/%/rule/match/length/to

Description Match packets with length between from and to

Relevant to QoS

Type 0 - 65535

Default Value

fw/policy/%/chain/%/rule/%/match/src_is_exclude

Description Return true only for packets NOT matched by the src net objects.

Relevant to Firewall

Type boolean

Default Value

fw/policy/%/chain/%/rule/%/match/dst_is_exclude

Description Return true only for packets NOT matched by the dst net objects.

Relevant to Firewall

Type boolean

Default Value

fw/policy/%/chain/%/rule/%/match/dscp_is_exclude

Description Return true only for packets NOT matched by the DSCP value/mask.

Relevant to Firewall

Type boolean

Default Value

fw/policy/%/chain/%/rule/%/match/priority_is_exclude

Description Return true only for packets NOT matched by the priority value.

Relevant to Firewall

Type boolean

Default Value

fw/policy/%/chain/%/rule/%/match/length_is_exclude

Description Return true only for packets NOT matched by a packet length.

Relevant to Firewall

Type boolean

Default Value

fw/policy/%/chain/%/rule/%/match/services_is_exclude

Description Return true only for packets NOT matched by the protocol.

Relevant to Firewall

Type boolean

Default Value

fw/rule/%/chain/%/rule/%/time_rule/time_rule_id

Description Reference to a global set of time enabling rules with which to match the packet. Mutually exclusive with **fw/policy/%/chain/%/rule/%/time_rule**. The time rules object entries are described in Chapter 40.

Relevant to Firewall

Type integer

Default Value

fw/policy/%/chain/%/rule/%/time_rule

Description An inline time rule object with which to match the packet (see entry /time_rule/% on page 275). Mutually exclusive with **fw/rule/%/chain/%/rule/%/time_rule/time_rule_id**. The structure of an inline time rule object is identical to that of a global time rule object, and its entries are described in Chapter 40.

Relevant to Firewall

Type integer

Default Value

fw/policy/chain/%/rule/%/rule_owner

Description Description of the entity to which this rule applies.

Relevant to Firewall

Type string

Default Value

fw/policy/%/chain/%/rule/%/action/type

Description Action to apply when rule matches the packet.

Relevant to Firewall

Type one string of:
"drop" (FW_ACTION_DROP),
"accept_conn" (FW_ACTION_ACCEPT_CONN),
"accept_packet" (FW_ACTION_ACCEPT_PACKET),
"nat" (FW_ACTION_NAT),
"napt" (FW_ACTION_NAPT),
"reject" (FW_ACTION_REJECT),
"redirect" (FW_ACTION_REDIRECT),
"call" (FW_ACTION_CALL),
"qos_conn" (FW_ACTION_QOS_CONN),
"qos_packet" (FW_ACTION_QOS_PACKET),
"call_sticky" (FW_ACTION_CALL_STICKY),
"drop_reply" (FW_ACTION_DROP_REPLY),
"bridge_classify" (FW_ACTION_BRIDGE_CLASSIFY),
"return" (FW_ACTION_RETURN),
"alg" (FW_ACTION_ALG)

Default Value

fw/policy/%/chain/%/rule/%/action/nat/%/net_obj

Description NAT IPs to be used by this rule. Reference to a NAT network object. Mutually exclusive with **fw/policy/%/chain/%/rule/%/action/napt/%**. The network object entries are described in Chapter 24.

Relevant to Firewall

Type 4.2

Default Value

fw/policy/%/chain/%/rule/%/action/nat/%

Description NAT IPs to be used by this rule. An inline source network object for NAPT IP. Mutually exclusive with **fw/policy/%/chain/%/rule/%/action/napt/%/net_obj**. The structure of an inline network object is identical to that of a global network object, and its entries are described in Chapter 24.

Relevant to Firewall

Type 4.2

Default Value

fw/policy/%/chain/%/rule/%/action/napt/%/net_obj

Description NAPT IPs to be used by this rule. Reference to a NAT network object. Mutually exclusive with **fw/policy/%/chain/%/rule/%/action/napt/%**. The network object entries are described in Chapter 24.

Relevant to Firewall

Type 4.2

Default Value

fw/policy/%/chain/%/rule/%/action/napt/%

Description NAPT IPs to be used by this rule. An inline source network object for NAPT IP. Mutually exclusive with **fw/policy/%/chain/%/rule/%/action/napt/%/net_obj**. The structure of an inline network object is identical to that of a global network object, and its entries are described in Chapter 24.

Relevant to Firewall

Type 4.2

Default Value

fw/policy/%/chain/%/rule/%/action/set_priority

Description The QoS priority of the rule. The value '-1' indicates there is no priority for this rule.

Relevant to Firewall

Type -1 to 7

Default Value -1

fw/policy/%/chain/%/rule/%/action/set_dscp

Description Differentiated Services Code Point (DSCP) value to be marked on packets that match the rule. The value '-1' indicates not to mark any DSCP value.

Relevant to Firewall

Type -1 to 63

Default Value -1

fw/policy/%/chain/%/rule/%/action/alg

Description ALG to be used with this rule.

Relevant to Firewall

Type one string of:
"none" (ALG_NONE),
"ftp" (ALG_FTP),
"irc" (ALG_IRC),
"port_trigger" (ALG_PORT_TRIGGER),
"ras" (ALG_RAS),
"csl" (ALG_CSL),
"h245" (ALG_H245),
"sip_udp" (ALG_SIP_UDP),
"sip_tcp" (ALG_SIP_TCP),
"rtsp" (ALG_RTSP),
"pptp" (ALG_PPTP),
"ipsec" (ALG_IPSEC),
"l2tp" (ALG_L2TP),
"aim" (ALG_AIM),
"msn" (ALG_MSN),
"gre" (ALG_GRE),
"dns" (ALG_DNS),
"dummy" (ALG_DUMMY),
"dhcp" (ALG_DHCP),

Default Value

fw/policy/%/chain/%/rule/%/action/alg_args

Description ALG context to pass to the ALG when a connection is opened.

Relevant to Firewall

Type binary

Default Value

fw/policy/%/chain/%/rule/%/action/context

Description User-defined context related to the action when action is **FW_ACTION_REDIRECT**.

Relevant to Firewall

Type unsigned integer

Default Value

fw/policy/%/chain/%/rule/%/action/log

Description Indicates whether to log packets matched by this rule.

Relevant to Firewall

Type boolean

Default Value

fw/policy/%/chain/%/rule/%/action/addr_start

Description IP Address to use as start of IP range for NAT/NAPT when the rule is **FW_ACCEPT_(NAT|NAPT)**, or as redirection IP if the rule is **FW_ACCEPT_REDIRECT**.

Relevant to Firewall

Type ip

Default Value

fw/policy/%/chain/%/rule/%/action/addr_end

Description IP Address to use as end of IP range for NAT/NAPT when the rule is **FW_ACCEPT_(NAT|NAPT)**.

Relevant to Firewall

Type ip

Default Value

fw/policy/%/chain/%/rule/%/action/wildcard_ip

Description Predefined IP Addresses to use as redirection IP when the rule is **FW_ACCEPT_REDIRECT**.

Relevant to Firewall

Type enum wildcard_ip_t
WC_IP_REGULAR = 0,
WC_IP_MAIN_WAN = 1,
WC_IP_LAN = 2,
WC_IP_FIRST_LAN = 3,
WC_IP_OPENRG_IP = 7

Default Value

fw/policy/%/chain/%/rule/%/action/ports_start

Description Start of TCP/UDP port range to use for NAPT when the rule is **FW_ACCEPT_NAPT** or for redirection when the rule is **FW_ACCEPT_REDIRECT**.

Relevant to Firewall

Type integer

Default Value

fw/policy/%/chain/%/rule/%/action/ports_end

Description End of TCP/UDP port range to use for NAPT.

Relevant to Firewall

Type integer

Default Value

fw/policy/%/chain/%/rule/%/action/chain

Description If the action is **FW_ACTION_CALL**, the chain that is to be called.

Relevant to Firewall

Type text[GROUP_SIZE]

Default Value

fw/policy/%/chain/%/rule/%/action/value

Description If the action is **FW_ACTION_RETURN**, the value which is returned from the chain.

Relevant to Firewall

Type text[GROUP_SIZE]

Default Value

12.7 Interception

Interception entries define firewall chains. Each chain is located under the path **interception/%**. The chains are traversed from the lower numbered chain upward. The following chains are defined:

- Web Authentication – **20**
- Nation Zone – **30**

interception/%/enabled

Description Indicates whether the chain is enabled.

Relevant to Firewall

Type boolean

Default Value

interception/%/if

Description The interface, if exists, through which the matching packet is sent/received.

Relevant to Firewall

Type text[IFNAME_SIZE]

Default Value

interception/%/wildcard_if

Description The interface type, if any, through which the packet matching the rule is sent/ received. The interface type belongs to the wild card group.

Relevant to Firewall

Type enum wildcard_if_t
WC_IF_REGULAR = 0,
WC_IF_ALL = 3,
WC_IF_LAN = 4,
WC_IF_WAN = 5,
WC_IF_DMZ = 6,
WC_IF_WAN_ONLY_DEV = 7

Default Value

interception/%/if_list/<if_entry>

Description Interface list, through which the packet matching the rule is sent/received.
Each interface entry may specify a specific interface name or a wildcard group optionally with a specified attribute. Wildcard group has the following format: <wildcard_name>[,<flags>...].
<wildcard_name> is one of the following string:
"regular" (= WC_IF_REGULAR),
"ch_wan" (= WC_IF_CH_WAN),
"ch_aggr_lan" (= WC_IF_CH_AGGR_LAN),
"all_devices" (= WC_IF_ALL),
"all_lan" (= WC_IF_LAN),
"all_wan" (= WC_IF_WAN),
"all_dmz" (= WC_IF_DMZ),
"wan_only_dev" (= WC_IF_WAN_ONLY_DEV).
<flags> is one of the following string:
"wireless" (= WC_IF_FLAG_WIRELESS),
"non_wireless" (= WC_IF_FLAG_NON_WIRELESS),
"web_auth" (= WC_IF_FLAG_WEB_AUTH),
"non_web_auth" (= WC_IF_FLAG_NON_WEB_AUTH),
"nz" (= WC_IF_FLAG_NZ),
"non_nz" (= WC_IF_FLAG_NON_NZ),
"has_ip" (= WC_IF_FLAG_HAS_IP),
"has_no_ip" (= WC_IF_FLAG_HAS_NO_IP).

Relevant to Firewall

Type string

Default Value

interception/%/output

Description Indicates the direction in which this chain applies for on the devices. Non zero means out direction.

Relevant to Firewall

Type boolean

Default Value

interception/%/redirect/url

Description The url the user should be redirected to when intercepted. Empty url denotes redirection to OpenRG.

Relevant to Firewall

Type string

Default Value

interception/%/redirect/params

Description Parameters added to the redirection. The parameters should be in HTTP-escaped form.

Relevant to Firewall

Type string

Default Value

interception/%/rule/%

Description Rules of the chain. The syntax is the same as specified in Section 12.6 for entries under fw/policy/%/chain/%/rule/%

Relevant to Firewall

Type

Default Value

13

FTP Server

OpenRG can operate as a File Transfer Protocol (FTP) server, allowing users and guests to access its internal disks, to easily (but securely) exchange files. OpenRG's FTP access consists of two levels:

- User Access Registered users can access predefined directories, which are protected by their username and password.
- Anonymous Access Guests can access predefined public directories. This feature allows you, for example, to let guests download a certain file.

ftp_server/enabled **Description** Is FTP server enabled **Relevant to** FTP Server **Type** boolean **Default Value** False=0
ftp_server/wan **Description** Indicates whether the FTP server is allowed to be accessed from the WAN. **Relevant to** FTP Server **Type** boolean **Default Value** False=0

ftp_server/idle

Description Maximum time in seconds the remote client can spend between FTP commands.

Relevant to FTP Server

Type integer (30-65535)

Default Value 300

ftp_server/is_max_clients

Description Is there a limit to the number of clients that can connect simultaneously to the FTP server. If there is, the number is specified under **ftp_server/max_clients**.

Relevant to FTP Server

Type boolean

Default Value False=0

ftp_server/max_clients

Description Maximum number of clients that can be connected to the FTP server. Relevant only if **ftp_server/is_max_clients** is true.

Relevant to FTP Server

Type integer (1-65535)

Default Value 0

ftp_server/is_common_root_dir

Description If true the root directory for all users will be the common directory. Otherwise each user's home directory is used.

Relevant to FTP Server

Type boolean

Default Value False=0

ftp_server/common_root_dir

Description The common directory all users will use if **ftp_server/is_common_root_dir** is true.

Relevant to FTP Server

Type text[MAX_PATH_LEN=100]

Default Value

ftp_server/welcome_msg

Description FTP Servers Welcome message on login.

Relevant to FTP Server

Type text

Default Value

ftp_server/anonymous/lan/enabled

Description Is anonymous FTP enabled from the LAN.

Relevant to FTP Server

Type boolean

Default Value False=0

ftp_server/anonymous/lan/root_dir

Description Root directory of anonymous FTP from the LAN.

Relevant to FTP Server

Type text[MAX_PATH_LEN=100]

Default Value home/ftp

ftp_server/anonymous/wan/enabled

Description Is anonymous FTP enabled from the WAN.

Relevant to FTP Server

Type boolean

Default Value False=0

ftp_server/anonymous/wan/dir

Description Root directory of anonymous FTP from the WAN.

Relevant to FTP Server

Type text[MAX_PATH_LEN=100]

Default Value home/ftp

14

Hybrid Bridge

OpenRG supports a hybrid bridge model, meaning it allows a configuration in which lan clients can be pre-defined as 'bridged clients', along with the default 'routed client' definition. When a client is defined as a 'bridged client', OpenRG behaves like a bridge regarding all traffic related to this client.

bridge/dhcp/%/uid **Description** the matched user id value **Relevant to** bridge **Type** string **Default Value**
bridge/dhcp/%/cid **Description** the matched client id value **Relevant to** bridge **Type** string **Default Value**

bridge/dhcp/%/vendor_id

Description the matched vendor id value

Relevant to bridge

Type string

Default Value

bridge/dhcp/%/hardware_mac

Description the source mac address that matched the dhcp option

Relevant to bridge

Type mac

Default Value

bridge/rules

Description Hybrid bridge classification rules. The structure is identical to that of firewall rules (fw/policy/%/chain). Its entries are described in Section 12.6.

Relevant to bridge

Type string

Default Value

bridge/rules/%/action/bridge

Description The bridge to which we send the traffic that matches this rule.

Relevant to bridge

Type string

Default Value

15

Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec) is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks. The IPSec protocols include:

- AH (Authentication Header) provides packet-level authentication.
- ESP (Encapsulating Security Payload) provides encryption and authentication.
- IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two services.

Services supported by the IPSec protocols (AH, ESP) include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering), and replay protection (defense against unauthorized resending of data). IPSec also specifies methodologies for key management. Internet Key Exchange (IKE), the IPSec key management protocol, defines a series of steps to establish keys for encrypting and decrypting information; it defines a common language on which communications between two parties is based. Developed by the Internet Engineering Task Force (IETF), IPSec and IKE together standardize the way data protection is performed, thus making it possible for security systems developed by different vendors to interoperate.

- General -- general IPSec entries (refer to Section 15.1).
- Block IP -- entries for blocking unauthorized IP packets to OpenRG (refer to Section 15.2).
- RSA -- RSA key settings (refer to Section 15.3).
- Log -- IPSec and IKE log settings (refer to Section 15.4).

15.1 General

ipsec/disable_anti_replay

Description Indicates whether anti-replay protection is disabled. When this entry is false, anti-replay is enabled. Anti-replay verifies that a certain packet is not received more than once.

Relevant to IPSec

Type boolean

Default Value

15.2 Block IP

ipsec/block_ip/enabled

Description Indicates whether block IP mechanism is enabled. The mechanism enables blocking an unauthorized IP that is rejected a number of times. The number of times is specified in **ipsec/block_ip/rejet_num**. The period the IP is blocked is specified in **ipsec/block_ip/period**.

Relevant to IPSec

Type boolean

Default Value True=1

ipsec/block_ip/reject_num

Description The number of Internet Key Exchange (IKE) rejects before a peer IP is blocked. This entry is relevant only if **ipsec/block_ip/enabled** is true.

Relevant to IPSec

Type integer

Default Value 5

ipsec/block_ip/period

Description The number of seconds an IP is blocked due to IKE rejects, before the counter is reset. This entry is relevant only if **ipsec/block_ip/enabled** is true.

Relevant to IPSec

Type integer

Default Value 60

15.3 RSA

ipsec/key/rsa/public

Description RSA key: public key. An RSA public key consists of an encryption exponent (**ipsec/key/rsa/public_exponent**) and an arithmetic modulus (**ipsec/key/rsa/modulus**).

Relevant to IPSec

Type text[1024]

Default Value

ipsec/key/rsa/modulus

Description RSA key: modulus. This is the arithmetic modulus part of the RSA public key.

Relevant to IPSec

Type text[1024]

Default Value

ipsec/key/rsa/public_exponent

Description RSA key: public exponent. This is the encryption exponent part of the RSA public key.

Relevant to IPSec

Type text[1024]

Default Value

ipsec/key/rsa/private_exponent

Description RSA key: private exponent. This is the encryption exponent part of the RSA private key.

Relevant to IPSec

Type text[1024]

Default Value

ipsec/key/rsa/prime1

Description RSA key: the first prime number (p) used in RSA key.

Relevant to IPSec

Type text[1024]

Default Value

ipsec/key/rsa/prime2

Description RSA key: the second prime number (q) used in RSA key.

Relevant to IPSec

Type text[1024]

Default Value

ipsec/key/rsa/exponent1

Description RSA key: the first exponent used in RSA key.

Relevant to IPSec

Type text[1024]

Default Value

ipsec/key/rsa/exponent2

Description RSA key: the second exponent used in RSA key.

Relevant to IPSec

Type text[1024]

Default Value

ipsec/key/rsa/coefficient

Description RSA key: the coefficient used in RSA key.

Relevant to IPSec

Type text[1024]

Default Value

15.4 Log

15.4.1 Internet Key Exchange Log

The Internet Key Exchange (IKE) Log can be used to identify and analyze the history of IKE messages.

ipsec/log/raw_bytes **Description** Indicates whether to show the raw bytes of messages in the IKE log. **Relevant to** IPSec **Type** boolean **Default Value** False=0
ipsec/log/encryption **Description** Indicates whether to show the encryption and decryption of messages in the IKE log. **Relevant to** IPSec **Type** boolean **Default Value** False=0
ipsec/log/input **Description** Indicates whether to show the structure of input messages in the IKE log. **Relevant to** IPSec **Type** boolean **Default Value** False=0
ipsec/log/output **Description** Indicates whether to show the structure of output messages in the IKE log. **Relevant to** IPSec **Type** boolean **Default Value** False=0

ipsec/log/pluto

Description Indicates whether to show Pluto's decision making in the IKE log. Pluto is an IPSec IKE keying daemon.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/klips

Description Indicates whether to show Pluto's interaction with Kernel IPSec Support (KLIPS) in IKE log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/private_keys

Description Indicates whether to show debugging output with private keys in IKE log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/verbose_ike_reject_info

Description Indicates whether to show verbose IKE reject packets in log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/no_rate_limit_ike

Description Indicates whether to show all IKE messages ignoring rate limit in IKE log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/nat_traversal

Description Indicates whether to show debugging output for NAT traversal

Relevant to IPSec

Type boolean

Default Value False=0

15.4.2 IPSec Log

The IPSec Log can be used to identify and analyze the history of the IPSec package commands, attempts to create connections, etc.

ipsec/log/tunneling

Description Indicates whether to show tunnelling code in IPSec log. The tunneling code is usually displayed together with the transmit code (**ipsec/log/transmit**).

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/transmit

Description Indicates whether to show transmit code in IPSec log. Transmit code includes packet information. The transmit code is usually displayed together with the tunneling code (**ipsec/log/tunneling**).

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/userspace

Description Indicates whether to show userspace communication code in IPSec log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/transform

Description Indicated whether to show transform selection and manipulation code in IPSec log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/eroute

Description Indicates whether to show the eroute table manipulation code in IPSec log. The eroute table consists of information regarding internal routes in IPSec and includes a security policy index, which is later used in Security Association (SA) table (**ipsec/log/sa**).

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/sa

Description Indicates whether to show SA table manipulation code in IPSec log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/radij

Description Indicates whether to show radij tree manipulation code in IPSec log. Radij code decides whether some IPSec transforms should be applied to an outgoing packet.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/enc_transform

Description Indicates whether to show encryptions transforms code in IPSec log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/auth_transform

Description Indicates whether to show authentication transforms code in IPSec log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/recieve

Description Indicates whether to show receive code in IPSec log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/compression

Description Indicates whether to show IP compression transforms code in IPSec log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/more

Description Indicates whether to show even more information in IPSec log.
Note: This will print authentication and encryption keys in the logs. This will probably trample the 4k kernel printk buffer giving inaccurate output.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/klips_reject

Description Indicates whether to show information about rejected packets in IPSec log.

Relevant to IPSec

Type boolean

Default Value False=0

ipsec/log/no_rate_limit_ipsec

Description Indicates whether to print all IPSec messages in IPSec log, ignoring rate limit.

Relevant to IPSec

Type boolean

Default Value False=0

16

IPv6

At the current stage of the IP network technology, an IPv4 WAN has no inherent support of Internet Protocol version 6 (IPv6). As a result, two IPv6 hosts cannot communicate with each other directly, if they are located at two separate IPv6 LANs interconnected by an IPv4 WAN (either the global Internet or a corporate WAN).

The easiest way to solve this problem is to establish a special network mechanism, called *IPv6-over-IPv4 Tunneling*. This mechanism encapsulates IPv6 packets into IPv4 packets, in order to transmit them via an IPv4 WAN to the target IPv6 host. OpenRG successfully implements the IPv6 technology.

ipv6/enabled

Description Enable IPv6.

Relevant to WBM, IPv6

Type boolean

Default Value True=1

17

Jungo.net

jnet/enabled **Description** Indicates whether the Jungo.net client is connected to JRMS and the management is enabled. **Relevant to** JNET_CLIENT **Type** boolean **Default Value** True=1
jnet/url **Description** The URL to the Jungo.net server **Relevant to** JNET_CLIENT **Type** text[MAX_DOMAIN_NAME_LEN=255] **Default Value** https://jnet.jungo.net/jnet_rg2.cgi
jnet/wbm_server **Description** The URL to the Jungo.net portal **Relevant to** JNET_CLIENT **Type** text[MAX_DOMAIN_NAME_LEN=255] **Default Value** www.jungo.net

jnet/wbm_server_scheme

Description Describes the protocol that is used for browsing in the Jungo.net portal.

Relevant to JNET_CLIENT

Type text

Default Value http

jnet/username

Description The username used to authenticate OpenRG when connecting to JRMS.

Relevant to JNET_CLIENT

Type text

Default Value

jnet/password

Description The password used to authenticate OpenRG when connecting to JRMS.

Relevant to JNET_CLIENT

Type text

Default Value

jnet/domain/id

Description The identifier of the JRMS domain to which OpenRG belongs.

Relevant to JNET_CLIENT

Type domain

Default Value Jungo.net

jnet/set_by_user

Description The Jungo.net username and password can either be set manually by the user during the installation wizard process, or detected and set automatically by JRMS server.

Relevant to JNET_CLIENT

Type boolean

Default Value False=0

18

Kerberos

kerb/nms/name **Description** NMS principle name (without realm). **Relevant to** CH Kerberos, main task **Type** text (length not bound) **Default Value**
kerb/ap_timeout **Description** Timeout in seconds between AP-REQ request to AP-REP. **Relevant to** CH Kerberos, main task **Type** integer **Default Value**

19

Layer 2 Tunneling Protocol (L2TP) Server

Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol, enabling your gateway to create VPN connections. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP Remote Access Concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP Network Server (LNS) at the corporate side. With OpenRG, L2TP is targeted at serving two purposes:

1. Connecting OpenRG to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established by authenticating your username and password.

2. Connecting OpenRG to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates, and user name and password for authentication.

- General -- general L2TPS entries (refer to Section 19.1).
- Remote -- remote tunnel entries (refer to Section 19.2).
- Authentication -- authentication entries (refer to Section 19.3).
- Encryption -- encryption entries (refer to Section 19.4).
- IPSec -- L2TP over IPSec entries (refer to Section 19.5).

19.1 General

l2tps/enabled

Description Indicates whether Layer 2 Tunneling Protocol (L2TP) Server accepts connections.

Relevant to L2TPS

Type boolean

Default Value

l2tps/idle_timeout

Description The number of seconds with no activity after which the connection is disconnected. This entry is passed to the PPP connection.

Relevant to PPP

Type integer

Default Value 30000

l2tps/shared_secret

Description The L2TP connection's shared secret.

Relevant to PPP

Type text[MAX_PPP_PASSWORD_LEN=100]

Default Value

19.2 Remote

l2tps/remote/from

Description The first IP address in the IP range for the connection on the remote side. The IP must be in the same local subnet as the OpenRG.

Relevant to L2TPS

Type ip

Default Value

l2tps/remote/to

Description The last IP address in the IP range for the connection on the remote side. The IP must be in the same local subnet as the OpenRG.

Relevant to L2TPS

Type ip

Default Value

19.3 Authentication

l2tps/auth/required

Description Indicates whether the user is required to authenticate. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

l2tps/auth/pap

Description Indicates whether Password Authentication Protocol (PAP) authentication is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value False=0

l2tps/auth/chap

Description Indicates whether CHAP authentication is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

l2tps/auth/ms_chap_v1

Description Indicates whether MS-CHAP authentication is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

l2tps/auth/ms_chap_v2

Description Indicates whether MS-CHAP-v2 authentication is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

19.4 Encryption

l2tps/encryption/required

Description Indicates whether encryption is required. If it is not, unencrypted connections may be established. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

l2tps/encryption/mppe_40

Description Indicates whether MPPE-40 encryption is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

l2tps/encryption/mppe_128

Description Indicates whether MPPE-128 encryption enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

l2tps/encryption/mppe_stateless

Description Indicates whether MPPE-stateless encryption is enabled. Stateless encryption means rekeying after every packet. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

19.5 IPSec

l2tps/ipsec/enabled

Description Indicates whether the L2TP connection is over IPSec.

Relevant to PPP

Type boolean

Default Value True=1

l2tps/ipsec/shared_secret

Description Shared secret for IPSec in the L2TP connection. Relevant if **l2tps/ipsec/enabled** is true.

Relevant to PPP

Type text[MAX_PPP_PASSWORD_LEN=100]

Default Value

20

Multicast Groups

mcast/enabled **Description** Indicates if multicast groups management (IGMP) is enabled or disabled. **Relevant to** IGMP, WBM, Firewall **Type** boolean **Default Value** True=1
mcast/fast_leave/enabled **Description** Indicates if IGMP fast leave is enabled or disabled. **Relevant to** IGMP **Type** boolean **Default Value** True=1
mcast/multicast_to_unicast/enabled **Description** Indicates if IGMP multicast to unicast is enabled or disabled. **Relevant to** IGMP **Type** boolean **Default Value** False=0

dev/<name>/mcast/enabled

Description Indicates if multicast groups management is enabled or disabled on the LAN device.

Relevant to IGMP

Type boolean

Default Value True=1

dev/<name>/mcast/igmp_proxy_default

Description Indicates if multicast groups management is enabled or disabled on the WAN device.

Relevant to IGMP

Type boolean

Default Value True=1

dev/<name>/mcast/version

Description IGMP version used in queries sent by OpenRG

Relevant to IGMP

Type integer

Default Value 3

21

Mail

- Email notification -- the entries needed for email notification (refer to Section 21.1).
- Email client -- the outgoing mail server settings, required by email clients (refer to Section 21.2).
- Mail server -- the mail server entries, including POP3, IMAP4 and IMAPS mail retrieval protocols (refer to Section 21.3).

21.1 Email Notification

enotify/send_period

Description Time in seconds between notification emails, if messages exist. For email notifications you must also specify the email address of the user (see entry admin/user/%/email on page 4) and the outgoing mail server details (see entry email/smtp/server on page 109).

Relevant to Email Notification

Type integer

Default Value

enotify/queue_length

Description Maximum number of messages allowed in email notification queue. For email notifications you must also specify the email address of the user (see entry admin/user/%/email on page 4) and the outgoing mail server details (see entry email/smtp/server on page 109).

Relevant to Email Notification

Type integer

Default Value

enotify/retry_period

Description Time in seconds to retry sending Email notification if it failed. For email notifications you must also specify the email address of the user (see entry admin/user/%/email on page 4) and the outgoing mail server details (see entry email/smtp/server on page 109).

Relevant to Email Notification

Type integer

Default Value

21.2 Email Client

email/smtp/server

Description Simple Mail Transport Protocol (SMTP) server hostname or IP. This is the outside server through which email notifications will be sent.

Relevant to eMail

Type text[MAX_HOSTNAME_LEN=64]

Default Value

email/smtp/from

Description When using email notification, this is the name that appears as the source of the email.

Relevant to eMail

Type text[MAX_EMAIL_LEN=320]

Default Value

email/smtp/port

Description SMTP server port.

Relevant to eMail

Type integer

Default Value 25

email/smtp/auth

Description Indicates whether Extended Simple Mail Transport Protocol (ESMTP) authentication is enabled.

Relevant to eMail

Type boolean

Default Value False=0

email/smtp/username

Description ESMTP authentication username. Relevant only if **email/smtp/auth** is enabled.

Relevant to eMail

Type text[MAX_USERNAME_LEN=100]

Default Value

email/smtp/password

Description ESMTP authentication password. This entry is obscured. Relevant only if **email/smtp/auth** is enabled.

Relevant to eMail

Type text[MAX_USERNAME_LEN=100]

Default Value

21.3 Mail Server

21.3.1 Mail Transfer Agent

email/mta/enabled

Description Indicates whether the mail server is enabled. This entry also enables Mail Transfer Agent (MTA) for outgoing mail. All the entries in this section depend on this entry being true.

Relevant to Mail Server

Type boolean

Default Value False=0

email/mta/wan

Description Indicates whether access to MTA is allowed from the WAN.

Relevant to Mail Server

Type boolean

Default Value False=0

email/mta/domain

Description The domain of the mail server.

Relevant to Mail Server

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

email/mta/quota

Description Default quota of a new mailbox in Megabytes. The entry's value is used in **admin/user/%/mailbox/quota**.

Relevant to Mail Server

Type integer

Default Value 30

email/mta/spf

Description Indicates whether 'Sender Policy Framework' spam filter is enabled.

Relevant to Mail Server

Type boolean

Default Value True=1

email/mta/log_messages

Description Indicates whether logging of relayed messages is enabled.

Relevant to Mail Server

Type boolean

Default Value False=0

email/mta/connections

Description Maximum number of allowed simultaneous connections to MTA. If 0, unlimited.

Relevant to Mail Server

Type integer

Default Value 3

email/mta/list/%/enabled

Description Indicates whether this mailing list is enabled.

Relevant to Mail Server

Type boolean

Default Value

email/mta/list/%/name

Description Name of the mailing list.

Relevant to Mail Server

Type text[MAX_USERNAME_LEN=100]

Default Value

email/mta/list/%/description

Description Description of mailing list.

Relevant to Mail Server

Type text[MAX_FULLNAME_LEN=128]

Default Value

email/mta/list/%/addresses

Description List of addresses for mailing list, separated by space, comma(',') or semicolon (';').

Relevant to Mail Server

Type text

Default Value

21.3.2 POP3

email/pop3/enabled

Description Indicates whether Post Office Protocol version 3 (POP3) is enabled (protocol used to retrieve e-mail from the mail server).

Relevant to Mail Server

Type boolean

Default Value False=0

email/pop3/wan

Description Indicates whether POP3 access to MTA is allowed from the WAN.

Relevant to Mail Server

Type boolean

Default Value False=0

21.3.3 Internet Message Access Protocol

email/imap/enabled

Description Indicates whether IMAP is enabled (protocol used to retrieve e-mail from the mail server).

Relevant to Mail Server

Type boolean

Default Value False=0

email/imap/wan

Description Indicates whether Internet Message Access Protocol (IMAP) access to MTA is allowed from the WAN.

Relevant to Mail Server

Type boolean

Default Value False=0

21.3.4 Internet Message Access Protocol over SSL

email/imaps/enabled

Description Indicates whether IMAPS is enabled (protocol used to retrieve e-mail from the mail server).

Relevant to Mail Server

Type boolean

Default Value False=0

email/imaps/wan

Description Indicates whether IMAPS access to MTA is allowed from the WAN.

Relevant to Mail Server

Type boolean

Default Value False=0

22

Manufacturer

manufacturer/hardware/version

Description The hardware version of the system, as it will be displayed in the WBM 'About' page. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to CH SNMP, main task, WBM

Type text[MAX_VAR_NAME=80]

Default Value

manufacturer/hardware/serial_num

Description The product serial number as it will be displayed in the WBM 'About' page. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to CH SNMP, main task, WBM

Type text[MAX_VAR_NAME=80]

Default Value

manufacturer/vendor_name

Description The vendor company name as it will be displayed in the WBM 'About' page. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to CH SNMP, WBM

Type text[MAX_VAR_NAME=80]

Default Value

manufacturer/description

Description The string used in DSLHome Inform message as InternetGatewayDevice.DeviceInfo.Description. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DSLHome

Type text[256]

Default Value

manufacturer/product_class

Description The string used in DSLHome Inform message as InternetGatewayDevice.DeviceInfo.ProductClass. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DSLHome

Type text[64]

Default Value

manufacturer/vendor_oui

Description The Vendor Organizational Unique Identifier (OUI), made up of six hexadecimal digits, using all uppercase letters and including any leading zeros. Used in DSLHome Inform message as \linebreak InternetGatewayDevice.DeviceInfo.ManufacturerOUI. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DSLHome

Type text[6]

Default Value

manufacturer/boot_rom_version

Description Boot Read Only Memory (ROM) version. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to CH SNMP

Type text[MAX_VAR_NAME=80]

Default Value

manufacturer/model_number

Description The model number. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to CH SNMP

Type text[MAX_VAR_NAME=80]

Default Value

manufacturer/sys_object_id

Description The specific system object ID value to be returned when queried by SNMP for sysObjectID. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SNMP, CH SNMP

Type text[MAX_VAR_NAME=80]

Default Value

network/rg_mac

Description OpenRG's initial MAC address, used for bridge devices. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to Ethernet

Type mac

Default Value

dev/<dev_name>_atm/pvc_scan/%/vpi

Description Virtual Path Identifier (VPI) parameter for an Asynchronous Transfer Mode (ATM) connection. This entry's value is used when performing a Permanent Virtual Circuit (PVC) scan. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to General, VoATM

Type integer

Default Value

dev/<dev_name>_atm/pvc_scan//%/vci

Description Virtual Circuit Identifier (VCI) parameter for an ATM connection. This entry's value is used when performing a PVC scan. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to General, VoATM

Type integer

Default Value

23

Network Connections

This chapter lists the entries that fall under **device/**. This includes the following sections:

- General – general device entries (refer to Section 23.1).
- Enslaved Devices – entries for devices enslaved under bridges (refer to Section 23.2).
- DNS – device entries related to DNS (refer to Section 23.3).
- Dynamic Host Configuration Protocol (DHCP) Relay – entries related to devices using a DHCP relay agent (refer to Section 23.4).
- Dynamic Host Configuration Protocol (DHCP) Server – entries related to devices using a DHCP server (refer to Section 23.5).
- Asynchronous Transfer Mode (ATM) – entries for ATM connections (refer to Section 23.6).
- Digital Subscriber Line (DSL) – entries for DSL connections (refer to Section 23.7).
- Point-to-Point Protocol (PPP) – entries for PPP connections (refer to Section 23.8).
- Internet Protocol Security (IPSec) – entries for IPSec connections (refer to Section 23.9).
- IPv6 – entries for devices using IPv6 (refer to Section 23.10).
- RADIUS – 802.1x authentication entries (refer to Section 23.11).
- Web Authentication – entries for Web Authentication for wireless clients (refer to Section 23.12).
- Wireless Local Area Network (WLAN) – entries for WLAN devices (refer to Section 23.13).

- Wireless LAN Access Point – entries for WLAN access-point devices (refer to Section 23.14).
- Wi-Fi Protected Access (WPA) – entries for WPA devices (refer to Section 23.15).
- Routing Information Protocol (RIP) – RIP-related entries for devices (refer to Section 23.16).
- Quality of Service (QoS) – QoS entries for devices, including traffic shaping and traffic classes (refer to Section 23.17).

23.1 General

This section includes general entries for devices, such as type, ID, MAC address, etc. In addition, there are a number of entries related to a device's static IP and fallback IP, dynamically obtained information, a device's alias and a device's statistics.

dev/<name>/type

Description The device type/protocol.

Relevant to General

Type one string of:
"79xx355_dsl" (DEV_IF_79XX355_DSL),
"79xx355_eth" (DEV_IF_79XX355_ETH),
"prism2" (DEV_IF_PRISM2),
"bcm43xx" (DEV_IF_BCM43XX),
"bcm963xx_eth" (DEV_IF_BCM963XX_ETH),
"bcm963xx_adsl" (DEV_IF_BCM963XX_ADSL),
"bcm963xx_rndis" (DEV_IF_BCM963XX_RNDIS),
"ar531x_eth" (DEV_IF_AR531X_ETH),
"ar531x_wlan_g" (DEV_IF_AR531X_WLAN_G),
"atm_null" (DEV_IF_ATM_NULL),
"bcm4710_eth" (DEV_IF_BCM4710_ETH),
"eepro100" (DEV_IF_EEPRO100),
"eth1394" (DEV_IF_ETH1394),
"incaip_eth" (DEV_IF_INCAIP_ETH),
"incaip_vlan" (DEV_IF_INCAIP_VLAN),
"isl38xx" (DEV_IF_ISL38XX),
"softmac" (DEV_IF_ISL_SOFTMAC)

Default Value

dev/<name>/type

Description Device type/protocol - continuation.

Relevant to General

Type one string of:
"ixp425_dsl" (DEV_IF_IXP425_DSL),
"ixp425_eth" (DEV_IF_IXP425_ETH),
"natsemi" (DEV_IF_NATSEMI),
"ne2000" (DEV_IF_NE2000),
"ne2000_vx" (DEV_IF_NE2K_VX),
"rtl8139" (DEV_IF_RTL8139),
"ti404_cbl" (DEV_IF_TI404_CBL),
"ti404_lan" (DEV_IF_TI404_LAN),
"uml" (DEV_IF_UML),
"usb_rndis" (DEV_IF_USB_RNDIS),
"vlan" (DEV_IF_VLAN),
"pppoa" (DEV_IF_PPPOA),
"pppoe" (DEV_IF_PPPOE),
"pppoes_conn" (DEV_IF_PPPOES_CONN),
"pppoh" (DEV_IF_PPPOH),
"pppos_conn" (DEV_IF_PPPOS_CONN),
"ethoa" (DEV_IF_ETHOA),
"pptpc" (DEV_IF_PPTPC),
"pptps_conn" (DEV_IF_PPTPS_CONN),
"ipsec_dev" (DEV_IF_IPSEC_DEV),
"ipsec_conn" (DEV_IF_IPSEC_CONN),
"ipsec_templ" (DEV_IF_IPSEC_TEMPL),
"ipsec_templ_transient" (DEV_IF_IPSEC_TEMPL_TRANSIENT),
"ipsec_templ_conn" (DEV_IF_IPSEC_TEMPL_CONN),
"bridge" (DEV_IF_BRIDGE),
"chwan_master" (DEV_IF_CHWAN_MASTER),
"docsis" (DEV_IF_DOCSIS),
"elcp" (DEV_IF_ELCP),
"cas" (DEV_IF_CAS),
"clip" (DEV_IF_CLIP),
"l2tpc" (DEV_IF_L2TPC),
"ti_cpe" (DEV_IF_TICPE),
"user_vlan" (DEV_IF_USER_VLAN),
"ipv6_over_ipv4_tun" (DEV_IF_IPV6_OVER_IPV4_TUN),
"ipoa" (DEV_IF_IPOA),
"cx821xx_eth" (DEV_IF_CX821XX_ETH),
"sl2312_eth" (DEV_IF_SL2312_ETH),
"adm5120_eth" (DEV_IF_ADM5120_ETH),
"cx8620x_switch" (DEV_IF_CX8620X_SWITCH),
"wds_conn" (DEV_IF_WDS_CONN),
"ar531x_wlan_a" (DEV_IF_AR531X_WLAN_A),
"rt2560" (DEV_IF_RT2560),
"agn100" (DEV_IF_AGN100),
"mpc82xx_eth" (DEV_IF_MPC82XX_ETH),
"ks8695_eth" (DEV_IF_KS8695_ETH),
"eepro1000" (DEV_IF_EEPRO1000),
"netpro_sierra" (DEV_IF_AD6834_ETH),

dev/<name>/enabled

Description Indicates whether the device is enabled.

Relevant to General

Type boolean

Default Value

dev/<name>/id

Description The device ID.

Relevant to main

Type integer

Default Value

dev/<name>/volatile_enabled

Description Indicates whether the device is enabled. This field is non-persistent. It is created upon device creation, and initialized with the device's corresponding persistent flag (dev/<name>/enabled). This entry is used for internal logic only.

Relevant to General

Type boolean

Default Value

dev/<name>/depend_on_name

Description The name of the device on which this device depends. For example, the device could be PPPoE, which depends on an Ethernet device.

Relevant to General

Type set

Default Value

dev/<name>/logical_depend_on

Description The name of the device that is logically the underlying device for this connection. Is displayed in Quick Setup and Connection Wizard.

Relevant to Quick Setup and Internet Connection Wizard

Type text[IFNAMSIZ]

Default Value

dev/<name>/has_ip

Description Indicates whether the device has an IP address assigned to it.

Relevant to General

Type boolean

Default Value

dev/<name>/mac

Description The MAC address of the device. Each device, either WAN or LAN, has a unique name under the **dev** entry. Each device must have a registered MAC address. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to General

Type mac

Default Value

dev/<name>/logical_network

Description External or internal network.

Relevant to General

Type DEV_IF_NET_EXT = 0x1
DEV_IF_NET_INT = 0x2
DEV_IF_NET_DMZ = 0x4

Default Value

dev/<name>/description

Description A textual description of the device.

Relevant to WBM

Type string[64]

Default Value

dev/<name>/tunnel/remote_endpoint

Description IPIP or GRE's remote endpoint IP address.

Relevant to IPIP, GRE

Type ip

Default Value

dev/<name>/is_hidden

Description Indicates whether the device is hidden from the WBM.

Relevant to WBM

Type flag

Default Value

dev/<name>/is_sync

Description Indicates whether the IP of the device is read from the OpenRG configuration settings (**rg_conf**), or obtained dynamically.

Relevant to General

Type enum dev_if_sync_t
DEV_IF_SYNC = 0,
DEV_IF_ASYNC = 1

Default Value

dev/<name>/mtu_mode

Description The Maximum Transmission Unit (MTU) mode of the device.

Relevant to General

Type one string of:
"manual", (MTU_MODE_MANUAL),
"auto", (MTU_MODE_AUTO),
"auto_by_dhcp" (MTU_MODE_AUTO_BY_DHCP)

Default Value "auto"

dev/<name>/mtu

Description The value for the MTU, if **dev/<name>/mtu_mode** is "manual".

Relevant to General

Type integer

Default Value

dev/<name>/is_advanced_wbm_routing

Description Indicates whether the 'Connection Settings' page in the WBM for this device is set to advanced routing mode.

Relevant to WBM

Type boolean

Default Value False=0

dev/<name>/default_route

Description Indicates whether a default route is set through this connection.

Relevant to General

Type boolean

Default Value

dev/<name>/route_level

Description Indicates the packet handling mode (Route, NAT, or NAPT), which is set on this connection.

Relevant to General

Type integer (1-4)

Default Value

dev/<name>/proxy_arp/enabled

Description Indicates whether the proxy Address Resolution Protocol (ARP) is enabled for this connection.

Relevant to Ethernet devices

Type boolean

Default Value False=0

dev/<name>/metric

Description The metric of the device. This default value is set according to the device type.

Relevant to General

Type integer

Default Value

dev/<name>/is_dns_neg

Description Indicates whether the device should negotiate with the server to get a DNS IP.

Relevant to PPP,PPTPC

Type boolean

Default Value

dev/<name>/is_trusted

Description Indicates whether the Firewall allows all traffic on this interface.

Relevant to Firewall

Type boolean

Default Value

dev/<name>/mcast/enabled

Description Indicates whether multicast groups management is enabled on this device.

Relevant to WBM, Firewall

Type boolean

Default Value True=1

dev/<name>/http_auth

Description Indicates whether this device uses HTTP authorization

Relevant to WBM, Firewall

Type boolean

Default Value

dev/<name>/rt_table_id

Description Table ID of the device's default route rule.

Relevant to Multitable Routing

Type integer

Default Value

dev/<name>/is_new_cams_ap

Description Indicates whether this device is an Access Point for new cameras

Relevant to Wireless LAN

Type boolean

Default Value False=0

23.1.1 Static

dev/<name>/static/ip

Description The static IP address of the device.

Relevant to General

Type ip

Default Value

dev/<name>/static/netmask

Description The static netmask of the device.

Relevant to General

Type ip

Default Value

dev/<name>/static/gateway

Description The static gateway (router) of the device.

Relevant to General

Type ip

Default Value

23.1.2 Fallback

dev/<name>/fallback/ip

Description The fallback IP address, in case the DHCP client does not receive a response from the server.

Relevant to DHCPC

Type ip

Default Value

dev/<name>/fallback/netmask

Description The fallback netmask, in case the DHCP client does not receive a response from the server.

Relevant to DHCPC

Type ip

Default Value

dev/<name>/fallback/gateway

Description The fallback gateway (router), in case the DHCP client does not receive a response from the server..

Relevant to DHCPC

Type ip

Default Value

23.1.3 Dynamically Obtained Information

dev/<name>/dyn/ip

Description Dynamically obtained IP of the device.

Relevant to DHCPC

Type ip

Default Value

dev/<name>/dyn/override_netmask

Description The netmask to override the dynamically obtained netmask.

Relevant to PPP, PPTPC

Type ip

Default Value

dev/<name>/dyn/use_override_netmask

Description Indicates whether or not to override the netmask, using **dev/<name>/dyn/override_netmask**.

Relevant to PPP, PPTPC

Type boolean

Default Value

23.1.4 Additional IP addresses

dev/<name>/ip_pool/%/item

Description Inline network object representation of an additional ip of the device

Relevant to main

Type

Default Value

dev/<name>/ip_pool/%/description

Description Describes the additional ip of the device

Relevant to main

Type

Default Value

dev/<name>/ip_pool/%/usage

Description Deescribes the usage the additional ip of the device

Relevant to main

Type one string of:
"nat_napt" (FW_NAT_NAPT),
"nat_napt_arp_replies" (FW_NAT_NAPT_ARP_REPLIES),
"nat_napt_rmt_access" (FW_NAT_NAPT_RMT_ACCESS),

Default Value

23.1.5 Statistics

dev/<name>/statistics/start_time

Description The time stamp from the last reboot or statistics reset. This entry is saved in **rg_conf_ram**.

Relevant to WBM

Type integer

Default Value

dev/<name>/auto_conf/enabled

Description Indicates whether auto-configuration task is enabled on this device.

Relevant to auto_conf

Type boolean

Default Value

23.2 Enslaved Devices

dev/<name>/enslaved/<dev>

Description List of devices enslaved under this bridge device, including the bridge itself.

Relevant to Bridge devices

Type text[IFNAMSIZ]

Default Value

dev/<name>/enslaved/<dev>/is_trusted

Description For enslaved WAN devices only. This entry is stored from the WAN device entry, **dev/<name>/is_trusted** (see entry dev/<name>/is_trusted on page 126). The entry is needed for restoring on unenslave.

Relevant to Bridge devices

Type boolean

Default Value

dev/<name>/enslaved/<dev>/route_level

Description For enslaved WAN device only. This entry is stored from the WAN device entry, **route_level**. This entry is needed for restoring on unenslave.

Relevant to Bridge devices

Type enum route_level_t
DEV_IF_RL_ROUTE = 1,
DEV_IF_RL_NAT = 2,
DEV_IF_RL_NAPT = 4

Default Value

dev/<name>/enslaved/<dev>/stp

Description Indicates whether the enslaved device uses the Spanning Tree Protocol (STP) algorithm.

Relevant to Bridge devices

Type boolean

Default Value True=1

dev/<name>/enslaved/<dev>/tagged

Description Indicates whether this enslaved device is connected to a tagged network, meaning the packets are VLAN packets.

Relevant to Bridge devices

Type boolean

Default Value False=0

dev/<name>/enslaved/<dev>/def_vlan

Description The ID of the VLAN defined for the device, when the device is connected to an untagged network (**dev/<name>/enslaved/<dev>/tagged** is false). Rx packets will have a VLAN header added and only Tx packets that by definition belong to this VLAN will be transmitted.

Relevant to Bridge devices

Type integer [-1,1..4094]

Default Value -1

dev/<name>/enslaved/<dev>/def_pri

Description The default priority to use on packets from devices connected to an untagged network.

Relevant to Bridge devices

Type integer [0..7]

Default Value 0

dev/<name>/enslaved/<dev>/trunk

Description Indicates whether the enslaved device is identified as a trunk - i.e. a member of all VLANs. This entry is relevant for devices connected to a tagged network (**dev/<name>/enslaved/<dev>/tagged** is true).

Relevant to Bridge devices

Type boolean

Default Value False=0

dev/<name>/enslaved/<dev>/vid/%

Description The VIDs of VLANs to which the device belongs. This entry is relevant for devices connected to a tagged network.

Relevant to Bridge devices

Type integer [1..4094]

Default Value

23.3 DNS

dev/<name>/name_server/% **Description** The primary and secondary name server settings for Ethernet/PPPoA/PPPoE connections. **Relevant to** WAN Device **Type** ip **Default Value**
dev/<name>/dns_disabled **Description** Determines whether DNS Server should not use dns server settings. **Relevant to** WAN Device **Type** boolean **Default Value** False=0
dev/<name>/dns_wait_time/% **Description** The time in milliseconds the DNS should wait for a device if it is running but cannot send DNS queries yet (PPP on demand). **Relevant to** WAN Devices **Type** unsigned integer **Default Value**
dev/<name>/domain_routing/disabled **Description** Indicates whether to disable domain routing on a device, even though domains are defined on it. **Relevant to** WAN Devices **Type** boolean **Default Value** False=0

23.4 Dynamic Host Configuration Protocol (DHCP) Relay

Your gateway can act as a DHCP relay in case you would like to dynamically assign IP addresses from a DHCP server other than your gateway's DHCP server.

dev/<name>/dhcpr/enabled **Description** Indicates whether a DHCP relay agent is enabled on this device. **Relevant to** DHCPR, DHCPS **Type** boolean **Default Value**
dev/<name>/dhcpr/dhcp_server/%/addr **Description** The IP Address of a DHCP server to which the relay agent should forward. **Relevant to** DHCPR **Type** ip **Default Value**

23.5 Dynamic Host Configuration Protocol (DHCP) Server

Your gateway's Dynamic Host Configuration Protocol (DHCP) server makes it possible to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to such hosts. OpenRG's default DHCP server is the LAN bridge. A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as `taken'. At this point the host is configured with an IP address for the duration of the lease.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease then it will also receive current information about network services, as it did with the original lease, allowing it to update its network configurations to reflect any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration it can send a release message to the DHCP server, which will then make the IP address available for use by others.

23.5.1 General Entries

dev/<name>/dhcps/enabled

Description Indicates whether a DHCP server is enabled on this device.

Relevant to DHCPS, DHCPR

Type boolean

Default Value

dev/<name>/dhcps/lease_time

Description The duration of time in seconds the device is allowed connection to the gateway with its currently issued lease.

Relevant to DHCPS, DNS

Type unsigned long

Default Value

dev/<name>/dhcps/start_ip

Description The IP address from which the gateway starts issuing addresses.

Relevant to DHCPS

Type ip

Default Value

dev/<name>/dhcps/end_ip

Description The ending IP of the lease IP range used to issue addresses.

Relevant to DHCPS

Type ip

Default Value

dev/<name>/dhcps/time_offset

Description The default value for time offset.

Relevant to DHCPS

Type integer

Default Value 0

dev/<name>/dhcps/ttl

Description The default value for time-to-live (TTL) option.

Relevant to DHCPS

Type integer

Default Value

dev/<name>/dhcps/mtu

Description The default MTU value.

Relevant to DHCPS

Type integer

Default Value

dev/<name>/dhcps/vendor_specific

Description The value for vendor-specific information. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DHCPS

Type text[513]

Default Value

dev/<name>/dhcps/dns_servers/%

Description The list of DNS server IP addresses that are given in a lease. You may use an external DNS, either on the LAN or on the WAN, rather than OpenRG's DNS. In this case, provide the IP address of the DNS, which will now be provided with every DHCP lease that OpenRG provides.

Relevant to DHCPS

Type ip

Default Value

dev/<name>/dhcps/routers/%

Description List of router IP addresses that are given in a lease. If empty, device IP is used.

Relevant to DHCPS

Type ip

Default Value

dev/<name>/dhcps/domain_name

Description Domain name that is given in a lease. If empty, OpenRG's domain name is used.

Relevant to DHCPS

Type text

Default Value

dev/<name>/dhcps/wins_server/0/ip

Description The Windows Internet Naming Service (WINS) Server IP that is given in a lease.

Relevant to DHCPS

Type ip

Default Value

dev/<name>/dhcps/syslog_servers/%

Description List of syslog server IPs that are given in a lease.

Relevant to DHCPS

Type ip

Default Value 0.0.0.0

dev/<name>/dhcps/router/%

Description List of IPs of routers that are given in a lease.

Relevant to DHCPS, DNS

Type boolean

Default Value

dev/<name>/dhcps/create_hostname

Description Determines whether the gateway should automatically assign network PCs with a host name, in case a host name is not provided by the user.

Relevant to DHCPS, DNS

Type boolean

Default Value

dev/<name>/dhcps/ip_auto_detect/disabled

Description Disable automatic IP detection on this device.

Relevant to DHCPS

Type boolean

Default Value 0

23.5.2 Lease

dev/<name>/dhcps/lease/%/ip

Description A single lease IP address.

Relevant to DHCPS, DNS

Type ip

Default Value

dev/<name>/dhcps/lease/%/hostname

Description A single lease host name.

Relevant to DHCPS, DNS

Type host

Default Value

dev/<name>/dhcps/lease/%/start_time

Description Starting time of the lease, relative to the system boot.

Relevant to DHCPS, DNS

Type time_t

Default Value

dev/<name>/dhcps/lease/%/end_time

Description Expiration time of the lease, relative to system boot.

Relevant to DHCPS, DNS

Type time_t

Default Value

dev/<name>/dhcps/lease/%/hardware_mac

Description MAC address of a static/dynamic DHCP lease. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DHCPS, DNS

Type mac

Default Value

dev/<name>/dhcps/lease/%/is_ms_null_terminated

Description Indicates whether the client requires all string data to be NULL-terminated (Microsoft).

Relevant to DHCPS

Type boolean

Default Value

dev/<name>/dhcps/lease/%/is_ever_acked

Description Indicates whether this lease has been acknowledged (ACK) sometime in its lifetime.

Relevant to DHCPS

Type boolean

Default Value

dev/<name>/dhcps/lease/%/is_abandoned

Description Indicates whether this lease has been dropped, either by a client or by the server.

Relevant to DHCPS

Type boolean

Default Value

dev/<name>/dhcps/lease/%/is_dynamic

Description Indicates whether this DHCP lease is dynamic (automatically retrieved from the server) or static (manually entered by MGT).

Relevant to DHCPS, DNS

Type boolean

Default Value

dev/<name>/dhcps/lease/%/visible_to_dns

Description Indicates whether this lease is included in the DNS entries list.

Relevant to DNS, WBM

Type boolean

Default Value

dev/<name>/dhcps/lease/%/uid

Description The unique ID of the lease client - null-terminated string of hexadecimal characters.

Relevant to DHCPS

Type text[513]

Default Value

dev/<name>/dhcps/lease/%/stability

Description Status of negotiation with the client for this lease.

Relevant to DHCPS, DNS, WBM

Type enum dhcps_lease_stable_t
DHCPS_LEASE_STABLE_NO = 0,
DHCPS_LEASE_STABLE_OFFERED = 1,
DHCPS_LEASE_STABLE_ACKED = 2

Default Value

dev/<name>/dhcps/lease/%/valid_time

Description Indicates whether the lease has not expired.

Relevant to DHCPS, DNS

Type boolean

Default Value

dev/<name>/dhcps/lease/%/vendor_id

Description The class ID of the lease vendor, written as a null-terminated string of hexadecimal characters. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to DHCPS

Type text[513]

Default Value

dev/<name>/dhcps/lease/%/is_hostname_fixed

Description Indicates whether the host name was overridden by a WBM user.

Relevant to DHCPS, WBM, DNS

Type boolean

Default Value

dev/<name>/dhcps/lease/%/is_detected

Description Indicates whether this lease represents an automatically-detected host.

Relevant to DHCPS

Type boolean

Default Value

dev/<name>/dhcps/lease/%/dev

Description Device that the client which received the lease is physically connected

Relevant to DHCPS

Type string

Default Value

dev/<name>/dhcps/lease/%/user_class_id

Description Contains a validated hex-bin buffer received via option-77.

Relevant to DHCPS, TR-098

Type string

Default Value

dev/<name>/dhcps/lease/%/dslforum_enterprise_data/vendor_oui

Description Option 125/DSLFORUM Enterprise option "VendorOUI"

Relevant to DHCPS, TR-111

Type string

Default Value

dev/<name>/dhcps/lease/%/dslforum_enterprise_data/serial_num

Description Option 125/DSLFORUM Enterprise option "SerialNumber"

Relevant to DHCPS, TR-111

Type string

Default Value

dev/<name>/dhcps/lease/%/dslforum_enterprise_data/product_class

Description Option 125/DSLFORUM Enterprise option "ProductClass"

Relevant to DHCPS, TR-111

Type string

Default Value

dev/<name>/dhcps/lease/%/dslforum_enterprise_data/manageable_dev_index

Description Identifies the host represented by the lease for TR-111

Relevant to DHCPS, TR-111

Type int

Default Value

internal/dhcps/manageable_dev_index

Description The value of the last allocated manageable_dev_index

Relevant to DHCPS, TR-111

Type int

Default Value

dev/<name>/dhcps/lease/%/user_class_id **Description** Contains a validated hex-bin buffer received via option-77. **Relevant to** DHCPS, TR-098 **Type** string **Default Value**
dev/<name>/dhcps/lease/%/history/%/time **Description** Displays a time of one of the last five DHCP events taken place on a host. This entry is stored in rg_conf_ram. **Relevant to** DHCPS **Type** int **Default Value**
dev/<name>/dhcps/lease/%/history/%/event **Description** Displays one of the last five DHCP events taken place on a host. An event can be: `acked`, `released` or `expired`. This entry is stored in rg_conf_ram. **Relevant to** DHCPS **Type** string **Default Value**

23.6 Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with other technologies. The small, constant cell size allows the transmission of video, audio, and computer data, assuring that no single type of data consumes the connection. ATM addressing consists of two identifiers that identify the virtual path (VPI) and the virtual connection (VCI). A virtual path consists of multiple virtual channels to the same endpoint.

dev/<name>/atm/pvc/%/vpi

Description Virtual Path Identifier (VPI) parameter for an Asynchronous Transfer Mode (ATM) connection.

Relevant to General, VoATM

Type integer

Default Value

dev/<name>/atm/pvc/%/vci

Description Virtual Circuit Identifier (VCI) parameter for an ATM connection.

Relevant to General, VoATM

Type integer

Default Value

dev/<name>/atm/pvc/%/auto

Description Indicates whether the automatic Permanent Virtual Circuit (PVC) acquiring method is enabled.

Relevant to General

Type boolean

Default Value

dev/<name>/atm/pvc/%/traffic_class

Description The traffic class for the ATM connection.

Relevant to General, VoATM

Type one string of:
"ubr" (ATM_TRAFFIC_CLASS_UBR),
"ubr_pcr" (ATM_TRAFFIC_CLASS_UBR_PCR),
"cbr" (ATM_TRAFFIC_CLASS_CBR),
"rtvbr" (ATM_TRAFFIC_CLASS_RTVBR),
"nrtvbr" (ATM_TRAFFIC_CLASS_NRTVBR)

Default Value

dev/<name>/atm/pvc/%/pcr

Description The Peak Cell Rate (PCR) for ATM traffic control.

Relevant to General, VoATM

Type integer

Default Value

dev/<name>/atm/pvc/%/scr

Description The Sustainable Cell Rate (SCR) for ATM traffic control.

Relevant to General, VoATM

Type integer

Default Value

dev/<name>/atm/pvc/%/mbs

Description The Maximum Burst Size (MBS) for ATM traffic control.

Relevant to General, VoATM

Type integer

Default Value

dev/<name>/atm/encaps

Description Ethernet over ATM (EthoA) encapsulation method.

Relevant to General

Type enum ethoa_method_t
ATM_METHOD_VC_BRDG = 0,
ATM_METHOD_LLC_BRDG = 2,
ATM_METHOD_VC_RTD = 2,
ATM_METHOD_LLC_RTD = 3

Default Value ATM_METHOD_LLC_BRDG

23.7 Digital Subscriber Line (DSL)

dev/<name>/dsl/line_mode

Description The DSL line mode.

Relevant to General

Type one string of:
"auto" (DSL_LINE_MODE_AUTO),
"g" (DSL_LINE_MODE_G),
"t1_413" (DSL_LINE_MODE_T1_413),
"g_dmt" (DSL_LINE_MODE_G_DMT),
"g_lite" (DSL_LINE_MODE_G_LITE)

Default Value "auto"

23.8 Point-to-Point Protocol (PPP)

Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

23.8.1 Authentication

dev/<name>/username

Description Username for PPP authentication.

Relevant to PPP

Type text[MAX_PPP_USERNAME_LEN=100]

Default Value

dev/<name>/password

Description Password for PPP authentication.

Relevant to PPP

Type text[MAX_PPP_PASSWORD_LEN=100]

Default Value

dev/<name>/ppp/auth/pap

Description Indicates whether Password Authentication Protocol (PAP) authentication is enabled.

Relevant to PPP

Type boolean

Default Value

dev/<name>/ppp/auth/chap

Description Indicates whether Challenge Handshake Authentication Protocol (CHAP) authentication is enabled.

Relevant to PPP

Type boolean

Default Value

dev/<name>/ppp/auth/ms-chap-v1

Description Indicates whether MS-CHAP authentication is enabled.

Relevant to PPP

Type boolean

Default Value

dev/<name>/ppp/auth/ms-chap-v2

Description Indicates whether MS-CHAP-v2 authentication is enabled.

Relevant to PPP

Type boolean

Default Value

persistent/ppp/username

Description Last successful username of a main WAN PPP connection. It is not removed when restore defaults is run.

Relevant to PPP

Type text

Default Value

persistent/ppp/password

Description Last successful password of a main WAN PPP connection. It is not removed when restore defaults is run.

Relevant to PPP

Type text

Default Value

23.8.2 Encryption

dev/<name>/ppp/encryption/required

Description Indicates whether encryption is required on the device's connections. If not, unencrypted connections may be established.

Relevant to PPP

Type boolean

Default Value

dev/<name>/ppp/encryption/mppe_40

Description Indicates whether Microsoft Point-to-Point Encryption (MPPE) -40 is enabled.

Relevant to PPP

Type boolean

Default Value

dev/<name>/ppp/encryption/mppe_128

Description Indicates whether MPPE-128 encryption is enabled.

Relevant to PPP

Type boolean

Default Value

dev/<name>/ppp/encryption/mppe_stateless

Description Indicates whether MPPE-stateless encryption is enabled.

Relevant to PPP

Type boolean

Default Value

23.8.3 Compression

dev/<name>/ppp/compression/bsdcomp

Description BSD compression option.

Relevant to PPPoH, PPPoE, PPPoA

Type enum ppp_comp_opt_t
PPP_COMP_REJECT = 0,
PPP_COMP_ALLOW = 1,
PPP_COMP_REQUIRE =2

Default Value

dev/<name>/ppp/compression/deflate

Description Deflate compression option.

Relevant to PPPoH, PPPoE, PPPoA

Type enum ppp_comp_opt_t
PPP_COMP_REJECT = 0,
PPP_COMP_ALLOW = 1,
PPP_COMP_REQUIRE =2

Default Value

23.8.4 Connection

dev/<name>/ppp/reconnect_time

Description Reconnection time in seconds for PPP connections.

Relevant to PPP

Type integer

Default Value 30

dev/<name>/ppp/local_ip

Description IP address that the PPP client requests from the PPP server.

Relevant to PPP

Type ip

Default Value

dev/<name>/is_on_demand

Description Indicates whether PPP connection is activated as an on-demand connection.

Relevant to PPP

Type boolean

Default Value

dev/<name>/max_idle

Description The maximum idle time in seconds for on-demand PPP connections.

Relevant to PPP

Type integer

Default Value

23.8.5 PPPoE

dev/<name>/pppoes/enabled

Description Indicates whether Point-to-Point Protocol over Ethernet (PPPoE) Server accepts connections (enabled) on this device.

Relevant to PPPOES

Type boolean

Default Value

dev/<name>/service_name

Description Identification of the desired service for a PPPoE connection.

Relevant to PPPoE

Type text[MAX_PPPOE_SERVICENAME_LEN=80]

Default Value

dev/<name>/is_clamp_mtu

Description Indicates whether the clamp option is used. If it is, the MTU is restricted to 1412 bytes.

Relevant to PPPoE

Type boolean

Default Value

23.8.6 Layer 2 and Point-to-Point Tunneling Protocols

dev/<name>/pptpc/remote_host

Description PPTP Server to which to connect.

Relevant to PPTPC

Type text[MAX_DOMAIN_NAME_LEN=256]

Default Value

dev/<name>/l2tpc/remote_host

Description L2TP Server to which to connect.

Relevant to L2TPC

Type text[MAX_DOMAIN_NAME_LEN=256]

Default Value

dev/<name>/l2tpc/shared_secret

Description Shared secret of L2TP connection and L2TP Server.

Relevant to L2TPC

Type text[96]

Default Value

23.9 Internet Protocol Security (IPSec)

23.9.1 General

dev/<name>/ipsec/trans_type

Description The IPSec transport type.

Relevant to IPSec

Type one string of:
"tunneling" (IPSEC_TRANS_TUNNEL),
"transport" (IPSEC_TRANSPORT)

Default Value "tunneling"

dev/<name>/ipsec/compressed

Description Indicates whether compression is enabled.

Relevant to IPSec

Type boolean

Default Value False=0

dev/<name>/ipsec/is_netbios_route

Description Indicates whether Network Basic Input/Output System (NetBIOS) broadcast packets should be routed through this connection.

Relevant to IPSec

Type boolean

Default Value

dev/<name>/ipsec/is_any_rmt_addr

Description Indicates whether the IPSec template accepts any remote address. Only valid if **dev/<name>/type** is either **DEV_IF_IPSEC_TEMPL** or **DEV_IF_IPSEC_TEMPL_TRANSIENT**.

Relevant to IPSec

Type boolean

Default Value

dev/<name>/ipsec/is_any_rmt_net

Description Indicates whether the IPSec template accept any remote network. Only valid if **dev/<name>/type** is either **DEV_IF_IPSEC_TEMPL** or **DEV_IF_IPSEC_TEMPL_TRANSIENT** and **dev/<name>/ipsec/trans_type** is **IPSEC_TRANS_TUNNELING**.

Relevant to IPSec

Type boolean

Default Value

dev/<name>/ipsec/kx_type

Description The method used for exchanging keys.

Relevant to IPSec

Type one string of:
"automatic" (IPSEC_KX_AUTO),
"manual" (IPSEC_KX_MANUAL)

Default Value

dev/<name>/ipsec/underlying_device

Description WAN device name to be used by IPSec connection.

Relevant to IPSec

Type text[IFNAMSIZ]

Default Value

23.9.2 Remote

dev/<name>/ipsec/remote/addr

Description Host name or IP address of the remote computer.

Relevant to IPSec

Type text[MAX_DOMAIN_NAME_LEN=256]

Default Value

dev/<name>/ipsec/remote/bcast_addr

Description Broadcast IP address of the remote subnet.

Relevant to IPSec

Type ip

Default Value

dev/<name>/ipsec/remote/range_type

Description Type of the remote range.

Relevant to IPSec

Type one string of:
"subnet" (RANGE_SEL_SUBNET),
"single" (RANGE_SEL_SINGLE),
"range" (RANGE_SEL_RANGE),
"any" (RANGE_SEL_ANY),
"none" (RANGE_SEL_NONE)

Default Value "subnet"

dev/<name>/ipsec/remote/network

Description LAN definition of the remote computer.

Relevant to IPSec

Type ip

Default Value 0.0.0.0

dev/<name>/ipsec/remote/netmask

Description LAN netmask definition of the remote computer.

Relevant to IPSec

Type ip

Default Value 0.0.0.0

dev/<name>/ipsec/remote/range_start

Description The start of the LAN IP range of the remote computer when the local range type is **RANGE_SEL_RANGE**.

Relevant to IPSec

Type ip

Default Value

dev/<name>/ipsec/remote/range_end

Description The end of the LAN IP range of the remote computer when the local range type is **RANGE_SEL_RANGE**.

Relevant to IPSec

Type ip

Default Value

23.9.3 Local

dev/<name>/ipsec/local/range_type

Description Type of the local range.

Relevant to IPSec

Type one string of:
"subnet" (RANGE_SEL_SUBNET),
"single" (RANGE_SEL_SINGLE),
"range" (RANGE_SEL_RANGE),
"any" (RANGE_SEL_ANY),
"none" (RANGE_SEL_NONE)

Default Value "subnet"

dev/<name>/ipsec/local/network

Description LAN definition of the local computer.

Relevant to IPSec

Type ip

Default Value

dev/<name>/ipsec/local/netmask

Description LAN netmask definition of the local computer.

Relevant to IPSec

Type ip

Default Value

dev/<name>/ipsec/local/range_start

Description The start of the LAN IP range of the local computer when the local range type is **RANGE_SEL_RANGE**.

Relevant to IPSec

Type ip

Default Value

dev/<name>/ipsec/local/range_end

Description The end of the LAN IP range of the local computer when the local range type is **RANGE_SEL_RANGE**.

Relevant to IPSec

Type ip

Default Value

23.9.4 Protect

dev/<name>/ipsec/protect/protocol

Description Protocol to protect.

Relevant to IPSec

Type one string of:
"all" (IPSEC_PROTECT_PROTO_ALL),
"icmp" (IPSEC_PROTECT_PROTO_ICMP),
"tcp" (IPSEC_PROTECT_PROTO_TCP),
"udp" (IPSEC_PROTECT_PROTO_UDP),
"gre" (IPSEC_PROTECT_PROTO_GRE)

Default Value "all"

dev/<name>/ipsec/protect/source/port_type

Description Type of source port protection.

Relevant to IPSec

Type one string of:
"all" (IPSEC_PROTECT_PORT_ALL),
"single" (IPSEC_PROTECT_PORT_SINGLE)

Default Value "all"

dev/<name>/ipsec/protect/source/port

Description Number of source port to protect.

Relevant to IPSec

Type integer

Default Value

dev/<name>/ipsec/protect/destination/port_type

Description Type of destination port protection.

Relevant to IPSec

Type one string of:
"all" (IPSEC_PROTECT_PORT_ALL),
"single" (IPSEC_PROTECT_PORT_SINGLE)

Default Value "all"

dev/<name>/ipsec/protect/destination/port

Description Number of destination port to protect.

Relevant to IPSec

Type integer

Default Value

23.9.5 Manual

dev/<name>/ipsec/manual/spi/local

Description Local Security Parameter Index (SPI) number for a manual connection, between 0x100 and 0xFFFF_FFFF.

Relevant to IPSec

Type unsigned integer

Default Value

dev/<name>/ipsec/manual/spi/remote

Description Remote SPI number for a manual connection, between 0x100 and 0xFFFF_FFFF.

Relevant to IPSec

Type unsigned integer

Default Value

dev/<name>/ipsec/manual/proto_type

Description The method used for exchanging keys.

Relevant to IPSec

Type one string of:
"ah" (IPSEC_PROTO_AH),
"esp" (IPSEC_PROTO_ESP)

Default Value

dev/<name>/ipsec/manual/different_keys

Description Indicates whether different remote and local keys are enabled.

Relevant to IPSec

Type boolean

Default Value False=0

dev/<name>/ipsec/manual/esp/encrypt/type

Description Encapsulated Security Payload (ESP) encryption to use for a manual connection.

Relevant to IPSec

Type one string of:
"null" (IPSEC_ENC_NULL),
"des" (IPSEC_ENC_DES),
"3des" (IPSEC_ENC_3DES),
"aes128" (IPSEC_ENC_AES128),
"aes192" (IPSEC_ENC_AES192),
"aes256" (IPSEC_ENC_AES256)

Default Value IPSEC_ENC_ESP_3DES

dev/<name>/ipsec/manual/esp/encrypt/local/key

Description Local key for ESP encryption algorithm for a manual connection.

Relevant to IPSec

Type DES -- text[17], 2 groups of 8 hexadecimal digits connected with '_' (64 bits)
3DES -- text[53], 6 groups of 8 hexadecimal digits connected with '_' (192 bits)

Default Value

dev/<name>/ipsec/manual/esp/encrypt/remote/key

Description Remote key for ESP encryption algorithm for manual connections. If **ipsec/manual/different_keys** is false, then the remote key is the same as the local key.

Relevant to IPSec

Type DES -- text[17], 2 groups of 8 hexadecimal digits connected with '_' (64 bits)
3DES -- text[53], 6 groups of 8 hexadecimal digits connected with '_' (192 bits)

Default Value

dev/<name>/ipsec/manual/[esp|ah]/hash/type

Description ESP or Authentication Header (AH) authentication to use for manual connections.

Relevant to IPSec

Type one string of:
"sha1" (IPSEC_AUTH_SHA1),
"md5" (IPSEC_AUTH_MD5)

Default Value "sha1"

dev/<name>/ipsec/manual/[esp|ah]/hash/local/key

Description Local key for ESP or AH authentication algorithm.

Relevant to IPSec

Type SHA1 -- text[35], 4 groups of 8 hexadecimal digits connected with '_' (128 bits)
MD5 -- text[44], 5 groups of 8 hexadecimal digits connected with '_' (160 bits).

Default Value

dev/<name>/ipsec/manual/[esp|ah]/hash/remote/key

Description Remote key for ESP or AH authentication algorithm. If **ipsec/manual/different_keys** is false, then the remote key is the same as the local key.

Relevant to IPSec

Type SHA1 -- text[35], 4 groups of 8 hexadecimal digits connected with '_' (128 bits) MD5 -- text[44], 5 groups of 8 hexadecimal digits connected with '_' (160 bits).

Default Value

23.9.6 Automatic

dev/<name>/ipsec/auto/negotiate_attempts

Description Number of attempts when negotiating automatic connections.

Relevant to IPSec

Type integer

Default Value 3

dev/<name>/ipsec/auto/rekey_margin

Description The number of seconds before connection expiry should attempts to negotiate a replacement begin.

Relevant to IPSec

Type integer

Default Value 540

dev/<name>/ipsec/auto/rekey_fuzz

Description The maximum percentage by which Rekey Margin should be randomly increased to randomize re-keying intervals.

Relevant to IPSec

Type integer (percents)

Default Value 100

dev/<name>/ipsec/auto/no_auto_reconnect

Description Indicates whether to prevent establishing a new connection when a peer disconnects.

Relevant to IPSec

Type boolean

Default Value False=0

23.9.7 Phase 1

dev/<name>/ipsec/auto/phase1/mode

Description Type of negotiation in phase1, either main or aggressive.

Relevant to IPSec

Type one string of:
"main" (IPSEC_MAIN_MODE),
"aggressive" (IPSEC_AGGRESSIVE_MODE)

Default Value "main"

dev/<name>/ipsec/auto/phase1/lifetime

Description Lifetime in seconds of the negotiated session.

Relevant to IPSec

Type unsigned integer

Default Value 3600

23.9.7.1 Authentication

dev/<name>/ipsec/auto/phase1/auth/type

Description Type of authentication in phase 1.

Relevant to IPSec

Type one string of:
"shared" (IPSEC_AUTH_TYPE_SHARED),
"rsa" (IPSEC_AUTH_TYPE_RSA),
"certificate" (IPSEC_AUTH_TYPE_CERT)

Default Value "shared"

dev/<name>/ipsec/auto/phase1/auth/shared_secret

Description The shared secret to be used in phase 1 of Internet Key Exchange (IKE).

Relevant to IPSec

Type text[MAX_PPP_PASSWORD_LEN=30]

Default Value

dev/<name>/ipsec/auto/phase1/auth/rsa/public

Description RSA key of remote side.

Relevant to IPSec

Type binary

Default Value

dev/<name>/ipsec/auto/phase1/auth/cert

Description OpenRG's certificate name, as specified in **cert/%/name** (see entry cert/%/name on page 19).

Relevant to IPSec

Type text[MAX_X509_NAME_LEN=64]

Default Value

dev/<name>/ipsec/auto/phase1/auth/peer_id

Description Peer ID when IPSec authentication type is "certificate".

Relevant to IPSec

Type text[MAX_CERT_SUBJECT_LEN=255]

Default Value

dev/<name>/ipsec/auto/phase1/auth/local_id

Description Local ID when IPSec authentication type is "certificate".

Relevant to IPSec

Type text[MAX_CERT_SUBJECT_LEN=255]

Default Value

23.9.7.2 Aggressive

dev/<name>/ipsec/auto/phase1/aggressive/hash

Description Specifies which hash algorithm is used in aggressive mode.

Relevant to IPSec

Type one string of:
"sha1" (IPSEC_AUTH_SHA1),
"md5" (IPSEC_AUTH_MD5)

Default Value "sha1"

dev/<name>/ipsec/auto/phase1/aggressive/encrypt

Description Specifies which encryption is used in aggressive mode.

Relevant to IPSec

Type one string of:
"null" (IPSEC_ENC_NULL),
"des" (IPSEC_ENC_DES),
"3des" (IPSEC_ENC_3DES),
"aes128" (IPSEC_ENC_AES128),
"aes192" (IPSEC_ENC_AES192),
"aes256" (IPSEC_ENC_AES256)

Default Value IPSEC_ENC_3DES=0x4

dev/<name>/ipsec/auto/phase1/aggressive/dh_group

Description Specifies which DH group is used in aggressive mode.

Relevant to IPSec

Type one string of:
"1" (IPSEC_DH_GROUP1),
"2" (IPSEC_DH_GROUP2),
"5" (IPSEC_DH_GROUP5)

Default Value "2"

23.9.7.3 Main

dev/<name>/ipsec/auto/phase1/main/hash/md5

Description Specifies whether MD5 is used in main mode.

Relevant to IPSec

Type boolean

Default Value True=1

dev/<name>/ipsec/auto/phase1/main/hash/sha1

Description Specifies whether SHA1 is used in main mode.

Relevant to IPSec

Type boolean

Default Value True=1

dev/<name>/ipsec/auto/phase1/main/encrypt/des

Description Specifies whether DES is used in main mode.

Relevant to IPSec

Type boolean

Default Value False=0

dev/<name>/ipsec/auto/phase1/main/encrypt/3des

Description Specifies whether 3DES is used in main mode.

Relevant to IPSec

Type boolean

Default Value True=1

dev/<name>/ipsec/auto/phase1/main/dh_group/grp1

Description Specifies whether Diffie-Hellman (DH) group 1 is used in main mode.

Relevant to IPSec

Type boolean

Default Value False=0

dev/<name>/ipsec/auto/phase1/main/dh_group/grp2 **Description** Specifies whether Diffie-Hellman (DH) group 2 is used in main mode. **Relevant to** IPSec **Type** boolean **Default Value** True=1
dev/<name>/ipsec/auto/phase1/main/dh_group/grp5 **Description** Specifies whether Diffie-Hellman (DH) group 5 is used in main mode. **Relevant to** IPSec **Type** boolean **Default Value** True=1

23.9.8 Phase 2

dev/<name>/ipsec/auto/phase2/lifetime **Description** Lifetime in seconds of the negotiated session. **Relevant to** IPSec **Type** unsigned integer (seconds) **Default Value** 28000
dev/<name>/ipsec/auto/phase2/use_pfs **Description** Indicates whether Perfect Forwarding Secrecy (PFS) should be used. **Relevant to** IPSec **Type** boolean **Default Value** True=1

dev/<name>/ipsec/auto/phase2/dh_group

Description Specifies which DH group is used in phase 2.

Relevant to IPSec

Type one string of:
"same_as_phase1" (IPSEC_DH_GROUP_SAME_AS_PHASE1),
"1" (IPSEC_DH_GROUP1),
"2" (IPSEC_DH_GROUP2),
"5" (IPSEC_DH_GROUP5)

Default Value "same_as_phase1"

23.9.8.1 Hash

dev/<name>/ipsec/auto/phase2/hash/md5

Description Specifies whether MD5 is used in phase2.

Relevant to IPSec

Type boolean

Default Value True=1

dev/<name>/ipsec/auto/phase2/hash/sha1

Description Specifies whether SHA1 is used in phase2.

Relevant to IPSec

Type boolean

Default Value True=1

23.9.8.2 ESP

dev/<name>/ipsec/auto/phase2/esp/hash/md5

Description Specifies whether MD5 is used in phase2 ESP protocol.

Relevant to IPSec

Type boolean

Default Value True=1

dev/<name>/ipsec/auto/phase2/esp/hash/sha1 **Description** Specifies whether SHA1 is used in phase2 ESP protocol. **Relevant to** IPSec **Type** boolean **Default Value** True=1
dev/<name>/ipsec/auto/phase2/esp/encrypt/null **Description** Specifies whether null ESP is used in phase2. **Relevant to** IPSec **Type** boolean **Default Value** False=0
dev/<name>/ipsec/auto/phase2/esp/encrypt/des **Description** Specifies whether DES ESP is used in phase2. **Relevant to** IPSec **Type** boolean **Default Value** False=0
dev/<name>/ipsec/auto/phase2/esp/encrypt/3des **Description** Specifies whether use 3DES ESP is used in phase2. **Relevant to** IPSec **Type** boolean **Default Value** True=1

23.9.9 Dead Peer Detection

dev/<name>/ipsec/dpd/enabled **Description** Indicates whether Dead Peer Detection (DPD) is enabled. **Relevant to** IPSec **Type** boolean **Default Value**

dev/<name>/ipsec/dpd/delay **Description** Determines the time (in seconds) without traffic through the IPsec tunnel. If during 'delay' seconds no packets are transferred over the IPSec tunnel, OpenRG sends a DPD packet. **Relevant to** IPSec **Type** integer **Default Value**
dev/<name>/ipsec/dpd/timeout **Description** The number of seconds OpenRG will wait for a reponse from the remote VPN router before closing the IPSec tunnel. **Relevant to** IPSec **Type** integer **Default Value**

23.10 IPv6

dev/<name>/ipv6/%/addr **Description** IPv6 address of the device. **Relevant to** WBM, IPv6 **Type** ipv6 **Default Value** fec0:0:0:<id>::(<id> is the ID of the device)
dev/<name>/ipv6/%/prefix_len **Description** IPv6 prefix length. **Relevant to** WBM, IPv6 **Type** integer [0-128] **Default Value** 64

dev/<name>/ipv6/%/is_eui64

Description Indicates whether to use the device MAC to create the lower 64 bits of this address.

Relevant to WBM, IPv6

Type boolean

Default Value True=1

dev/<name>/route6/%/addr6

Description IPv6 destination network address for the route.

Relevant to General

Type ipv6

Default Value

dev/<name>/route6/%/prefix_len

Description IPv6 destination network prefix length for the route.

Relevant to General

Type integer [0-128]

Default Value

dev/<name>/route6/%/gateway

Description Address of route gateway.

Relevant to General

Type ip

Default Value

23.11 RADIUS

dev/<name>/8021x_auth/port_auth

Description Indicates whether 802.1x authentication is enabled.

Relevant to 8021x Authentication

Type boolean

Default Value

dev/<name>/8021x_auth/re_auth_period

Description 802.1x Authentication re-authentication period in seconds.

Relevant to 8021x Authentication

Type integer

Default Value

dev/<name>/8021x_auth/tx_period

Description 802.1x Authentication identity request retransmission period in seconds.

Relevant to 8021x Authentication

Type integer

Default Value

dev/<name>/8021x_auth/pre_auth

Description WPA2 pre-authentication mode.

Relevant to 8021x Authentication

Type boolean

Default Value Disabled=0

dev/<name>/8021x_auth/pmk_cache_period

Description WPA2 PMK cache period, after time out (in minutes), the cached key will be deleted.

Relevant to 8021x Authentication

Type integer [0..]

Default Value 10

23.12 Web Authentication

web_auth/authenticated_clients/<mac>

Description MAC address of an authenticated clients.

Relevant to Wireless LAN

Type text[MAX_MAC_SIZE=18]

Default Value

web_auth/blocked_clients/<mac>

Description MAC address of an blocked clients.

Relevant to Wireless LAN

Type text[MAX_MAC_SIZE=18]

Default Value

23.13 Wireless Local Area Network (WLAN)

23.13.1 General

dev/<name>/wlan/key_mgt

Description Wired Equivalent Privacy (WEP) Encryption and key management method to be used in wireless LAN.

Relevant to Wireless LAN

Type one string of:
"disabled" (WEP_TYPE_DISABLED),
"fixed" (WEP_TYPE_FIXED),
"mixed" (WEP_TYPE_MIXED),
"dynamic" (WEP_TYPE_DYNAMIC)

Default Value

dev/<name>/wlan/active_key

Description The chosen transmit key.

Relevant to Wireless LAN

Type integer [0..3]

Default Value

dev/<name>/wlan/key_passphrase

Description TR-069: A passphrase from which the WEP keys were generated (write only field).

Relevant to Wireless LAN

Type string

Default Value

dev/<name>/wlan/location_description

Description TR-069: An XML dexcription of information used to idenfity the access pint by name and physical location (write only field)

Relevant to Wireless LAN

Type string

Default Value

dev/<name>/wlan/8021x/rekey_timeout

Description The rekeying timeout in seconds.

Relevant to Wireless LAN

Type integer

Default Value

dev/<name>/wlan/frameburst

Description Indicates whether framebursts are enabled.

Relevant to Wireless LAN

Type boolean

Default Value

/dev/<name>/wlan/operation_mode

Description Specifies the Wireless Local Area Network (WLAN) operation mode.

Relevant to Wireless LAN

Type one string of:
"ap" (WLAN_OP_MODE_AP),
"repeater" (WLAN_OP_MODE_REPEATER)

Default Value

dev/<name>/network_name

Description 802.11b internal device network name.

Relevant to 802.11b

Type text[MAX_80211B_NETWORK_NAME_LEN=63]

Default Value

dev/<name>/encryption/key

Description Key for 802.11b internal device network encryption.

Relevant to 802.11b

Type text[MAX_ENC_KEY_LEN=20]

Default Value

23.13.2 Key

dev/<name>/wlan/key/%/length

Description Length of the encryption key in bits. The key index can be 0-3.

Relevant to Wireless LAN

Type integer [40,104]

Default Value

dev/<name>/wlan/key/%/key

Description The encryption key in hexadecimal representation. The key index can be 0-3

Relevant to Wireless LAN

Type string

Default Value

23.13.3 Repeater

dev/<name>/wlan/repeater/root_ap_ssid

Description Service Set Identifier (SSID) of root AP. This is the unique wireless network name.

Relevant to Wireless LAN

Type string

Default Value

dev/<name>/wlan/repeater/privacy_enabled

Description Specifies whether WEP is used in repeater mode.

Relevant to Wireless LAN

Type boolean

Default Value False=0

dev/<name>/wlan/repeater/key/%/length

Description Length in bits of the WEP encryption key used in repeater mode.

Relevant to Wireless LAN

Type integer [40,104]

Default Value

dev/<name>/wlan/repeater/key/%/key

Description The WEP encryption key used in repeater mode in hexadecimal representation.

Relevant to Wireless LAN

Type string

Default Value

dev/<name>/wlan/repeater/active_key

Description Index of WEP encryption key used for transmission in repeater mode.

Relevant to Wireless LAN

Type integer [0..3]

Default Value

23.14 Wireless LAN Access Point

dev/<name>/wl_ap/wl_ssid **Description** Service Set Identifier (SSID). This is the unique wireless network name. **Relevant to** 80211G Access Point **Type** string **Default Value** openrg
dev/<name>/wl_ap/wl_ssid_broadcast_enabled **Description** Indicates whether SSID broadcast is enabled. **Relevant to** 80211G Access Point **Type** boolean **Default Value** True=1
dev/<name>/wl_ap/wl_wmm/enabled **Description** Indicates whether Wi-FI Multimedia (WMM) is enabled. **Relevant to** Wireless LAN **Type** boolean **Default Value** True=1
dev/<name>/wl_ap/wl_wmm/access_category/ack_policy **Description** 802.11e ACK policy for all access category classes. **Relevant to** Wireless LAN **Type** enum wl_ack_policy_t WL_ACK_POLICY_NORMAL = 0, WL_AC_NONE = 1 **Default Value**

dev/<name>/wl_ap/wl_wmm/access_category/background/ack_policy

Description 802.11e ACK policy for background access category class.

Relevant to Wireless LAN

Type enum wl_ack_policy_t
WL_ACK_POLICY_NORMAL = 0,
WL_AC_NONE = 1

Default Value

dev/<name>/wl_ap/wl_wmm/access_category/best_effort/ack_policy

Description 802.11e ACK policy for best effort access category class.

Relevant to Wireless LAN

Type enum wl_ack_policy_t
WL_ACK_POLICY_NORMAL = 0,
WL_AC_NONE = 1

Default Value

dev/<name>/wl_ap/wl_wmm/access_category/video/ack_policy

Description 802.11e ACK policy for video access category class.

Relevant to Wireless LAN

Type enum wl_ack_policy_t
WL_ACK_POLICY_NORMAL = 0,
WL_AC_NONE = 1

Default Value

dev/<name>/wl_ap/wl_wmm/access_category/voice/ack_policy

Description 802.11e ACK policy for voice access category class.

Relevant to Wireless LAN

Type enum wl_ack_policy_t
WL_ACK_POLICY_NORMAL = 0,
WL_AC_NONE = 1

Default Value

dev/<name>/wl_ap/wl_lazywds

Description Indicates whether Lazy Wireless Data System (WDS) Discovery is enabled.

Relevant to 80211G Access Point

Type boolean

Default Value False=0

dev/<name>/wl_ap/wl_plcphdr_long

Description Indicates whether the Physical Layer Convergence Protocol (PLCP) header is long.

Relevant to 80211G Access Point

Type boolean

Default Value True=1

dev/<name>/wl_ap/wl_bcn

Description Beacon Interval in milliseconds for the Access Point (AP).

Relevant to 80211G Access Point

Type integer

Default Value 100

dev/<name>/wl_ap/wl_dtim

Description Wakeup Interval for clients in power-save mode.

Relevant to 80211G Access Point

Type integer

Default Value 1

dev/<name>/wl_ap/wl_rts

Description Threshold in bytes for Request To Send (RTS).

Relevant to 80211G Access Point

Type integer

Default Value 2346

dev/<name>/wl_ap/wl_frag

Description Fragmentation threshold in bytes.

Relevant to 80211G Access Point

Type integer

Default Value 2346

dev/<name>/wl_ap/wl_rate

Description Data Rate in Kbps to be used, or **-1** for automatic.

Relevant to 80211G Access Point

Type integer

Default Value -1

dev/<name>/wl_ap/wl_channel

Description WLAN channel. The default for 802.11G is 11, otherwise 52.

Relevant to 80211G Access Point

Type integer

Default Value

dev/<name>/wl_ap/wl_channel_width_mode

Description WLAN 802.11n channel width mode.

Relevant to 80211N Access Point

Type enum wl_channel_width_t
WL_CWM_MODE20 = 0,
WL_CWM_MODE2040 = 1,
WL_CWM_MODE40 = 2

Default Value WL_CWM_MODE20

dev/<name>/wl_ap/wl_macmode

Description Indicates whether MAC filtering is off (0), allowed (1) or denied (2) on this device.

Relevant to 80211G Access Point

Type integer

Default Value 1

dev/<name>/wl_ap/wl_auth

Description Authentication mode.

Relevant to 80211G Access Point

Type enum wl_auth_t
WL_AUTH_OPEN = 0,
WL_AUTH_SHARED = 1,
WL_AUTH_BOTH = 2,
WL_AUTH_NONE = 3

Default Value 0

dev/<name>/wl_ap/wl_mode_ap

Description Indicates whether the device is in access point mode. Otherwise it is in station mode.

Relevant to 80211G Access Point

Type boolean

Default Value True=1

dev/<name>/wl_ap/wl_dot11_mode

Description 802.11 mode.

Relevant to 80211G Access Point

Type one string of:
"mixed" (DOT11_MODE_MIXED),
"g_only" (DOT11_MODE_G_ONLY),
"b_only" (DOT11_MODE_B_ONLY),
"108g_dynamic" (DOT11_MODE_G_DYNAMIC_TURBO),
"lrs" (DOT11_MODE_LRS)

Default Value

dev/<name>/wl_ap/wl_cts_mode

Description Clear To Send (CTS) protection mode.

Relevant to 80211G Access Point

Type one string of:
"none" (DOT11_CTS_MODE_NONE),
"always" (DOT11_CTS_MODE_ALWAYS),
"auto" (DOT11_CTS_MODE_AUTO)

Default Value "auto"

dev/<name>/wl_ap/wl_cts_type

Description CTS protection type.

Relevant to 80211G Access Point

Type one string of:
"cts" (DOT11_CTS_TYPE_CTS),
"rts_cts" (DOT11_CTS_TYPE_RTS_CTS)

Default Value "cts"

dev/<name>/wl_ap/wl_burst_time

Description Burst time.

Relevant to 80211G Access Point

Type integer [0..1023]

Default Value 2

dev/<name>/wl_ap/wl_superg_mode

Description SuperG mode.

Relevant to 80211G Access Point

Type one string of:
"enabled" (SUPERG_MODE_ENABLED),
"disabled" (SUPERG_MODE_DISABLED)

Default Value

dev/<name>/wl_ap/wl_burst_seq_threshold

Description Burst sequence threshold.

Relevant to 80211G Access Point

Type integer

Default Value

dev/<name>/wl_ap/wl_inter_client_privacy

Description Inter Client Privacy.

Relevant to 80211G Access Point

Type boolean

Default Value Disabled=0

dev/<name>/wl_ap/wl_inter_bssid_privacy

Description Inter BSSID Privacy.

Relevant to 80211G Access Point

Type boolean

Default Value Disabled=0

dev/<name>/wl_ap/wl_tx_power

Description Transmit Power.

Relevant to 80211G Access Point

Type integer [1..100]

Default Value 100

dev/<name>/wl_ap/wl_basic_rates/g_phy

Description TR-069 queries: Maximum AP data transmit rates in Mbps for unicast, multicast and broadcast frames in 802.11g mode.

Relevant to 80211G Access Point

Type comma separated string of rates

Default Value

dev/<name>/wl_ap/wl_basic_rates/b_phy

Description TR-069 queries: Maximum AP data transmit rates in Mbps for unicast, multicast and broadcast frames in 802.11b mode.

Relevant to 80211G Access Point

Type comma separated string of rates

Default Value

dev/<name>/wl_ap/wl_basic_rates/bg_phy

Description TR-069 queries: Maximum AP data transmit rates in Mbps for unicast, multicast and broadcast frames in 802.11 mixed-bg mode.

Relevant to 80211G Access Point

Type comma separated string of rates

Default Value

dev/<name>/wl_ap/wl_op_rates/g_phy

Description TR-069 queries: Maximum AP data transmit rates in Mbps for unicast frames in 802.11g mode.

Relevant to 80211G Access Point

Type comma separated string of rates

Default Value

dev/<name>/wl_ap/wl_op_rates/b_phy

Description TR-069 queries: Maximum AP data transmit rates in Mbps for unicast frames in 802.11b mode.

Relevant to 80211G Access Point

Type comma separated string of rates

Default Value

dev/<name>/wl_ap/wl_op_rates/bg_phy

Description TR-069 queries: Maximum AP data transmit rates in Mbps for unicast frames in 802.11 mixed-bg mode.

Relevant to 80211G Access Point

Type comma separated string of rates

Default Value

23.15 Wi-Fi Protected Access (WPA)

dev/<name>/wpa/privacy_enabled

Description Specifies whether security is enabled for the device.

Relevant to WPA

Type boolean

Default Value False=0

dev/<name>/wpa/accept_wpa_stas

Description Specifies whether Wi-Fi Protected Access (WPA) stations should be accepted by the AP.

Relevant to WPA

Type boolean

Default Value True=1

dev/<name>/wpa/accept_wpa2_stas

Description Specifies whether WPA2 stations should be accepted by the AP.

Relevant to WPA

Type boolean

Default Value False=0

dev/<name>/wpa/accept_8021x_wep_stas

Description Specifies whether 802.1X WEP stations should be accepted by the AP.

Relevant to WPA

Type boolean

Default Value False=0

dev/<name>/wpa/accept_non_8021x_wep_stas

Description Specifies whether non-802.1X WEP stations should be accepted by the AP.

Relevant to WPA

Type boolean

Default Value False=0

dev/<name>/wpa/auth_mode

Description The WPA authentication method.

Relevant to WPA

Type one string of:
"none" (WPA_PSK_PARAM_NONE),
"hex" (WPA_PSK_PARAM_HEX),
"ascii" (WPA_PSK_PARAM_ASCII)

Default Value "none"

dev/<name>/wpa/preshared_key

Description The preshared key in hexadecimal or text representation, depending on the authentication mode (**dev/<name>/wpa/auth_mode**).

Relevant to WPA

Type string

Default Value

dev/<name>/wpa/auto_key_mgt_disabled

Description Specifies whether to disable automatic key generation.

Relevant to WPA

Type boolean

Default Value False=0

dev/<name>/wpa/wep_rekeying_key_length

Description Length in bits of the encryption key generated for 802.1X stations.

Relevant to WPA

Type integer [40,104]

Default Value

dev/<name>/wpa/cipher

Description Type of encryption algorithm used by WPA.

Relevant to WPA

Type one string of:
"tkip" (CFG_WPA_CIPHER_TKIP),
"tkip_aes" (CFG_WPA_CIPHER_TKIP_AES),
"aes" (CFG_WPA_CIPHER_AES)

Default Value

dev/<name>/wpa/beacon_type/type

Description TR-069 queries: Type of security used.

Relevant to WPA

Type one string of:
"None",
"Basic",
"WPA",
"11i",
"WPAand11i"

Default Value

dev/<name>/wpa/beacon_type/basic/encrypt_mode

Description TR-069 queries: Type of encryption used for wep.

Relevant to WPA

Type one string of:
"WEPEncryption"

Default Value

dev/<name>/wpa/beacon_type/basic/auth_mode

Description TR-069 queries: Type of authentication used for wep.

Relevant to WPA

Type one string of:
"None",
"EAPAuthentication"

Default Value

dev/<name>/wpa/beacon_type/wpa/encrypt_mode

Description TR-069 queries: Type of encryption used for wpa and wpa2.

Relevant to WPA

Type one string of:
"TKIPEncryption",
"AESEncryption",
"TKIPandAESEncryption"

Default Value

dev/<name>/wpa/beacon_type/wpa/auth_mode

Description TR-069 queries: Type of authentication used for wpa and wpa2.

Relevant to WPA

Type one string of:
"PSKAuthentication",
"EAPAuthentication"

Default Value

dev/<name>/wpa/radius/ip

Description RADIUS server IP. When you define a server you must specify its IP.

Relevant to RADIUS

Type ip

Default Value

dev/<name>/wpa/radius/port

Description RADIUS server Port. When you define a server you must specify its port.

Relevant to RADIUS

Type integer

Default Value

dev/<name>/wpa/radius/shared_secret

Description RADIUS shared secret. When you define a server you must specify its shared secret. This entry is encrypted.

Relevant to RADIUS

Type text[RADIUS_SECRET_LEN=64]

Default Value

dev/<name>/wpa/8021x/pre_auth

Description Enable WPA-2 802.1x pre authentication.

Relevant to WPA-2

Type boolean

Default Value 1

dev/<name>/wpa/8021x/pmk_cache_period **Description** Set the PMK caching timeout period in minutes. **Relevant to** WPA-2 **Type** integer **Default Value** 10
dev/<name>/wpa/wps/enabled **Description** Specifies whether WPS is enabled for the device. **Relevant to** WPA **Type** boolean **Default Value** False=0
dev/<name>/wpa/wps/manual_create_key **Description** Specifies whether WPS preshared key of WPA/WPA2 should be configured manually. **Relevant to** WPA **Type** boolean **Default Value** False=0

23.16 Routing Information Protocol (RIP)

dev/<name>/rip/enabled **Description** Indicates if Routing Information Protocol (RIP) feature is enabled on this device. RIP can be enabled on devices only if **rip/enabled** is true (refer to Section 32.2). **Relevant to** rip **Type** boolean **Default Value**

dev/<name>/rip/input_version

Description Version of RIP messages to which to listen on this device. Relevant only if RIP is enabled for this device.

Relevant to rip

Type enum rip_input_version_t
RIP_INPUT_NONE = 0,
RIP_INPUT_V1 = 1,
RIP_INPUT_V2 = 2,
RIP_INPUT_ALL = 3

Default Value

dev/<name>/rip/output_version

Description Version of RIP messages to send from this device. Relevant only if RIP is enabled for this device.

Relevant to rip

Type enum rip_output_version_t
RIP_OUTPUT_NONE = 0,
RIP_OUTPUT_V1 = 1,
RIP_OUTPUT_V2_BROADCAST = 2,
RIP_OUTPUT_V2_MULTICAST = 3

Default Value

23.17 Quality of Service (QoS)

23.17.1 Shaping

dev/<name>/qos/shaping/enabled

Description Indicates whether Quality of Service (QoS) feature is enabled for the device.

Relevant to QoS

Type boolean

Default Value

dev/<name>/qos/shaping/tx_bandwidth

Description Transmission (Tx) traffic limit in Kbps for the device.

Relevant to QoS

Type integer

Default Value

dev/<name>/qos/shaping/rx_bandwidth

Description Reception (Rx) traffic limit in Kbps for the device.

Relevant to QoS

Type integer

Default Value

dev/<name>/qos/shaping/tcp_ser_enable

Description Indicates whether TCP serialization delay limiting is enabled for the device.

Relevant to QoS

Type boolean

Default Value

dev/<name>/qos/shaping/tcp_ser_max_delay

Description The value of the TCP serialization delay limit in milliseconds, using Maximum Segment Size (MSS) clamping.

Relevant to QoS

Type integer

Default Value

dev/<name>/qos/shaping/tx_queue_policy

Description Indicates the devices egress queueing policy.

Relevant to QoS

Type one string of:
"class_based" (QOS_QUEUE_POLICY_CLASS_BASED),
"strict_priority" (QOS_QUEUE_POLICY_STRICT_PRIORITY)

Default Value

dev/<name>/qos/shaping/rx_queue_policy

Description Indicates the devices ingress queueing policy.

Relevant to QoS

Type one string of:
"policer" (QOS_QUEUE_POLICY_POLICER),
"class_based" (QOS_QUEUE_POLICY_CLASS_BASED),
"strict_priority" (QOS_QUEUE_POLICY_STRICT_PRIORITY)

Default Value

23.17.2 Traffic Class

dev/<name>/qos/traffic_class/<tx/rx>/%/name

Description The class name.

Relevant to General

Type string[0-256]

Default Value

dev/<name>/qos/traffic_class/<tx/rx>/%/enable

Description Indicates whether the class is enabled.

Relevant to General

Type boolean

Default Value 1

dev/<name>/qos/traffic_class/<tx/rx>/%/priority

Description The class priority when competing with others on loaned bandwidth. Note that 0 is the highest priority and 7 is the lowest.

Relevant to General

Type 0-7

Default Value 0

dev/<name>/qos/traffic_class/<tx/rx>/%/policy

Description The forward policy of the class.

Relevant to General

Type one string of
"priority" (QOS_POLICY_PRIORITY),
"fifo" (QOS_POLICY_FIFO),
"fairness" (QOS_POLICY_FAIRNESS),
"red" (QOS_POLICY_RED)

Default Value 0

dev/<name>/qos/traffic_class/<tx/rx>/%/max_bandwidth

Description The maximum bandwidth value for the class in Kbps.

Relevant to General

Type integer, -1 means unlimited

Default Value -1

dev/<name>/qos/traffic_class/<tx/rx>/%/min_bandwidth

Description The guarantied bandwidth value for the class in Kbps.

Relevant to General

Type integer

Default Value 0

dev/<name>/qos/traffic_class/tx/%/if

Description Specifies the interface to which this TX class should be applied.

Relevant to QOS

Type string

Default Value

dev/<name>/qos/traffic_class/tx/%/wildcard_if

Description In case the device 'dev' is a wildcard device this field specifies the group of interfaces to which this TX class should be applied.

Relevant to QOS

Type enum WC_IF_WAN = 1,
WC_IF_LAN = 2

Default Value

dev/<name>/qos/traffic_class/tx/%/parent

Description Specifies the index of this classes parent, if any.

Relevant to QOS

Type integer

Default Value

dev/<name>/qos/traffic_class/tx/%/weight

Description Specifies the weight of this class.

Relevant to QOS

Type integer (1-INT_MAX)

Default Value

23.17.3 VLAN to DSCP

dev/<name>/qos/vlan_to_dscp/enabled

Description Indicates whether remarking DSCP in the IP header according to 802.1p is performed for all incoming packets on this VLAN device.

Relevant to QoS & VLAN

Type boolean

Default Value

dev/<name>/qos/vlan_to_dscp/map/%/8021p

Description 802.1p to DSCP map. A frame with this 802.1p value is set with the corresponding DSCP value in its IP header.

Relevant to QoS & VLAN

Type integer 0-7

Default Value

dev/<name>/qos/vlan_to_dscp/map/%/dscp

Description 802.1p to DSCP map. Sets the IP header's DSCP field to this value for the corresponding 802.1p CoS value.

Relevant to QoS & VLAN

Type integer 0-63

Default Value

23.18 Route

dev/<name>/route/dscp/%

Description When adding automatic routes for this device (default gateway, subnet, DNS routes), add routes matching these DCSP values.

Relevant to Policy Based Routing

Type integer (0-63)

Default Value

dev/<name>/route/load_balancing/enabled

Description Indicates whether the device will be used for load balancing.

Relevant to Load Balancing

Type boolean

Default Value False=0

dev/<name>/route/load_balancing/weight

Description Device weight in load balancing process.

Relevant to Load Balancing

Type integer 1-256

Default Value

dev/<name>/route/failover/enabled

Description Indicates whether failover is enabled for this device.

Relevant to Failover

Type boolean

Default Value

dev/<name>/route/failover/rollover

Description Indicates whether this is a possible rollover device for a failover event.

Relevant to Failover

Type boolean

Default Value

dev/<name>/route/failover/%/enabled

Description Indicates whether failover code should test DNS connectivity for this device.

Relevant to Failover

Type boolean

Default Value

dev/<name>/route/failover/%/name

Description The URL of the host queried for its address when performing a failover DNS connectivity test.

Relevant to Failover

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

24

Network Objects

Network Objects is a method used to abstractly define a set of LAN hosts, according to specific criteria, such as MAC address, IP address, or host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring OpenRG's security filtering settings such as IP address filtering, host name filtering or MAC address filtering. You can use network objects in order to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time.

It is also possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings. Moreover, OpenRG supports several DHCP options—60, 61, and 77, enabling the gateway to apply security and QoS rules on a network object according to its unique vendor, client, or user class ID, respectively. For example, a Dell OpenRG™ IP telephone can be identified and applied with specific QoS priority rules.

net_obj/%/description

Description Description of Network Object. A network object item can be a hostname, an IP address, a subnet, a MAC address or a range of IP addresses.

Relevant to MGT, Firewall

Type text

Default Value

net_obj/%/item/%/hostname

Description Network Object item with hostname data.

Relevant to MGT, Firewall

Type text[MAX_HOSTNAME_LEN=63]

Default Value

net_obj/%/item/%/ip

Description The single IP address of an item.

Relevant to MGT, Firewall

Type ip

Default Value

net_obj/%/item/%/netmask

Description Network mask of item with subnet data.

Relevant to MGT, Firewall

Type ip

Default Value

net_obj/%/item/%/mac

Description Network Object item with masked MAC address.

Relevant to MGT, Firewall

Type mac

Default Value

net_obj/%/item/%/mask

Description Network Object item with masked MAC address.

Relevant to MGT, Firewall

Type mac

Default Value ff:ff:ff:ff:ff:ff

net_obj/%/item/%/start_ip

Description The start IP address of an IP range.

Relevant to MGT, Firewall

Type ip

Default Value

net_obj/%/item/%/end_ip

Description The end IP address of an IP range.

Relevant to MGT, Firewall

Type ip

Default Value

net_obj/%/item/%/dhcp_option/code

Description Code of DHCP Option object.

Relevant to MGT, Firewall

Type int

Default Value

net_obj/%/item/%/dhcp_option/value

Description Value of DHCP Option object.

Relevant to MGT, Firewall

Type string

Default Value

net_obj/%/item/%/dhcp_option/is_mac

Description Determines whether the firewall translates the dhcp options as an ip list from the dhcp server leases or as mac list from the hybrid model dhcp list.

Relevant to MGT, Firewall

Type boolean

Default Value

25

Point-to-Point Protocol over Ethernet (PPPoE) Relay

Point-to-Point Protocol over Ethernet (PPPoE) relies on two widely accepted standards, PPP and Ethernet. PPPoE enables your home network PCs that communicate on an Ethernet network to exchange information with PCs on the Internet. PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the multipoint architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.

pppoe_relay/disabled **Description** Indicates whether PPPoE Relay is disabled or not. When false, PPPoE is enabled. **Relevant to** PPPoE **Type** boolean **Default Value** True=1
pppoe_relay/expiration_timeout **Description** The timeout in seconds for expiring unused PPPoE Relay session. 0 means indefinite timeout. **Relevant to** PPPoE **Type** integer **Default Value** 0

26

Point-to-Point Tunneling Protocol (PPTP) Server

- General -- general PPTP server entries (refer to Section 26.1).
- Remote -- remote user entries (refer to Section 26.2).
- Authentication -- authentication entries to be passed to the PPP connection (refer to Section 26.3).
- Encryption -- encryption entries to be passed to the PPP connection (refer to Section 26.4).

26.1 General

pptps/enabled

Description Indicates whether Point-to-Point Tunneling Protocol (PPTP) Server accepts connections.

Relevant to PPTPS

Type boolean

Default Value False=0

pptps/idle_timeout

Description The number of seconds with no activity after which the connection is disconnected. This entry is passed to the PPP connection.

Relevant to PPP

Type integer

Default Value 1200

26.2 Remote

pptps/remote/from

Description The first IP address in the IP range for the connection on the remote side. The IP must be in the same local subnet as the OpenRG.

Relevant to PPTPS

Type ip

Default Value

pptps/remote/to

Description The last IP address in the IP range for the connection on the remote side. The IP must be in the same local subnet as the OpenRG.

Relevant to PPTPS

Type ip

Default Value

26.3 Authentication

pptps/auth/required

Description Indicates whether the user is required to authenticate. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

pptps/auth/pap

Description Indicates whether Password Authentication Protocol (PAP) authentication is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value False=0

pptps/auth/chap

Description Indicates whether CHAP authentication is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value False=0

pptps/auth/ms_chap_v1

Description Indicates whether MS-CHAP authentication is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

pptps/auth/ms_chap_v2

Description Indicates whether MS-CHAP-v2 authentication is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

26.4 Encryption

pptps/encryption/required

Description Indicates whether encryption is required. If it is not, unencrypted connections may be established. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

pptps/encryption/mppe_40

Description Indicates whether MPPE-40 encryption is enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

pptps/encryption/mppe_128

Description Indicates whether MPPE-128 encryption enabled. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

pptps/encryption/mppe_stateless

Description Indicates whether MPPE-stateless encryption is enabled. Stateless encryption means rekeying after every packet. This entry is passed to the PPP connection.

Relevant to PPP

Type boolean

Default Value True=1

27

Print Server

1. Internet Printing Protocol (IPP) -- The recommended protocol is IPP, offering fast installation and ease of use.

2. Microsoft Shared Printing (Samba) -- The Samba protocol allows the administrator to upload Windows print drivers to OpenRG, enabling all Windows-based LAN hosts to connect to the network printer with a single click. It is advised that this protocol be set up by a technical administrator.

3. Line Printer Daemon (LPD) -- LPD is a legacy network printing protocol, which should only be used for printing from computers that do not support IPP.

print_server/enabled **Description** Indicates whether the print server is enabled or disabled. **Relevant to** print_server **Type** boolean **Default Value** True=1
print_server/max_spool_size **Description** Maximum spool size in bytes. The default value is defined per distribution. **Relevant to** print_server **Type** integer **Default Value**

print_server/printer/%/name

Description The name of the printer.

Relevant to print_server

Type text

Default Value

print_server/printer/%/hw_signature

Description The hardware signiture of the printer, raw device information from Universal Serial Bus (USB).

Relevant to print_server

Type text

Default Value

print_server/printer/%/default_devmode_enabled

Description Indicates whether Microsoft Shared printing creates a default device mode for the printer.

Relevant to print_server

Type boolean

Default Value False=0

print_server/guest_printing_enabled

Description Allow access to all users on all printers.

Relevant to Print Server

Type boolean

Default Value True=1

print_server/printer/%/permissions/%/id

Description The ID of a user or a group with access to this printer. The type entry specifies whether it is a group or a user. The ID is the index of the user or group you used in **admin/user/%/** and **admin/group/%/**.

Relevant to Print Server

Type integer

Default Value

print_server/printer/%/permissions/%/type

Description Specifies whether a group or a user has access to this printer. The user or group ID is specified in the id entry.

Relevant to Print Server

Type one string of:
"user" (ACCESS_OBJ_USER),
"group" (ACCESS_OBJ_GROUP)

Default Value

print_server/printer/%/permissions/%/access_level

Description Access level of the user or group with access to this printer. The possible levels are admin, read-write or read only.

Relevant to Print Server

Type one string of:
"admin" (ACCESS_ADMIN),
"rw" (ACCESS_RW)

Default Value

28

Quality of Service (QoS)

qos/8021p/%/priority **Description** The priority queue number. **Relevant to** QoS **Type** one string of: "low" (QOS_PRIO_LOW), "medium" (QOS_PRIO_MEDIUM), "high" (QOS_PRIO_HIGH) **Default Value**
qos/dscp/%/priority **Description** DSCP to 8021p mapping table, the index is the DSCP value. **Relevant to** QoS **Type** 0-7 **Default Value**
qos/dev/<name> **Description** Wild device for QoS (WAN/LAN/DMZ). The structure is the same as dev/<name> (see entry dev/<name>/enabled on page 122). **Relevant to** QoS **Type** device **Default Value**

qos/wizard/profile

Description QoS profile.

Relevant to QoS

Type one string of:
"default" (QOS_PROFILE_DEFAULT)
"p2p_user" (QOS_PROFILE_P2P_USER)
"gamer" (QOS_PROFILE_GAMER)
"home_worker" (QOS_PROFILE_HOME_WORKER)
"triple_play_user" (QOS_PROFILE_TRIPLE_PLAY_USER)
"prio_by_host" (QOS_PROFILE_PRIO_BY_HOST)

Default Value

qos/wizard/low_prio_host

Description Host to be defined as low priority when QoS profile is 'prio_by_host'.

Relevant to QoS

Type netobj

Default Value

qos/wizard/high_prio_host

Description Host to be defined as high priority when QoS profile is 'prio_by_host'.

Relevant to QoS

Type netobj

Default Value

qos/conn_utilization/view

Description Internet connection utilization screen view mode.

Relevant to QoS

Type one string of:
"by_application" (QOS_UTILIZATION_VIEW_BY_APPLICATION)
"by_computer" (QOS_UTILIZATION_VIEW_BY_COMPUTER)

Default Value

qos/queue_enabled

Description Flag indicating whether or not traffic class queueing (Tx) is enabled.

Relevant to QoS

Type boolean

Default Value True=1

qos/chain/

Description QoS classfication chains. The structure is identical to that of firewall rules (fw/policy/%/chain), except for the additions below. Its entries are described in Section 12.6.

Relevant to QoS

Type string

Default Value

qos/chain/%/rule/%/name

Description Name of a rule which represents a TR-098 application or flow.

Relevant to QoS

Type string

Default Value

qos/chain/%/rule/%/app_urn

Description The protocol identifier field of a TR-098 application rule. Used by TR-098 to set action/alg.

Relevant to QoS

Type one string of:
"urn:dslforum-org:sip" (ALG_SIP_UDP),
"urn:dslforum-org:h.323" (ALG_CSL),
"urn:dslforum-org:mgcp" (ALG_MGCP_UDP),
"urn:dslforum-org:rtsp" (ALG_RTSP),
"urn:dslforum-org:ftp" (ALG_FTP)

Default Value

qos/chain/%/rule/%/flow_urn

Description The flow type URN of a TR-098 flow rule.

Relevant to QoS

Type one string of:
"urn:dslforum-org:sip-control" (ALG_FLOW_CONTROL),
"urn:dslforum-org:sip-data" (ALG_FLOW_DATA),
"urn:dslforum-org:h.323-control" (ALG_FLOW_CONTROL),
"urn:dslforum-org:h.323-data" (ALG_FLOW_DATA),
"urn:dslforum-org:mgcp-control" (ALG_FLOW_CONTROL),
"urn:dslforum-org:mgcp-data" (ALG_FLOW_DATA),
"urn:dslforum-org:sdp-video-rtpavp" (ALG_FLOW_VIDEO_RTPAVP),
"urn:dslforum-org:sdp-video-udp" (ALG_FLOW_VIDEO_UDP),
"urn:dslforum-org:sdp-audio-rtpavp" (ALG_FLOW_AUDIO_RTPAVP),
"urn:dslforum-org:sdp-audio-udp" (ALG_FLOW_AUDIO_UDP),
"urn:dslforum-org:sdp-data-udp" (ALG_FLOW_DATA_UDP),
"urn:dslforum-org:sdp-data-tcp" (ALG_FLOW_DATA_TCP),
"urn:dslforum-org:rtsp-control" (ALG_FLOW_CONTROL),
"urn:dslforum-org:rtsp-data" (ALG_FLOW_DATA),
"urn:dslforum-org:ftp-control" (ALG_FLOW_CONTROL),
"urn:dslforum-org:ftp-data" (ALG_FLOW_DATA)

Default Value

qos/chain/%/rule/%/match/app_id

Description Matches the rule for a connection with an application ID.

Relevant to QoS

Type integer

Default Value -1

qos/chain/%/rule/%/match/flow_id.

Description Matches the rule for a connection with an ALG flow type. Derived from **flow_urn** above.

Relevant to QoS

Type enum fw_alg_flow_type_t
ALG_FLOW_NONE = 0,
ALG_FLOW_CONTROL = 1,
ALG_FLOW_DATA = 2,
ALG_FLOW_VIDEO_RTPAVP = 3,
ALG_FLOW_VIDEO_UDP = 4,
ALG_FLOW_AUDIO_RTPAVP = 5,
ALG_FLOW_AUDIO_UDP = 6,
ALG_FLOW_DATA_UDP = 7,
ALG_FLOW_DATA_TCP = 8

Default Value ALG_FLOW_NONE

qos/chain/%/rule/%/action/set_app.

Description Sets the connection's application ID.

Relevant to QoS

Type integer

Default Value

qos/conn_utilization/sort_by

Description Sort the data in the QoS Utilization screen according to this field

Relevant to QoS

Type one string of:
"application" (QOS_CONN_UTILZ_APP),
"protocol" (QOS_CONN_UTILZ_PROTO),
"port" (QOS_CONN_UTILZ_PORT),
"tx_throughput" (QOS_CONN_UTILZ_TX_THROUGHPUT),
"rx_throughput" (QOS_CONN_UTILZ_RX_THROUGHPUT),
"tx_priority" (QOS_CONN_UTILZ_TX_PRIO),
"rx_priority" (QOS_CONN_UTILZ_RX_PRIO),
"computer" (QOS_CONN_UTILZ_COMP)

Default Value "rx_throughput"

qos/conn_utilization/is_ascending

Description Determines if the sort in the QoS utilization screen is ascending

Relevant to QoS

Type boolean

Default Value

qos/conn_utilization/no_service_grouping

Description Determines if the protocols in the QoS utilization screen and the home page are grouped by type.

Relevant to QoS

Type boolean

Default Value

qos/conn_utilization/advanced

Description Determines the value of the basic/advanced button on the QoS utilization screen. In advanced mode, the QoS screen doesn't group the services.

Relevant to QoS

Type boolean

Default Value

29

RADIUS Client

A Remote Authentication Dial-in User Service (RADIUS) server is most commonly a "third party" server, used for authentication of wireless clients who wish to connect to an access point. The wireless client contacts an access point (a RADIUS client), which in turn communicates with the RADIUS server. The RADIUS server performs the authentication by verifying the client's credentials, to determine whether the device is authorized to connect to the access point's LAN. If the RADIUS server accepts the client, it responds by exchanging data with the access point, including security keys for subsequent encrypted sessions. OpenRG can act both as a RADIUS client and a server, and can be used for the authentication of any clients—wireless or wired.

radius/auth/enabled **Description** Indicates whether the RADIUS client is enabled or disabled. **Relevant to** RADIUS **Type** boolean **Default Value** False=0
radius/auth/servers/%/ip **Description** RADIUS server IP. When you define a server you must specify its IP. **Relevant to** RADIUS **Type** ip **Default Value**

radius/auth/servers/%/port

Description RADIUS server Port. When you define a server you must specify its port.

Relevant to RADIUS

Type integer

Default Value

radius/auth/servers/%/shared_secret

Description RADIUS shared secret. When you define a server you must specify its shared secret. This entry is encrypted.

Relevant to RADIUS

Type text[RADIUS_SECRET_LEN=64]

Default Value

radius/auth/servers/%/auth_method

Description RADIUS authentication method. When you define a server you must specify its authentication method.

Relevant to RADIUS

Type one string of:
"pap" (RADIUS_AUTH_PAP),
"chap" (RADIUS_AUTH_CHAP),
"ms-chap" (RADIUS_AUTH_MSCHAP),
"ms-chap_v2" (RADIUS_AUTH_MSCHAPV2)

Default Value

30

RADIUS Server

A Remote Authentication Dial-in User Service (RADIUS) server is most commonly a "third party" server, used for authentication of wireless clients who wish to connect to an access point. The wireless client contacts an access point (a RADIUS client), which in turn communicates with the RADIUS server. The RADIUS server performs the authentication by verifying the client's credentials, to determine whether the device is authorized to connect to the access point's LAN. If the RADIUS server accepts the client, it responds by exchanging data with the access point, including security keys for subsequent encrypted sessions. OpenRG can act both as a RADIUS client and a server, and can be used for the authentication of any clients—wireless or wired.

radius/server/enabled **Description** Indicates whether the RADIUS server is enabled or disabled. **Relevant to** RADIUS **Type** boolean **Default Value** False=0
radius/server/port **Description** The bound UDP port for sending and receiving RADIUS packets. **Relevant to** RADIUS **Type** port **Default Value** 1812

radius/server/default_secret

Description The default shared secret to be used with clients for which a specific shared secret is not defined (see below), if it exists. This entry is obscured.

Relevant to RADIUS

Type string

Default Value

radius/server/client/%/host

Description This is the client's IP address or hostname.

Relevant to RADIUS

Type ip or host

Default Value

radius/server/client/%/secret

Description The specific shared secret to be used with the client. This entry is obscured.

Relevant to RADIUS

Type string

Default Value

radius/server/use_selected_certs

Description If true, use only the CA certificates specified in the following cert section for client authentication. If false - use all CA certificates.

Relevant to RADIUS

Type boolean

Default Value

radius/server/cert/%/id

Description Index of CA certificate to be used for client authentication.

Relevant to RADIUS

Type integer

Default Value

31

Remote Update

The **Remote Update** mechanism helps you keep your software image up-to-date, by performing routine daily checks for newer software versions, as well as letting you perform manual checks.

rmt_upd/url **Description** The URL of the first image or redirection file. For instance: 'http://update.jungo.com/openrg.rmt'. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide. **Relevant to** Remote Update, WBM **Type** text[MAX_LINE_SIZE=1024] **Default Value** http://update.jungo.com/openrg.rmt
rmt_upd/check_interval **Description** The interval (in seconds) between two subsequent WAN upgrade auto checks. **Relevant to** Remote Update, WBM **Type** integer **Default Value** 24 hours

rmt_upd/last_status

Description Status of the last upgrade auto check or upgrade.

Relevant to Remote Update

Type one string of:
"in_progress" (RMT_UPD_IN_PROGRESS),
"bad_signature" (RMT_UPD_BAD_SIG),
"no_matching_header" (RMT_UPD_NO_MATCHING_HEADER),
"done_error" (RMT_UPD_DONE_ERROR),
"ok" (RMT_UPD_DONE_OK),
"no_redirect" (RMT_UPD_REDIRECT),
"file_not_found" (RMT_UPD_FILE_NOT_FOUND),
"no_response" (RMT_UPD_NO_RESPONSE),
"internal_error" (RMT_UPD_INTERNAL_ERROR),
"resolution_error" (RMT_UPD_HOSTNAME_RESOLUTION_ERROR),
"login_error" (RMT_UPD_LOGIN_ERROR),
"unexpected_error" (RMT_UPD_UNEXPECTED_DOWNLOAD_ERROR),
"write_error" (RMT_UPD_PERMANENT_STORAGE_WRITE_ERROR),
"OSS" (RMT_UPD_MGT_CMD)

Default Value

rmt_upd/wan_upgrade_type

Description The mode of automatic WAN upgrade (auto check and upgrade, auto check and notify, auto check disabled).

Relevant to Remote Update, WBM

Type enum wan_upgrade_t
WAN_UPGRADE_CHECK_AND_UPGRADE = 1,
WAN_UPGRADE_CHECK_AND_NOTIFY = 2,
WAN_UPGRADE_DISABLED = 3

Default Value WAN_UPGRADE_CHECK_AND_UPGRADE

rmt_upd/wan_ver

Description The OpenRG version descriptor of the remote image version.

Relevant to Remote Update, WBM

Type integer

Default Value string

rmt_upd/wan_ext_ver

Description The external version descriptor of the remote image version.

Relevant to Remote Update, WBM

Type string

Default Value

rmt_upd/is_jcms_outgoing

Description Indicates whether the remote upgrade server manages OpenRG via a remote upgrade connection.

Relevant to Remote Update, WBM

Type boolean

Default Value True=1

32

Routing

This chapter lists the configuration entries for:

- Each of the routes
- Supported routing protocols: RIP, BGP and OSPF
- Zebra--IP routing management daemon of the Quagga routing software package

32.1 Routes

The following are entries for each of the routes:

route/static/%/dev **Description** Device for the route. **Relevant to** General **Type** text[MAX_VAR_NAME] **Default Value**
route/static/%/addr **Description** Network address for the route. **Relevant to** General **Type** ip **Default Value**

route/static/%/netmask

Description Network mask for the route.

Relevant to General

Type ip

Default Value

route/static/%/gateway

Description Gateway for the route.

Relevant to General

Type ip

Default Value

route/static/%/metric

Description Metric for the route.

Relevant to General

Type unsigned integer

Default Value

route/load_balancing/enabled

Description Indicates whether load balancing is enabled.

Relevant to LB

Type boolean

Default Value

route/failover/enabled

Description Indicates whether failover is enabled.

Relevant to Failover

Type boolean

Default Value

32.2 Routing Information Protocol (RIP)

Routing Information Protocol (RIP) determines a route based on the smallest hop count between a source and a destination.

rip/enabled **Description** Indicates whether RIP feature is enabled or disabled. **Relevant to** RIP, WBM, Firewall **Type** boolean **Default Value** False=0
rip/gen_limit **Description** The limit of routing entries for a Classless Inter-Domain Routing (CIDR) route. If the limit is exceeded, a supernet route will be created instead. **Relevant to** RIP **Type** integer **Default Value**
rip/poison_reverse **Description** Indicates whether poisoned reverse split horizon is enabled instead of simple split horizon. **Relevant to** RIP **Type** boolean **Default Value**
rip/suppress_direct_routes **Description** Indicates whether the direct connected routes should not be advertised. **Relevant to** RIP **Type** boolean **Default Value**

32.3 Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) is the core routing protocol of the Internet.

bgp/enabled **Description** Indicates whether BGP feature is enabled or disabled **Relevant to** BGP, WBM, Firewall **Type** boolean **Default Value** False=0
bgp/conf **Description** Configuration of the BGP daemon in the Quagga format **Relevant to** BGP **Type** string **Default Value**

32.4 Open Shortest Path First (OSPF)

The Open Shortest Path First (OSPF) protocol is a link-state, hierarchical interior gateway protocol (IGP) for network routing.

ospf/enabled **Description** Indicates whether OSPF feature is enabled or disabled **Relevant to** OSPF, WBM, Firewall **Type** boolean **Default Value** False=0
ospf/conf **Description** Configuration of the OSPF daemon in the Quagga format **Relevant to** OSPF **Type** string **Default Value**

32.5 Zebra

Zebra is an IP routing manager. It provides kernel routing table updates, interface lookups, and redistribution of routes between different routing protocols.

zebra/conf

Description Configuration of the Zebra daemon in the Quagga format

Relevant to Zebra

Type string

Default Value

33

Secure Shell

The Secure Shell enables users to remotely and securely log into OpenRG via a shell for remote configuration purposes.

ssh/enabled **Description** Indicates whether a Secure Shell (SSH) is enabled. **Relevant to** SSH **Type** boolean **Default Value** True=1
ssh/server_port **Description** Indicates which TCP port the server listens on for incoming connections. **Relevant to** SSH **Type** integer **Default Value**
ssh/remote_access **Description** Indicates if a Secure Shell (SSH) server can be accessed from the WAN. **Relevant to** SSH **Type** boolean **Default Value** False=0

ssh/host_rsa_1/private

Description SSH private host key for protocol version 1. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SSH

Type binary

Default Value

ssh/host_rsa_1/public

Description SSH public host key for protocol version 1. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SSH

Type binary

Default Value

ssh/host_rsa_2/private

Description SSH private RSA host key for protocol version 2. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SSH

Type binary

Default Value

ssh/host_rsa_2/public

Description SSH public RSA host key for protocol version 2. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SSH

Type binary

Default Value

ssh/host_dsa_2/private

Description SSH private DSA host key for protocol version 2. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SSH

Type binary

Default Value

ssh/host_dsa_2/public

Description SSH public DSA host key for protocol version 2. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SSH

Type binary

Default Value

34

Secure Socket Layer Virtual Private Network

Secure Socket Layer Virtual Private Network (SSL VPN) provides simple and secure remote access to home and office network resources. It provides the security level of IPSec but with the simplicity of using a standard Web browser.

ssl_vpn/enabled **Description** Indicates whether Secure Socket Layer Virtual Private Network (SSL VPN) is enabled. **Relevant to** SSL VPN **Type** boolean **Default Value**
ssl_vpn/greeting_message **Description** A user-defined greeting message for the SSL VPN portal **Relevant to** SSL VPN **Type** text **Default Value**

ssl_vpn/image_url_location

Description The location from which the top left image in the portal should be taken from

Relevant to SSL VPN

Type url

Default Value

ssl_vpn/shortcuts/%/name

Description The name of the shortcut (example: "Telnet office")

Relevant to SSL VPN

Type text

Default Value

ssl_vpn/shortcuts/%/application

Description The application invoked when clicking the shortcut

Relevant to SSL VPN

Type one string of:
"telnet" (SSL_VPN_APP_TELNET),
"remote_desktop" (SSL_VPN_APP_RDP)

Default Value

ssl_vpn/shortcuts/%/ip

Description The IP address of the destination host

Relevant to SSL VPN

Type text

Default Value

ssl_vpn/shortcuts/%/is_private

Description Was the shortcut created in the SSL-VPN portal (not a global shortcut) ?

Relevant to SSL VPN

Type boolean

Default Value

ssl_vpn/shortcuts/%/override_port

Description Indicates if the connection should be established to a non-default port

Relevant to SSL VPN

Type boolean

Default Value 0

ssl_vpn/shortcuts/%/port

Description The port number to connect to, if connecting to a non-default port

Relevant to SSL VPN

Type integer

Default Value

ssl_vpn/shortcuts/%/login_info

Description Indicates if login information (username and password) are specified

Relevant to SSL VPN

Type boolean

Default Value 1

ssl_vpn/shortcuts/%/username

Description The username to be used in the connection

Relevant to SSL VPN

Type text

Default Value

ssl_vpn/shortcuts/%/password

Description The password to use in the connection

Relevant to SSL VPN

Type text

Default Value

ssl_vpn/shortcuts/%/is_full_screen

Description Should the application be opened as full screen

Relevant to SSL VPN

Type boolean

Default Value

ssl_vpn/shortcuts/%/size

Description The window size of the application (if not full screen)

Relevant to SSL VPN

Type one string of:
"640x480" (APPLICATION_SIZE_640_480),
"800x600" (APPLICATION_SIZE_800_600),
"1024x768" (APPLICATION_SIZE_1024_768),
"1280x1024" (APPLICATION_SIZE_1280_1024)

Default Value 800x600

ssl_vpn/shortcuts/%/initial_dir

Description The initial directory for the application

Relevant to SSL VPN

Type text

Default Value

ssl_vpn/shortcuts/%/share

Description The initial share for the application

Relevant to SSL VPN

Type text

Default Value

ssl_vpn/shortcuts/%/show_hidden_files

Description Indicates if the application should show hidden files

Relevant to SSL VPN

Type text

Default Value

ssl_vpn/shortcuts/%/list_command

Description The command to use for retrieving file names in remote host

Relevant to SSL VPN

Type one string of:
"list" (FTP_LIST_COMMAND_LIST),
"nlst" (FTP_LIST_COMMAND_NLST),
"nlst_f" (FTP_LIST_COMMAND_NLST_F),
"nlst_p" (FTP_LIST_COMMAND_NLST_P),
"nlst_la" (FTP_LIST_COMMAND_NLST_LA)

Default Value list

ssl_vpn/shortcuts/%/permissions/%/id

Description The ID of a user or a group with access to this shortcut. The type entry specifies whether it is a group or a user. The ID is the index of the user or group you used in **admin/user/%/** and **admin/group/%/**.

Relevant to SSL VPN

Type integer

Default Value

ssl_vpn/shortcut/%/permissions/%/type

Description Specifies whether a group or a user has access to this shortcut. The user or group ID is specified in the id entry.

Relevant to SSL VPN

Type one string of:
"user" (ACCESS_OBJ_USER),
"group" (ACCESS_OBJ_GROUP)

Default Value

ssl_vpn/shortcut/%/permissions/%/access_level

Description Access level of the user or group with access to this shortcut. The possible levels are admin, read-write or read only.

Relevant to SSL VPN

Type one string of:
"admin" (ACCESS_ADMIN),
"rw" (ACCESS_RW),
"ro" (ACCESS_RO)

Default Value

ssl_vpn/restricted_access

Description Is the SSL-VPN user restricted to view only the global shortcuts in the SSL-VPN portal, or is he allowed to add his own private shortcuts.

Relevant to SSL VPN

Type boolean

Default Value

35

Services

Each service is defined by a protocol and a port number or range. The service has **trigger** and **open** associated to it. Both the **trigger** and the **open** are defined by protocol and ports. In filtering, matching is performed on the **trigger** only. The **trigger** is also used in Port Triggering, where the **trigger** is the regular open ports and **open** ports are opened if there is a connection to the **trigger** ports.

service/%/name **Description** The name of the service. **Relevant to** MGT, firewall **Type** text[MAX_LINE_SIZE=1024] **Default Value**
service/%/old_id **Description** The old ID of the service, for compatibility purposes. **Relevant to** MGT, firewall **Type** integer **Default Value**

service/%/advanced

Description Indicates the services advanced level. '0' is a basic service, level '1' is displayed when advanced services display is chosen, level '2' services are not loaded to the boards memory at all in case of a low-memory board.

Relevant to MGT, firewall

Type 0-2

Default Value

service/%/description

Description The description of the service.

Relevant to MGT, firewall

Type string

Default Value

service/%/group_id

Description The group which the service belongs to.

Relevant to qos

Type one string of:
"networking" (SVC_GRP_NETWORKING),
"web" (SVC_GRP_WEB),
"email_news" (SVC_GRP_EMAIL_NEWS),
"diagnostic_management" (SVC_GRP_DIAG_MNG),
"voice_video" (SVC_GRP_VOICE_VIDEO),
"vpn" (SVC_GRP_VPN),
"im_chat" (SVC_GRP_IM_CHAT),
"gaming" (SVC_GRP_GAMING),
"file_sharing" (SVC_GRP_FILE)

Default Value

service/%/<trigger|open>/%/protocol

Description The protocol of the trigger/open of the service. The protocol value is obtained from `http://www.iana.org/assignments/protocol-numbers`.

Relevant to MGT, fw_config

Type integer

Default Value

service/%/<trigger|open>/%/dst/start

Description The 'start' property of the destination-side port range of either trigger or open.

Relevant to MGT, fw_config

Type integer

Default Value

service/%/<trigger|open>/%/dst/end

Description The 'end' property of the destination-side port range of either trigger or open.

Relevant to MGT, fw_config

Type integer

Default Value

service/%/<trigger|open>/%/src/start

Description The 'start' property of the source-side port range of either trigger or open.

Relevant to MGT, fw_config

Type integer

Default Value

service/%/<trigger|open>/%/src/end

Description The 'end' property of the source-side port range of either trigger or open.

Relevant to MGT, fw_config

Type integer

Default Value

service/%/<trigger|open>/%/icmp_code

Description The Internet Control Message Protocol (ICMP) code for the ICMP protocol.

Relevant to MGT, fw_config

Type integer

Default Value

service/%/<trigger|open>/%/icmp_type

Description The ICMP type for the ICMP protocol.

Relevant to MGT, fw_config

Type integer

Default Value

service/%/owner

Description The MGT entity that was used to create this service.

Relevant to MGT, fw_config

Type enum loc_srv_src_t
LS_SRC_NO_OWNER = 0,
LS_SRC_WBM = 1,
LS_SRC_UPNP = 2,
LS_SRC_VOIP = 3,
LS_SRC_ALG = 4

Default Value LS_SRC_NO_OWNER

36

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) enables network management systems to remotely configure and monitor OpenRG. Your Internet Service Provider (ISP) may use SNMP in order to identify and resolve technical problems.

36.1 General Entries

snmp/enabled

Description Indicates whether Simple Network Management Protocol (SNMP) is enabled.

Relevant to SNMP

Type boolean

Default Value True=1

snmp/trusted_ip

Description Determines SNMP's trusted peer(s). There are 3 options for trusted peers: any, a single peer or a subnet of peers. For any peer, leave this entry and **snmp/trusted_mask** at their default values (0.0.0.0). For a single peer or a subnet of peers, specify an IP address in this entry and either 255.255.255.255 or a subnet mask in **snmp/trusted_mask**. Changing this entry triggers automatic generation of entries in the following Management Information Base (MIB) tables (under **/snmp/mibs/**): snmpCommunityTable, snmpTargetAddrTable, vacmSecurityToGroupTable, vacmViewTreeFamilyTable and vacmAccessTable.

Relevant to SNMP

Type ip

Default Value 0.0.0.0

snmp/trusted_mask

Description Along with trusted_ip, determines SNMP's trusted peer(s): If trusted_mask is 0.0.0.0, any peer is trusted. If trusted_mask is 255.255.255.255, a single peer is trusted, specified by the IP address in **trusted_ip**. Otherwise, the combined values of **trusted_ip** and **trusted_mask** define a subnet of trusted IPs. Changing this entry triggers automatic generation of entries in the following MIB tables (under **/snmp/mibs/**): snmpCommunityTable, snmpTargetAddrTable, vacmSecurityToGroupTable, vacmViewTreeFamilyTable and vacmAccessTable.

Relevant to SNMP

Type ip

Default Value 0.0.0.0

snmp/trap_enabled

Description Indicates whether traps are enabled. Changing this entry triggers automatic generation of entries in the following MIB tables (under **/snmp/mibs/**): snmpCommunityTable, snmpTargetAddrTable, snmpTargetParamsTable and snmpNotifyTable.

Relevant to SNMP

Type boolean

Default Value False=0

snmp/trap_version

Description The version of the SNMP traps. Changing this entry triggers automatic generation of entries in the following MIB tables (under **/snmp/mibs/**): snmpCommunityTable, snmpTargetAddrTable, snmpTargetParamsTable and snmpNotifyTable.

Relevant to SNMP

Type one string of:
"v1" (SNMP_VER_V1),
"v2" (SNMP_VER_V2)

Default Value

snmp/trap_community

Description Community name used on ongoing SNMP traps. Changing this entry triggers automatic generation of entries in the following MIB tables (under **/snmp/mibs/**): snmpCommunityTable, snmpTargetAddrTable, snmpTargetParamsTable and snmpNotifyTable.

Relevant to SNMP

Type string

Default Value

snmp/trap_destination

Description IP address destination of the SNMP traps. Changing this entry triggers automatic generation of entries in the following MIB tables (under **/snmp/mibs/**): snmpCommunityTable, snmpTargetAddrTable, snmpTargetParamsTable and snmpNotifyTable.

Relevant to SNMP

Type ip

Default Value

snmp/ch_cdp_lan_not_active

Description A list of LAN side leases that are not SNMP active and should not be available to the Dynamic Host Configuration Protocol (DHCP). It has the same format as **dev/<name>/dhcps/lease** (see entry dev/<name>/dhcps/lease/%/ip on page 138).

Relevant to SNMP

Type

Default Value

snmp/persist_conf

Description The rgconf version of the SNMP configuration (.conf) files.

Relevant to SNMP

Type

Default Value

snmp/persist_conf/0/engineboots

Description The number of boots the SNMP engine has performed.

Relevant to SNMP

Type integer

Default Value

snmp/persist_conf/1/oldEngineID

Description The engine ID of the SNMP agent.

Relevant to SNMP

Type integer

Default Value

snmp/rocomm

Description The default SNMP Read-Only community name. Changing this entry triggers automatic generation of entries in the following MIB tables (under **/snmp/mibs/**): snmpCommunityTable, snmpTargetAddrTable, vacmSecurityToGroupTable, vacmViewTreeFamilyTable and vacmAccessTable.

Relevant to SNMP

Type string

Default Value "public"

snmp/rwcomm

Description The default SNMP Read-Write community name. Changing this entry triggers automatic generation of entries in the following MIB tables (under **/snmp/mibs/**): snmpCommunityTable, snmpTargetAddrTable, vacmSecurityToGroupTable, vacmViewTreeFamilyTable and vacmAccessTable.

Relevant to SNMP

Type string

Default Value "private"

snmp/dsl_nms_name

Description Domain name of the default Network Monitoring System (NMS) for Digital Subscriber Line (DSL)-CableHome.

Relevant to SNMP

Type string

Default Value rms.corenetworks.com

snmp/dsl_dh_rsa_pub_key

Description Rivest Shamir Adelman (RSA) Public key used to validate digital signature on a DSL CableHome (CH) Diffie-Hellman (DH) Manager Public key.

Relevant to SNMP

Type binary

Default Value

36.2 Community MIB

snmp/mibs/community_mib

Description Community MIB SNMP objects, taken from RFC 2576.

Relevant to SNMP

Type

Default Value

snmp/mibs/community_mib/community_table

Description snmpCommunityTable entries.

Relevant to SNMP

Type

Default Value

snmp/mibs/community_mib/community_table/%/

Description String representation of a snmpCommunityTable row index Object Identifier (OID).

Relevant to SNMP

Type string

Default Value

snmp/mibs/community_mib/community_table/%/community_name

Description snmpCommunityName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/community_mib/community_table/%/security_name

Description snmpCommunitySecurityName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/community_mib/community_table/%/context_engine_id

Description snmpCommunityContextEngineID column. The default value is the snmpEngineID of the entity in which this object is instantiated.

Relevant to SNMP

Type string

Default Value

snmp/mibs/community_mib/community_table/%/context_name

Description snmpCommunityContextName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/community_mib/community_table/%/transport_tag

Description snmpCommunityTransportTag column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/community_mib/community_table/%/storage_type

Description snmpCommunityStorageType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/community_mib/community_table/%/row_status

Description snmpCommunityStatus column.

Relevant to SNMP

Type integer

Default Value

36.3 View-Based Access Control Model MIB

snmp/mibs/vacm_mib

Description View-Based Access Control Model (VACM) MIB objects, taken from RFC 3415.

Relevant to SNMP

Type

Default Value

36.3.1 Context Table

snmp/mibs/vacm_mib/context_table

Description vacmContextTable entries.

Relevant to SNMP

Type

Default Value

snmp/mibs/vacm_mib/context_table/%/

Description String representation of a vacmContextEntry index OID.

Relevant to SNMP

Type string

Default Value

snmp/mibs/vacm_mib/context_table/%/context_name

Description vacmContextName column.

Relevant to SNMP

Type string

Default Value

36.3.2 Security to Group Table

snmp/mibs/vacm_mib/sec_to_group **Description** vacmSecurityToGroupTable entries. **Relevant to** SNMP **Type** **Default Value**
snmp/mibs/vacm_mib/sec_to_group/%/ **Description** String representation of a vacmSecurityToGroupEntry index OID. **Relevant to** SNMP **Type** string **Default Value**
snmp/mibs/vacm_mib/sec_to_group/%/sec_model **Description** vacmSecurityModel column. **Relevant to** SNMP **Type** integer **Default Value**
snmp/mibs/vacm_mib/sec_to_group/%/security_name **Description** vacmSecurityName column. **Relevant to** SNMP **Type** string **Default Value**
snmp/mibs/vacm_mib/sec_to_group/%/group_name **Description** vacmGroupName column. **Relevant to** SNMP **Type** string **Default Value**

snmp/mibs/vacm_mib/sec_to_group/%/storage_type **Description** vacmSecurityToGroupStorageType column. **Relevant to** SNMP **Type** integer **Default Value**
snmp/mibs/vacm_mib/sec_to_group/%/row_status **Description** vacmSecurityToGroupStatus column. **Relevant to** SNMP **Type** integer **Default Value**

36.3.3 Access Table

snmp/mibs/vacm_mib/access_table **Description** vacmAccessTable entries. **Relevant to** SNMP **Type** **Default Value**
snmp/mibs/vacm_mib/access_table/%/ **Description** String representation of a vacmAccessEntry index OID. **Relevant to** SNMP **Type** string **Default Value**
snmp/mibs/vacm_mib/access_table/%/group_name **Description** vacmGroupName column. **Relevant to** SNMP **Type** string **Default Value**

snmp/mibs/vacm_mib/access_table/%/context_prefix

Description vacmAccessContextPrefix column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/vacm_mib/access_table/%/sec_model

Description vacmAccessSecurityModel column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/vacm_mib/access_table/%/sec_level

Description vacmAccessSecurityLevel column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/vacm_mib/access_table/%/context_match

Description vacmAccessContextMatch column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/vacm_mib/access_table/%/read_view

Description vacmAccessReadViewName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/vacm_mib/access_table/%/write_view

Description vacmAccessWriteViewName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/vacm_mib/access_table/%/notify_view

Description vacmAccessNotifyViewName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/vacm_mib/access_table/%/storage_type

Description vacmAccessStorageType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/vacm_mib/access_table/%/row_status

Description vacmAccessStatus column.

Relevant to SNMP

Type integer

Default Value

36.3.4 View Tree Table

snmp/mibs/vacm_mib/view_tree_table

Description vacmViewTreeFamilyTable entries.

Relevant to SNMP

Type

Default Value

snmp/mibs/vacm_mib/view_tree_table/%/

Description String representation of a vacmViewTreeFamilyEntry index OID.

Relevant to SNMP

Type string

Default Value

snmp/mibs/vacm_mib/view_tree_table/%/view_name

Description vacmViewTreeFamilyViewName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/vacm_mib/view_tree_table/%/view_subtree

Description vacmViewTreeFamilySubtree column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/vacm_mib/view_tree_table/%/family_mask

Description vacmViewTreeFamilyMask column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/vacm_mib/view_tree_table/%/family_type

Description vacmViewTreeFamilyType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/vacm_mib/view_tree_table/%/storage_type

Description vacmViewTreeFamilyStorageType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/vacm_mib/view_tree_table/%/row_status

Description vacmViewTreeFamilyStatus column.

Relevant to SNMP

Type integer

Default Value

36.4 Notification MIB

snmp/mibs/notification_mib

Description SNMP notification MIB objects, taken from RFC 3413.

Relevant to SNMP

Type

Default Value

36.4.1 Notify Table

snmp/mibs/notification_mib/notify_table

Description snmpNotifyTable entries.

Relevant to SNMP

Type

Default Value

snmp/mibs/notification_mib/notify_table/%/

Description String representation of a snmpNotifyEntry index OID.

Relevant to SNMP

Type string

Default Value

snmp/mibs/notification_mib/notify_table/%/notify_tag

Description snmpNotifyTag column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/notification_mib/notify_table/%/notify_type

Description snmpNotifyType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/notification_mib/notify_table/%/storage_type

Description snmpNotifyStorageType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/notification_mib/notify_table/%/row_status

Description snmpNotifyRowStatus column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/notification_mib/notify_table/%/is_external_entry

Description True if this entry is created by a different MIB (not local to the snmpNotifyTable).

Relevant to SNMP

Type boolean

Default Value

36.4.2 Filter Profile Table

snmp/mibs/notification_mib/filter_profile_table

Description snmpNotifyFilterProfileTable entries.

Relevant to SNMP

Type

Default Value

snmp/mibs/notification_mib/filter_profile_table/%/

Description String representation of a snmpNotifyFilterProfileEntry index OID.

Relevant to SNMP

Type string

Default Value

snmp/mibs/notification_mib/filter_profile_table/%/params_name

Description snmpTargetParamsName index column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/notification_mib/filter_profile_table/%/profile_name

Description snmpNotifyFilterProfileName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/notification_mib/filter_profile_table/%/storage_type **Description** snmpNotifyFilterProfileStorType column. **Relevant to** SNMP **Type** integer **Default Value**
snmp/mibs/notification_mib/filter_profile_table/%/row_status **Description** snmpNotifyFilterProfileRowStatus column. **Relevant to** SNMP **Type** integer **Default Value**

36.4.3 Filter Table

snmp/mibs/notification_mib/filter_table **Description** snmpNotifyProfileTable entries. **Relevant to** SNMP **Type** **Default Value**
snmp/mibs/notification_mib/filter_table/%/ **Description** String representation of a snmpNotifyFilterEntry index OID. **Relevant to** SNMP **Type** string **Default Value**
snmp/mibs/notification_mib/filter_table/%/profile_name **Description** snmpNotifyFilterProfileName index column. **Relevant to** SNMP **Type** string **Default Value**

snmp/mibs/notification_mib/filter_table/%/filter_subtree

Description snmpNotifyFilterSubtree column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/notification_mib/filter_table/%/filter_mask

Description snmpNotifyFilterMask column.

Relevant to SNMP

Type binary

Default Value

snmp/mibs/notification_mib/filter_table/%/filter_type

Description snmpNotifyFilterType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/notification_mib/filter_table/%/storage_type

Description snmpNotifyFilterStorageType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/notification_mib/filter_table/%/row_status

Description snmpNotifyFilterRowStatus column.

Relevant to SNMP

Type integer

Default Value

36.5 Target MIB

snmp/mibs/target_mib

Description SNMP target MIB objects, taken from RFC 3413.

Relevant to SNMP

Type

Default Value

36.5.1 Target Address Table

snmp/mibs/target_mib/target_addr_table

Description snmpTargeAddrTable entries.

Relevant to SNMP

Type

Default Value

snmp/mibs/target_mib/target_addr_table/%/

Description String representation of a snmpTargetAddrEntry index OID.

Relevant to SNMP

Type string

Default Value

snmp/mibs/target_mib/target_addr_table/%/name

Description snmpTargetAddrName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/target_mib/target_addr_table/%/tdomain

Description snmpTargetAddrTDomain column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/target_mib/target_addr_table/%/taddress

Description snmpTargetAddrTAddress column.

Relevant to SNMP

Type binary

Default Value

snmp/mibs/target_mib/target_addr_table/%/timeout

Description snmpTargetAddrTimeout column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_addr_table/%/retry_count

Description snmpTargetAddrRetryCount column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_addr_table/%/tag_list

Description snmpTargetAddrTagList column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/target_mib/target_addr_table/%/params

Description snmpTargetAddrParams column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/target_mib/target_addr_table/%/storage_type

Description snmpTargetAddrStorageType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_addr_table/%/row_status

Description snmpTargetAddrRowStatus column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_addr_table/%/tmask

Description snmpTargetAddrTmask column.

Relevant to SNMP

Type binary

Default Value

snmp/mibs/target_mib/target_addr_table/%/mms

Description snmpTargetAddrMMS column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_addr_table/%/time_stamp

Description A local time stamp used by SNMP, which represents the last time the entry was updated.

Relevant to SNMP

Type integer

Default Value

36.5.2 Target Parameters Table

snmp/mibs/target_mib/target_params_table

Description snmpTargetParamsTable entries.

Relevant to SNMP

Type

Default Value

snmp/mibs/target_mib/target_params_table/%/

Description String representation of a snmpTargetParamsEntry index OID.

Relevant to SNMP

Type string

Default Value

snmp/mibs/target_mib/target_params_table/%/params_name

Description snmpTargetParamsName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/target_mib/target_params_table/%/mp_model

Description snmpTargetParamsMPModel column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_params_table/%/sec_model

Description snmpTargetParamsSecurityModel column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_params_table/%/security_name

Description snmpTargetParamsSecurityName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/target_mib/target_params_table/%/sec_level

Description snmpTargetParamsSecurityLevel column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_params_table/%/storage_type

Description snmpTargetParamsStorageType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_params_table/%/row_status

Description snmpTargetParamsRowStatus column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/target_mib/target_params_table/%/time_stamp

Description A local time stamp used by SNMP which represents last time the entry was updated.

Relevant to SNMP

Type integer

Default Value

36.6 USM MIB

snmp/mibs/usm_mib

Description USM-MIB taken from RFC 3414 and usmDHUserKeyTable from RFC 2786.

Relevant to SNMP

Type

Default Value

snmp/mibs/usm_mib/usmuser_table

Description usmUserTable, usmDHUserKeyTable entries.

Relevant to SNMP

Type

Default Value

snmp/mibs/usm_mib/usmuser_table/%/

Description String representation of a usmUserTable index OID.

Relevant to SNMP

Type string

Default Value

snmp/mibs/usm_mib/usmuser_table/%/engine_id

Description usmUserEngineID column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/usm_mib/usmuser_table/%/name

Description usmUserName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/usm_mib/usmuser_table/%/security_name

Description usmUserSecurityName column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/usm_mib/usmuser_table/%/clone_from

Description usmUserCloneFrom column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/usm_mib/usmuser_table/%/auth_protocol

Description usmUserAuthProtocol column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/usm_mib/usmuser_table/%/priv_protocol

Description usmUserPrivProtocol column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/usm_mib/usmuser_table/%/public

Description usmUserPublic column.

Relevant to SNMP

Type string

Default Value

snmp/mibs/usm_mib/usmuser_table/%/storage_type

Description usmUserStorageType column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/usm_mib/usmuser_table/%/row_status

Description usmUserStatus column.

Relevant to SNMP

Type integer

Default Value

snmp/mibs/usm_mib/usmuser_table/%/is_auth_key_usable

Description Indicates if the authentication key is changed and valid for use.

Relevant to SNMP

Type boolean

Default Value

snmp/mibs/usm_mib/usmuser_table/%/is_priv_key_usable

Description Indicates if the private key is changed and valid for use.

Relevant to SNMP

Type boolean

Default Value

snmp/mibs/usm_mib/usmuser_table/%/auth_key

Description The user authentication key.

Relevant to SNMP

Type binary

Default Value

snmp/mibs/usm_mib/usmuser_table/%/priv_key

Description The user privacy key column.

Relevant to SNMP

Type binary

Default Value

snmp/mibs/usm_mib/usmuser_table/%/auth_dh_public

Description The Diffie-Hellman public key used to change the user's authentication key.

Relevant to SNMP

Type binary

Default Value

snmp/mibs/usm_mib/usmuser_table/%/auth_dh_random

Description The Diffie-Hellman private key used to change the user's authentication key.

Relevant to SNMP

Type binary

Default Value

snmp/mibs/usm_mib/usmuser_table/%/priv_dh_public

Description The Diffie-Hellman public key used to change the user's privacy key.

Relevant to SNMP

Type binary

Default Value

snmp/mibs/usm_mib/usmuser_table/%/priv_dh_random

Description The Diffie-Hellman private key used to change the user's privacy key.

Relevant to SNMP

Type binary

Default Value

37

Support Cost Reduction

scr/bad_ip_no_interception/%/ip

Description The IP address of a LAN computer through which the user was prompted with a static IP interception warning, but chose to ignore it. These IPs are stored so the interception will not recur.

Relevant to WBM, HTTP

Type ip

Default Value

38

System

system/panic_timeout

Description The time in seconds to wait before rebooting on a panic situation. Should be set to a value different from zero, otherwise the board will not reboot on panic. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to main

Type integer

Default Value

system/boot/failure_boots

Description Counts consecutive unsuccessful reboots. Set to zero after a successful boot.

Relevant to main

Type integer

Default Value

system/mac_cur

Description The first available MAC address from which a random MAC address will be generated for logic devices that need MAC. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to main

Type mac

Default Value

system/mac_company_id

Description The first three octets of the MAC address, which are vendor specific. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to main

Type text[10]

Default Value

system/version

Description OpenRG configuration file version, represented by 3 numbers separated by dots, e.g. "2.0.2"

Relevant to Remote Update, WBM

Type text[MAX_VAR_NAME=80]

Default Value

system/external_version

Description OpenRG configuration file additional version, for customer use.

Relevant to Remote Update, WBM

Type integer

Default Value

system/release

Description OpenRG release date (date on which system/version was released).

Relevant to WBM

Type date

Default Value

system/contact

Description The specific contact information to be returned when queried by SNMP for sysContact. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SNMP, WBM

Type text[MAX_VAR_NAME=255]

Default Value rg_support@jungo.com

system/name

Description The specific administratively-assigned name for the product to be returned when queried by SNMP for sysName. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SNMP, WBM

Type text[MAX_VAR_NAME=255]

Default Value

system/location

Description The textual description of the specific location of the node to be returned when queried by SNMP for sysLocation. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to SNMP,WBM

Type text[MAX_VAR_NAME=255]

Default Value

system/log/login_success

Description Indicates whether to log the successfull login attempts.

Relevant to WBM, Serial, Telnet

Type boolean

Default Value True=1

system/log/login_fail

Description Indicates whether to log the failed login attempts.

Relevant to WBM, Serial, Telnet

Type boolean

Default Value True=1

system/rg_disable_features

Description When set to 1, will cause on boot disabling of all OpenRG management, apart from SNMP, Universal Plug-and-Play (UPnP), Telnet and CLI.

Relevant to General

Type boolean

Default Value

system/equiv_dist/%/distribution

Description List of equivalent distributions from which you can update without requiring to restore defaults.

Relevant to Backward Compatibilty

Type text[MAX_VAR_NAME=255]

Default Value

system/network/initial_setup

Description A flag for OpenRG initial network configuration. This flag is set when OpenRG's Internet connection is initially defined by the user. This flag, once set by defining an Internet connection, cannot be reset to zero.

Relevant to WBM, HTTP, DNS

Type boolean

Default Value False=0

system/network/http_interception

Description Indicates whether HTTP interception is enabled when the network is configured, and there is no running Internet connection.

Relevant to WBM, HTTP, DNS

Type boolean

Default Value True=1

system/network/net_health_monitor_interception

Description Indicates whether HTTP interception should occur upon connectivity problems to the Internet Service Provider.

Relevant to WBM, HTTP

Type boolean

Default Value False=0

system/network/cable_modem_monitor

Description Indicates whether OpenRG is connected to a cable modem. Its value changes the messages presented to the user upon HTTP interception due to connectivity problems with the Internet Service Provider.

Relevant to WBM, HTTP

Type boolean

Default Value False=0

system/network/web_auth_over_https

Description Web authentication will be performed through an HTTPS WBM page

Relevant to HTTP Authentication

Type boolean

Default Value False=0

system/network/internet_url

Description External URL to ping and DNS lookup in order to verify Internet connectivity.

Relevant to Diagnostics, Network Health Monitor

Type text

Default Value www.jungo.com

system/network/bad_ip_interception_mode

Description Defines the type of HTTP interception that will occur when a LAN computer, with a static IP address that is not in the LAN subnet, attempts to browse the web.

Relevant to WBM, HTTP

Type one string of:
"inactive" (BAD_IP_INTERCEPT_INACTIVE),
"warn" (BAD_IP_INTERCEPT_WARN),
"block" (BAD_IP_INTERCEPT_BLOCK)

Default Value "warn"

system/network/usfs/enabled

Description Whether to allow lan to lan communication in a multi-bridge configuration. Requires reboot after changing.

Relevant to Bridge

Type boolean

Default Value

system/country_code

Description ISO3166 country code representation.

Relevant to 80211B/G Access Point

Type text[2]

Default Value

system/factory_version

Description The version of the factory settings.. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide.

Relevant to

Type integer

Default Value

39

System Log

The System Log displays a list of the most recent activity that has taken place on OpenRG. This chapter lists the sytem log settings.

syslog/buffers/%/policy **Description** Policy of System Log (syslog) buffer maintenance. **Relevant to** syslogt **Type** enum syslog_buf_policy_t BUF_POLICY_STOP_ON_FULL = 1, BUF_POLICY_CYCLIC = 2 **Default Value** BUF_POLICY_CYCLIC
syslog/buffers/%/buf_type **Description** Buffer type **Relevant to** syslogt **Type** enum syslog_buf_type_t SYSLOG_BT_VARLOG = 0, SYSLOG_BT_FW = 1, **Default Value**

syslog/buffers/%/ip

Description IP address for remote syslog server.

Relevant to syslogt

Type ip

Default Value 0.0.0.0

syslog/buffers/%/max_size

Description The maximum size of this syslog buffer in bytes.

Relevant to syslogt

Type integer

Default Value 16*1024

syslog/buffers/%/severity_threshold

Description Minimum severity threshold for buffer. Messages with higher severity will be sent to remote Syslog server whose address is specified in **syslog/buffers/%/ip**. LLEVEL_MASK value is treated as 'None', meaning that remote logging for this buffer is disabled.

Relevant to syslogt

Type LLEVEL_MASK 0xf
LEMERG 0
LALERT 1
LCRIT 2
LERR 3
LWARNING 4
LNOTICE 5
LINFO 6
LDEBUG 7

Default Value LLEVEL_MASK

40

Time Enabling Rules

Scheduler rules are used for limiting the activation of Firewall rules to specific time periods, specified in weekdays and hours.

time_rule/%/day/%/ **Description** The day in the week for which to apply the given time rule (can be multiple days). **Relevant to** Time enabled components **Type** enum time_rule_days_t TR_DAY_ALLWEEK = -1, TR_DAY_SUN = 0, TR_DAY_MON = 1, TR_DAY_TUE = 2, TR_DAY_WED = 3, TR_DAY_THU = 4, TR_DAY_FRI = 5, TR_DAY_SAT = 6 **Default Value**
time_rule/%/hour/%/start **Description** The given time rule is activated after this number of seconds from the start of the day. **Relevant to** Time enabled components **Type** integer **Default Value**

time_rule/%/hour/%/end

Description The given time rule is deactivated after this number of seconds from the start of the day.

Relevant to Time enabled components

Type integer

Default Value

/time_rule/%

Description The global set of time enabling rules, mainly referred to by the firewall rules (see entry fw/rule/<type>/%/time_rule on page 52).

Relevant to Time enabled components

Type time_set

Default Value

/time_rule/%/description

Description User definable name of rule.

Relevant to Time enabled components

Type string[MAX_DESCR_LEN=64]

Default Value

/time_rule/%/is_disabling

Description Indicates whether the dependent feature is to be disabled instead of enabled when time is matched.

Relevant to Time enabled components

Type boolean

Default Value False=0

41

Transparent Proxy

OpenRG has an interface layer for customers who wish to add a transparent proxy for OpenRG in order to perform HTTP URL filtering, for example. The transparent proxy uses the Firewall Destination NAT mechanism in order to perform redirecting of packets passing through OpenRG to the transparent proxy. Basically, the firewall intercepts packets and redirects them to OpenRG itself, to a port listened to by a transparent proxy. The transparent proxy can process the data and decide whether to redirect it or not.

proxy/%/name **Description** Name of proxy. **Relevant to** Generic proxy **Type** text[MAX_PROXY_NAME=20] **Default Value**
proxy/%/vendor **Description** Generic proxy's vendor. **Relevant to** Generic proxy **Type** text[MAX_VENDOR=10] **Default Value**

proxy/%/vendor_id

Description Generic proxy's vendor ID.

Relevant to Generic proxy

Type text[MAX_VENDOR=10]

Default Value

proxy/%/enabled

Description Indicates whether the proxy is enabled or disabled.

Relevant to Generic proxy

Type boolean

Default Value

proxy/%/version

Description Generic proxy version.

Relevant to Generic proxy

Type text[MAX_VERSION_LEN=10]

Default Value

proxy/%/registration_url/

Description Vendor's "registration to service" URL.

Relevant to Generic proxy

Type Text[MAX_HOSTNAME_LEN=64]

Default Value

proxy/%/server_get_url/

Description URL from which you receive the server that the proxy uses.

Relevant to Generic proxy

Type Text[MAX_HOSTNAME_LEN=64]

Default Value

proxy/%/expiry_get_url

Description URL from which to get the expiry date of the subscription.

Relevant to Generic Proxy

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

proxy/%/server_refresh

Description Refresh time of active server in days.

Relevant to Generic Proxy

Type integer

Default Value

proxy/%/type

Description Proxy type

Relevant to Generic proxy

Type one string of:
"pop3" (GENERIC_PROXY_POP3),
"smtp" (GENERIC_PROXY_SMTP),
"surfcontrol" (GENERIC_PROXY_SURFCONTROL),
"av_http" (GENERIC_PROXY_AV_HTTP),
"av_pop3" (GENERIC_PROXY_AV_POP3),
"av_smtp" (GENERIC_PROXY_AV_SMTP),
"av_nac" (GENERIC_PROXY_AV_NAC)

Default Value

proxy/%/error_policy

Description Expected proxy behavior on failure to access server.

Relevant to Generic proxy

Type one string of:
"block" (GENERIC_PROXY_ERROR_BLOCK),
"pass" (GENERIC_PROXY_ERROR_PASS),
"no_server" (GENERIC_PROXY_NO_SERVER)

Default Value

proxy/%/log

Description Indicates whether to log all transactions envolving the proxy.

Relevant to Generic proxy

Type boolean

Default Value

proxy/%/server/%/host

Description Server hostname or IP - in rg_conf_ram.

Relevant to Generic proxy

Type text[MAX_HOSTNAME_LEN=64]

Default Value

proxy/%/server/%/port

Description Server port - in rg_conf_ram.

Relevant to Generic proxy

Type integer

Default Value

proxy/%/server/%/location

Description Server location - in rg_conf_ram.

Relevant to Generic proxy

Type text

Default Value

42

Antivirus

antivirus/nac/required/%/type

Description Type of required version for NAC

Relevant to Antivirus NAC

Type one string of:
"product",
"dat",
"engine"

Default Value

antivirus/nac/required/%/version

Description Required version for NAC

Relevant to Antivirus NAC

Type string

Default Value

antivirus/nac/url

Description URL for antivirus installation and update

Relevant to Antivirus NAC

Type string

Default Value

43

Universal Plug and Play (UPnP)

Universal Plug-and-Play is a networking architecture that provides compatibility among networking equipment, software and peripherals. UPnP OpenRG™-enabled products can seamlessly connect and communicate with other Universal Plug-and-Play enabled devices, without the need for user configuration, centralized servers, or product-specific device drivers. This technology leverages existing standards and technologies, including TCP/IP, HTTP 1.1 and XML, facilitating the incorporation of Universal Plug-and-Play capabilities into a wide range of networked products for the home.

Universal Plug-and-Play technologies are rapidly adopted and integrated into widely-used consumer products such as Windows XP. Therefore it is critical that today's Residential Gateways be UPnP-compliant. Your gateway is at the forefront of this development, offering a complete software platform for UPnP devices. This means that any UPnP-enabled *control point* (client) can dynamically join the network, obtain an IP address and exchange information about its capabilities and those of other computers on the network. They can subsequently communicate with each other directly, thereby further enabling peer-to-peer networking. And this all happens automatically, providing a truly zero-configuration network.

upnp/igd/enabled

Description Indicates if the UPnP Internet Gateway Device (IGD) feature is enabled.

Relevant to UPnP

Type boolean

Default Value True=1

upnp/readonly

Description If true, forces any UPnP operation that requires rg_conf update to fail.

Relevant to UPnP

Type boolean

Default Value False=0

upnp/conn_readonly

Description If true, forces any connection-related UPnP operations, e.g. connection enable/disable, to fail.

Relevant to UPnP

Type boolean

Default Value False=0

upnp/max_rules

Description Maximal number of rules that may be defined for UPnP.

Relevant to UPnP

Type integer

Default Value 256

upnp/rules_autoclean/enabled

Description Indicates if auto cleaning of invalid services is enabled or not.

Relevant to UPnP

Type boolean

Default Value False=0

upnp/rules_autoclean/check_interval

Description Interval in minutes to check services validity and remove invalid services. Relevant only if auto cleaning of invalid services is enabled.

Relevant to UPnP

Type integer

Default Value 5

upnp/wan_conns_to_publish

Description Selects the devices published in the description document.

Relevant to UPnP

Type one string of:
"main_wan" (UPNP_PUBLISH_MAIN_WAN),
"all_wans" (UPNP_PUBLISH_ALL_WANS)

Default Value "main_wan"

upnp/tr064/enabled

Description Indicates whether TR-064 (IGD variant) is enabled.

Relevant to TR-064

Type boolean

Default Value True=1

upnp/tr064/persistent_data

Description Arbitrary data that should persist across boots.

Relevant to TR-064

Type text[256]

Default Value

upnp/av/enabled

Description Indicates whether UPnP AV (Media Server) is enabled.

Relevant to UPnP AV

Type boolean

Default Value True=1

upnp/av/version

Description Protocol version.

Relevant to UPnP AV

Type integer (1-2)

Default Value 1

upnp/av/auto_share **Description** If true, then automatically share all disks, otherwise use the following entries. **Relevant to** UPnP AV **Type** boolean **Default Value** True=1
upnp/av/share_all_files **Description** If true, then share also files with unknown extensions. **Relevant to** UPnP AV **Type** boolean **Default Value** True=1
upnp/av/dir/%/path **Description** Directory path, relative to DISK_MOUNT_POINT_BASE, e.g. "A/Music". **Relevant to** UPnP AV **Type** text **Default Value**
upnp/av/dir/%/title **Description** Directory title. If empty then last path element is used as title. **Relevant to** UPnP AV **Type** text **Default Value**

44

Voice over Asynchronous Transfer Mode (VoATM)

voatm/l3addr/% **Description** Series of L3 addresses for Public Switched Telephone Nerwork (PSTN) ports. **Relevant to** Telephony, VoATM **Type** integer **Default Value**
voatm/cas_emu **Description** Use Channel Associated Signalling (CAS) emulation (enable back-to-back testing). **Relevant to** Telephony, VoATM **Type** boolean **Default Value** False=0

45

Voice over IP (VoIp)

This chapter lists the Voice over IP (VoIP) entries according to the following sections:

- General -- general VoIP entries (refer to Section 45.1).
- Codec -- codec entries, which define the method of relaying voice data (refer to Section 45.2). Relevant to ATA only.
- Signalling -- SIP, H323 and MGCP signalling entries (refer to Section 45.3).
- IP Phone -- IP phone settings (refer to Section 45.4).
- Line -- line entries, including general, SIP proxy and outbound SIP proxy settings (refer to Section 45.5). Relevant to ATA only.
- Phonebook -- speed dial settings (refer to Section 45.6). Relevant to ATA only.
- Audio -- audio entries, including general, echo cancellation and jitter settings (refer to Section 45.7).
- MSS Clamping -- MSS clamping settings, for reducing voice delay (refer to Section 45.8).

45.1 General

voip/disabled

Description Diable the VOIP service, only relevant when VOIP stack is Asterisk

Relevant to WBM, VoIP, Asterisk

Type boolean

Default Value 0

voip/dial_timeout

Description The timeout in seconds between dialing one digit and the next. Media Gateway Control Protocol (MGCP) does not use this entry. Relevant to ATA only.

Relevant to WBM, VoIP

Type integer

Default Value 5

voip/call_waiting_enabled

Description Indicates whether call waiting is enabled. Relevant only to RADVISION-based ATA.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/phone_number_max_size

Description The largest number of digits considered a phone number. MGCP does not use this entry. Relevant to ATA only.

Relevant to WBM, VoIP

Type integer (3-15)

Default Value 15

voip/out_of_band_dtmf

Description If set, Dual Tone Multi Frequency (DTMF) will be sent out-of-band (on a different channel) using Real-time Transport Protocol (RTP) telephone-event codec. Relevant only to oSIP and RADVISION-based ATA.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/media_port

Description The port number of the first port in a contiguous range of ports used for media traffic.

Relevant to WBM, VoIP

Type integer (1024-65535)

Default Value 5004

voip/media_tos

Description Type Of Service value, set for RTP packets.

Relevant to WBM, VoIP, QoS

Type text[4] (hex value)

Default Value 0xb8

45.2 Codec

voip/codec/%/enabled

Description Indicates whether codec is enabled.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/codec/%/name

Description The encoding name of the codec. The name must correspond with the payload type.

Relevant to WBM, VoIP

Type one string of:
"pcmu" (VOIP_CODEC_PCMU),
"g723" (VOIP_CODEC_G723),
"pcma" (VOIP_CODEC_PCMA),
"g722" (VOIP_CODEC_G722),
"g728" (VOIP_CODEC_G728),
"g729" (VOIP_CODEC_G729),
"comfort-noise" (VOIP_CODEC_CN),
"telephone-event" (VOIP_CODEC_DTMF)

Default Value

voip/codec/%/bit_rate_hi

Description Indicates whether a high bit rate is used for codec G723 (payload 4). If this flag is true, a bit rate of 6.3 Kbps is used instead of 5.3 Kbps.

Relevant to WBM, VoIP

Type boolean

Default Value

voip/codec/%/ptime

Description The packetization time in milliseconds. There are a number of possible values limited by codec.

Relevant to WBM, VoIP

Type integer

Default Value

45.3 Signalling

45.3.1 General

voip/signalling/protocol

Description The signalling protocol in use. Note that only one signalling protocol can be active at a given time. Relevant to ATA only.

Relevant to WBM, VoIP

Type one string of:
"sip" (VOIP_PROT_SIP),
"h.323" (VOIP_PROT_H323),
"mgcp" (VOIP_PROT_MGCP)

Default Value

45.3.2 MGCP Call Agent

voip/signalling/mgcp_call_agent/port

Description MGCP call agent listening port number.

Relevant to WBM, VoIP, PBX

Type integer (1025-65535)

Default Value 2727

45.3.3 SIP

voip/signalling/sip/transport_protocol

Description The transport protocol used for SIP (UDP, TCP). This entry is relevant for RADVISION stack only.

Relevant to WBM, VoIP

Type one string of:
"udp" (VOIP_SIP_TRANSPORT_UDP),
"tcp" (VOIP_SIP_TRANSPORT_TCP)

Default Value UDP

voip/signalling/sip/port

Description Port number used for SIP.

Relevant to WBM, VoIP

Type integer (1024-65535)

Default Value 5060

voip/signalling/sip/use_proxy

Description Indicates whether SIP proxy is used. This entry is relevant for RADVISION stack only.

Relevant to WBM, VoIP

Type boolean

Default Value

voip/signalling/sip/proxy_address

Description Manually entered SIP proxy hostname or IP address. This entry is relevant for RADVISION stack only.

Relevant to WBM, VoIP

Type host/ip

Default Value

voip/signalling/sip/proxy_username

Description The username used for registration to SIP proxy. This entry is relevant for RADVISION stack only.

Relevant to WBM, VoIP

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/signalling/sip/proxy_password

Description The obscured password, used for registration to SIP proxy. This entry is relevant for RADVISION stack only.

Relevant to WBM, VoIP

Type text[MAX_PASSWORD_LEN=64]

Default Value

voip/signalling/sip/proxy_timeout

Description The SIP proxy registration timeout (in seconds). This entry is relevant for RADVISION stack only.

Relevant to WBM, VoIP

Type unsigned integer

Default Value 3600

45.3.4 H323

voip/signalling/h323/port

Description Port number for H.323 signalling.

Relevant to WBM, VoIP

Type integer (1024-65535)

Default Value 1720

voip/signalling/h323/fast_start_enable

Description Indicates whether H.323 works in fast-start mode.

Relevant to WBM, VoIP

Type boolean

Default Value False=0

voip/signalling/h323/h245_tunneling_enable

Description Indicates whether H.245 packets should be encapsulated within H.225 packets. This entry is not relevant for RADVISION.

Relevant to WBM, VoIP

Type boolean

Default Value False=0

voip/signalling/h323/gatekeeper_registry

Description Indicates whether H.323 is registered with a gatekeeper.

Relevant to WBM, VoIP

Type boolean

Default Value False=0

voip/signalling/h323/gatekeeper_address

Description Optional H.323 Gatekeeper hostname or IP address. Relevant only if **voip/signalling/h323/gatekeeper_registry** is true.

Relevant to WBM, VoIP

Type host/ip

Default Value

voip/signalling/h323/gatekeeper_port

Description Port number used for Remote Access Service (RAS). Relevant only if **voip/signalling/h323/gatekeeper_registry** is true.

Relevant to WBM, VoIP

Type integer (1024-65535)

Default Value 1719

voip/signalling/h323/specify_gatekeeper_id

Description Indicates whether a gatekeeper ID is required.

Relevant to WBM, VoIP

Type boolean

Default Value False=0

voip/signalling/h323/gatekeeper_id

Description The ID of the gatekeeper.

Relevant to WBM, VoIP

Type text[MAX_DESCR_LEN=64]

Default Value

voip/signalling/h323/time_to_live

Description The H.323 gatekeeper registration timeout (in seconds).

Relevant to WBM, VoIP

Type integer (30-INT_MAX)

Default Value 86400

voip/signalling/h323/use_alternate_gatekeeper

Description Indicates whether an alternative gatekeeper should be used.

Relevant to WBM, VoIP

Type boolean

Default Value False=0

voip/signalling/h323/alternate_gatekeeper_address

Description The hostname or IP address of the alternative gatekeeper. Relevant only if **voip/signalling/h323/use_alternate_gatekeeper** is true.

Relevant to WBM, VoIP

Type host/ip

Default Value

voip/signalling/h323/alternate_gatekeeper_port

Description The port number of the alternative gatekeeper. Relevant only if **voip/signalling/h323/use_alternate_gatekeeper** is true.

Relevant to WBM, VoIP

Type integer (1024-65535)

Default Value 1719

voip/signalling/h323/dtmf_mode

Description The DTMF transmission method. This entry is not relevant for RADVISION and oSIP. For the equivalent entry, see voip/out_of_band_dtmf on page 288).

Relevant to WBM, VoIP

Type one string of:
"inband" (VOIP_DTMF_INBAND),
"rfc2833_always" (VOIP_DTMF_RFC2833_ALWAYS),
"q931_keypad" (VOIP_DTMF_Q931_KEYPAD),
"h245_alphanumeric" (VOIP_DTMF_H245_ALPHANUMERIC),
"h245_signal" (VOIP_DTMF_H245_SIGNAL)

Default Value "rfc2833_always"

45.3.5 MGCP Media Gateway

voip/signalling/mgcp/mgc_address

Description Call Agent hostname or IP address. This entry is used by MGCP.

Relevant to WBM, VoIP

Type host/ip

Default Value

voip/signalling/mgcp/mgc_port

Description Call Agent port number. This entry is used by MGCP.

Relevant to WBM, VoIP

Type integer (1025-65535)

Default Value 2727

voip/signalling/mgcp/mg_port

Description Media Gateway listening port number. This entry is used by MGCP.

Relevant to WBM, VoIP

Type integer (1025-65535)

Default Value 2427

voip/signalling/mgcp/specify_mg_domain_name

Description Indicates whether the domain name should be used to override the IP address.

Relevant to WBM, VoIP

Type boolean

Default Value false=0

voip/signalling/mgcp/mg_domain_name

Description Media Gateway domain name.

Relevant to WBM, VoIP

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

voip/signalling/mgcp/persistent_on_hook_events_enbaled

Description Indicates whether to send persistent on-hook events to the call agent.

Relevant to WBM, VoIP

Type boolean

Default Value true=1

voip/signalling/mgcp/persistent_off_hook_events_enbaled

Description Indicates whether to send persistent off-hook events to the call agent.

Relevant to WBM, VoIP

Type boolean

Default Value true=1

voip/signalling/mgcp/persistent_hook_flash_events_enbaled

Description Indicates whether to send persistent hook flash events to the call agent.

Relevant to WBM, VoIP

Type boolean

Default Value true=1

45.4 IP Phone

voip/ipphone/ringing/mute

Description Indicates whether the ringer is off.

Relevant to WBM, VoIP

Type boolean

Default Value False=0

voip/ipphone/ringing/volume

Description The volume of the ringer.

Relevant to WBM, VoIP

Type integer (0-15)

Default Value 15

voip/ipphone/handset/volume

Description The volume of the handset speaker.

Relevant to WBM, VoIP

Type integer (0-15)

Default Value 15

voip/ipphone/loudspeaker/volume

Description The volume of the loudspeaker.

Relevant to WBM, VoIP

Type integer (0-15)

Default Value 15

45.5 Line

45.5.1 General

voip/line/%/id **Description** The line identification. **Relevant to** WBM, VoIP **Type** text[MAX_USER_ID_LEN=20] **Default Value**
voip/line/%/enabled **Description** Indicates whether the line is enabled. **Relevant to** WBM, VoIP **Type** boolean **Default Value** True=1
voip/line/%/description **Description** Description of the user of the line. **Relevant to** WBM, VoIP **Type** text[MAX_DESCRIPTION_LEN=64] **Default Value**
voip/line/%/snd_callerid **Description** Indicates whether caller identification is enabled. MGCP does not use this entry. **Relevant to** WBM, VoIP **Type** boolean **Default Value** True=1

voip/line/%/dtmf_mode

Description The DTMF transmission method. This entry is not relevant for RADVISION and oSIP. For the equivalent entry, see voip/out_of_band_dtmf on page 288).

Relevant to WBM, VoIP

Type one string of:
"inband" (VOIP_DTMF_INBAND),
"rfc2833_always" (VOIP_DTMF_RFC2833_ALWAYS),
"rfc2833_negotiated" (VOIP_DTMF_RFC2833_NEGOTIATED),
"sip_info" (VOIP_DTMF_SIP_INFO)

Default Value "rfc2833_negotiated"

voip/line/%/call_waiting_enabled

Description Indicates whether call waiting is enabled. This entry is not relevant for RADVISION and oSIP. For the equivalent entry, see voip/call_waiting_enabled on page 287).

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/line/%/3_way_calling_enabled

Description Indicates whether three-way calling is enabled. This entry is not relevant for RADVISION and oSIP. For the equivalent entry, see voip/3_way_calling_enabled.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/line/%/do_not_disturb_enabled

Description Indicates whether the line is in do-not-disturb mode, preventing all incoming calls.

Relevant to WBM, VoIP

Type boolean

Default Value False=1

voip/line/%/call_forwarding_unconditional/enabled

Description Indicates whether the line is in call-forwarding mode, causing all incoming calls to be forwarded to the specified destination.

Relevant to WBM, VoIP

Type boolean

Default Value False=1

voip/line/%/call_forwarding_unconditional/destination

Description Destination to which calls are forwarded.

Relevant to WBM, VoIP

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/line/%/call_forwarding_on_busy/enabled

Description Indicates whether the line is in call-forwarding mode, causing incoming calls to be forwarded if the line is busy.

Relevant to WBM, VoIP

Type boolean

Default Value False=1

voip/line/%/call_forwarding_on_busy/destination

Description Destination to which calls are forwarded, if line is busy.

Relevant to WBM, VoIP

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/line/%/call_forwarding_on_no_answer/enabled

Description Indicates whether the line is in call-forwarding mode, causing incoming calls to be forwarded if the line is not answered.

Relevant to WBM, VoIP

Type boolean

Default Value False=1

voip/line/%/call_forwarding_on_no_answer/destination

Description Destination to which calls are forwarded, if there is no answer.

Relevant to WBM, VoIP

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/line/%/numbering_plan/min_digits

Description The minimum number of digits that must be collected before an outgoing request can be initiated.

Relevant to WBM, VoIP

Type integer (1-40)

Default Value 1

voip/line/%/numbering_plan/max_digits

Description The maximum number of digits that may be collected before an outgoing request must be initiated.

Relevant to WBM, VoIP

Type integer (1-40)

Default Value 40

voip/line/%/numbering_plan/inter_digit_timer_open

Description The maximum allowable time (expressed in milliseconds) between the dialing of digits once the minimum number of digits has been reached.

Relevant to WBM, VoIP

Type integer (1-50000)

Default Value 3000

voip/line/%/numbering_plan/prefix_info/%/prefix_range

Description A string representation of a range of prefixes.

Relevant to WBM, VoIP

Type text[42]

Default Value

voip/line/%/numbering_plan/prefix_info/%/min_digits

Description The minimum number of allowable digits for the prefix range.

Relevant to WBM, VoIP

Type integer (1-40)

Default Value 1

voip/line/%/numbering_plan/prefix_info/%/min_digits

Description The maximum number of allowable digits for the prefix range.

Relevant to WBM, VoIP

Type integer (1-40)

Default Value 40

voip/line/%/numbering_plan/prefix_info/%/num_digits_to_remove

Description Number of digits to be removed from the beginning of the prefix range.

Relevant to WBM, VoIP

Type integer (0-40)

Default Value 0

voip/line/%/numbering_plan/prefix_info/%/facility_action

Description A string representing a Facility Action implemented by the VoIP device.

Relevant to WBM, VoIP

Type one string of:
"voip_call" (VOIP_FACILITY_ACTION_VOIP_CALL),
"pstn_call" (VOIP_FACILITY_ACTION_PSTN_CALL),
"activate_dnd" (VOIP_FACILITY_ACTION_ACTIVATE_DND),
"deactivate_dnd" (VOIP_FACILITY_ACTION_DEACTIVATE_DND),
"activate_cfwd_always" (VOIP_FACILITY_ACTION_ACTIVATE_CFWD_ALWAYS),
"deactivate_cfwd_always" (VOIP_FACILITY_ACTION_DEACTIVATE_CFWD_ALWAYS),
"activate_cfwd_busy" (VOIP_FACILITY_ACTION_ACTIVATE_CFWD_BUSY),
"deactivate_cfwd_busy" (VOIP_FACILITY_ACTION_DEACTIVATE_CFWD_BUSY),
"activate_cfwd_no_answer" (VOIP_FACILITY_ACTION_ACTIVATE_CFWD_NO_ANSWER),
"deactivate_cfwd_no_answer" (VOIP_FACILITY_ACTION_DEACTIVATE_CFWD_NO_ANSWER)

Default Value "voip_call"

voip/line/%/mwi_enabled

Description Indicates whether audible message waiting indication is enabled for the line.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/line/%/fax_tx/method

Description A string representing the fax transmission method.

Relevant to WBM, VoIP

Type one string of:
"none" (VOIP_FAX_TX_NONE),
"t38_auto" (VOIP_FAX_TX_T38_AUTO),
"passthrough_auto" (VOIP_FAX_TX_PASSTHROUGH_AUTO),
"passthrough_force" (VOIP_FAX_TX_PASSTHROUGH_FORCE)

Default Value "none"

voip/line/%/fax_tx/passthrough_codec

Description A string representing the fax passthrough codec.

Relevant to WBM, VoIP

Type one string of:
"pcmu" (JRTP_PAYLOAD_PCMU),
"pcma" (JRTP_PAYLOAD_PCMA)

Default Value "pcmu"

voip/line/%/pstn_failover_enabled

Description Indicates whether calls should be routed through PSTN when failover mode is in use.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/line/%/failover_if_server_not_responding

Description Indicates whether to switch to failover mode when the SIP server doesn't respond to keep-alive messages (SIP "OPTIONS" messages). Relevant for SIP only.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/line/%/failover_if_wan_down

Description Indicates whether to switch to failover mode on loss of WAN connectivity.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/line/%/failover_if_register_failed

Description Indicates whether to switch to failover mode on registration failure.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/line/%/reg_fail_dialtone

Description A string representing the type of dial tone to be used when the line hasn't registered successfully.

Relevant to WBM, VoIP

Type one string of:
"none" (VOIP_DIALTONE_NONE),
"normal" (VOIP_DIALTONE_NORMAL),
"stutter" (VOIP_DIALTONE_STUTTER)

Default Value "normal"

voip/line/%/disconnect_supervision/fwd_disconnect_enabled

Description Indicates whether incoming hang-up events from the remote party should generate a momentary pause in the power sent to this line's telephone device, in order to signal hang-up.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/line/%/hotline/enabled

Description Indicates whether the hotline feature is enabled. If so, then placing this line off-hook will automatically generate a call to the number configured as the hotline's destination.

Relevant to VoIP

Type boolean

Default Value False=0

voip/line/%/hotline/destination

Description A string representing the destination of the hotline feature. This is the number that the auto-generated call will be directed to.

Relevant to VoIP

Type text

Default Value

voip/line/%/hotline/host

Description A string representing the hostname or IP address that the automatic hotline call will be directed to. When this parameter is set, the call will be a direct SIP call and will not pass through any proxy.

Relevant to VoIP

Type host/ip

Default Value

voip/line/%/hotline/display_name

Description A string representing the display name that will be sent in the automatic hotline call.

Relevant to VoIP

Type text

Default Value

45.5.2 Proxy

voip/line/%/proxy/enabled

Description Indicates whether SIP proxy is enabled for a specific line. This entry is relevant for oSIP and SIP Asterisk only.

Relevant to VoIP

Type boolean

Default Value False=0

voip/line/%/proxy/address

Description Manually entered SIP proxy hostname or IP address for a specific line.

Relevant to VoIP

Type host/ip

Default Value

voip/line/%/proxy/port

Description Proxy SIP port for a specific line.

Relevant to VoIP

Type integer (0-65535)

Default Value 5060

voip/line/%/proxy/auth_name

Description The username used for registration into SIP proxy.

Relevant to VoIP

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/line/%/proxy/auth_password

Description The obscured password used for registration into SIP proxy.

Relevant to VoIP

Type text[MAX_PASSWORD_LEN=64]

Default Value

voip/line/%/proxy/register_with_proxy

Description Indicates whether to perform registration with proxy.

Relevant to VoIP

Type boolean

Default Value True=1

voip/line/%/proxy/register_expires

Description The SIP proxy registration timeout (in seconds).

Relevant to VoIP

Type integer (10-86400)

Default Value 3600

voip/line/%/proxy/specify_user_agent_domain

Description Indicates whether the user_agent_domain field should be used.

Relevant to VoIP

Type boolean

Default Value False=0

voip/line/%/proxy/user_agent_domain

Description The domain name to use in the from field of outgoing SIP messages.

Relevant to VoIP

Type host/ip

Default Value

45.5.3 Outbound Proxy

voip/line/%/outbound_proxy/enabled

Description Indicates whether an outbound SIP proxy is enabled for a specific line.

Relevant to VoIP

Type boolean

Default Value False=0

voip/line/%/outbound_proxy/address

Description Manually entered hostname or IP address of the outbound proxy.

Relevant to VoIP

Type host/ip

Default Value

voip/line/%/outbound_proxy/port

Description Manually entered port for the outbound proxy.

Relevant to VoIP

Type integer (0-65535)

Default Value 5060

45.6 Phonebook

voip/phonebook/%/number

Description Locally defined speed-dial number for the user. MGCP does not use this entry.

Relevant to WBM, VoIP

Type text[15]

Default Value

voip/phonebook/%/destination_type

Description The destination type for the speed dial option. MGCP does not use this entry.

Relevant to WBM, VoIP

Type one string of
"proxy" (VOIP_DESTINATION_TYPE_PROXY),
"local" (VOIP_DESTINATION_TYPE_LOCAL),
"direct" (VOIP_DESTINATION_TYPE_DIRECT)

Default Value

voip/phonebook/%/user_id

Description Identification to be used in VoIP signalling matching the dialed speed-dial number. This entry is relevant only for **voip/phonebook/%/destination_type** "direct" or "proxy". MGCP does not use this entry.

Relevant to WBM, VoIP

Type text[MAX_USER_ID_LEN=20]

Default Value

voip/phonebook/%/local_line

Description The index of the line used only for **voip/phonebook/%/destination_type** "local". MGCP does not use this entry.

Relevant to WBM, VoIP

Type integer

Default Value

45.7 Audio

45.7.1 General

voip/audio/silence_suppression_enabled

Description Indicates whether silence suppression is enabled (available on Vinetic chipset only).

Relevant to VoIP

Type boolean

Default Value False=0

voip/audio/comfort_noise_enabled

Description Indicates whether comfort noise is enabled (available on Vinetic chipset only).

Relevant to VoIP

Type boolean

Default Value False=0

voip/audio/flash_time_max

Description Indicates the maximum on-hook time to qualify as hook-flash (available on Comcerto chipset only.

Relevant to VoIP

Type integer (250, 450, 550, 750, 850)

Default Value 850

45.7.2 Echo Cancellation

voip/audio/echo_cancellation/enabled

Description Indicates whether echo cancellation is enabled or not (available on Vinetic / IXP425 / Comcerto chipsets only).

Relevant to VoIP

Type boolean

Default Value True=1

voip/audio/echo_cancellation/tail_length

Description Indicates the tail length in milliseconds for echo cancellation (available on IXP425 / Comcerto chipsets only).

Relevant to VoIP

Type integer (2-64)

Default Value 3

voip/audio/echo_cancellation/nlp_level

Description Indicates the echo cancellation non-linear process level (available on IXP425 / Comcerto chipsets only).

Relevant to VoIP

Type one string of
"off" (VOIP_ECHO_CANCEL_NLP_OFF),
"normal" (VOIP_ECHO_CANCEL_NLP_ON),
"high" (VOIP_ECHO_CANCEL_NLP_SUP)

Default Value off

voip/audio/echo_cancellation/freeze_enabled

Description Indicates whether echo cancellation freeze is enabled (available on IXP425 / Comcerto chipsets only).

Relevant to VoIP

Type boolean

Default Value False=0

voip/audio/echo_cancellation/delay_compensation

Description Indicates the delay compensation in milliseconds for echo cancellation (available on IXP425 / Comcerto chipsets only).

Relevant to VoIP

Type integer (0-240)

Default Value 20

voip/audio/echo_cancellation/level

Description Indicates the level of echo cancellation (available on Vinetic chipset only).

Relevant to VoIP

Type one string of
"low" (VOIP_ECHO_CANCEL_LOW),
"medium" (VOIP_ECHO_CANCEL_MEDIUM),
"high" (VOIP_ECHO_CANCEL_HIGH)

Default Value "medium"

45.7.3 DSP

voip/audio/digital/input_gain

Description Indicates the digital gain (in decibels) that is applied to the signal sent via the the High Speed Serial Port (HSS) (available on IXP425 chipset only).

Relevant to VoIP

Type integer (-40-15)

Default Value 0

voip/audio/digital/output_gain

Description Indicates the digital gain (in decibels) that is applied to the signal received by the HSS (available on IXP425 chipset only).

Relevant to VoIP

Type integer (-40-15)

Default Value 0

voip/audio/digital/encoder_vol

Description Indicates the volume level (in decibels) that is applied to the voice payload by the DSP encoder (available on IXP425 chipsets only).

Relevant to VoIP

Type integer (-40-15)

Default Value -4

voip/audio/digital/decoder_vol

Description Indicates the volume level (in decibels) that is applied to the voice payload by the DSP decoder (available on IXP425 chipsets only).

Relevant to VoIP

Type integer (-40-15)

Default Value -4

voip/audio/digital/tone_gen_vol

Description Indicates the volume level (in decibels) of the tone generator. This controls the volume of DTMF tones and other tones such as dial tone, reorder tone, etc (available on IXP425 chipsets only).

Relevant to VoIP

Type integer (-20-15)

Default Value -4

45.7.4 Call Waiting

voip/audio/call_waiting/ack_spoofing_enabled

Description Indicates whether ACK spoofing is enabled or not. A positive value means we don't wait for ACK before sending the caller ID in call waiting (available on IXP425 chipset only).

Relevant to VoIP

Type boolean

Default Value False=0

voip/audio/call_waiting/ack_spoofing_fsk_delay

Description Indicates the period of time (in milliseconds) after sending CAS and before sending the caller ID on call waiting when ACK spoofing is enabled (available on IXP425 chipset only).

Relevant to VoIP

Type integer (10, 20, 30, ...)

Default Value 330

45.7.5 FXS Ports

voip/audio/electric/ringing_voltage

Description Indicates the ringing voltage in Volts (available on IXP425 chipset only).

Relevant to VoIP

Type integer (1-94)

Default Value 70

voip/audio/electric/ringing_frequency

Description Indicates the ringing frequency in Hertz (available on IXP425 chipset only).

Relevant to VoIP

Type integer (15-100)

Default Value 25

voip/audio/electric/ringing_waveform

Description Indicates the ringing waveform (available on IXP425 chipsets only).

Relevant to VoIP

Type one string of
"sinusoid" (VOIP_WAVEFORM_SINUSOID),
"trapezoid" (VOIP_WAVEFORM_TRAPEZOID)

Default Value sinusoid

voip/audio/electric/on_hook_voltage

Description Indicates the on-hook voltage in Volts (available on IXP425 chipset only).

Relevant to VoIP

Type integer (0-94)

Default Value 48

voip/audio/electric/off_hook_current

Description Indicates the off-hook current in milliamperes (available on IXP425 chipset only).

Relevant to VoIP

Type integer (20, 23, 26, .. 41)

Default Value 26

voip/audio/electric/impedance

Description Indicates the two-wire impedance. The possible values are limited by the combo-box options (available on IXP425 chipset only).

Relevant to VoIP

Type one string of
"600ohm" (VOIP_IMPEDANCE_600),
"900ohm" (VOIP_IMPEDANCE_900),
"600ohm_2_16uf" (VOIP_IMPEDANCE_600_2_16), /* 600 ohm + 2.16 uF */
"900ohm_2_16uf" (VOIP_IMPEDANCE_900_2_16), /* 900 ohm + 2.16 uF */
"270ohm_750ohm_150nf" (VOIP_IMPEDANCE_270_750_150), /* 270 ohm + (750 ohm || 150 nF) */
"220ohm_820ohm_120nf" (VOIP_IMPEDANCE_220_820_120), /* 220 ohm + (820 ohm || 120 nF) */
"220ohm_820ohm_115nf" (VOIP_IMPEDANCE_220_820_115), /* 220 ohm + (820 ohm || 115 nF) */
"370ohm_620ohm_310nf" (VOIP_IMPEDANCE_370_620_310) /* 370 ohm + (620 ohm || 310 nF) */

Default Value 600ohm

voip/audio/electric/tx_gain

Description Indicates the transmit gain in 0.1 decibel units (available on IXP425 chipset only).

Relevant to VoIP

Type integer (-35, 0, 35)

Default Value 0

voip/audio/electric/rx_gain

Description Indicates the receive gain in 0.1 decibel units (available on IXP425 chipset only).

Relevant to VoIP

Type integer (-35, 0, 35)

Default Value 0

45.7.6 Jitter

voip/audio/jitter_buffer/type

Description Indicates the type of the jitter buffer (available on Vinetic / Comcerto chipsets only).

Relevant to VoIP

Type one string of
"adaptive" (VOIP_JB_TYPE_ADAPTIVE),
"fixed" (VOIP_JB_TYPE_FIXED)

Default Value "adaptive"

voip/audio/jitter_buffer/adapt_by

Description Indicates the jitter buffer means of adaptation (available on Vinetic / Comcertro chipsets only). This entry is relevant only if **voip/audio/jitter_buffer/type** is "adaptive".

Relevant to VoIP

Type one string of
"estimated_jitter" (VOIP_JB_ADAPT_BY_ESTIMATED_JITTER),
"packet_size" (VOIP_JB_ADAPT_BY_PACKET_SIZE)

Default Value "estimated_jitter"

voip/audio/jitter_buffer/scaling_factor

Description Indicates the factor used to determine the size of the jitter buffer (available on Vinetic chipset only).

Relevant to VoIP

Type integer (0-16)

Default Value 8

voip/audio/jitter_buffer/local_adaptation

Description Indicates the type of local adaptation (available on Vinetic / Comcerto chipsets only).

Relevant to VoIP

Type one string of
"off" (VOIP_JB_LOCAL_ADAPT_OFF),
"on" (VOIP_JB_LOCAL_ADAPT_ON),
"on_with_interpolation" (VOIP_JB_LOCAL_ADAPT_ON_WITH_INTERPOLATION)

Default Value "off"

voip/audio/jitter_buffer/initial_size

Description Indicates the initial size in milliseconds of the jitter buffer (available on Vinetic / Comcerto chipsets only).

Relevant to VoIP

Type integer

Default Value 16

voip/audio/jitter_buffer/max_size

Description Indicates the maximum size in milliseconds of the jitter buffer (available on Vinetic / Comcerto chipsets only).

Relevant to VoIP

Type integer

Default Value 160

voip/audio/jitter_buffer/min_size

Description Indicates the minimum size in milliseconds of the jitter buffer (available on Vinetic / Comcerto chipsets only).

Relevant to VoIP

Type integer

Default Value 0

voip/audio/jitter_buffer/adaptation_period

Description Indicates the speed, in milliseconds, at which the jitter buffer can adapt downwards when current network conditions allow. The larger the value, the slower the jitter buffer adapts down, when jitter decreases (available on Comcerto chipset only).

Relevant to VoIP

Type integer (1000-10000)

Default Value 10000

45.7.7 Caller ID

voip/audio/cid/onhook/transmission_phase

Description Indicates the timing in which the caller ID information is transmitted to the phone, when on-hook caller ID is generated (available on Comcerto chipset only).

Relevant to VoIP

Type one string of
"before_first_ring" (VOIP_CID_TRANSMISSION_BEFORE_FIRST_RING),
"after_first_ring" (VOIP_CID_TRANSMISSION_AFTER_FIRST_RING)

Default Value "after_first_ring"

voip/audio/cid/onhook/modulation

Description Specifies the Caller ID modulation frequency, when on-hook caller ID is generated (available on Comcerto chipset only).

Relevant to VoIP

Type one string of
"bell_202" (VOIP_CID_BELL_202),
"itu_v23" (VOIP_CID_ITU_V23)

Default Value "bell_202"

voip/audio/cid/onhook/fsk_amplitude

Description Specifies the FSK tone amplitude level in dBm0 units, when on-hook caller ID is generated (available on Comcerto chipset only).

Relevant to VoIP

Type integer (-15-0)

Default Value -13

voip/audio/cid/onhook/alert_info

Description Specifies the method used for caller ID alert signaling, when on-hook caller ID is generated (available on Comcerto chipset only).

Relevant to VoIP

Type one string of
"not_required" (VOIP_CID_ALERT_NOT_REQUIRED),
"dt_as" (VOIP_CID_ALERT_DT_AS)

Default Value "not_required"

voip/audio/cid/offhook/modulation

Description Specifies the Caller ID modulation frequency, when off-hook caller ID is generated (available on Comcerto chipset only).

Relevant to VoIP

Type one string of
"bell_202" (VOIP_CID_BELL_202),
"itu_v23" (VOIP_CID_ITU_V23)

Default Value "bell_202"

voip/audio/cid/offhook/fsk_amplitude

Description Specifies the FSK tone amplitude level in dBm0 units, when off-hook caller ID is generated (available on Comcerto chipset only).

Relevant to VoIP

Type integer (-15-0)

Default Value -13

voip/audio/cid/offhook/alert_info

Description Specifies the method used for caller ID alert signaling, when off-hook caller ID is generated (available on Comcerto chipset only).

Relevant to VoIP

Type one string of
"not_required" (VOIP_CID_ALERT_NOT_REQUIRED),
"dt_as" (VOIP_CID_ALERT_DT_AS)

Default Value "dt_as"

45.8 MSS Clamping

voip/mss_clamping/enabled

Description Indicates whether Maximum Segment Size (MSS) clamping is enabled when VoIP traffic exists. Setting the MSS enables clamping on TCP packets.

Relevant to VoIP

Type boolean

Default Value False=0

voip/mss_clamping/value

Description The MSS value to be used for MSS clamping when VoIP traffic exists. If **voip/mss_clamping/enabled** is true, TCP packets are clamped according to the segment size defined here.

Relevant to VoIP

Type integer (400-1460)

Default Value 540

45.9 Trunk

voip/trunk/%/name

Description Description of the trunk.

Relevant to WBM, VoIP, PBX

Type text[MAX_DESCR_LEN=64]

Default Value "VoIP Line 0"

voip/trunk/%/type

Description Indicates the signalling protocol used by this trunk.

Relevant to WBM, VoIP, PBX

Type one string of:
"sip" (VOIP_PROT_SIP),
"h.323" (VOIP_PROT_H323)

Default Value "sip"

voip/trunk/%/limit_number_of_calls

Description Indicates whether limitation of the number of simultaneous calls is enabled.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=0

voip/trunk/%/max_number_of_calls

Description The maximum number of simultaneous calls.

Relevant to WBM, VoIP, PBX

Type integer (0-65535)

Default Value 2

voip/trunk/%/group

Description The index of the trunk-group that the trunk belongs to.

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 0

voip/trunk/%/sip/username

Description The username associated with the trunk.

Relevant to WBM, VoIP, PBX

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/trunk/%/sip/auth_name

Description The username used for registration with the SIP proxy.

Relevant to WBM, VoIP, PBX

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/trunk/%/sip/auth_password

Description The obscured password used for registration with the SIP proxy.

Relevant to WBM, VoIP, PBX

Type text[MAX_PASSWORD_LEN=64]

Default Value

voip/trunk/%/sip/proxy/address

Description Manually entered SIP proxy hostname or IP address for the trunk.

Relevant to WBM, VoIP, PBX

Type host/ip

Default Value

voip/trunk/%/sip/proxy/port

Description Proxy SIP port for the trunk.

Relevant to WBM, VoIP, PBX

Type integer (0-65535)

Default Value 5060

voip/trunk/%/sip/proxy/register_with_proxy

Description Indicates whether to perform registration with proxy.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value True=1

voip/trunk/%/sip/proxy/register_expires

Description The SIP proxy registration timeout (in seconds).

Relevant to WBM, VoIP, PBX

Type integer (10-86400)

Default Value 3600

voip/trunk/%/sip/proxy/specify_user_agent_domain

Description Indicates whether the user_agent_domain field should be used.

Relevant to VoIP

Type boolean

Default Value False=0

voip/trunk/%/sip/proxy/user_agent_domain

Description The domain name to use in the from field of outgoing SIP messages.

Relevant to VoIP

Type host/ip

Default Value

voip/trunk/%/sip/outbound_proxy/enabled

Description Indicates whether an outbound SIP proxy is used for the trunk.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=0

voip/trunk/%/sip/outbound_proxy/address

Description Manually entered hostname or IP address of the outbound proxy.

Relevant to WBM, VoIP, PBX

Type host/ip

Default Value

voip/trunk/%/sip/outbound_proxy/port

Description Manually entered port for the outbound proxy.

Relevant to WBM, VoIP, PBX

Type integer (0-65535)

Default Value 5060

voip/trunk/%/sip/dtmf_mode

Description The DTMF transmission method.

Relevant to WBM, VoIP, PBX

Type one string of:
"inband" (VOIP_DTMF_INBAND),
"rfc2833_always" (VOIP_DTMF_RFC2833_ALWAYS),
"rfc2833_negotiated" (VOIP_DTMF_RFC2833_NEGOTIATED),
"sip_info" (VOIP_DTMF_SIP_INFO)

Default Value "rfc2833_negotiated"

voip/trunk/%/sip/compat_mode

Description The compatibility mode with Broadsoft SIP server. When enabling this entry, out of band DTMF is sent according to the Broadsoft SIP server specifications. This entry is not relevant for RADVISION and oSIP.

Relevant to WBM, VoIP, PBX

Type one string of:
"off" (VOIP_SIP_COMPAT_MODE_OFF),
"broadsoft" (VOIP_SIP_COMPAT_MODE_BROADSOFT)

Default Value "off"

voip/trunk/%/sip/use_reinvite

Description Indicates whether re-invite should be used to optimize the RTP path.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=0

voip/trunk/%/h323/e164_alias

Description The E.164 phone number associated with the trunk.

Relevant to WBM, VoIP, PBX

Type text[15] (digits)

Default Value

voip/trunk/%/incoming_calls/<day|night>/action

Description The action that should be applied to a call that comes in through the trunk during the day/night time. Day and night times are determined according to the day mode schedule.

Relevant to WBM, VoIP, PBX

Type one string of:
"transfer_to_extension" (VOIP_PBX_ACTION_TRANSFER_TO_EXTENSION),
"play_auto_attendant" (VOIP_PBX_ACTION_PLAY_AUTO_ATTENDANT),
"transfer_to_hunt_group" (VOIP_PBX_ACTION_TRANSFER_TO_HUNT_GROUP),
"ring_all_extensions" (VOIP_PBX_ACTION_RING_ALL_EXTENSIONS)

Default Value "play_auto_attendant" (or "ring_all_extensions" if the auto attendant is disabled)

voip/trunk/%/incoming_calls/<day|night>/extension

Description The index of the extension that the incoming call should be transfered to during the day/night time.

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 0

voip/trunk/%/incoming_calls/<day|night>/auto_attendant

Description The index of the auto attendant that should be played when a call comes in through this trunk during the day/night time.

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 0

voip/trunk/%/incoming_calls/<day|night>/auto_attendant_on_no_answer

Description Indicates whether the call that came in through the trunk should be forwarded to an auto attendant if there was no answer.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=0

voip/trunk/%/failover_if_server_not_responding

Description Indicates whether outgoing calls should not be attempted through this trunk when the SIP server doesn't respond to keep-alive messages (SIP "OPTIONS" messages). Relevant for SIP trunks only.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/trunk/%/failover_if_wan_down

Description Indicates whether outgoing calls should not be attempted through this trunk on loss of WAN connectivity.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/line/%/failover_if_register_failed

Description Indicates whether outgoing calls should not be attempted through this trunk on registration failure.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

45.10 Trunk Group

voip/trunk_group/%/name

Description Description of the trunk group.

Relevant to WBM, VoIP, PBX

Type text[MAX_DESCR_LEN=64]

Default Value "Trunk Group 0"

45.11 Voice Mail

voip/voicemail/no_answer_timeout

Description The number of seconds an extension will ring before the call is forwarded to a voice mail.

Relevant to WBM, VoIP, PBX

Type integer (0-65535)

Default Value 20

voip/voicemail/max_message_length

Description The maximum length of a voicemail message in seconds.

Relevant to WBM, VoIP, PBX

Type integer (1-65535)

Default Value 180

voip/voicemail/enabled

Description Indicates whether the voicemail feature is enabled.

Relevant to VoIP, PBX

Type boolean

Default Value True=1 for full PBX, False=0 for home PBX

45.12 Music on Hold

voip/moh/enabled

Description Indicates whether the music on hold feature is enabled.

Relevant to VoIP, PBX

Type boolean

Default Value True=1 for full PBX, False=0 for home PBX

45.13 Call Park

voip/call_park/park_extension

Description Extension to dial to park a call.

Relevant to WBM, VoIP, PBX

Type integer (100-999)

Default Value 700

voip/call_park/min_extension

Description Minimal extension number on which a call may be parked.

Relevant to WBM, VoIP, PBX

Type integer (100-999)

Default Value 701

voip/call_park/max_extension

Description Maximal extension number on which a call may be parked.

Relevant to WBM, VoIP, PBX

Type integer (100-999)

Default Value 720

voip/call_park/timeout

Description Number of seconds a call can be parked.

Relevant to WBM, VoIP, PBX

Type integer (1-65535)

Default Value 60

45.14 Extension

voip/extension/%/number

Description The directory number assigned to the extension.

Relevant to WBM, VoIP, PBX

Type text[3] (digits)

Default Value 100 + 0-based FXS index

voip/extension/%/type

Description The type of the extension.

Relevant to WBM, VoIP, PBX

Type one string of:
"sip" (VOIP_PROT_SIP),
"mgcp" (VOIP_PROT_MGCP),
"fxs" (VOIP_PROT_FXS)

Default Value "fxs"

voip/extension/%/last_name

Description Last name of the extension owner.

Relevant to WBM, VoIP, PBX

Type text[MAX_FULLNAME_LEN=128]

Default Value

voip/extension/%/first_name

Description First name of the extension owner.

Relevant to WBM, VoIP, PBX

Type text[MAX_FULLNAME_LEN=128]

Default Value

voip/extension/%/sip/require_auth

Description Indicates whether the registration process of the SIP extension should include authentication.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=0

voip/extension/%/sip/auth_name

Description The username with which the SIP extension should register.

Relevant to WBM, VoIP, PBX

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/extension/%/sip/auth_password

Description The obscured password with which the SIP extension should register.

Relevant to WBM, VoIP, PBX

Type text[MAX_PASSWORD_LEN=64]

Default Value

voip/extension/%/sip/use_reinvite

Description Indicates whether re-invite should be used to optimize the RTP path.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=0

voip/extension/%/mgcp/media_gateway_address

Description The hostname or IP address of the MGCP extension.

Relevant to WBM, VoIP, PBX

Type host/ip

Default Value

voip/extension/%/call_waiting_enabled

Description Indicates whether the call waiting feature is enabled for the extension.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=1

voip/extension/%/3way_calling_enabled

Description Indicates whether the extension will be able to place a call on hold, transfer a call or initiate a conference call.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=1

voip/extension/%/do_not_disturb_enabled

Description Indicates whether the extension is in do-not-disturb mode, causing all incoming calls to be answered by the voice mail immediately.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=1

voip/line/%/call_forwarding_unconditional/enabled

Description Indicates whether the line is in call-forwarding mode, causing all incoming calls to be forwarded to the specified destination.

Relevant to WBM, VoIP

Type boolean

Default Value False=1

voip/line/%/call_forwarding_unconditional/destination

Description Destination to which calls are forwarded.

Relevant to WBM, VoIP

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/line/%/call_forwarding_on_busy/enabled

Description Indicates whether the line is in call-forwarding mode, causing incoming calls to be forwarded if the line is busy.

Relevant to WBM, VoIP

Type boolean

Default Value False=1

voip/line/%/call_forwarding_on_busy/destination

Description Destination to which calls are forwarded, if line is busy.

Relevant to WBM, VoIP

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/line/%/call_forwarding_on_no_answer/enabled

Description Indicates whether the line is in call-forwarding mode, causing incoming calls to be forwarded if the line is not answered.

Relevant to WBM, VoIP

Type boolean

Default Value False=1

voip/line/%/call_forwarding_on_no_answer/destination

Description Destination to which calls are forwarded, if there is no answer.

Relevant to WBM, VoIP

Type text[MAX_USERNAME_LEN=64]

Default Value

voip/extension/%/voicemail/enabled

Description Indicates whether the voicemail feature is enabled for the extension.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=1

voip/extension/%/voicemail/password

Description The obscured password used for accessing the extension's voicemail.

Relevant to WBM, VoIP, PBX

Type text[MAX_PASSWORD_LEN=64]

Default Value "0000"

voip/extension/%/mwi_enabled

Description Indicates whether audible message waiting indication is enabled for the extension.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value True=1

voip/extension/%/disconnect_supervision/fwd_disconnect_enabled

Description Indicates whether incoming hang-up events from the remote party should generate a momentary pause in the power sent to this extension's telephone device, in order to signal hang-up.

Relevant to WBM, VoIP

Type boolean

Default Value True=1

voip/extension/%/hotline/enabled

Description Indicates whether the hotline feature is enabled. If so, then placing this extension off-hook will automatically generate a call to the number configured as the hotline's destination. Relevant for analog extensions only.

Relevant to VoIP

Type boolean

Default Value False=0

voip/extension/%/hotline/destination

Description A string representing the destination of the hotline feature. This is the number that the auto-generated call will be directed to. Relevant for analog extensions only.

Relevant to VoIP

Type text

Default Value

voip/extension/%/hotline/host

Description A string representing the hostname or IP address that the automatic hotline call will be directed to. When this parameter is set, the call will be a direct SIP call and will not pass through any proxy. Relevant for analog extensions only.

Relevant to VoIP

Type host/ip

Default Value

voip/extension/%/hotline/display_name

Description A string representing the display name that will be sent in the automatic hotline call. Relevant for analog extensions only.

Relevant to VoIP

Type text

Default Value

45.15 Auto Attendant

voip/auto_attendant/attendant/%/name

Description Description of the auto attendant.

Relevant to WBM, VoIP, PBX

Type text[MAX_DESCR_LEN=64]

Default Value "Main"

voip/auto_attendant/attendant/%/selection_timeout

Description The number of seconds to wait for the caller's input after playing the auto attendant recording. If the selection timeout is up and no input was received, the caller's selection will be classified as no_selection.

Relevant to WBM, VoIP, PBX

Type integer (5-20)

Default Value 8

In the following set of entries, the `<dial_selection>` must be one of the following phone keys, representing the caller's selection:

- Digits -- **0** through **9**
- Pound -- **#**
- Asterisk -- *****
- No Selection -- **no_selection**

voip/auto_attendant/attendant/%/key/<dial_selection>/action

Description The action that should be applied to an incoming call when the caller has selected the dial_selection.

Relevant to WBM, VoIP, PBX

Type one string of:
"none" (VOIP_PBX_ACTION_NONE),
"transfer_to_extension" (VOIP_PBX_ACTION_TRANSFER_TO_EXTENSION),
"play_auto_attendant" (VOIP_PBX_ACTION_PLAY_AUTO_ATTENDANT),
"transfer_to_hunt_group" (VOIP_PBX_ACTION_TRANSFER_TO_HUNT_GROUP),
"replay_greeting" (VOIP_PBX_ACTION_REPLAY_GREETING)

Default Value "none" (or "replay_greeting" if dial_selection is no_selection)

voip/auto_attendant/attendant/%/key/<dial_selection>/extension

Description The index of the extension that the incoming call should be transfered to when the caller has selected dial_selection.

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 0

voip/auto_attendant/attendant/%/key/<dial_selection>/auto_attendant

Description The index of the auto attendant that should be played when the caller has selected dial_selection.

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 0

voip/auto_attendant/attendant/%/key/<dial_selection>/hunt_group

Description The index of the hunt group that the incoming call should be transfered to when the caller has selected dial_selection.

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 0

voip/auto_attendant/max_repetitions

Description Number of times to repeat an Auto Attendant message without user interaction before hanging up.

Relevant to WBM, VoIP, PBX

Type integer (2-20)

Default Value 8

voip/auto_attendant/enabled

Description Indicates whether the auto attendant feature is enabled.

Relevant to VoIP, PBX

Type boolean

Default Value True=1 for full PBX, False=0 for home PBX

45.16 Dial Plan

voip/dial_plan/%/pattern

Description The pattern of this dial plan entry.

Relevant to WBM, VoIP, PBX

Type text[32] (may include digits, *, #, X, Z, N, ., and square brackets)

Default Value

voip/dial_plan/%/route/%/trunk_group

Description The index of the trunk group through which the outgoing call will be routed.

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 0

voip/dial_plan/%/route/%/remove_digits

Description Indicates whether any digits should be removed from the beginning of the dial pattern before attempting to make the call.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=0

voip/dial_plan/%/route/%/num_digits_to_remove

Description Specifies the number of digits that should be removed from the dial pattern before attempting to make the call.

Relevant to WBM, VoIP, PBX

Type integer (1 through the pattern's length)

Default Value 1

voip/dial_plan/%/route/%/add_prefix

Description Indicates whether a prefix should be added to the dial string before attempting to make the call.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=0

voip/dial_plan/%/route/%/prefix

Description Specifies the prefix that should be added to the dial string before attempting to make the call.

Relevant to WBM, VoIP, PBX

Type text[32] (may include digits, * or #)

Default Value

voip/dial_plan/%/route/%/use_fallback_route

Description Indicates whether to continue on to the next route in the list when all of the trunks in this route's trunk group are in use.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value False=0

45.17 Day Mode Schedule

voip/day_mode_schedule/start_day

Description Indicates the first day of the week that will be included in the day mode schedule. Specify 0 (Sunday) to 6 (Saturday).

Relevant to WBM, VoIP, PBX

Type integer (0-6)

Default Value 1

voip/day_mode_schedule/end_day

Description Indicates the last day of the week that will be included in the day mode schedule. Specify 0 (Sunday) to 6 (Saturday).

Relevant to WBM, VoIP, PBX

Type integer (0-6)

Default Value 5

voip/day_mode_schedule/start_time

Description Specifies the time of day that indicates the beginning of the day mode schedule. The time is specified as the number of minutes that have passed since midnight.

Relevant to WBM, VoIP, PBX

Type integer (0-86340)

Default Value 28800 (08:00)

voip/day_mode_schedule/end_time

Description Specifies the time of day that indicates the beginning of the day mode schedule. The time is specified as the number of minutes that have passed since midnight.

Relevant to WBM, VoIP, PBX

Type integer (0-86340)

Default Value 61200 (17:00)

45.18 Hunt Group

voip/hunt_group/group/%/name

Description Description of the hunt group.

Relevant to WBM, VoIP, PBX

Type text[MAX_DESCR_LEN=64]

Default Value "Hunt Group 0"

voip/hunt_group/group/%/extension/%

Description The list of extensions within this hunt group. The order of the extensions in the list defines the order in which they will ring on incoming calls. The indices in this list are references to extension indices in the list voip/extension.

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value

voip/hunt_group/group/%/ring_mode

Description The type of ring for incoming calls to the hunt group.

Relevant to WBM, VoIP, PBX

Type one string of:
"ring_simultaneously" (VOIP_RING_SIMULTANEOUS),
"ring_one_at_a_time" (VOIP_RING_MODE_SEQUENTIAL)

Default Value "ring_simultaneously"

voip/hunt_group/group/%/time_to_ring_each_extension

Description The length in seconds that each extension in the hunt group should ring before the call is forwarded to the next extension (only relevant when the ring mode is ring_one_at_a_time).

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 15

voip/hunt_group/group/%/ring_order

Description This defines upon each new call which of the extensions in the hunt group should ring first (only relevant when the ring mode is ring_one_at_a_time).

Relevant to WBM, VoIP, PBX

Type one string of:
"round_robin" (VOIP_RING_ORDER_ROUND_ROBIN),
"least_recent" (VOIP_RING_ORDER_LEAST_RECENT),
"random" (VOIP_RING_ORDER_RANDOM)

Default Value "round_robin"

voip/hunt_group/group/%/hold_time_announcement/mode

Description Indicates whether a hold announcement should be played, stating caller's number in the queue.

Relevant to WBM, VoIP, PBX

Type one string of:
"no" (VOIP_ANNOUNCE_MODE_NO),
"once" (VOIP_ANNOUNCE_MODE_ONCE),
"periodic" (VOIP_ANNOUNCE_MODE_PERIODIC)

Default Value "periodic"

voip/hunt_group/group/%/hold_time_announcement/interval

Description The length in seconds between each hold announcement (relevant only if the hold announcement mode is periodic).

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 90

voip/hunt_group/group/%/wait_announcement/mode

Description Indicates whether a wait announcement should be played to the caller.

Relevant to WBM, VoIP, PBX

Type one string of:
"no" (VOIP_ANNOUNCE_MODE_NO),
"once" (VOIP_ANNOUNCE_MODE_ONCE),
"periodic" (VOIP_ANNOUNCE_MODE_PERIODIC)

Default Value "periodic"

voip/hunt_group/group/%/wait_announcement/interval

Description The length in seconds between each wait announcement (relevant only if the wait announcement mode is periodic).

Relevant to WBM, VoIP, PBX

Type unsigned integer

Default Value 90

voip/hunt_group/enabled

Description Indicates whether the hunt group feature is enabled.

Relevant to VoIP, PBX

Type boolean

Default Value True=1 for full PBX, False=0 for home PBX

45.19 Feature Codes

voip/feature_codes/facility_action

Description A string representing the Feature Code's name.

Relevant to WBM, VoIP, PBX

Type one string of:

Default Value

voip/feature_codes/code

Description Code to dial for using the Feature.

Relevant to WBM, VoIP, PBX

Type text[42]

Default Value

voip/feature_codes/enabled

Description Indicates whether Feature Code is enabled.

Relevant to WBM, VoIP, PBX

Type boolean

Default Value True=1

46

Web-Based Management (WBM)

Web-based management allows you to control various OpenRG system parameters, using a user-friendly graphical interface. The Web-based management includes a connection wizard, a graphic network map, multiple sessions, authentication data kept on gateway, multiple-user support, multilingual support, a connection diagnostics screen and more.

wbm/license_agreed **Description** Indicates that a user has agreed to the license agreement. Relevant only for evaluation images. **Relevant to** WBM **Type** boolean **Default Value** False=0
wbm/session_lifetime **Description** Idle time in milliseconds before releasing a session. Session lifetime should be '1' and above. When a session is released, you will have to login again to start a new session. Change this entry in the factory settings to comply with your device. Refer to the 'Changing the Factory Settings' section of the Programmer's Guide. **Relevant to** WBM **Type** integer **Default Value** 900000

wbm/auto_refresh

Description Should system monitoring page be automatically refreshed.

Relevant to WBM

Type boolean

Default Value True=1

wbm/confirm_needed

Description Indicates whether WBM ask for confirmation of major networking actions.

Relevant to WBM

Type boolean

Default Value True=1

wbm/diagnostics/ping_dest

Description Last address that was used in diagnostics page Ping test.

Relevant to WBM

Type domain

Default Value

wbm/diagnostics/arp_dest

Description Last address that was used in diagnostics page ARP test.

Relevant to WBM

Type IP

Default Value

wbm/conn_list/advanced

Description Should the connection list screen be displayed in advanced mode. When this entry is False, the connection list screen is displayed in basic mode.

Relevant to WBM

Type boolean

Default Value False=0

wbm/advanced_services

Description Indicates whether advanced services should be displayed.

Relevant to WBM

Type boolean

Default Value

wbm/local_network_full_list

Description Should the full list of network items be displayed. When this entry is False, a maximum of 6 items for each type is displayed.

Relevant to WBM

Type boolean

Default Value False=0

wbm/is_login_welcome_done

Description Indicates that WBM has been accessed at least once.

Relevant to WBM

Type boolean

Default Value False=0

wbm/is_login_setup_done

Description Indicates that a user has defined his first user and password for login.

Relevant to WBM

Type boolean

Default Value False=0

wbm/is_installation_done

Description Indicates that a user has finished the installation.

Relevant to WBM

Type boolean

Default Value False=0

wbm/is_dormant_mode_rw

Description Indicates if the WBM is read-write in dormant mode (CableHome). When this entry is true, it overrides the entry which disables WBM, called **system/rg_disable_features** (page system/rg_disable_features).

Relevant to WBM

Type boolean

Default Value False=0

wbm/theme

Description Active user interface theme (schema/skin).

Relevant to WBM

Type one string of:
"openrg" (GUI_RG),
"opensmb" (GUI_SMB),
"cisco_linksys" (GUI_LINKSYS),
"netgear" (GUI_NETGEAR),
"welltech" (GUI_WELLTECH),
"belkin" (GUI_BELKIN),
"openrg2" (GUI_RG2),
"opensmb2" (GUI_SMB2),
"jungo_net_rg2" (GUI_JNET_RG2),
"jungo_net_smb2" (GUI_JNET_SMB2),
"custrg2" (GUI_CUST_RG2),
"custsmb2" (GUI_CUST_SMB2)

Default Value OpenRG

wbm/readonly

Description Determines if new WBM sessions are opened in readonly mode. Useful for debugging.

Relevant to WBM

Type boolean

Default Value False=0

wbm/ch_ui_selection

Description The CableHome User Interface (UI) mode, as described by cabhPsDevUISelection in CH-SP-MIB-PSDEV document.

Relevant to WBM

Type one string of:
"manufacturer_local" (UI_MFG_LOCAL),
"operator_local" (UI_OPERATOR_LOCAL),
"operator_server" (UI_OPERATOR_SERVER),
"disabled" (UI_DISABLED)

Default Value manufacturer_local

wbm/ch_ui_server_url

Description Uniform Resource Location (URL) of the external UI to present (redirect) to the user when UI mode is UI_OPERATOR_SERVER (see the **wbm/ch_ui_selection** entry).

Relevant to WBM

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

wbm/ch_ui_disabled_body_text

Description Default text for the HTTP body tag to include in the response to UI requests when the UI mode is UI_DISABLED (see the **wbm/ch_ui_selection** entry).

Relevant to WBM

Type text[255]

Default Value

wbm/allow_tcp_detection

Description Indicates whether to allow automatic detection of TCP services on the LAN devices.

Relevant to WBM

Type boolean

Default Value True=1

wbm/ajax/enabled

Description Indicates whether AJAX content should be displayed in the WBM.

Relevant to WBM

Type boolean

Default Value False=0

wbm/ajax/server/%/address

Description An AJAX server address.

Relevant to WBM

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

47

Web Filtering

The abundance of harmful information on the Internet is posing a serious challenge for employers and parents alike - "How can I regulate what my employee/child does on the net?" OpenRG's Web-filtering allows parents and employers to regulate, control and monitor Internet access. By classifying and categorizing online content, it is possible to create numerous Internet access policies, and easily apply them to your home network computers. As a result, you may keep your children from harm's way by limiting access to adult and violent material, or increase employee productivity by regulating access to non work-related Internet content.
A filtering policy defines what sites will be blocked based on their category. OpenRG provides four built-in policies:

Block All Blocks all access to the Internet.

Allow All Allows unlimited Internet access.

Home Blocks sites under the 'Child Protection' category.

Empolyee Blocks sites from non work-related categories.

filter/http/policy/%/name

Description Specifies the name of the policy, adult, child etc.

Relevant to HTTP filtering

Type text[MAX_POLICY_NAME_LEN=32]

Default Value

filter/http/policy/%/description

Description Description of the policy.

Relevant to HTTP filtering

Type text[MAX_FULLNAME_LEN=128]

Default Value

filter/http/policy/%/cat/<no>/block

Description Should category <no> be blocked for the specified policy.

Relevant to HTTP filtering

Type boolean

Default Value

filter/http/policy/%/url_filter/keywords

Description List of URL keywords to be either blocked or allowed, according to **filter/http/policy/%/url_filter/action**.

Relevant to HTTP filtering

Type text

Default Value

filter/http/policy/%/url_filter/web_sites

Description List of Web sites to be either blocked or allowed, according to **filter/http/policy/%/url_filter/action**.

Relevant to HTTP filtering

Type text

Default Value

filter/http/policy/%/url_filter/action

Description Defines if the matching Web sites or URL keywords are to blocked or allowed access.

Relevant to HTTP filtering

Type one string of:
"allow" (HTTP_PROXY_FILTER_ALLOW),
"block" (HTTP_PROXY_FILTER_BLOCK)

Default Value

filter/http/redirect_url

Description The URL of the page to which to redirect when the site is blocked.

Relevant to HTTP filtering

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

filter/http/liccode

Description License code to be used instead of \prd box ID.

Relevant to HTTP filtering

Type text[12]

Default Value

48

Web Server

OpenRG can operate as a Web server, hosting one or more Web sites which are accessible from the LAN or the WAN. The advantages of this feature are:

- The Web site is hosted on OpenRG, eliminating the need to assign a station on the LAN to act as a Web server, or to outsource expensive hosted services.
- LAN security: users from the Internet can access your Web site without entering your LAN.
- Simple and fast configuration.

48.1 General

web_server/enabled **Description** Indicates whether the Web server is enabled. **Relevant to** web server **Type** boolean **Default Value** True=1
web_server/log_requests **Description** Indicates if HTTP requests for the Web server should be logged. **Relevant to** web server **Type** boolean **Default Value** False=0

web_server/basedir

Description File pathname of base directory for content of Web server (static html pages).

Relevant to web server

Type text[MAX_PATH_LEN=100]

Default Value

48.2 HTTP Server

web_server/https/ports/%/port

Description Port number of HTTP server. The HTTP server indexes can be 0 or 1 representing unsecured server and over SSL respectively.

Relevant to web server

Type integer (1-65535)

Default Value Port 80, 443 for index 0 and 1 respectively

web_server/https/ports/%/ssl_mode

Description Indicates if this server port is over SSL, and if it is, how to authenticate the client. The HTTP server indexes can be 0 or 1 representing unsecured server and over SSL respectively.

Relevant to web server

Type one string of:
"none" (MGT_SRV_SSL_NONE),
"no_verify" (MGT_SRV_SSL_NO_PEER_VERIFY),
"verify" (MGT_SRV_SSL_VERIFY_PEER),
"verify_fail_no_cert" (MGT_SRV_SSL_VERIFY_FAIL_IF_NO_PEER_CERT)

Default Value "none" for index 0, "no_verify" for index 1

web_server/https/ports/%/remote_access

Description Indicates if this server port can be accessed from the WAN.

Relevant to web server

Type boolean

Default Value False=0

48.3 User Directory

web_server/userdir/enable

Description Indicates if the user directory feature is enabled for the Web server.

Relevant to web server

Type boolean

Default Value

web_server/userdir/path

Description Subdirectory below user's home directory containing \~\{\}**user** html files.

Relevant to web server

Type text[MAX_PATH_LEN=100]

Default Value

48.4 Virtual Host

web_server/vhost/%/domain_name

Description Fully qualified domain name of virtual host (e.g. `http://www.jungo.com`).

Relevant to web server

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

web_server/vhost/%/basedir

Description Base directory for the virtual host.

Relevant to web server

Type text[MAX_PATH_LEN=100]

Default Value

web_server/vhost/%/aliases/%/name

Description Alias for domain name of the virtual host.

Relevant to web server

Type text[MAX_DOMAIN_NAME_LEN=255]

Default Value

49

Licensing Acknowledgement and Source Code Offering

The OpenRG/OpenSMB product may contain code that is subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), and BSD (BSDS) license. The OpenRG/OpenSMB Open Source and GNU Public Licenses page contains:

- With respect to GPL/LGPL: the code package names, license types and locations for the license files, and
- With respect to BSD (BSDS): the code package names with the license texts.

To receive the source code of the GPL/LGPL packages, refer to http://www.jungo.com/openrg/download_gpl.html.

50

Contact Jungo

For additional support, please contact Jungo Software Technologies Ltd.:

Web site:	http://www.jungo.com
E-mail:	Sales: openrg@jungo.com
	Support: rg_support@jungo.com

Jungo Headquarters
3031 Tisch Way
San Jose, CA 95128
U.S.A
Tel. +1 (408) 423 9540
+1 (877) 514 0537
Fax. +1 (877) 514 0538

EMEA
One Heathrow Blvd.
286 Bath Road
West Drayton
Middlesex UB7 0DQ
United Kingdom
Tel. +44 (20) 8476 8481
Fax. +44 (20) 8476 8482

Asia Pacific
P.O.Box 118-757 Taipei
Taipei City 10599
Taiwan (R.O.C)
Tel. +886 (9) 1938 2709

R&D Center
1 Hamachshev Street
Netanya 42504
Israel
Tel. +972 (74) 721 2121
Fax. +972 (74) 721 2122