



Wi² Controller CLI

Reference Guide

SW Version 5.2
June 2008
P/N 215029

Legal Rights

© Copyright 2008 Alvarion Ltd. All rights reserved.

The material contained herein is proprietary, privileged, and confidential and owned by Alvarion or its third party licensors. No disclosure thereof shall be made to third parties without the express written permission of Alvarion Ltd.

Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

Trade Names

Alvarion[®], BreezeCOM[®], WALKair[®], WALKnet[®], BreezeNET[®], BreezeACCESS[®], BreezeMANAGE[™], BreezeLINK[®], BreezeConfig[™], BreezeMAX[™], AlvariSTAR[™], AlvariCRAFT[™], BreezeLITE[™], MGW[™], eMGW[™], and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion Ltd.

All other names are or may be the trademarks of their respective owners.

Statement of Conditions

The information contained in this manual is subject to change without notice. Alvarion Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranties and Disclaimers

All Alvarion Ltd. ("Alvarion") products purchased from Alvarion or through any of Alvarion's authorized resellers are subject to the following warranty and product liability terms and conditions.

Exclusive Warranty

(a) Alvarion warrants that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of fourteen (14) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). Alvarion will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Alvarion's standard R&R procedure.

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from

invoice date (the "Warranty Period"). During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

Additional hardware, if required, to install or use Firmware updates must be purchased by the Customer. Alvarion will be obligated to support solely the two (2) most recent Software major releases.

ALVARION SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY PURCHASER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR IMPROPER TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

Disclaimer

(a) The Software is sold on an "AS IS" basis. Alvarion, its affiliates or its licensors MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. ALVARION SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE. UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. ALVARION SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER

WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ALVARION' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

(a) ALVARION SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OF ALVARION OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY (EXCEPT IN THE CASE OF A BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS).

Disposal of Electronic and Electrical Waste



Disposal of Electronic and Electrical Waste

Pursuant to the WEEE EU Directive electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Important Notice

This user manual is delivered subject to the following conditions and restrictions:


- This manual contains proprietary information belonging to Alvarion Ltd. Such information is supplied solely for the purpose of assisting properly authorized users of the respective Alvarion products.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Alvarion Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that license.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.
- The information contained herein is merely descriptive in nature, and does not constitute an offer for the sale of the product described herein.
- Any changes or modifications of equipment, including opening of the equipment not expressly approved by Alvarion Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.



About This Guide

This guide explains how to work with the Command Line Interface (CLI) on Alvarion Wi² Controllers.

This guide comprises the following parts:

- Chapter 1 - Introduction
 - Chapter 2 - CLI commands
- 



Contents

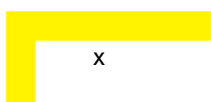
Chapter 1 - Introduction

1.1 About This Guide	2
1.1.1 Products Covered	2
1.1.2 Important Terms	2
1.1.3 Typographical Conventions.....	2
1.2 Configuring CLI Support	4
1.3 SSH Client Support	6
1.4 Entering Strings	7
1.5 Context Hierarchy	8
1.6 Sample CLI Session	12
1.7 File Transfer	13

Chapter 2 - CLI Commands

2.1 View Context.....	16
arping	16
curl	16
enable	18
nslookup	19
ping	19
ps	19
quit	19
show license	19
show logging filtered	19
top	19
traceroute	20
2.2 Enable Context	21
reboot device	21
show certificate	21
show certificate binding	21
ping	21
arping	21
arp	22
end	22

quit	22
rcapture	22
show arp	22
show bridge	22
show bridge forwarding	22
show dns cache	23
show interfaces	23
show ip route	23
show system info	23
show ip dhcp database	23
show dot11 associations	23
show dot11 statistics client-traffic	23
show local mesh	24
show wireless neighborhood	24
show wireless rogue-ap	24
show satellites	24
show client log	24
show radius statistics	24
show radius users	24
show users	25
show discrete pin	25
config	25
show all config	25
controlled network	25
show controlled network config	25
2.3 Config Context.....	26
certificate	26
certificate binding	26
certificate revocation	26
end	26
factory settings	26
interface ethernet	26
reboot device	27
show certificate	27
show certificate binding	27
show config factory	27
username	27
interface ip	27
interface wireless	27
local mesh profile	28
interface pptp client-default	28
interface gre	28
virtual ap	28
show subscription plan	28
subscription plan	28
ipsec policy	29
admin authentication local fallback	29
admin authentication radius	29
clock summer-time	29
clock timezone	29
ip http port	30



ip https port	30
ntp protocol	30
ntp server	30
snmp-server trap certificate-expired	30
snmp-server trap certificate-expires-soon	31
snmp-server trap web-fail	31
snmp-server trap web-login	31
snmp-server trap web-logout	31
web admin kickout	31
web allow	32
world-mode dot11 country code	32
web access internet-port	32
web access lan-port	32
web access wireless	32
web access interface vlan	33
web access interface gre	33
web access local mesh	33
web access lan	33
web access vpn	33
dhcp mode	33
dhcp server	34
dhcp server default domain name	34
dhcp server default lease period	34
dhcp server default permanent lease period	34
dhcp server logout html user	34
dhcp relay	34
dhcp relay circuit id	34
dhcp relay remote id	35
clock	35
ntp server	35
ntp server failure trap	35
config-update automatic	35
config-update operation	36
config-update time	36
config-update uri	36
config-update weekday	36
snmp-server trap config-change	36
snmp-server trap config-update	37
logging destination	37
snmp-server trap syslog-severity	37
snmp-server	37
snmp-server access port-1	37
snmp-server allow	38
snmp-server chassis-id	38
snmp-server contact	38
snmp-server heartbeat period	38
snmp-server location	39
snmp-server port	39
snmp-server readonly	39
snmp-server readwrite	39
snmp-server trap	39
snmp-server trap community	40

snmp-server trap destination	40
snmp-server trap heartbeat	40
snmp-server trap link-state	40
snmp-server trap snmp-authentication	40
snmp-server version	41
snmp-server access interface vlan	41
snmp-server access local mesh	41
snmp-server access interface gre	41
snmp-server access wireless	41
snmp-server access port-2	41
snmp-server access lan	42
snmp-server access vpn	42
snmp-server trap new-satellite-detected	42
snmp-server trap satellite-unreachable	42
soap-server	42
soap-server access interface vlan	43
soap-server access port-1	43
soap-server access port-2	43
soap-server allow	43
soap-server http authentication	43
soap-server http authentication password	44
soap-server http authentication username	44
soap-server port	44
soap-server ssl	44
soap-server ssl with client certificate	44
soap-server access interface gre	44
soap-server access wireless	45
soap-server access local mesh	45
soap-server access lan	45
soap-server access vpn	45
snmp-server trap low-snr	45
snmp-server trap low-snr interval	46
snmp-server trap low-snr level	46
snmp-server trap new-association	46
snmp-server trap new-association interval	46
snmp-server trap vpn-connection	46
snmp-server trap wireless-association-fail	46
snmp-server trap wireless-association-success	47
snmp-server trap wireless-authentication-fail	47
snmp-server trap wireless-authentication-success	47
snmp-server trap wireless-deauthentication-fail	47
snmp-server trap wireless-deauthentication-success	47
snmp-server trap wireless-disassociation-fail	48
snmp-server trap wireless-disassociation-success	48
snmp-server trap wireless-reassociation-fail	48
snmp-server trap wireless-reassociation-success	48
snmp-server trap syslog-matches	48
snmp-server trap syslog-matches regex	49
snmp-server trap syslog-severity level	49
snmp-server trap network-trace	49
firmware-update automatic	49
firmware-update start	50

firmware-update time	50
firmware-update uri	50
firmware-update weekday	50
snmp-server trap firmware-update	50
ip name-server	50
ip name-server cache	51
ip name-server dynamic	51
ip name-server switch-on-servfail	51
ip name-server switch-over	51
ip name-server logout-host-name	52
ip name-server logout-ip-address	52
snmp-server trap unauthorized-ap	52
snmp-server trap unauthorized-ap interval	52
wireless-scan	52
wireless-scan period	52
wireless-scan url	53
access controller shared secret	53
radius-server profile	53
ip-qos profile	53
access controller	54
certificate ipsec ca	54
certificate ipsec local	54
certificate ipsec revocation	54
certificate ssl	54
session profile default	55
session profile	55
show session profile	55
remote configuration	55
dot11 igmp snooping-helper	55
discovery protocol	55
discovery protocol device-id	56
service controller ap authentication credentials	56
service controller ap authentication enable	56
service controller ap authentication file	56
service controller ap authentication radius-server	56
service controller ap authentication refresh-rate	57
service controller ap authentication source file	57
service controller ap authentication source local	57
service controller ap authentication source radius	57
service controller discovery	57
service controller primary	57
service controller primary ip addr	58
service controller provisioning	58
bridge priority	58
bridge protocol ieee	58
bandwidth control internet-port	58
bandwidth control internet-port high	59
bandwidth control internet-port low	59
bandwidth control internet-port max-rate	59
bandwidth control internet-port normal	60
bandwidth control internet-port very-high	60
ip route gateway	60

firmware distribution	61
firmware distribution default username	61
firmware distribution load cim	61
firmware distribution load list	61
firewall mode	62
show user profiles	62
show user profiles details	62
user profile	62
renew user profile subscription	62
dot1x reauth	62
dot1x reauth period	63
dot1x reauth terminate	63
dot1x supplicant timeout	63
dynamic key	63
dynamic key interval	63
add wireless ip-qos profile	64
delete wireless ip-qos profile all	64
delete wireless ip-qos profile	64
wireless link qos	64
key chain	64
config-version	64
radius-server accounting session	65
radius-server client	65
use default shared secret	65
use default shared secret	65
radius-server local chap	65
radius-server local eap-md5	65
radius-server local eap-peap	66
radius-server local eap-tls	66
radius-server local eap-ttls	66
radius-server local Controllerhap	66
radius-server local Controllerhapv2	66
radius-server local pap	66
radius-server ssid detection nas-id	67
show radius-server	67
active-directory check attribute	67
active-directory check user access	67
active-directory device name	67
active-directory domain	68
active-directory group	68
active-directory group order	68
active-directory join	68
show active-directory	68
show active-directory group	68
radius-server client	68
user tracking	69
user tracking destination	69
user tracking filter	69
user tracking port	69
persistent user information	69
persistent user information period	69
2.4 Access Controller Context	70

end	70
station allocate source ip address	70
station allow any ip address	70
station free access	71
station http proxy support	71
station idle detection	71
system accounting	72
authentication http	72
authentication https	72
noc access internet	72
noc access vpn	72
noc allow	73
noc authentication	73
secure login	73
noc access interface vlan	73
noc access interface gre	74
ipass id	74
ipass name	74
wispr abort login url	74
wispr login url	74
wispr logoff url	75
access-list	75
use access-list	76
config file	76
https ssl certificate	76
mac-address	76
fail page	77
goodbye url	77
ipass login url	77
login error url	77
login page	78
login url	78
logo	78
messages	78
noc ssl ca-certificate	78
noc ssl certificate	79
session page	79
transport page	79
welcome url	79
notify user location changes	79
2.5 Default Session Profile Context.....	80
accounting interim update	80
idle timeout	80
maximum input octets	80
maximum input packets	80
maximum output octets	81
maximum output packets	81
maximum total octets	81
maximum total packets	81
nat one-to-one	81
session timeout	82

smtp redirection setup	82
end	82
smtp redirection	82
2.6 Session Profile Context	83
end	83
access controlled	83
access list	83
accounting interim update	83
arp polling interval	84
arp polling max count	84
bandwidth level	84
egress vlan access-controlled	84
egress vlan regular	85
idle timeout	85
intercept traffic	85
max input rate	85
max output rate	86
nat one-to-one	86
session profile	86
smtp redirection setup	86
termination action	87
user defined attribute	87
2.7 User Profile Context	89
end	89
access controlled	89
access-controlled profile	90
access-controlled virtual ap	90
active	90
chargeable user identity	90
control method	91
egress vlan	91
end time	91
idle timeout	91
max user sessions	91
password	91
regular profile	92
regular virtual ap	92
session timeout	92
subscription plan	92
username	92
2.8 Internet Interface Context	93
duplex	93
end	93
speed	93
interface vlan	93
ipsec vlan interface	94
2.9 LAN Interface Context	95
duplex	95

end	95
speed	95
interface vlan	95
ipsec vlan interface	96
2.10WAN IP Interface Context	97
pppoe client user	97
ip address mode	97
ip address	97
ip nat	98
nat limit port range	98
nat limit port range size	98
ip address dhcp client-id	98
end	98
pppoe auto-reconnect	99
pppoe mru	99
pppoe mtu	99
pppoe unnumbered	99
ip nat outside source static	100
ip rip authentication key-chain	100
ip rip authentication mode	100
ip rip authentication string	100
passive-interface	101
router rip	101
ip address alternate	101
2.11LAN IP Interface Context.....	102
end	102
ip address	102
ip address management	102
passive-interface	102
router rip	103
2.12Wireless Context.....	104
end	104
radio active	104
rts threshold	104
distance	105
dot11	105
transmit power	105
antenna bidirectionnal	106
autochannel skip	106
beacon interval	106
dot11 automatic frequency	106
dot11 automatic frequency period	107
dot11 automatic frequency time	107
dot11 automatic transmit-power	107
dot11 automatic transmit-power period	107
multicast rate	107
station distance	108
dot11 mode	108
2.13RADIUS Remote Configuration	109

end	109
active	109
credentials	109
interval	109
radius server profile	109
2.14 Virtual AP Context	110
virtual ap name	110
access control	110
ingress interface	111
egress unauthenticated	111
max-association	112
ssid name	112
vlan	112
guest-mode	112
encryption key 1	113
encryption key format	113
transmit key	113
authentication server access controller	113
authentication server accounting	114
authentication server accounting radius profile	114
authentication server radius	114
wpa-psk	114
authentication server request radius cui	114
mac authentication accounting	115
mac authentication accounting radius profile	115
mandatory authentication	115
mac authentication radius profile	115
mac authentication remote	116
mac authentication request radius cui	116
mac authentication local	116
mac authentication	116
html authentication	116
dot1x mandatory authentication	116
html authentication accounting	117
html authentication accounting radius profile	117
html authentication local	117
html authentication radius	117
html authentication radius profile	117
html authentication request radius cui	118
html authentication timeout	118
active	118
beacon dtim count	118
public forwarding	118
fast authentication	118
layer3 mobility	119
access lan stations	119
beacon transmit power	119
data rate maximum	119
data rate minimum	119
add ip-qos profile	120

delete ip-qos profile all	120
delete ip-qos profile	120
qos	120
upstream diffserv tagging	121
wmm advertising	121
html redirection	122
bandwidth	122
bandwidth default rates	122
bandwidth default rates maximum	122
radius accounting realms	122
radius authentication realms	122
location-aware group	123
location-aware called-station-id content	123
dhcp relay	123
dhcp relay active	123
dhcp relay circuit id	123
dhcp relay not active	124
dhcp relay remote id	124
dhcp relay subnet	124
dhcp server	124
dhcp server dns	124
dhcp server gateway	124
dhcp server range	125
dhcp server subnet	125
radius-framed-protocol-attribute	125
end	125
security	125
2.15VLAN Interface Context.....	127
end	127
ip address	127
ip address mode	127
vlan name	128
ip default-gateway	128
ip nat	128
2.16Local Mesh Context.....	129
end	129
active	129
interface	129
local mesh name	129
remote mac	129
security	130
security mode	130
security psk	130
security wep	130
speed	130
interface vlan	130
accept forced links	131
allowed downtime	131
dynamic local mesh	131
dynamic mode	131

initial discovery time	131
mesh id	131
minimum snr	132
preserve master link	132
promiscuous mode	132
promiscuous mode startup delay	132
snr cost per hop	132
2.17RADIUS Context.....	133
end	133
radius-server accounting port	133
radius-server alternate hosts	133
radius-server authentication method	133
radius-server authentication port	134
radius-server deadtime	134
radius-server host	134
radius-server key 2	134
radius-server message-authenticator	134
radius-server name	135
radius-server nasid	135
radius-server timeout	135
radius-server timeout	135
radius-server force-nas-port-to-vlanid	135
radius-server realm	135
radius-server realm name	136
2.18IP_QOS Context	137
end	137
end-port	137
priority	137
profile name	137
protocol	137
start-port	138
2.19DHCP Server Context	139
end	139
active	139
gateway	139
range	139
permanent leases	139
2.20GRE Interface Context.....	140
end force	140
gre name	140
ip address	140
peer ip address	140
remote ip address	140
2.21IPsec Policy Context	141
end	141
active	141
authentication	141

cipher	141
dns domain	141
dns server	142
incoming nat	142
incoming traffic network	142
interface	142
local id	142
mode	142
outgoing traffic network	142
peer id	143
peer ip address	143
perfect forward secrecy	143
preshared key	143
2.22 Syslog Destination Context	144
active	144
logging facility	144
logging host	144
logging prefix	144
name	144
end	145
level	145
level	145
matches	145
message	145
message	146
process	146
process	146
2.23 PTP Client Interface	147
active	147
pptp client credentials	147
pptp client domain name	147
pptp client server address	147
end	147
ip nat	147
pptp client auto route discovery	148
pptp client lcp echo	148
passive-interface	148
router rip	148
2.24 Keychain Context	149
end	149
key	149
key chain name	149
2.25 Keys Context	150
end	150
key-string	150
2.26 Subscription Plan	151
end	151

daily restriction	151
end time	151
initial login time allocation	151
online time limit	152
online time limit	152
start time	152
subscription plan name	152
2.27 Active Directory Group Context	153
end	153
access controlled	153
access-controlled profile	153
access-controlled virtual ap	153
active	154
active-directory group name	154
egress vlan	154
regular profile	154
regular virtual ap	154
2.28 Controlled Network AP Context	156
end	156
execute action	156
execute system action	156
show config factory	156
ap group	156
ap name	156
contact	157
location	157
product type	157
2.29 Controlled Network AP Group Context.....	158
execute action	158
show config factory	158
end	158
config	158
group name	158
virtual ap binding	158
2.30 Controlled Network Base Group Context.....	159
execute action	159
show config factory	159
config	159
end	159
2.31 Controlled Network Context	160
end	160
interface wireless	160
local mesh group	160
local mesh provisioning group	160
provisioning connectivity	160
provisioning discovery	160
radius profile	161

syslog	161
sensor server name	161
sensor server id	161
sensor discovery mode	161
sensor network detector	162
inherit sensor	162
dynamic key	162
dynamic key interval	162
dot1x reauth	163
dot1x reauth period	163
dot1x reauth terminate	163
dot1x supplicant timeout	163
inherit 8021x	163
bridge protocol ieee	164
inherit untagged stp	164
bridge protocol ieee vlan	164
inherit vlan stp	164
centralized access control	164
inherit access control	164
inherit local mesh qos	165
local mesh ip qos profile	165
local mesh qos mechanism	165
inherit service availability	165
virtual network services on-failure	165
inherit l3subnets	166
l3subnet	166
2.32Virtual AP Binding Context.....	167
egress vlan	167
egress vlan	167
end	167
location aware	167
2.33Syslog Context.....	168
message	168
message	168
process	168
process	168
level	169
level	169
matches	169
end	169
inherit	169
2.34Provisioning Connectivity Context	171
end	171
inherit	171
interface	171
interface provisioninig	171
ip assignation	171
vlan	172
vlan	172


ip static	172
provisioning local mesh group	172
provisioning local mesh key	172
provisioning local mesh port	172
provisioning local mesh security	172
provisioning local mesh security	173
provisioning local mesh type	173
country code	173
2.35 Provisioning Discovery Context	174
end	174
dns name	174
dns provisioning	174
inherit	174
dns domain name	175
dns server	175
discovery provisioning	175
ip address	175
ip provisioning	175
2.36 Controlled Mode Wireless Interface Context	176
distance	176
transmit power	176
multicast rate	177
dot11 automatic frequency	177
dot11 automatic frequency period	177
dot11 automatic frequency time	177
dot11 automatic transmit-power	177
dot11 automatic transmit-power period	178
antenna bidirectionnal	178
autochannel skip	178
station distance	178
beacon interval	179
rts threshold	179
dot11 mode	179
radio active	179
end	180
inherit	180
spectralink view	180
2.37 RADIUS Profile Context	181
end	181
inherit	181
radius nas id	181
2.38 Local Mesh Profile Context.....	182
security	182
security mode	182
security psk	182
security wep	182
dynamic mode	183
mesh id	183

allowed downtime	183
minimum snr	183
snr cost per hop	183
initial discovery time	183
active	183
end	184
inherit	184
name	184
radio active	184
2.39 Local Mesh Provisioning Profile Context	185
accept connection	185
end	185
inherit	185
multiple radio	185





Chapter 1 - Introduction



In This Chapter:

- “About This Guide” on page 2
- “Configuring CLI Support” on page 4
- “SSH Client Support” on page 6
- “Entering Strings” on page 7
- “Context Hierarchy” on page 8
- “Sample CLI Session” on page 12

1.1 About This Guide

This guide explains how to work with the Command Line Interface (CLI) on Alvarion MultiService Controllers.

1.1.1 Products Covered

This guide covers these products:

- Wi²-CTRL-10, Wi²-CTRL-40, Wi²-CTRL-200

1.1.2 Important Terms

The following terms are used in this guide.

Term	Description
AP	These terms are used interchangeably to refer to any Alvarion MultiService Access Point
controller (service controller)	These terms are used interchangeably to refer to any Alvarion Service Controller as defined in <i>Products Covered</i> above.
local mesh	Previously referred to as WDS. Some older commands refer to “wireless links” whereas newer commands use the “local mesh” terminology and they also provide dynamic functionality.
Virtual map, VAP	In this document, the terms “Virtual map” and “VAP” are used in place of “VSC” (Virtual Service Community).

1.1.3 Typographical Conventions

1.1.3.1 Command Syntax

Command syntax is formatted in a monospaced font as follows:

Example	Description
<code>use-access-list</code>	Command name. Specify it as shown.

Example	Description
<pre>ip-qos profile <name></pre>	<p>A single item enclosed in angle brackets and all formatted in italic indicates a user-supplied item. Specify the item. Do not include the angle brackets. In this example, a valid QoS profile name is required. For example:</p> <pre>ip-qos profile voice</pre>
<pre>wireless interface (1 2)</pre>	<p>Multiple Items enclosed in parenthesis and separated by vertical bars indicate a mandatory choice. Include one of the mandatory items, without the parenthesis and without the vertical bar. In this example, either 1 or 2 must be included. For example:</p> <pre>wireless interface 2</pre>
<pre>show logging [filtered]</pre>	<p>Items enclosed in square brackets are optional. You can either include them or not. Do not include the brackets. In this example you can specify the command in one of two ways:</p> <pre>show logging show logging filtered</pre>

1.1.3.2 Management Tool

When referring to the management tool interface, the Main menu name is presented first followed by a right angle-bracket and then the sub-menu name, as in **Network > Ports**.

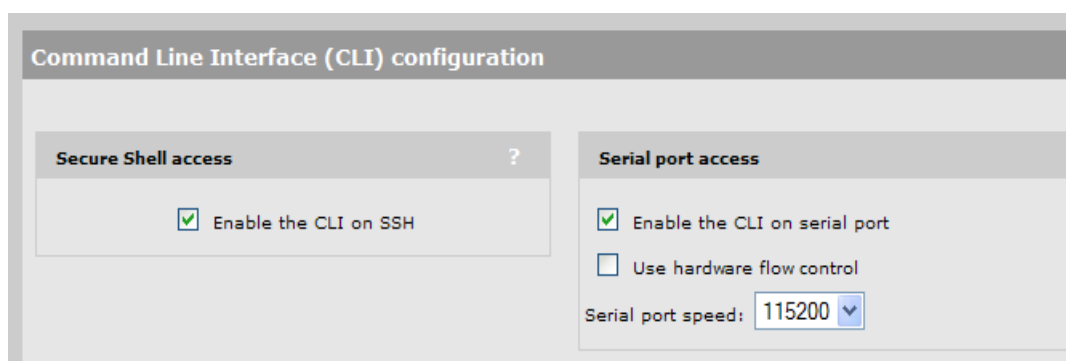
(Wi² controller series only.) Double angle brackets >> separate elements that appear in the Network Tree from main menu and sub-menu references, as in **Service Controller >> Status**.

1.2 Configuring CLI Support

Using the service controller's management tool, open the CLI configuration page:

- On the Wi² controller series, select **Service controller >> Management > CLI**.

Use this page to enable/disable CLI support via an SSH or serial connection. A maximum of three concurrent CLI sessions are supported regardless of the connection type.



The screenshot shows the 'Command Line Interface (CLI) configuration' page. It has two main sections: 'Secure Shell access' and 'Serial port access'. In the 'Secure Shell access' section, there is a checkbox labeled 'Enable the CLI on SSH' which is checked. In the 'Serial port access' section, there is a checkbox labeled 'Enable the CLI on serial port' which is checked, and another checkbox labeled 'Use hardware flow control' which is unchecked. Below these checkboxes, there is a dropdown menu for 'Serial port speed' set to '115200'.

Figure 1-1: Command Line Interface Configuration

The CLI supports SSH on the standard TCP port (22).

Connectivity and login credentials for SSH connections use the same settings as defined for management tool administrators on the **Management tool** page.

- On the Wi² controller series, select **Service controller >> Management > Management tool** (illustrated)..

Management tool configuration

Administrator authentication ?

Authenticate via:

Username:

Current password:

New password:

Confirm new password:

Security ?

Access to the management tool is enabled for the addresses and interfaces that are specified below.

Allowed addresses:

IP address:

Mask:

Active interfaces:

LAN port

Internet port

VPN

VLAN/GRE

Select from the list:

Login control ?

If an administrator is logged in, then a new administrator login:

Terminates the current administrator session

Is blocked until the current administrator logs out

Web server ?

Secure web server port:

Web server port:

Auto-Refresh ?

Interval: seconds

Web inactivity logout ?

Timeout: minutes

Figure 1-2: Management Tool Configuration

- SSH connections to the CLI can be made on any active interface. Support for each interface must be explicitly enabled under **Security**.
- The login credentials for SSH connections are the same as those defined under **Administrator authentication**. By default, both username and password are set to **admin**.

NOTE

SSH logins always use the local administrator username and password, even if **Administrator authentication** is set to use an external RADIUS server.

1.3 SSH Client Support

The following SSH clients have been tested with the CLI. Others may work as well:

- OpenSSH
- Tectia
- SecureCRT
- Putty

1.4 Entering Strings

When entering a value that contains spaces, you must enclose it in quotation marks. For example, if the command syntax is:

```
ssid <name>
```

you must specify one of the following:

```
ssid ANameWithNoSpaces  
ssid "A name with spaces"
```

1.5 Context Hierarchy

CLI commands are grouped into functional contexts. The following tables show the context hierarchy and the command used to switch from the parent context.

Wi²controller series:

Context hierarchy	Command to switch from parent context
View context	(This is the first context.)
Enable context	enable
Config context	config
WAN IP interface context	interface ip wan
LAN IP interface context	interface ip lan
Internet interface context	interface ethernet port-2
VLAN interface context	interface vlan <id>[-<id2>]
LAN interface context	interface ethernet port-1
VLAN interface context	interface vlan <id>[-<id2>]
PPTP client interface	interface pptp client-default
GRE interface context	interface gre <name>
Virtual AP context	virtual ap <name>
Subscription plan	subscription plan <name>
IPsec policy context	ipsec policy <name>
DHCP server context	dhcp server lan
Syslog destination context	logging destination <name>
RADIUS context	radius-server profile <name>
Access Controller context	access controller
Default Session profile context	session profile default
Session profile context	session profile <name>
RADIUS remote configuration	remote configuration radius
User Profile context	user profile <name>
Keychain context	key chain <name>
Keys context	key <number>

Context hierarchy	Command to switch from parent context
Active Directory Group context	active-directory group <name>
Controlled Network AP context	controlled network (ap group base) [<name>] [<mac>]
Controlled Network context	config
Controlled Mode Wireless interface context	interface wireless (single dual triple) <number>
RADIUS Profile context	radius profile <profile>
Local mesh profile context	local mesh group <group>
Local mesh provisioning profile context	local mesh provisioning group
Provisioning connectivity context	provisioning connectivity
Provisioning discovery context	provisioning discovery
Syslog context	syslog
Controlled Network AP Group context	controlled network (ap group base) [<name>] [<mac>]
Virtual AP Binding context	virtual ap binding <profile>
Controlled Network context	config
Controlled Mode Wireless interface context	interface wireless (single dual triple) <number>
RADIUS Profile context	radius profile <profile>
Local mesh profile context	local mesh group <group>
Local mesh provisioning profile context	local mesh provisioning group
Provisioning connectivity context	provisioning connectivity
Provisioning discovery context	provisioning discovery
Syslog context	syslog
Controlled Network Base Group context	controlled network (ap group base) [<name>] [<mac>]
Controlled Network context	config
Controlled Mode Wireless interface context	interface wireless (single dual triple) <number>

Context hierarchy	Command to switch from parent context
RADIUS Profile context	radius profile <profile>
Local mesh profile context	local mesh group <group>
Local mesh provisioning profile context	local mesh provisioning group
Provisioning connectivity context	provisioning connectivity
Provisioning discovery context	provisioning discovery
Syslog context	syslog

Wi² Controller series:

Context hierarchy	Command to switch from parent context
View context	(This is the first context.)
Enable context	enable
Config context	config
WAN IP interface context	interface ip wan
LAN IP interface context	interface ip lan
Internet interface context	interface ethernet port-2
VLAN interface context	interface vlan <id>[-<id2>]
LAN interface context	interface ethernet port-1
VLAN interface context	interface vlan <id>[-<id2>]
Wireless context	interface wireless <number>
Local mesh context	local mesh profile <name>
VLAN interface context	interface vlan <number>
PPTP client interface	interface pptp client-default
GRE interface context	interface gre <name>
Virtual AP context	virtual ap <name>
IPsec policy context	ipsec policy <name>
DHCP server context	dhcp server lan
Syslog destination context	logging destination <name>
RADIUS context	radius-server profile <name>

Context hierarchy	Command to switch from parent context
IP_QOS context	<code>ip-qos profile <name></code>
Access Controller context	<code>access controller</code>
Default Session profile context	<code>session profile default</code>
Session profile context	<code>session profile <name></code>
RADIUS remote configuration	<code>remote configuration radius</code>
User Profile context	<code>user profile <name></code>
Keychain context	<code>key chain <name></code>
Keys context	<code>key <number></code>

1.6 Sample CLI Session

This sample CLI session shows you how to set the WAN port to use a static IP address, disable NAT, and add an alternate IP address.

```
Wi 2-CTRL-40 V. 5.2
CLI> enable
CLI# config
CLI(config)# interface ip wan
CLI(config-if-ip)# ip address 192.168.66.1/24
CLI(config-if-ip)# ip address mode static
CLI(config-if-ip)# no ip nat
CLI(config-if-ip)# ip address alternate 192.168.23.56
CLI(config-if-ip)# end
CLI(config)# end
CLI# quit
```

1.7 File Transfer

In some cases you need to transfer files (certificates or configuration) to the service controller. Commands that have this capability typically include `<uri>` or `<url>` in their parameter list.



NOTE

When you enter the commands discussed here, the files are transferred immediately.

File transfer can be performed in two ways



To Give the file to the service controller using a ULR

Replace parameter, set this parameters to the location of the file on an ftp or http server. For example:

```
certificate ipsec ca ftp://ftp.example.com/certificate/my-root-certificate.pem
```



To send a file to the service controller

Using SFTP (available with OpenSSH or SSH), authenticate with the CLI credentials. Then send the file to the service controller. For example:

```
sftp Wi2-CTRL-40.mycompany.com
>login: admin
>password: ****
>put my-root-certificate.pem
file transferred (1k)
>quit
```

In the CLI, use the `local://<filename>` parameter in the URL. Replace `<filename>` with the filename you used to transfer using SFTP. For example:

```
CLI(config)# certificate ipsec ca local://my-root-certificate.pem
```




2

Chapter 2 - CLI Commands



2.1 View Context

Context path: View

This is the root of the command tree.

arping

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
arping [ -AbDfhqUV] [ -c <count>] [ -w <deadline>] [ -s <source>]
-I <interface> <destination>
```

Pings a destination on a device interface using ARP packets.

curl

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
curl [parameter] <url>
```

Use the curl command to get/send files to/from the Controller.

Parameters

-a	Specifies append to target file when uploading. FTP only.
-A <string>	Specifies the User-Agent to send to server. HTTP only.
-b <name=string>	Specifies the cookie string or file to read cookies from. HTTP only.
-B	Specifies to use ASCII/text transfer.
-c <file>	Specifies to write all cookies to this file after operation. HTTP only.
-C <offset>	Specifies the absolute resume offset.
-d data <data>	Specifies HTTP POST data. HTTP only.
--data-ascii <data>	Specifies HTTP POST ASCII data. HTTP only.
--data-binary <data>	Specifies HTTP POST binary data. HTTP only.
--data-epsv <data>	Prevents curl from using EPSV. FTP only.
-D <file>	Specifies to write the headers to this file.
--egd-file <file>	Specifies EGD socket path for random data. SSL only.
-E <cert[:passwd]>	Specifies a certificate file and password. HTTPS only.
--cert-type <type>	Specifies the certificate file type. HTTPS only.
--key <key>	Specifies the private key file. HTTPS only.
--key-type <type>	Specifies the private key file type. HTTPS only.
--pass <pass>	Specifies the passphrase for the private key. HTTPS only.
--engine <eng>	Specifies the crypto engine to use. HTTPS only.
--cacert <file>	Specifies the CA certificate to verify peer against. SSL only.
--capath <dir>	Specifies the CA directory to verify peer against. SSL only.

<code>--ciphers <list></code>	Specifies the SSL ciphers to use. SSL only.
<code>--compressed</code>	Specifies to request a compressed response (using deflate).
<code>--compressed</code>	Specifies to request a compressed response (using deflate).
<code>--connect-timeout <sec></code>	Specifies the maximum time allowed for connection.
<code>--create-dirs</code>	Specifies to create the necessary local directory hierarchy.
<code>--crlf</code>	Specifies to convert LF to CRLF in upload.
<code>-f</code>	Specifies to fail silently (no output at all) on errors. HTTP only.
<code>-F <name=content></code>	Specifies HTTP POST data. HTTP only.
<code>-g</code>	Specifies to disable URL sequences and ranges using {} and [].
<code>-G <name=content></code>	Specifies to send the -d data with a HTTP GET. HTTP only.
<code>-h</code>	Displays this help text.
<code>-H <line></code>	Specifies the custom header to pass to the server. HTTP only.
<code>-i</code>	Specifies to include the HTTP-header in the output. HTTP only.
<code>-I</code>	Specifies to fetch document info only.
<code>-j <cert[:passwd]></code>	Specifies to ignore session cookies read from file. HTTP only.
<code>--interface <interface></code>	Specifies the interface to use.
<code>--krb4 <level></code>	Specifies to enable krb4 with specified security level. FTP only.
<code>-k</code>	Specifies to disallow curl to connect to SSL sites without certificates. HTTP only.
<code>-K</code>	Specifies which config file to read.
<code>-l</code>	Specifies to list only names of an FTP directory FTP only.
<code>--limit-rate <rate></code>	Specifies the speed limit for transfers.
<code>-L</code>	Specifies Follow Location: hints. HTTP only.
<code>-m <seconds></code>	Specifies the maximum time allowed for the transfer.
<code>-M</code>	Specifies to display huge help text.
<code>-n</code>	Specifies to read .netrc for user name and password
<code>--netrc-optional</code>	Specifies to use either .netrc or URL; overrides -n
<code>-N</code>	Optional parameter that disables the buffering of the output stream
<code>-o <file></code>	Specifies to write output to <file> instead of stdout.
<code>-O</code>	Specifies to write output to a file named as the remote file.
<code>-p</code>	Specifies to perform non-HTTP services through a HTTP proxy.
<code>-P <address></code>	Specifies to use PORT with address instead of PASV when ftping. FTP only.

<code>-q</code>	When used as the first parameter disables .curlrc
<code>-Q <cmd></code>	Specifies to send QUOTE command to FTP before file transfer. FTP only.
<code>-r <range></code>	Specifies to retrieve a byte range from a HTTP/1.1 or FTP server.
<code>-R</code>	Sets the remote file's time on the local output.
<code>-s</code>	Specifies silent mode. Don't output anything.
<code>-S</code>	Specifies show error. With -s, make curl show errors when they occur.
<code>--stderr <file></code>	Specifies where to redirect stderr. - means stdout.
<code>-t <OPT=val></code>	Sets the telnet option.
<code>--trace <file></code>	Dumps a network/debug trace to the given file.
<code>--trace-ascii <file></code>	Specifies --trace but without the hex output.
<code>-T <file></code>	Specifies to transfer/upload <file> to remote site.
<code>--url <URL></code>	Specifies another way to specify URL to work with.
<code>-ur <user[:pass]></code>	Specifies user and password to use. Overrides -n and --netrc-optional
<code>-U <user[:pass]></code>	Specifies proxy authentication.
<code>-v</code>	Makes the operation more talkative.
<code>-V</code>	Outputs version number then quits.
<code>-w [format]</code>	Specifies what to output after completion.
<code>-x <host[:port]></code>	Specifies to use proxy. (Default port is 1080).
<code>--random-file <file></code>	Specifies the file to use for reading random data from (SSL).
<code>-X <command></code>	Specifies the request command to use.
<code>-y</code>	Specifies the time needed to trig speed-limit abort. Defaults to 30.
<code>-Y</code>	Specifies to stop transfer if below speed-limit for 'speed-time' secs.
<code>-z <time></code>	Includes a time condition to the server. HTTP only.
<code>-Z <num></code>	Sets the maximum number of redirections allowed. HTTP only.
<code>-0</code>	Forces usage of HTTP 1.0. HTTP only.
<code>-1</code>	Forces usage of TLSv1. HTTP only.
<code>-2</code>	Forces usage of SSLv2. HTTP only.
<code>-3</code>	Forces usage of SSLv3. HTTP only.

enable

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

enable

Switches to the enable context.

nslookup

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
nslookup [ -option authentication ] [ <host-to-find> | - [ <server> ] ]
```

Queries DNS servers for information on hosts or domains.

ping

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ping <host> [-c <count>] [-s <length>] [-q]
```

Determines if the specified remote IP address is active.

Parameters

<-c host>	The IP address or DNS name of the host to ping.
<-c count>	Number of pings.
<-s length>	Length of the ping datagram.
<-q>	Quiet mode. No output.

ps

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ps
```

Displays all running processes.

quit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
quit
```

Quits the CLI.

show license

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
show license (EULA | gpl | other)
```

Displays license information.

show logging filtered

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
show logging [filtered]
```

Displays the system log.

top

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
top
```

Displays all running processes.

traceroute

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
traceroute [-n] [-r] [-v] [-m <max_ttl>] [-p <port#>] [-q  
<nqueries>] [-s <src_addr>] [-t <tos>] [-w <wait>] <host> [<data  
size>]
```

Show the hosts that are traversed to reach the specified IP address.

2.2 Enable Context

Context path: View > Enable

This context provides access to various utilities.

reboot device

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

reboot device

Restarts the system.

show certificate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show certificate

Display current certificates.

show certificate binding

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show certificate binding

Display how the certificates are used.

ping

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ping <host> [-c <count>] [-s <length>] [-q]

Determines if the specified remote IP address is active.

Parameters

<-c host>	The IP address or DNS name of the host to ping.
<-c count>	Number of pings.
<-s length>	Length of the ping datagram.
<-q>	Quiet mode. No output.

arping

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

arping [-AbDfhqUV] [-c <count>] [-w <deadline>] [-s <source>]
-I <interface> <destination>

Pings a destination on a device interface using ARP packets.

arp

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
arp [-evn] [-H <type>] [-i if] ?- [<hostname>] arp [-v] [-i if] -d
<hostname> [pub] arp [-v] [-H <type>] [-i if] -s <hostname>
<hw_addr> [temp] arp [-v] [-H <type>] [-i if] -s <hostname>
<hw_addr> [<netmask> <nm>] <pub> arp [-v] [-H <type>] [-i if] -Ds
<hostname> ifa [<netmask> <nm>] <pub>
```

Displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
end
```

Switches to parent context.

quit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
quit
```

Exit the enable context.

rcapture

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
rcapture [<a>] [<b>] [<c>] [<d>] [<e>] [<f>] [<g>] [<h>]
```

Sends port capture to an FTP server.

Refer to Linux documentation for a complete description of this command and its options.

show arp

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
show arp
```

Show the ARP table.

show bridge

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
show bridge
```

Show bridge information.

show bridge forwarding

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
show bridge forwarding
```

Show bridge forwarding information.

show dns cache

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show dns cache [<serial>]

Show DNS cache entries. Specify a serial number to display detailed information.

show interfaces

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show interfaces

Show networking interfaces.

show ip route

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show ip route

Show all IP routes.

show system info

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show system info

Show basic system information.

show ip dhcp database

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show ip dhcp database

Show the DHCP server lease database.

show dot11 associations

Supported on:

show dot11 associations

Show all current wireless associations.

show dot11 statistics client-traffic

Supported on:

show dot11 statistics client-traffic

Show current client matrix statistics.

show local mesh

Supported on:

show local mesh

Show current local mesh interfaces.

show wireless neighborhood

Supported on:

show wireless neighborhood

Show all access points detected nearby.

show wireless rogue-ap

Supported on:

show wireless rogue-ap

Show all rogue access points detected nearby.

show satellites

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show satellites [*<deviceid>*]

Show current satellites of this access point.

show client log

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show client log [*<macaddr>*]

Display client station log. Enter the MAC address to display more details for a specific client station.

show radius statistics

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show radius statistics

Show RADIUS server statistics.

show radius users

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show radius users [*<filter>*]

Show users that are using RADIUS accounting.

show users

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show users [*<filter>*]

Show all users of this service controller.

show discrete pin

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show discrete pin

Display the state of the discrete pin.

config

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

config

Switches to the config context.

show all config

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show all config

Print all configuration that applies to this device.

controlled network

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

controlled network (ap | group | base) [*<name>*] [*<mac>*]

Create/use the controlled network entity.

show controlled network config

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show controlled network config

Print configuration for all Controlled Network entities.

2.3 Config Context

Context path: View > Enable > Config

This is the root context for all configuration commands.

certificate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

certificate (authority | local) <uri> <certname> [<password>]

Add a new certificate to the store, using the friendly name.

certificate binding

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

certificate binding (web-management | html-auth | soap | eap)
<certname>

Assign a certificate to a service.

no certificate binding (web-management | html-auth | soap | eap)
<certname>

Unassign a certificate from a service.

certificate revocation

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

certificate revocation <uri> <certname>

Add a Certificate Revocation List to an existing authority certificate.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

factory settings

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

factory settings

Resets the system configuration to factory default settings.

interface ethernet

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

interface ethernet (port-1|port-2)

Switches to the specified Ethernet interface context.

reboot device

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

reboot device

Restarts the system.

show certificate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show certificate

Display current certificates.

show certificate binding

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show certificate binding

Display how the certificates are used.

show config factory

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show config [factory]

Generates a list of CLI commands that can be used to define the currently loaded configuration.

username

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

username <user> <password>

Changes the current administrator username and password.

Parameters

<user>

New administrator username.

<password>

New administrator password.

interface ip

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

interface ip (lan | wan)

Switches to the specified IP interface context.

interface wireless

Supported on:

interface wireless <interface number>

Switches to the specified wireless interface context.

```
no subscription plan <name>
```

Delete a subscription plan.

ipsec policy

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ipsec policy <name>
```

Switches to the specified IPsec policy or creates a new IPsec policy with the specified name.

admin authentication local fallback

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
admin authentication local fallback
```

Allow administrators to login via the local account if the RADIUS server is unreachable.

```
no admin authentication local fallback
```

Do not allow administrators to login via the local account if the RADIUS server is unreachable.

admin authentication radius

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
admin authentication radius <name>
```

Sets the RADIUS profile to use for authentication of administrator logins.

```
no admin authentication radius
```

Sets the authentication of administrator logins to occur using the specified RADIUS profile.

Parameters

<name> RADIUS profile name.

clock summer-time

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
clock summer-time
```

Enables support for daylight savings time.

```
no clock summer-time
```

Disables support for daylight savings time.

clock timezone

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
clock timezone <gmtdiff>
```

Sets the time zone the Controller is operating in.

Parameters

`<gmtdiff>`

Offset from GMT as follows: +-HOUR:MIN. For example, Eastern Standard time is -5:00.

ip http port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip http port <number>`

Sets the port number to use for HTTP access to the Controller.

Parameters

`<number>`

Port number. Range: 1 - 65535.

Description

HTTP connections made to this port are met with a warning and the browser is redirected to the secure web server port. By default, this parameter is set to port 80.

ip https port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip https port <number>`

Sets the port number used for HTTPS access to the Controller.

Parameters

`<number>`

Port number. Range: 1 - 65535.

ntp protocol

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ntp protocol (ntp | sntp)`

Sets the network time protocol to use.

ntp server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ntp server`

Enable this option to have the Controller periodically contact a network time server to update its internal clock.

`no ntp server`

Disables the use of a network time server.

snmp-server trap certificate-expired

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`snmp-server trap certificate-expired`

Send a trap when the SSL certificate has expired. A trap is sent every 12 hours.

```
no snmp-server trap certificate-expired
```

Do not send a trap when the SSL certificate has expired.

snmp-server trap certificate-expires-soon

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap certificate-expires-soon
```

Send a trap when the SSL certificate is about to expire. A trap is sent every 12 hours starting 15 days before the certificate expires.

```
no snmp-server trap certificate-expires-soon
```

Do not send a trap when the SSL certificate is about to expire.

snmp-server trap web-fail

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap web-fail
```

Send a trap each time an administrator login is refused.

```
no snmp-server trap web-fail
```

Do not send a trap each time an administrator login is refused.

snmp-server trap web-login

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap web-login
```

Send a trap each time an administrator login is accepted.

```
no snmp-server trap web-login
```

Do not send a trap each time an administrator login is accepted.

snmp-server trap web-logout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap web-logout
```

Send a trap each time an administrator logs out.

```
no snmp-server trap web-logout
```

Do not send a trap each time an administrator logs out.

web admin kickout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
web admin kickout
```

Enables a new administrator login to terminate an existing administrator session.

```
no web admin kickout
```

Stops a new administrator from logging in until an existing administrator logs out.

web allow

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`web allow <ip address>/<mask>`

Adds an address to the list of hosts that can access the management tool.

`no web allow <ip address>/<mask>`

Removes the specified address from the list of hosts that can access the management tool.

Parameters

`<address>`

IP address.

`</mask>`

Subnet mask in CIDR format. Specifies the number of bits in the mask.

world-mode dot11 country code

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`world-mode dot11 country code <code>`

Specifies the country the Controller is operating in.

Parameters

`<code>`

An ISO3166 three-letter country code.

web access internet-port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`web access internet-port`

Enables access to the management tool via the Internet port.

`no web access internet-port`

Blocks access to the management tool via the Internet port.

web access lan-port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`web access lan-port`

Enables access to the management tool via the LAN port.

`no web access lan-port`

Blocks access to the management tool via the LAN port.

web access wireless

Supported on:

`web access wireless`

Enables access to the management tool via the wireless port.

`no web access wireless`

Blocks access to the management tool via the wireless port.

web access interface vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

web access interface vlan <name>

Enables access to the management tool via the specified VLAN.

no web access interface vlan <name>

Removes access to the management tool for the specified VLAN.

web access interface gre

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

web access interface gre <name>

Enables access to the management tool via the specified GRE tunnel.

no web access interface gre <name>

Disables access to the management tool via the specified GRE tunnel.

web access local mesh

Supported on:

web access local mesh <name>

Enables access to the management tool via the specified local mesh.

no web access local mesh <name>

Disables access to the management tool via the specified local mesh.

web access lan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

web access lan

Enables access to the management tool via the LAN port.

no web access lan

Blocks access to the management tool via the LAN port.

web access vpn

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

web access vpn

Enables access to the management tool via a VPN connection.

no web access vpn

Blocks access to the management tool via a VPN connection.

dhcp mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp mode (server | relay | none)

Sets whether the Controller operates as a DHCP server or DHCP relay agent.

dhcp server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp server lan

Switches to the DHCP server context.

dhcp server default domain name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp server default domain name <domain>

Sets the DHCP server domain name.

dhcp server default lease period

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp server default lease period <number>

Sets the default lease time for the DHCP server.

dhcp server default permanent lease period

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp server default permanent lease period <number>

Sets the permanent lease time for the DHCP server.

dhcp server logout html user

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp server logout html user

Logout HTML user upon discover request.

no dhcp server logout html user

Do not logout HTML user upon discover request.

dhcp relay

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp relay <primary-ip-address> <[secondary-ip-address]>

Sets the primary and secondary DHCP server for the relay.

dhcp relay circuit id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp relay circuit id <string>

Sets the Option 82 circuit ID.

no dhcp relay circuit id

Clears the Option 82 circuit ID.

dhcp relay remote id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp relay remote id *<string>*

Sets the Option 82 remote ID.

no dhcp relay remote id

Clears the Option 82 remote ID.

clock

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

clock *<time>* *<date>*

Sets the system time and date.

Parameters

<time>

Time as hh:mm:ss. For example: 15:44:00.

<date>

Date as dd Month yyyy. For example: 17 Oct 2004

ntp server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ntp server *<index>**<host>*

Adds a network time server.

Parameters

<index>

Index of the time server in the list. Up to 20 time servers are supported. Time servers are checked in the order that they appear in the list.

<host>

DNS name or IP address of the time server.

ntp server failure trap

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ntp server failure trap

Send a trap each time a time server synchronization failed.

no ntp server failure trap

Do not send a trap each time a time server synchronization failed.

config-update automatic

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

config-update automatic

Enables scheduled configuration restore or backup.

no config-update automatic

Disables scheduled configuration restore or backup.

The Controller can automatically download the configuration file from a local or remote URL (restore). It is also possible to upload the current configuration to a given URL (backup). These operations can be done at preset times.

config-update operation

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`config-update operation (restore | backup)`

Sets the type of operation that will take place at the preset time.

config-update time

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`config-update time <time>`

Sets the time of day when the scheduled configuration operation (backup or restore) will take place.

Parameters

`<time>`

Time as hh:mm:ss. For example: 15:44:00.

config-update uri

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`config-update uri <uri>`

Sets the URI where the Controller will download or upload the configuration file.

`no config-update uri`

Clears the configuration file URI.

config-update weekday

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`config-update weekday (everyday | monday | tuesday | wednesday | thursday | friday | saturday | sunday)`

Sets the day when the scheduled configuration operation (backup or restore) will take place.

snmp-server trap config-change

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`snmp-server trap config-change`

Send a trap whenever the configuration is changed.

`no snmp-server trap config-change`

Do not send this trap.

snmp-server trap config-update

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server trap config-update

Send a trap whenever the firmware is updated.

no snmp-server trap config-update

Do not send this trap.

logging destination

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

logging destination <name>

Creates a new remote destination for syslog.

no logging destination <name>

Deletes the specified syslog destination.

Parameters

<name>

Name of syslog destination. Use the name "local" to edit your local log file settings. Any other name will edit/create a remote log destination.

snmp-server trap syslog-severity

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server trap syslog-severity

Set the severity level of syslog messages that will trigger a trap.

no snmp-server trap syslog-severity

Do not send this trap.

snmp-server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server

Enables the SNMP agent.

no snmp-server

Disables the SNMP agent.

snmp-server access port-1

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server access port-1

Enables SNMP access on the downstream port.

no snmp-server access port-1

Blocks SNMP access on the downstream port.

snmp-server allow

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server allow <ip address>/<mask>
```

Adds a host to the list of IP address from which access to the SNMP interface is permitted.

```
no snmp-server allow <ip address>/<mask>
```

Removes a host from the list of IP address from which access to the SNMP interface is permitted.

Parameters

<address>

IP address.

</mask>

Subnet mask in CIDR format. Specifies the number of bits in the mask.

snmp-server chassis-id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server chassis-id <name>
```

Specifies a name to identify the Controller. By default, this is set to the serial number of the Controller.

```
no snmp-server chassis-id
```

Deletes the system name.

snmp-server contact

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server contact <email>
```

Specifies contact information.

```
no snmp-server contact
```

Deletes contact information.

Parameters

<email>

Email address.

snmp-server heartbeat period

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server heartbeat period <seconds>
```

Sets the interval between sending heartbeat traps.

Parameters

<seconds>

Heartbeat interval in seconds.

snmp-server trap community

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server trap community <str>

Sets the password required by the remote host that will receive the trap.

no snmp-server trap community

Deletes the password required by the remote host that will receive the trap.

snmp-server trap destination

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server trap destination <host> <[port number]>

Add a new trap destination.

no snmp-server trap destination <host> [<port>]

Deletes the specified trap destination.

Parameters

<host>

Sets the IP address or domain name of the host that the Controller will send traps to.

<[port number]>

SNMP port number. Range 1 - 65535. By default port 162 is used

snmp-server trap heartbeat

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server trap heartbeat

Enables sending of heartbeat traps at regular intervals.

no snmp-server trap heartbeat

Disables sending of heartbeat traps at regular intervals.

snmp-server trap link-state

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server trap link-state

Send a trap when the link state changes on any interface.

no snmp-server trap link-state

Do not send this trap.

snmp-server trap snmp-authentication

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server trap snmp-authentication

Send a trap each time an SNMP request fails to supply the correct community name.

snmp-server version

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server version (1 | 2c)
```

Sets the SNMP version.

snmp-server access interface vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server access interface vlan <name>
```

Enables access to SNMP via the specified VLAN.

```
no snmp-server access interface vlan <name>
```

Disables access to SNMP via the specified VLAN.

Parameters

<name> Specifies the name of the VLAN.

snmp-server access local mesh

Supported on:

```
snmp-server access local mesh <profile>
```

Enables access to SNMP via the specified local mesh.

```
no snmp-server access local mesh <profile>
```

Enables access to SNMP via the specified local mesh.

snmp-server access interface gre

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server access interface gre <name>
```

Enables access to SNMP via the specified GRE tunnel.

```
no snmp-server access interface gre <name>
```

Removes access to SNMP via the specified GRE tunnel.

snmp-server access wireless

Supported on:

```
snmp-server access wireless
```

Enables SNMP access on the wireless port.

```
no snmp-server access wireless
```

Blocks SNMP access on the wireless port.

snmp-server access port-2

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server access port-2
```

Enables SNMP access on the upstream port.

```
no snmp-server access port-2
```

Blocks SNMP access on the upstream port.

snmp-server access lan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server access lan
```

Enables access to the management tool via the LAN port.

```
no snmp-server access lan
```

Blocks access to the management tool via the LAN port.

snmp-server access vpn

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server access vpn
```

Enables access to the management tool via a VPN connection.

```
no snmp-server access vpn
```

Blocks access to the management tool via a VPN connection.

snmp-server trap new-satellite-detected

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap new-satellite-detected
```

Send a trap when a new satellite is detected.

```
no snmp-server trap new-satellite-detected
```

Do not send a trap when a new satellite is detected.

snmp-server trap satellite-unreachable

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap satellite-unreachable
```

Send a trap when a satellite cannot be reached.

```
no snmp-server trap satellite-unreachable
```

Ignore unreachable satellites.

soap-server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server
```

Enables the SOAP server.

```
no soap-server
```

Disables the SOAP server.

soap-server access interface vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server access interface vlan <name>
```

Enables access to SOAP via this VLAN.

```
no soap-server access interface vlan <name>
```

Disables access to SOAP via this VLAN.

soap-server access port-1

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server access port-1
```

Enables SOAP access on the downstream port.

```
no soap-server access port-1
```

Blocks SOAP access on the downstream port.

soap-server access port-2

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server access port-2
```

Enables SOAP access on the upstream port.

```
no soap-server access port-2
```

Blocks SOAP access on the upstream port.

soap-server allow

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server allow <ip address>/<mask>
```

Adds a host to the list of IP address from which access to the SOAP interface is permitted.

```
no soap-server allow <ip address>/<mask>
```

Removes a host from the list of IP address from which access to the SOAP interface is permitted.

Parameters

<address>

IP address.

</mask>

Subnet mask in CIDR format. Specifies the number of bits in the mask.

soap-server http authentication

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server http authentication
```

Enable the SOAP server HTTP authentication.

```
no soap-server http authentication
```

Disable the SOAP server HTTP authentication.

soap-server http authentication password

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server http authentication password
```

Set the SOAP server HTTP authentication password.

soap-server http authentication username

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server http authentication username
```

Set the SOAP server HTTP authentication username.

soap-server port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server port <port number>
```

Sets the port the Controller will use to respond to SOAP requests.

Parameters

<port number> **SOAP port number. Range 1 - 65535.**

soap-server ssl

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server ssl
```

SSL enabled for SOAP server.

```
no soap-server ssl
```

SSL disabled for SOAP server.

soap-server ssl with client certificate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server ssl with client certificate
```

Enable the use of client certificate with SSL for SOAP server.

```
no soap-server ssl with client certificate
```

Disable the use of client certificate with SSL for SOAP server.

soap-server access interface gre

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server access interface gre <name>
```

Enables access to SOAP via the specified GRE tunnel.

```
no soap-server access interface gre <name>
```

Removes access to SOAP via the specified GRE tunnel.

soap-server access wireless

Supported on:

```
soap-server access wireless
```

Enables SOAP access on the wireless port.

```
no soap-server access wireless
```

Blocks SOAP access on the wireless port.

soap-server access local mesh

Supported on:

```
soap-server access local mesh <profile>
```

Enables access to the management tool via the specified local mesh.

```
no soap-server access local mesh <profile>
```

Disables access to the management tool via the specified local mesh.

soap-server access lan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server access lan
```

Enables access to the management tool via the LAN port.

```
no soap-server access lan
```

Blocks access to the management tool via the LAN port.

soap-server access vpn

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
soap-server access vpn
```

Enables access to the management tool via a VPN connection.

```
no soap-server access vpn
```

Blocks access to the management tool via a VPN connection.

snmp-server trap low-snr

Supported on:

```
snmp-server trap low-snr
```

Send a trap when the average signal to noise ratio on a VAP (virtual network) exceeds a specified level.

```
no snmp-server trap low-snr
```

Do not send this trap.

snmp-server trap low-snr interval

Supported on:

```
snmp-server trap low-snr interval <number>
```

Sets the interval at which the average SNR level is checked for each VAP (virtual network).

snmp-server trap low-snr level

Supported on:

```
snmp-server trap low-snr level <number>
```

Sets the SNR level that will trigger a trap.

snmp-server trap new-association

Supported on:

```
snmp-server trap new-association
```

Send trap on when a new wireless client station associates with any VAP (virtual network).

```
no snmp-server trap new-association
```

Do not send this trap.

snmp-server trap new-association interval

Supported on:

```
snmp-server trap new-association interval <number>
```

Interval, in minutes, between notifications.

snmp-server trap vpn-connection

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap vpn-connection
```

Send a trap when a customer establishes a VPN connection with the Controller.

```
no snmp-server trap vpn-connection
```

Do not send this trap.

snmp-server trap wireless-association-fail

Supported on:

```
snmp-server trap wireless-association-fail
```

Send a trap when a wireless client station fails to associate with the Controller.

```
no snmp-server trap wireless-association-fail
```

Do not send this trap.

snmp-server trap wireless-association-success

Supported on:

```
snmp-server trap wireless-association-success
```

Send a trap when a wireless client station successfully associates with the Controller.

```
no snmp-server trap wireless-association-success
```

Do not send this trap.

snmp-server trap wireless-authentication-fail

Supported on:

```
snmp-server trap wireless-authentication-fail
```

Send a trap when a wireless client station fails to authenticate.

```
no snmp-server trap wireless-authentication-fail
```

Do not send this trap.

snmp-server trap wireless-authentication-success

Supported on:

```
snmp-server trap wireless-authentication-success
```

Send a trap when a wireless client station is successfully associated.

```
no snmp-server trap wireless-authentication-success
```

Do not send this trap.

snmp-server trap wireless-deauthentication-fail

Supported on:

```
snmp-server trap wireless-deauthentication-fail
```

Send a trap when a wireless client station fails to deauthenticate from the Controller.

```
no snmp-server trap wireless-deauthentication-fail
```

Do not send this trap.

snmp-server trap wireless-deauthentication-success

Supported on:

```
snmp-server trap wireless-deauthentication-success
```

Send a trap when a wireless client station deauthenticates from the Controller.

```
no snmp-server trap wireless-deauthentication-success
```

Do not send this trap.

snmp-server trap wireless-disassociation-fail

Supported on:

snmp-server trap wireless-disassociation-fail

Send a trap when a wireless client station fails to disassociate from the Controller.

no snmp-server trap wireless-disassociation-fail

Do not send this trap.

snmp-server trap wireless-disassociation-success

Supported on:

snmp-server trap wireless-disassociation-success

Send a trap when a wireless client station disassociates from the Controller.

no snmp-server trap wireless-disassociation-success

Do not send this trap.

snmp-server trap wireless-reassociation-fail

Supported on:

snmp-server trap wireless-reassociation-fail

Send a trap when a wireless client station fails to reassociate with the Controller.

no snmp-server trap wireless-reassociation-fail

Do not send this trap.

snmp-server trap wireless-reassociation-success

Supported on:

snmp-server trap wireless-reassociation-success

Send a trap when a wireless client station reassociates with the Controller.

no snmp-server trap wireless-reassociation-success

Do not send this trap.

snmp-server trap syslog-matches

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server trap syslog-matches

Send a trap when syslog messages matches a specified regular expression.

no snmp-server trap syslog-matches

Do not send this trap.

snmp-server trap syslog-matches regex

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap syslog-matches regex <regex>
```

Sets the regular expression used to match the syslog messages.

snmp-server trap syslog-severity level

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap syslog-severity level (debug | info | notice |  
warning | error | critical | alert | emergency)
```

Set the severity level of syslog messages that will trigger a trap.

snmp-server trap network-trace

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
snmp-server trap network-trace
```

Send a trap when a network trace is started or stopped.

```
no snmp-server trap network-trace
```

Do not send this trap.

firmware-update automatic

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
firmware-update automatic
```

Enables scheduled firmware upgrades.

```
no firmware-update automatic
```

Disables scheduled firmware upgrade.

The Controller can automatically retrieve and install firmware from a local or remote URL at preset times. By placing Controller firmware on a web or ftp server, you can automate the update process for multiple units.

When the update process is triggered the Controller retrieves the first 2K of the firmware file to determine if it is different from the active version. If different, the entire firmware file is then downloaded and installed.

(Different means older or newer. This enables you to return to a previous firmware version if required).

Configuration settings are preserved during the update unless stated otherwise in the release notes for the firmware. However, all active connections will be terminated. Customers will have to log in again after the Controller restarts

firmware-update start

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

firmware-update start

Upload the firmware based on a specified URI. This URI can be set with the command: firmware-update uri.

firmware-update time

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

firmware-update time *<time>*

Sets the time of day the scheduled firmware upgrade will take place.

Parameters

<time> Time as hh:mm:ss. For example: 15:44:00.

firmware-update uri

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

firmware-update uri *<uri>*

Sets the URI where the Controller will retrieve new firmware.

no firmware-update uri

Clears the firmware URI.

firmware-update weekday

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

firmware-update weekday (everyday | monday | tuesday | wednesday | thursday | friday | saturday | sunday)

Sets the day when the scheduled firmware upgrade will take place.

snmp-server trap firmware-update

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snmp-server trap firmware-update

Send a trap on firmware update.

no snmp-server trap firmware-update

Do not send a trap on firmware update.

ip name-server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip name-server *<primary>* [*<secondary>*]

Sets the primary and secondary DNS servers overriding dynamically assigned ones.

Parameters

<primary> IP address of the primary DNS server.

<secondary>

IP address of the secondary DNS server.

ip name-server cache

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip name-server cache`

Enables the DNS cache.

`no ip name-server cache`

Disables the DNS cache.

Once a host name has been successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, as the remote DNS server now does not have to be queried for subsequent requests for this host.

The entry stays in the cache until:

- **an error occurs when connecting to the remote host**
 - **the time to live (TTL) of the DNS request expires**
 - **the Controller is restarted.**
-

ip name-server dynamic

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip name-server dynamic`

Enables dynamic assignment of DNS servers.

`no ip name-server dynamic`

Disables dynamic DNS assignment.

ip name-server switch-on-servfail

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip name-server switch-on-servfail`

Switch to next server when server failure is received.

`no ip name-server switch-on-servfail`

Do not switch to next server when server failure is received.

ip name-server switch-over

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip name-server switch-over`

Switch over to primary when active.

`no ip name-server switch-over`

Do not switch over to primary when active.

ip name-server logout-host-name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ip name-server logout-host-name <host>
```

Sets the logout host name.

ip name-server logout-ip-address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ip name-server logout-ip-address <ip address>
```

Sets the logout IP address.

snmp-server trap unauthorized-ap

Supported on:

```
snmp-server trap unauthorized-ap
```

Send a trap when a rogue access point is detected.

```
no snmp-server trap unauthorized-ap
```

Do not send this trap.

snmp-server trap unauthorized-ap interval

Supported on:

```
snmp-server trap unauthorized-ap interval <number>
```

If set to 0, then traps are only sent when a rogue access point is detected. If set to 0, the entire list of rogue access points is sent each time the interval expires.

wireless-scan

Supported on:

```
wireless-scan
```

Enables wireless neighborhood scanning.

```
no wireless-scan
```

Disables wireless neighborhood scanning.

wireless-scan period

Supported on:

```
wireless-scan period <seconds>
```

Specifies the interval between wireless neighborhood scans.

Parameters

<seconds>

Scanning interval. Range: 10 - 600 seconds.

wireless-scan url

Supported on:

```
wireless-scan url <location>
```

Sets the URL of the file that contains a list of all authorized access points.

```
no wireless-scan url
```

Deletes the URL of the file that contains a list of all authorized access points.

The format of this file is XML. Each entry in the file is composed of two items: MAC address and SSID. Each entry should appear on a new line.

For example:

```
00:03:52:07:f5:11 "AP_1"
```

```
00:03:52:07:f5:23 "AP_2"
```

```
00:03:52:07:f5:12 "AP_3"
```

access controller shared secret

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
access controller shared secret <secret>
```

Sets the shared secret used to communicate with the service controller.

```
no access controller shared secret
```

Sets the shared secret used to communicate with the access controller.

The service controller will only accept authentication/location-aware information from Alvarion satellites that have a matching shared secret to its own.

radius-server profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
radius-server profile <name>
```

Creates a new RADIUS profile or switches to the RADIUS context with the specified profile name.

```
no radius-server profile <name>
```

Deletes the specified RADIUS profile.

ip-qos profile

Supported on:

```
ip-qos profile <name>
```

Creates a new IP QoS profile or switches to the IP QoS context with the specified profile name.

```
no ip-qos profile <name>
```

Deletes the specified IP QoS profile.

access controller

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access controller

Switches to the access controller context.

certificate ipsec ca

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

certificate ipsec ca *<uri>*

Loads a new CA certificate from the specified URI.

The URI can be local:

- local://FILENAME

or remote

- ftp://host/path
-

certificate ipsec local

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

certificate ipsec local *<uri>* *<password>*

Loads a new local certificate from the specified URI.

no certificate ipsec local

Removes the local certificate.

The URI can be local:

- local://FILENAME

or remote

- ftp://host/path
-

certificate ipsec revocation

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

certificate ipsec revocation *<uri>*

Loads a new CRL file from the specified URI.

The URI can be local:

- local://FILENAME

or remote

- ftp://host/path
-

certificate ssl

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

certificate ssl *<uri>* *<password>*

Loads a new SSL certificate using the URI.

session profile default

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

session profile default

Switches to the session profile context.

session profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

session profile <name>

Switches to the session profile context.

no session profile <name>

Remove a session profile.

show session profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show session profile

Display all session profiles.

remote configuration

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

remote configuration (radius)

Switches to the RADIUS remote configuration context.

dot11 igmp snooping-helper

Supported on:

dot11 igmp snooping-helper

Enables IGMP snooping helpers which ensure that the Controller correctly delivers multicast packets to roaming client stations that are part of a multicast group.

no dot11 igmp snooping-helper

Disable IGMP snooping helpers.

discovery protocol

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

discovery protocol

Enables broadcast of Alvarion device information for interoperability with CDP-enabled networking hardware.

no discovery protocol

Disable broadcast of Alvarion device information.

discovery protocol device-id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

discovery protocol device-id <name>

Overwrite the device-id field of information packets (the Controller serial number is not used).

no discovery protocol device-id

Do not overwrite the device-id field of information packets (use the Controller serial number).

service controller ap authentication credentials

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller ap authentication credentials <username>
<password>

When the RADIUS authentication source is selected, this option specifies the RADIUS username and password assigned to the Controller.

no service controller ap authentication credentials

Clears the RADIUS username/password.

service controller ap authentication enable

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller ap authentication enable

Enables authentication of discovered controlled APs.

no service controller ap authentication enable

Disables AP authentication.

service controller ap authentication file

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller ap authentication file <name>

Sets the file to use for authentication of controlled access points. This must be an ASCII file with one or more MAC addresses in it. Each address must appear on a separate line.

service controller ap authentication radius-server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller ap authentication radius-server <name>

Sets the RADIUS profile to use for authentication of controlled access points.

service controller ap authentication refresh-rate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller ap authentication refresh-rate <number>

Specifies the interval at which the Controller retrieves authentication list entries from the selected authentication source(s).

service controller ap authentication source file

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller ap authentication source file

Enables the use of a file authentication source.

no service controller ap authentication source file

Disables the use of a file authentication source.

service controller ap authentication source local

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller ap authentication source local

Enables the use of local authentication source.

no service controller ap authentication source local

Disables the use of local authentication source.

service controller ap authentication source radius

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller ap authentication source radius

Enables the use of RADIUS authentication source.

no service controller ap authentication source radius

Disables the use of RADIUS authentication source.

service controller discovery

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller discovery

Enable service controller discovery.

no service controller discovery

Disable service controller discovery.

service controller primary

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

service controller primary

Become the Primary service controller.

```
no service controller primary
```

Become a secondary service controller.

service controller primary ip addr

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
service controller primary ip addr <ip address>
```

Configure a static ip address for the primary service controller.

service controller provisioning

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
service controller provisioning
```

Enable the Wi² AP provisioning system.

```
no service controller provisioning
```

Disable the Wi² AP provisioning system.

bridge priority

Supported on:

```
bridge priority <number>
```

Sets the bridge priority for the spanning tree.

The spanning tree uses the bridge ID to elect the root bridge and the designated bridges. The bridge ID is built with the MAC address of the bridge and the bridge priority. The first 2 most significant bytes are the bridge priority and the next 6 bytes are the MAC address. To control which bridge will become the root bridge, you can configure the bridge priority parameter on the bridges. The root will be the bridge with the lowest bridge ID. The Bridge priority has a valid range of 0 to 0xFFFF. The default value is the middle value: 0x8000.

bridge protocol ieee

Supported on:

```
bridge protocol ieee
```

Enable the bridge spanning tree protocol to prevent undesirable loops from occurring in the network that may result in decreased throughput.

```
no bridge protocol ieee
```

Disable the bridge spanning tree protocol.

bandwidth control internet-port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
bandwidth control internet-port
```

Enables bandwidth control on the Internet port.

```
no bandwidth control internet-port
```

Disables bandwidth control on the Internet port.

bandwidth control internet-port high

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
bandwidth control internet-port high <min-tx-%> <min-rx-%>
<max-tx-%> <max-rx-%>
```

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as High.

bandwidth control internet-port low

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
bandwidth control internet-port low <min-tx-%> <min-rx-%>
<max-tx-%> <max-rx-%>
```

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Low.

bandwidth control internet-port max-rate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
bandwidth control internet-port max-rate<transmit><receive>
```

Sets the maximum transmit and receive rates on the Internet port in kbps.

These settings enable you to limit the total incoming or outgoing data rate on the Internet port. If traffic exceeds the rate you set for short bursts, it is buffered. Long overages will result in data being dropped. To utilize the full available bandwidth, the transmit and receive limits should be set to match the incoming and outgoing data rates on the Internet port.

Parameters

<code><transmit></code>	Sets the maximum transmit rate in kbps.
<code><receive></code>	Sets the maximum receive rate in kbps.

About bandwidth control

Bandwidth rates for each level are defined by taking a percentage of the maximum transmit and receive rates defined for the Internet port. Each bandwidth level has four rate settings:

- **Transmit rate - guaranteed minimum:** This is the minimum amount of bandwidth that will be assigned to a level as soon as outgoing traffic is present on the level.
- **Transmit rate - maximum:** This is the maximum amount of outgoing bandwidth that can be consumed by the level. Traffic in excess will be buffered for short bursts, and dropped for sustained overages.
- **Receive rate - guaranteed minimum:** This is the minimum amount of bandwidth that will be assigned to a level as soon as incoming traffic is present on the level.

- **Receive rate - maximum:** This is the maximum amount of incoming bandwidth that can be consumed by the level. Traffic in excess will be buffered for short bursts, and dropped for sustained overages.

Bandwidth levels are arranged in order of priority from Very High to Low. Priority determines how free bandwidth is allocated once the minimum rate has been met for each level. Free bandwidth is always assigned to the higher priority levels first.

Assigning traffic to bandwidth levels

- Customer traffic is assigned to a bandwidth level on a per-VAP (virtual network) basis.
- Management traffic (RADIUS, SNMP, management tool admin sessions) is assigned to bandwidth level Very High and cannot be changed.
- All traffic assigned to a particular bandwidth level shares the allocated bandwidth for that level.

bandwidth control internet-port normal

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
bandwidth control internet-port normal <min-tx-%> <min-rx-%>
<max-tx-%> <max-rx-%>
```

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Normal.

bandwidth control internet-port very-high

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
bandwidth control internet-port very-high <min-tx-%> <min-rx-%>
<max-tx-%> <max-rx-%>
```

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Very High.

ip route gateway

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ip route gateway<destination>/<mask> <gateway> <[metric]>
```

Adds a static route.

```
no ip route gateway <destination>/<mask> <gateway> <[metric]>
```

Removes the specified static route.

Parameters

<destination>

Traffic addressed to this IP address will be routed.

<mask>

Indicates the number of bits in the destination address that is checked for a match.

<gateway>

Indicates the IP address of the gateway the Controller will forward routed traffic to. The gateway address must be on the same subnet as one of the available interfaces (Internet port or LAN port).

`<metric>` Indicates the priority of a route. If two routes exist for a destination address then the Controller chooses the one with the lower metric.

firmware distribution

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

firmware distribution (start | stop)

Starts the firmware distribution.

firmware distribution default username

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

firmware distribution default username `<username>` `<password>`

Specify the default administrator username and password to use for firmware distribution.

The default username and password are used for satellites that do not have a username and password specified in the distribution list.

firmware distribution load cim

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

firmware distribution load cim `<uri>`

Loads the distribution firmware file (*.cim) from the specified URI into the cache.

firmware distribution load list

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

firmware distribution load list `<uri>`

Loads the distribution list from the specified URI.

The distribution list defines the set of access points that the firmware will be installed on. The list is in XML format, with each entry composed of four fields:

- **Serial number:** The serial number of the target access point.
- **IP address:** The IP address of the target access point.
- **Username:** The administrator username on the target access point.
- **Password:** The administrator password on the target access point.

The serial number and IP address are mandatory. The username and password are optional. If all your satellites have the same username and password, you can leave the username and password for every entry blank and instead specify them with the *firmware distribution default username* command.

firewall mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

firewall mode (high|low|none)

Sets the firewall mode.

Parameters

high	Permits all outgoing traffic. Blocks all externally initiated connections.
low	Permits all incoming and outgoing traffic, except for NetBIOS traffic. Use this option if you require active FTP sessions.
none	Disables the firewall.

show user profiles

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show user profiles [<pattern>]

Display current local users.

show user profiles details

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show user profiles details <name>

Display detailed information about one user.

user profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

user profile <name>

Adds or edits the specified username in the local user list.

no user profile <name>

Removes the specified username from the local user list.

renew user profile subscription

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

renew user profile subscription [<username>]

Renew a user with its subscription plan.

dot1x reauth

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot1x reauth

Enable this option to force 802.1X client stations to reauthenticate.

no dot1x reauth

Disables 802.1X reauthentication.

add wireless ip-qos profile

Supported on:

```
add wireless ip-qos profile <name>
```

Adds the specified profile to the list of IP QoS profiles in effect for the wireless links.

<profile-name> **Name of an existing IP QoS profile.**

delete wireless ip-qos profile all

Supported on:

```
delete wireless ip-qos profile all
```

Clears the list of IP QoS profiles currently in effect for the wireless links.

delete wireless ip-qos profile

Supported on:

```
delete wireless ip-qos profile <name>
```

Removes the specified profile from the list of IP QoS profiles in effect for the wireless links.

<profile-name> **Name of an existing IP QoS profile currently in the profile list for the wireless links.**

wireless link qos

Supported on:

```
wireless link qos (disabled | 802.1p | wme | very-high | high | normal | low | tos | diffsrv)
```

Sets the wireless link QoS policy.

key chain

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
key chain <name>
```

Switch to the specified key chain or create a new key chain.

```
no key chain <name>
```

Remove the specified key chain.

config-version

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
config-version <string>
```

Sets a string to identify the user configuration version.

radius-server accounting session

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server accounting session <number>

Set the maximum number of accounting sessions.

radius-server client

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server client

Enable radius clients list.

no radius-server client

Disable radius clients list.

use default shared secret

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

use default shared secret

Use the default shared secret.

no use default shared secret

Do not use the default shared secret.

use default shared secret

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

use default shared secret

Use the default shared secret.

radius-server local chap

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server local chap

Allow CHAP.

no radius-server local chap

Disallow CHAP.

radius-server local eap-md5

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server local eap-md5

Allow EAP-MD5.

no radius-server local eap-md5

Disallow EAP-MD5.

radius-server local eap-peap

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server local eap-peap

Allow EAP-PEAP.

no radius-server local eap-peap

Disallow EAP-PEAP.

radius-server local eap-tls

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server local eap-tls

Allow EAP-TLS.

no radius-server local eap-tls

Disallow EAP-TLS.

radius-server local eap-ttls

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server local eap-ttls

Allow EAP-TTLS.

no radius-server local eap-ttls

Disallow EAP-TTLS.

radius-server local Controllerhap

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server local Controllerhap

Allow MS-CHAP.

no radius-server local Controllerhap

Disallow MS-CHAP.

radius-server local Controllerhapv2

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server local Controllerhapv2

Allow MS-CHAPv2.

no radius-server local Controllerhapv2

Disallow MS-CHAPv2.

radius-server local pap

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server local pap

Allow PAP.

```
no radius-server local pap
```

Disallow PAP.

radius-server ssid detection nas-id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
radius-server ssid detection nas-id
```

Use NAS-ID for SSID detection.

```
no radius-server ssid detection nas-id
```

Do not use NAS-ID for SSID detection.

show radius-server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
show radius-server
```

Display current RADIUS server configuration.

active-directory check attribute

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
active-directory check attribute <ldapattr>
```

Set the name of the AD attribute to check for.

```
no active-directory check attribute
```

Unset the name of the AD attribute to check for.

active-directory check user access

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
active-directory check user access
```

Check AD for user access.

```
no active-directory check user access
```

Do not check AD for user access.

active-directory device name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
active-directory device name <name>
```

Set the device NetBIOS name.

```
no active-directory device name
```

Unset the device NetBIOS name.

active-directory domain

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active-directory domain <domain>

Set the AD's Windows domain.

no active-directory domain

Reset the AD's Windows domain.

active-directory group

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active-directory group <name>

Create or go to an Active Directory group.

no active-directory group <name>

Remove an Active Directory group.

active-directory group order

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active-directory group order <number> <name>

Reorder an Active Directory group.

active-directory join

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active-directory join <username> <password>

Join with Active Directory.

show active-directory

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show active-directory

Display Active Directory settings.

show active-directory group

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show active-directory group <name>

Display details about an Active Directory group.

radius-server client

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server client <ip address>/<mask> <secret>

Add a new radius client.

```
no radius-server client <ip address>/<mask>
```

Delete an existing radius client.

user tracking

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
user tracking
```

Enable capture of usage data.

```
no user tracking
```

Disable capture of usage data.

user tracking destination

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
user tracking destination <host>
```

Specify to where the detailed syslog packets should be sent.

user tracking filter

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
user tracking filter <filter>
```

A comma-separated list of filters (username or subnet).

user tracking port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
user tracking port <number>
```

Specify to which UDP port capture data should be sent.

persistent user information

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
persistent user information
```

Save user account information locally .

```
no persistent user information
```

Do not save user account information locally.

persistent user information period

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
persistent user information period <number>
```

Period, in minutes, at which to update user information.

2.4 Access Controller Context

Context path: View > Enable > Config > Access Controller

All global access controller configuration takes place here.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

station allocate source ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

station allocate source ip address

Allow dynamic IP addresses.

no station allocate source ip address

Disallow dynamic IP addresses.

Enable this option to provide network address translation for client stations with static IP addresses. This permits the Controller to assign an alias address to the client that puts it on the same subnet as the virtual network the client is associated with. This option cannot be used if NAT is enabled on the Internet port.

station allow any ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

station allow any ip address

Enable this option to permit wireless client stations that are using a static IP address to connect to the Controller, even if they are on a different subnet.

no station allow any ip address

Do not allow client stations with any IP addresses to connect.

This option enables customers to access the wireless network without reconfiguring their networking settings. For example, by default the Controller creates the wireless network on the subnet 192.168.1.0. If a client station is pre-configured with the address 10.10.4.99, it will still be able to connect to the Controller without changing its address, or its settings for DNS server and default gateway.

station free access

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

station free access

When enabled, all customers are automatically granted access when the RADIUS server is down or unreachable.

no station free access

Customers cannot connect when the RADIUS server is unreachable.

Once the RADIUS server is available again, free customer sessions remain active until the customer logs out. This does not apply to customers using 802.1x or WPA.

station http proxy support

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

station http proxy support

Enables support for client stations that are configured to use a proxy server for HTTP and HTTPS, without requiring customers to reconfigure their systems.

no station http proxy support

Disables support for client stations that are configured to use a proxy server for HTTP and HTTPS.

station idle detection

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

station Idle detection *<interval>* *<count>*

The Controller continuously polls authenticated client stations to ensure they are active. If no response is received and the number of retries is reached, the client station is disconnected.

Parameters

<interval>

Specify how long to wait between polls.

<retries>

Specify how many polls a client station can fail to reply to before it is disconnected.

Description

This feature enables the Controller to detect if two client stations are using the same IP address but have different MAC addresses. If this occurs, access is terminated for this IP address removing both stations from the network.

Changing these values may have security implications. A large interval provides a greater opportunity for a session to be hijacked.

The initial query is always done after the client station has been idle for 60 seconds. If there is no answer to this query, the settings for Interval and Retries are used to control additional retries.

system accounting

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

system accounting

Enables RADIUS accounting support.

no system accounting

Disables RADIUS accounting support.

authentication http

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

authentication http <number>

Specifies the port number the Controller will use to provide standard HTTP access to the management tool.

HTTP connections made to this port are met with a warning and the browser is redirected to the secure web server port. By default this parameter is set to port 80.

authentication https

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

authentication https <number>

Specifies the port number the Controller will use to provide secure access to the management tool (HTTPS). By default this parameter is set to port 443.

noc access internet

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

noc access internet

Accept authentication requests on the Internet port.

no noc access internet

Do not accept authentication requests on the Internet port..

noc access vpn

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

noc access vpn

Accept authentication requests on VPN connections.

no noc access vpn

Do not accept authentication requests on VPN connections.

noc allow

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
noc allow <ip address>/<mask>
```

Adds an IP address or subnet to the list of destinations that the Controller will accept customer login authentication requests from when NOC authentication is active.

```
no noc allow <ip address>/<mask>
```

Removes the specified IP address or subnet from the list of destinations that the Controller will accept customer login authentication requests from when NOC authentication is active.

When the list is empty, authentication requests are accepted from any address.

noc authentication

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
noc authentication
```

Enables support for NOC authentication.

```
no noc authentication
```

Disables support for NOC authentication.

secure login

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
secure login
```

Enables secure login.

```
no secure login
```

Disables secure login.

noc access interface vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
noc access interface vlan <name>
```

Adds the specified VLAN to the list of interfaces that authentication requests are accepted on.

```
no noc access interface vlan <name>
```

Removes the specified VLAN from the list of interfaces that authentication requests are accepted on.

noc access interface gre

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

noc access interface gre <name>

Adds the specified GRE tunnel to the list of interfaces that authentication requests are accepted on.

no noc access interface gre <name>

Removes the specified GRE tunnel from the list of interfaces that authentication requests are accepted on.

ipass id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ipass id <name>

Specifies the WISPr location ID assigned to the Controller.

no ipass id

Deletes the WISPr location ID assigned to the Controller.

ipass name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ipass name <name>

Specifies the WISPr location name assigned to the Controller.

no ipass name

Deletes the WISPr location name assigned to the Controller.

wispr abort login url

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

wispr abort login url <url>

Specifies the WISPr abort login url assigned to the Controller.

no wispr abort login url

Deletes the WISPr abort login url assigned to the Controller.

wispr login url

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

wispr login url <url>

Specifies the WISPr login url assigned to the Controller.

no wispr login url

Deletes the WISPr login url assigned to the Controller.

wispr logoff url

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

wispr logoff url <url>

Specifies the WISPr logoff url assigned to the Controller.

no wispr logoff url

Deletes the WISPr logoff url assigned to the Controller.

access-list

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access-list <index> <rule>

Adds a new rule to an access list at the specified index position.

no use access-list

Do not use an access list.

Parameters

index

Index position of the rule within the access list.

rule

Access list rule definition in the format:

<listname>[,OPTIONAL],<action>,<protocol>,<address>
,<port>[,<account>[,<interval>]]

<listname>

Specifies a name (up to 32 characters long) to identify the access list this rule applies to. If a list with this name does not exist, a new list is created. If a list with this name exists, the rule is added to it.

OPTIONAL

Allows the access list to be activated even if this rule fails to initialize. For example, if you specify a rule that contains an address which cannot be resolved for some reason, the other rules that make up the access list will still be initialized. If you do not specify optional, a failed rule will cause the entire list to fail. Critical access list definitions (such as for a remote login page, certificates) should not use the OPTIONAL setting because if these definitions fail to initialize there will be no indication in the log.

<action>

Specifies what action the rule takes when it matches incoming traffic. Two options are available:

- **ACCEPT - Allow traffic matching this rule.**
- **DENY - Reject traffic matching this rule.**
- **WARN - Redirect traffic matching this rule to an error page.**

<protocol>

Specify the protocol to check: tcp, udp, icmp, all

<address>

Specify one of the following:

- **IP address or domain name (up to 107 characters in length)**
- **Subnet address. Include the network mask as follows: address/subnet mask For example: 192.168.30.0/24**
- **Use the keyword all to match any address.**

- Use the keyword **none** if the protocol does not take an address range (ICMP for example).

`<port>` Specify a specific port to check or a port range as follows:

- **none**: Used with ICMP (since it has no ports).
- **all**: Check all ports.
- **1-65535[:1-65535]** - Specify a specific port or port range.

`<account>` Specify the name of the customer account the Controller will send billing information to for this rule. Account names must be unique and can be up to 32 characters in length.

`<interval>` Specify time between interim accounting updates. If you do not enable this option, accounting information is only sent when a customer connection is terminated. Range: 5-99999 seconds in 15 second increments.

use access-list

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`use access-list <listname>`

Specifies the name of the access list to use.

`no use access-list`

Do not use an access list.

config file

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`config file <url>`

Specifies the URL that points to a new configuration file to load.

`no config file`

Do not load a new configuration file.

https ssl certificate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`https ssl certificate <url>`

Specifies the URL that points to an SSL certificate that will replace the default certificate on the Controller.

`no https ssl certificate`

Do not load a custom SSL certificate.

mac-address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`mac-address <macaddr> [<username>] [<password>]`

Adds a MAC address to the local configuration list.

When the MAC authentication option is enabled (in a VAP (virtual network) profile), you can define local configuration settings to validate MAC addresses.

Parameters

macaddr	MAC address of the device as 12 hexadecimal numbers, with the values 'a' to 'f' in lowercase. For example: 0003520a0f01.
username	Username assigned to the device.
password	Password assigned to the device.

fail page

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

fail page <url>

Specifies the URL of a new fail page.

no fail page

No new fail page. Use default.

goodbye url

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

goodbye url <url>

Specifies the URL of a goodbye page.

no goodbye url

No goodbye page.

ipass login url

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ipass login url <url>

Specifies the URL of the IPass login page. The Controller will automatically redirect customers with IPass client software to this page.

no ipass login url

No IPass login URL.

login error url

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

login error url <url>

Specifies the URL of a login error page.

no login error url

No login error page.

login page

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

login page <url>

Specifies the URL of the new login page.

no login page

No new login page. Use default.

login url

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

login url <url>

Specifies the URL of a remote login page.

no login url

No remote login page.

logo

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

logo <url>

Specifies the URL of a new logo.

no logo

No new logo. Use default.

messages

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

messages <url>

Specifies the URL of a new message file.

no messages

No new messages file. Use default.

noc ssl ca-certificate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

noc ssl ca-certificate <url>

Specifies the URL of the certificate from the certificate authority (CA) that issued the NOC certificate.

no noc ssl ca-certificate

No CA certificate.

noc ssl certificate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

noc ssl certificate <url>

Specifies the URL of the certificate issued to the application on the remote web server that will send customer info to the Controller for authentication.

no noc ssl certificate

No certificate.

session page

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

session page <url>

Specifies the URL of a new session page.

no session page

No new session page. Use default.

transport page

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

transport page <url>

Specifies the URL of a new transport page.

no transport page

No new transport page. Use default.

welcome url

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

welcome url <url>

Specifies the URL of a welcome page.

no welcome url

No welcome page.

notify user location changes

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

notify user location changes

Notify RADIUS on location changes.

no notify user location changes

Do not notify RADIUS on location changes.

2.5 Default Session Profile Context

Context path: View > Enable > Config > Default Session profile

This context provides attributes that define settings for customer sessions. Most of these attributes can be overridden by adding settings to a customer's RADIUS account.

In this context, all commands add an attribute to the list, in some cases (access-list & mac-address) several entries are added. The "no" form will remove the attributes.

accounting interim update

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

accounting interim update *<number>*

Sets the default accounting interim update interval (in seconds) for all customers that do not have a specific interval set in their profile.

no accounting interim update

Removes this attribute.

idle timeout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

idle timeout *<number>*

Sets the default idle time out for all customers that do not have a specific limit set in their profile.

no idle timeout

Removes this attribute.

maximum input octets

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

maximum input octets *<value>*

Sets the maximum input limit in octets for all customers that do not have a specific limit set in their profile.

no maximum input octets

Removes this attribute.

maximum input packets

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

maximum input packets *<number>*

Sets the maximum input limit in packets for all customers that do not have a specific limit set in their profile.

no maximum input packets

Removes this attribute.

maximum output octets

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

maximum output octets <value>

Sets the maximum output limit in octets for all customers that do not have a specific limit set in their profile.

no maximum output octets

Removes this attribute.

maximum output packets

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

maximum output packets <number>

Sets the maximum output limit in packets for all customers that do not have a specific limit set in their profile.

no maximum output packets

Removes this attribute.

maximum total octets

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

maximum total octets <value>

Sets the maximum total limit in octets for all customers that do not have a specific limit set in their profile.

no maximum total octets

Removes this attribute.

maximum total packets

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

maximum total packets <number>

Sets the maximum total limit in packets for all customers that do not have a specific limit set in their profile.

no maximum total packets

Removes this attribute.

nat one-to-one

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

nat one-to-one

Enables one-to-one NAT support for all customers that do not have a specific value set in their profile.

no nat one-to-one

Removes this attribute.

session timeout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

session timeout <number>

Sets the default session timeout for all customers that do not have a specific limit set in their profile.

no session timeout

Removes this attribute.

smtp redirection setup

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

<hostname>[:<port>t][,<username>,<password>]

Sets basic SMTP redirection info: hostname[:port][,username,password].

no smtp redirection setup

Clears basic SMTP redirection info.

Parameters

<hostname>

Specify the IP address or domain name of the e-mail server. Maximum length is 253 characters.

<port>

Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25

<username>

Specify the username required to log on to the SMTP server. Maximum 32 characters.

<password>

Specify the password required to log on to the SMTP server. Maximum 32 characters.

Description

Sets the default SMTP server address for all customer sessions. This attribute is used if a specific server is not set for a particular customer

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

smtp redirection

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

smtp redirection

Enables SMTP proxy support.

no smtp redirection

Disables SMTP proxy support.

2.6 Session Profile Context

Context path: View > Enable > Config > Session profile

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

access controlled

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access controlled

Set profile as 'access controlled'.

no access controlled

Set profile as not 'access controlled'.

access list

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access list <name>

Set the access list.

use access list

Use this access list.

no use access list

Do not use this access list.

accounting interim update

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

accounting interim update <number>

Sets the default accounting interim update interval (in seconds) for all customers that do not have a specific interval set in their profile.

use accounting interim update

Use attribute.

no use accounting interim update

Removes this attribute.

arp polling interval

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

arp polling interval <number>

Set the ARP polling interval.

use arp polling interval

Use the ARP polling interval.

no use arp polling interval

Do not use the ARP polling interval.

arp polling max count

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

arp polling max count <number>

Set the polling ARP count.

use arp polling max count

Use the polling ARP count.

no use arp polling max count

Do not use the polling ARP count.

bandwidth level

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

bandwidth level (very-high | high | normal | low)

Set Bandwidth level.

use bandwidth level

Use Bandwidth level.

no use bandwidth level

Don't use Bandwidth level.

egress vlan access-controlled

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

egress vlan access-controlled <number>

Set the tunnel private group id.

use egress vlan access-controlled

Use the tunnel private group id.

no use egress vlan access-controlled

Do not use the tunnel private group id.

egress vlan regular

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

egress vlan regular <number>

Set the tunnel private group id.

use egress vlan regular

Use the tunnel private group id.

no use egress vlan regular

Do not use the tunnel private group id.

idle timeout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

idle timeout <number>

Sets the default idle time out for all customers that do not have a specific limit set in their profile.

use idle timeout

Use this attribute.

no use idle timeout

Removes this attribute.

intercept traffic

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

intercept traffic

Turn on legal traffic interception.

no intercept traffic

Turn off legal traffic interception.

use intercept traffic

Use legal traffic interception.

no use intercept traffic

Do not use legal traffic interception.

max input rate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

max input rate <number>

Set the maximum input rate.

use max input rate

Use the maximum input rate.

no use max input rate

Do not use the maximum input rate.

max output rate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

max output rate <number>

Set the maximum output rate.

use max output rate

Use the maximum output rate.

no use max output rate

Do not use the maximum output rate.

nat one-to-one

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

nat one-to-one

Enables one-to-one NAT support for all customers that do not have a specific value set in their profile.

no nat one-to-one

Removes this attribute.

use nat one-to-one

Use this attribute.

no use nat one-to-one

Do not use this attribute.

session profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

session profile <name>

Change this profile's name.

smtp redirection setup

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

smtp redirection setup
<hostname>[:<port>] [, <username>, <password>]

Sets basic SMTP redirection info: hostname[:port][,username,password].

no smtp redirection setup

Clears basic SMTP redirection info.

use smtp redirection setup

Use SMTP redirection.

no use smtp redirection setup

Do not use SMTP redirection.

Parameters

<code><hostname></code>	Specify the IP address or domain name of the e-mail server. Maximum length is 253 characters.
<code><port></code>	Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25
<code><username></code>	Specify the username required to log on to the SMTP server. Maximum 32 characters.
<code><password></code>	Specify the password required to log on to the SMTP server. Maximum 32 characters.

Description

Sets the default SMTP server address for all customer sessions. This attribute is used if a specific server is not set for a particular customer

termination action

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

termination action (logout | reauthenticate)

Set the termination action.

use termination action

Use the termination action.

no use termination action

Do not use the termination action.

user defined attribute

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

user defined attribute

`<name>:<type>:<vendor-id>:<vendor-type>:<format>:<value>`

Add a new user defined attribute.

no user defined attribute `<description>`

Add a new user-defined attribute.

Parameters

<code><name></code>	Friendly name for this attribute.
<code><type></code>	Numerical RADIUS type, 26 is Vendor-Specific.
<code><vendor-id></code>	If RADIUS type is 26, contains the Vendor-Id. Put 0 if not.
<code><vendor-type></code>	If RADIUS type is 26, contains the Vendor-Type. Put 0 if not.
<code><format></code>	Is either 'integer', 'address', 'text', 'string' or 'time'.
<code><value></code>	Contains the actual value.

Format description and values:

- **integer:** value is a numerical string.
- **address:** value is a legal IP address, or possibly a host name.
- **text:** value is any string of alphanumerical characters.
- **string:** value is a series of hexadecimal digits.

- **time:** value is a time string.

For related information, see RFC 2138, Section 5.

2.7 User Profile Context

Context path: View > Enable > Config > User Profile

Use this context to modify settings for a specific user in the local user list.

Back end example:

```
subscription plan "silver"
  use online time limit
  online time limit 60 minutes
  restrictions
  no use initial login time allocation
  use daily restriction
  daily restriction 08:00:00 17:00:00
  no use start time
  no use end time
end
session profile "guest"
  access controlled
  idle timeout 600
  use idle timeout
  tunnel private group id ac 55
  use tunnel private group id ac
end
user profile "zoe"
  password gadbois
  max user sessions 1
  active
  control method subscription
  subscription plan "silver"
  use access-controlled profile
  access-controlled profile "guest"
  no restrict access-controlled virtual ap
end
```

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

access controlled

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access controlled

Make this user access controlled.

no access controlled

Make this user not access controlled.

access-controlled profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access-controlled profile <name>

Use this session profile for this account.

no access-controlled profile <name>

Do not use this session profile for this account.

use access-controlled profile

Use the Access Controlled profiles.

no use access-controlled profile

Use the Access Controlled profiles.

access-controlled virtual ap

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access-controlled virtual ap <name>

Add to the list of allowed virtual APs.

no access-controlled virtual ap <name>

Remove from the list of allowed virtual APs.

use access-controlled virtual ap

Use only allowed Virtual AP (virtual network) for this profile.

active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active

Enable this user account.

no active

Disable this user account.

chargeable user identity

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

chargeable user identity <id>

Set the CUI.

use chargeable user identity

Use the CUI.

no use chargeable user identity

Do not use the CUI.

control method

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

control method (subscription | endtime | none)

How is this account controlled?

egress vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

egress vlan <number>

Set the VLAN tunnel ID.

use egress vlan

Use the VLAN tunnel ID.

no use egress vlan

Do not use the VLAN tunnel ID.

end time

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end time <time>

Set expiration time: "YYYY-MM-DD HH:MM:SS".

idle timeout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

idle timeout <number>

Sets the idle timeout for this user.

no idle timeout

This user never times out.

max user sessions

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

max user sessions <number>

Sets the maximum concurrent sessions for this user.

no max user sessions

This user doesn't have a maximum concurrent sessions limit.

password

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

password <secret>

Change the password for this user.

regular profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

regular profile *<name>*

Apply a non-ac profile.

no regular profile *<name>*

Remove a non-ac profile.

use regular profile

Use the non-Access Controlled profiles.

no use regular profile

Do not use the non-Access Controlled profiles.

regular virtual ap

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

regular virtual ap *<name>*

Add to the list of allowed virtual APs.

no regular virtual ap *<name>*

Remove from the list of allowed virtual APs.

use regular virtual ap

Use only allowed Virtual AP (virtual network) for this profile.

session timeout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

session timeout *<number>*

Sets the session timeout for this user.

no session timeout

This user session never times out.

subscription plan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

subscription plan *<name>*

Set the subscription plan to use.

no subscription plan

Delete a subscription plan.

username

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

username *<name>*

Change the name for this user.

2.8 Internet Interface Context

Context path: View > Enable > Config > Internet interface

This context provides commands for configuring Internet .

duplex

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

duplex (auto | half | full)

Sets the duplex mode on Internet .

Parameters

auto	Lets the Controller automatically set duplex mode based on the type of equipment it is connected to.
half	Forces the port to operate in half duplex mode.
full	Forces the port to operate in full duplex mode.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

speed

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

speed (auto | 10 | 100)

Sets the speed of Internet .

Parameters

auto	Lets the Controller automatically set port speed based on the type of equipment it is connected to.
100	Forces the port to operate at 100 mbps.
10	Forces the port to operate at 10 mbps.

interface vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

interface vlan <id>[-<id2>]

Switches to the specified VLAN interface or create a new VLAN interface with the specified ID.

no interface vlan <id>[-<id2>]

Deletes the specified VLAN.

Parameters

<id> VLAN ID. Range: 1 - 4094.

<id2>

VLAN ID. When specified, this is the last value in a range.

ipsec vlan interface

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ipsec vlan interface *<name>*

Specifies which VLAN is used by IPsec.

no ipsec vlan interface

Do not use a VLAN for IPsec.

2.9 LAN Interface Context

Context path: View > Enable > Config > LAN interface

This context provides commands for configuring LAN.

duplex

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

duplex (auto | half | full)

Sets the duplex mode on LAN.

Parameters

auto	Lets the Controller automatically set duplex mode based on the type of equipment it is connected to.
half	Forces the port to operate in half duplex mode.
full	Forces the port to operate in full duplex mode.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

speed

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

speed (auto | 10 | 100)

Sets the speed of LAN.

Parameters

auto	Lets the Controller automatically set port speed based on the type of equipment it is connected to.
100	Forces the port to operate at 100 mbps.
10	Forces the port to operate at 10 mbps.

interface vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

interface vlan <id>[-<id2>]

Switches to the specified VLAN interface or create a new VLAN interface with the specified ID.

no interface vlan <id>[-<id2>]

Deletes the specified VLAN interface.

Parameters

<id>	VLAN ID. Range: 1 - 4094.
<id2>	VLAN ID. When specified, is the last value in a range.

ipsec vlan interface

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ipsec vlan interface <name>`

Specifies which VLAN is used by IPsec.

`no ipsec vlan interface`

Do not use a VLAN for IPsec.

2.10 WAN IP Interface Context

Context path: View > Enable > Config > WAN IP interface

This context provides commands for configuring various IP-networking related settings.

pppoe client user

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pppoe client user <username> <password>

Sets the PPPoE username and password.

no pppoe client user

Deletes the PPPoE username.

Parameters

<username>

The username assigned to you by your ISP. The Controller will use this username to log on to your ISP when establishing a PPPoE connection.

<password>

The password assigned to you by your ISP. The Controller will use this username to log on to your ISP when establishing a PPPoE connection.

ip address mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip address mode (dhcp | pppoe | static | none)

Sets the IP addressing mode for Internet .

Parameters

dhcp

Dynamic host configuration protocol. The DHCP server will automatically assign an address to the Controller, which functions as a DHCP client.

pppoe

Point-to-point protocol over Ethernet. The PPPoE server will automatically assign an IP address to the Controller. You need to supply a username and password so the Controller can log on.

static

This option enables you to manually assign an IP address to the Controller.

none

No IP address.

ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip address <ip address>/<mask>

Sets a static IP address for the port.

Parameters

<address>

IP address.

`</mask>` **Subnet mask in CIDR format. Specifies the number of bits in the mask.**

ip nat

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip nat`

Enables Network Address Translation.

`no ip nat`

Disables Network Address Translation.

nat limit port range

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`nat limit port range`

Reserves a range of TCP and UDP ports for each customer starting at port 5000.

`no nat limit port range`

Use any port for NAT.

All outgoing traffic for the customer is mapped within the range.

Applications that set an incoming port (Active FTP, for example) may choose a port that is outside of the allocated port range. If you enable this feature you should not assign static NAT mappings in the range 5000 to 32768.

nat limit port range size

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`nat limit port range size <number>`

Determine the size of the range to use per user, this will limit the number of user authentication supported if too high.

ip address dhcp client-id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip address dhcp client-id <id>`

Specifies an ID to identify the Controller to a DHCP server. This parameter is not required by all ISPs.

`no ip address dhcp client-id`

Deletes the specified DHCP client id.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`end`

Switches to parent context.

pppoe auto-reconnect

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pppoe auto-reconnect

The Controller will automatically attempt to reconnect if the connection is lost.

no pppoe auto-reconnect

The Controller will not automatically attempt to reconnect if the connection is lost.

pppoe mru

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pppoe mru <bytes>

Specifies the maximum receive unit.

Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Parameters

<bytes>

Maximum size (in bytes) of a PPPoE packet when receiving. Range: 500 - 1500 bytes.

pppoe mtu

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pppoe mtu <bytes>

Specifies the maximum transmit unit.

Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Parameters

<bytes>

Maximum size (in bytes) of a PPPoE packet when transmitting. Range: 500 - 1500 bytes.

pppoe unnumbered

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pppoe unnumbered

Enable unnumbered mode.

no pppoe unnumbered

Disable unnumbered mode.

This feature is useful when the Controller is connected to the Internet and NAT is not being used. Instead of assigning two IP addresses to the Controller, one to the Internet port and one to the LAN port, both ports can share a single IP address. This is especially useful when a limited number of IP addresses are available to you.

ip nat outside source static

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ip nat outside source static (tcp|udp) <visible-port>
<internal-addr> <internal-port>
```

Adds a static NAT mapping which routes the specified incoming traffic to the specified IP address on the internal network.

Parameters

tcp | udp

Selects the protocol that the mapping will operate on.

<visible-port>

The protocol port number that the incoming traffic uses.

<internal addr>

IP address of the device on the internal network that traffic will be routed to.

<internal-port>

The protocol port number that the incoming traffic will be mapped to.

ip rip authentication key-chain

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ip rip authentication key-chain <name>
```

Specifies a keyed MD5 chain.

```
no ip rip authentication key-chain
```

Do not use this Keyed MD5 chain.

ip rip authentication mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ip rip authentication mode (md5 | text)
```

Select RIPv2 authentication mode.

```
no ip rip authentication mode
```

Use no RIPv2 authentication.

ip rip authentication string

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ip rip authentication string <secret>
```

Sets the RIP shared password.

```
no ip rip authentication string
```

Clears the RIP shared password.

passive-interface

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`passive-interface`

Sets RIP to operate in passive mode (listen for routing broadcasts to update the routing table, but do not broadcast own routes).

`no passive-interface`

Sets RIP to operate in active mode (listen for routing broadcasts to update the routing table, and also broadcast own routes).

router rip

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`router rip`

Enable RIP.

`no router rip`

Disable RIP.

ip address alternate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip address alternate <ip address>`

Assigns an alternate IP addresses to the Internet port. The address must be valid on the Internet.

`no ip address alternate <ip address>`

Deletes the specified alternate IP address.

The Controller uses these addresses to support its one-to-one NAT feature. The Controller will not respond to pings directed at these IP addresses:

2.11 LAN IP Interface Context

Context path: View > Enable > Config > LAN IP interface

This context provides commands for configuring various IP-networking related settings for the LAN interface.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip address <ip address>/<mask>

Sets a static IP address for the port.

Parameters

<address>

IP address.

</mask>

Subnet mask in CIDR format. Specifies the number of bits in the mask.

ip address management

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip address management <ip address>/<mask>

Sets a management IP address for this device.

Parameters

<address>

IP address.

</mask>

Subnet mask in CIDR format. Specifies the number of bits in the mask.

passive-interface

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

passive-interface

Sets RIP to operate in passive mode (listen for routing broadcasts to update the routing table, but do not broadcast own routes).

no passive-interface

Sets RIP to operate in active mode (listen for routing broadcasts to update the routing table, and also broadcast own routes).

router rip

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

router rip

Enable RIP.

no router rip

Disable RIP.

2.12 Wireless Context

Context path: View > Enable > Config > Wireless

This context provides commands for configuring the wireless network.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

radio active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radio active

Enables the radio.

no radio active

Disables the radio.

rts threshold

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

rts threshold <value>

Sets the RTS threshold.

no rts threshold

Deletes the RTS threshold value.

Parameters

< value >

Threshold value in the range 128 and 1540.

Description

Use this parameter to control collisions on the link that can reduce throughput. If the Status Wireless page on the management tool shows increasing values for Tx multiple retry frames or Tx single retry frames, you should adjust this value until the errors clear up. Start with a value of 1024 and then decrease to 512 until errors are reduced or eliminated.

Using a small value for RTS threshold can affect throughput.

If a packet is larger than the threshold, the Controller will hold it and issue a request to send (RTS) message to the client station. Only when the client station replies with a clear to send (CTS) message will the Controller send the packet. Packets smaller than the threshold are transmitted without this handshake.

distance

Supported on:

distance (small | medium | large)

Sets the distance between access points.

Use this parameter to adjust the receiver sensitivity of the Controller. This parameter should only be changed if:

- you have more than one wireless access point installed in your location
- you are experiencing throughput problems

In all other cases, use the default setting of Large.

If you have installed multiple Controllers, reducing the receiver sensitivity of the Controller from its maximum will help to reduce the amount of crosstalk between the wireless stations to better support roaming clients. By reducing the receiver sensitivity, client stations will be more likely to connect with the nearest access point.

dot11

Supported on:

dot11 <mode> <frequency>

Sets the wireless mode and the frequency the Controller will operate at.

Parameters

<mode>

Sets the transmission speed and frequency band. The available options are determined by the wireless card installed in the Controller, and may include:

- **b:** Selects 802.11b providing 11 Mbps in the 2.4 GHz frequency band.
- **g:** Selects 802.11g providing 54 Mbps in the 2.4 GHz frequency band.
- **bg:** Selects 802.11b + 802.11g providing 11 and 54 Mbps in the 2.4 GHz frequency band.

<frequency>

Sets the operating frequency by specifying a number in GHz or by specifying a channel number. The frequencies that are available are determined by the radio installed in the Controller and the regulations that apply in your country.

For optimum performance when operating in 802.11b or 802.11g modes, choose a frequency that differs from other wireless access points operating in neighboring cells by at least 25 MHz.

transmit power

Supported on:

transmit power (DB | max)

Sets the maximum transmission power of the wireless radio.

Parameters`<db>`

Power is specified in steps of 1dBm. The maximum setting is 18 dBm.

Note: The actual transmit power used may less than the value specified. The Controller determines the power to used based on the settings you made for regulatory domain, wireless mode, and operating frequency.

antenna bidirectionnal**Supported on:**`antenna bidirectionnal (diversity | main | auxiliary)`

Sets the antenna to transmit and receive on. Select diversity to transmit and receive on both antennas.

Parameters`diversity`

In this mode both antennas are used to transmit and receive. The Controller supports both transmit and receive diversity.

`main`

Transmit and receive on the main antenna only.

`aux`

Transmit and receive on the aux antenna only.

autochannel skip**Supported on:**`autochannel skip <chan>`

Adds the specified channel to the list of channels that are not allowed to be selected by the Auto Channel algorithm.

`no autochannel skip <chan>`

Removes the specified channel to the list of channels that are not allowed to be selected by the Auto Channel algorithm.

beacon interval**Supported on:**`beacon interval <value>`

Sets the beacon interval.

Parameters`< value>`

Beacon interval value in the range 20 and 500 time units (TU) (1 TU = 1024us).

dot11 automatic frequency**Supported on:**`dot11 automatic frequency`

Enable this option to have the Controller automatically determine the best operating frequency.

```
no dot11 automatic frequency
```

Disable automatic frequency selection.

dot11 automatic frequency period

Supported on:

```
dot11 automatic frequency period (disabled | 1h | 2h | 4h | 8h | 12h | 24h)
```

Specify how often the frequency setting is re-evaluated when automatic frequency selection is enabled.

dot11 automatic frequency time

Supported on:

```
dot11 automatic frequency time <time>
```

Specify when the channel should be re-evaluated.

dot11 automatic transmit-power

Supported on:

```
dot11 automatic transmit-power
```

Enables automatic transmit power selection.

```
no dot11 automatic transmit-power
```

Disables automatic transmit power selection.

dot11 automatic transmit-power period

Supported on:

```
dot11 automatic transmit-power period (1h | 2h | 4h | 8h | 12h | 24h)
```

Sets the interval at which the transmit power setting is re-evaluated when automatic power selection is enabled.

multicast rate

Supported on:

```
multicast rate (1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54)
```

Sets the transmit rate for multicast traffic.

This is a fixed rate, which means that if a station is too far away to receive traffic at this rate, then the multicast will not be seen by the station. By raising the multicast rate you can increase overall throughput significantly.

station distance

Supported on:

station distance (0km | 5km | 10km | 15km | 20km | 25km | 30km | 35km)

Fine tunes internal timeout settings to account for the distance that wireless links span. For normal operation, the CNx is optimized for links of less than 1 km.

This is a global setting that is useful when creating wireless links to remote sites. However, it also applies to all wireless connection made with the radio, not just for wireless links. Therefore, if you are also using the radio to serve local wireless client stations, adjusting this setting may lower the performance for clients with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)

dot11 mode

Supported on:

dot11 mode (monitor | ap+wds | ap-only | wds-only | sensor)

Sets the operating mode for the radio.

2.13 RADIUS Remote Configuration

Context path: View > Enable > Config > RADIUS remote configuration

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active

Use a RADIUS server to fetch configuration information for the public access network.

no active

Do not use a RADIUS for remote configuration.

credentials

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

credentials <username> <password>

Sets the username/password to use for RADIUS configuration.

no credentials

Resets the username/password to use for RADIUS configuration.

interval

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

interval <number>

Sets the intervals at which the Controller will retrieve configuration information from the RADIUS server.

radius server profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius server profile <name>

Sets the RADIUS profile to use.

no radius server profile

Do not use a RADIUS profile.

2.14 Virtual AP Context

Context path: View > Enable > Config > Virtual AP

This context provides commands for configuring Virtual AP profiles (VAP (virtual network)s).

By default one profile exists with the name "Alvarion Network". This is the default profile and cannot be deleted.

The following example shows how to add a new VAP (virtual network) with egress mapped to an existing VLAN named "hongkong":

```
CLI(config)# virtual ap newap
CLI(virtual-ap)# access control
CLI(virtual-ap)# egress any vlan hongkong
CLI(virtual-ap)# ssid name "newap"
CLI(virtual-ap)# ingress ssid
CLI(virtual-ap)# bandwidth high
CLI(virtual-ap)# end
CLI(config)#
```

virtual ap name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

virtual ap name <name>

Change the VAP (virtual network) name.

access control

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access control

Sets this profile to use the services of the Controller's access control mechanism for authentication and control of client sessions.

no access control

Do not provide access control with this VAP (virtual network).

When enabled

- **The Controller provides a variety of methods for customer authentication, including: MAC, 802.1x, and HTML via either the local user list or a RADIUS server.**
- **Egress traffic can be routed based on the customer state: authenticated, unauthenticated, or intercepted.**

When disabled

- **The Controller does not perform customer authentication, either via RADIUS or the local user list. All authentication must be handled by a remote device.**

- **All wireless traffic is bridged to an egress VLAN.**
- **No access controller functions are available. This means no support for RADIUS attributes for the Controller.**
- **802.1x support is available, including support for RADIUS attributes for users.**

ingress interface

Supported on:

```
ingress (wireless <ssid> | vlan <vlan-name>)
```

Sets the ingress traffic that this profile will accept.

Parameters

<code><ssid></code>	Accepts incoming traffic with the specified SSID
<code><vlan-name></code>	Accepts incoming traffic on the LAN port tagged with the VLAN ID defined for the specified VLAN name.

Description

If the ingress traffic has both SSID and VLAN tags, then the VLAN tag takes precedence. Ingress traffic is either routed through the access control mechanism (if access control is enabled), or bridged directly to the VAP (VSC) egress (if access control is disabled). Untagged traffic on the LAN port that is from wired client stations or third-party access points is always routed through the first VAP (virtual network)

ingress interface

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
ingress vlan <name>
```

Sets the specified interface as the ingress interface traffic will be accepted on.

This command takes a *selector* as its input. A selector is used to differentiate traffic, and decide which parameters should be used to select the VAP (virtual network) this user/traffic applies to.

egress unauthenticated

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
egress ( unauthenticated | authenticated | intercepted ) ( default | vlan <vlan-name> | gre <gre-name> )
```

Sets the output interface that this profile forwards data traffic to.

Parameters

<code>unauthenticated</code>	This is any traffic from client stations that have not attempted to be authenticated by the Controller. For example, a client station that fails to authenticate via 802.1x is not considered to be unauthenticated.
<code>authenticated</code>	This is any traffic from client stations that have been authenticated by the Controller and given access to the public access interface.

<code>intercepted</code>	Traffic from specific customers can be intercepted and redirected. To enable traffic interception for a specific customer, you must specify the appropriate setting in their RADIUS account. See the Controller Administrator,Â’s Guide for details.
<code>default</code>	Sends traffic without specifying a specific interface. The interface that is used will be selected by the routing module based on the traffic destination
<code><vlan-name></code>	Sends traffic tagged with the VLAN ID defined for the specified VLAN name.
<code><gre-name></code>	Sends traffic on the specified GRE tunnel.

max-association

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`max-association <stations>`

Sets the maximum number of clients stations that can associate with this VAP (virtual network).

`<stations>` **Number of client stations. Range: 1 - 255.**

ssid name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ssid name <name>`

Specifies the WLAN name (SSID) for the profile.

vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`vlan <id>`

Assigns a VLAN ID to this VAP (virtual network).

`no vlan`

Deletes the VLAN ID for this VAP (virtual network).

Parameters

`<id>` **VLAN ID. Range: 1 - 4094.**

guest-mode

Supported on:

`guest-mode`

Enables broadcast of the wireless network name (SSID).

`no guest-mode`

Disables broadcast of the wireless network name (SSID).

encryption key 1

Supported on:

```
encryption key <key> <value>
```

Sets WEP key 1.

```
no encryption key <key>
```

Deletes WEP key 1.**Parameters**

<key>

WEP key number. Range: 1 - 4. Keys 2 to 4 are only supported on the first WLAN profile.

<value>

Key value. The number of characters you specify for a key determines the level of encryption the Controller will provide.

For 40-bit encryption, specify 5 ASCII characters or 10 HEX digits.

For 128-bit encryption, specify 13 ASCII characters or 26 HEX digits.

encryption key format

Supported on:

```
encryption key format (hex | ascii)
```

Specify the WEP key format.**Parameters**

hex

Hex keys should only include the following digits: 0-9, a-f, A-F

ascii

ASCII keys are much weaker than carefully chosen hex keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.

transmit key

Supported on:

```
transmit key <key number>
```

Sets the key the Controller will use to encrypt transmitted data. All four keys are used to decrypt received data.

Parameters

<key number>

Transmit key number. Range: 1 -4.

authentication server access controller

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
authentication server access controller
```

Use the access controller to authenticate 802.1x or WPA logins.

authentication server accounting

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

authentication server accounting

Enables RADIUS accounting for this VAP (virtual network).

no authentication server accounting

Disables RADIUS accounting for this VAP (virtual network).

authentication server accounting radius profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

authentication server accounting radius profile <name>

Sets RADIUS accounting to use the specified RADIUS profile.

no authentication server accounting radius profile

Removes accounting support for 802.1x.

authentication server radius

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

authentication server radius <name>

Sets the RADIUS profile to use for 802.1x or WPA authentication.

wpa-psk

Supported on:

wpa-psk <key>

Sets the WPA preshared key.

no wpa-psk

Deletes the WPA preshared key.

Parameters

password

Specify a key that is between 8 and 64 ASCII characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers.

Description

The Controller uses the key you specify to generate the TKIP keys that encrypt the wireless data stream. Since this is a static key, it is not as secure as using dynamically generated keys.

authentication server request radius cui

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

authentication server request radius cui

Include in the authentication request a request for a CUI.

dot1x session page

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot1x session page

IEEE802dot1x authenticated users will be presented with the Session page and the Welcome page after a successful authentication.

no dot1x session page

IEEE802dot1x authenticated users will NOT be presented with the Session page and the Welcome page after a successful authentication.

mac authentication accounting

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mac authentication accounting

Enables RADIUS accounting for this VAP (virtual network).

no mac authentication accounting

Disables RADIUS accounting for this VAP (virtual network).

mac authentication accounting radius profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mac authentication accounting radius profile <name>

Sets RADIUS accounting to use the specified RADIUS profile.

no mac authentication accounting radius profile

Disables accounting support for MAC authentication.

mandatory authentication

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mandatory authentication

MAC-based authentication is mandatory.

no mandatory authentication

MAC-based authentication is not mandatory.

mac authentication radius profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mac authentication radius profile <radiusname>

Specifies the name of the RADIUS profile to use for MAC-based authentication.

no mac authentication radius profile

Do not use a RADIUS profile.

mac authentication remote

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mac authentication remote

Sets MAC-based authentication to use a RADIUS profile.

no mac authentication remote

MAC-based authentication will not use a RADIUS profile.

mac authentication request radius cui

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mac authentication request radius cui

Include a request for a CUI in authentication requests.

mac authentication local

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mac authentication local

Sets MAC-based authentication to use the local user list to validate the MAC addresses of client stations.

no mac authentication local

Do not use the local user list for MAC-based authentication.

mac authentication

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mac authentication

Enables support for MAC-based authentication.

no mac authentication

Disable support for MAC-based authentication.

html authentication

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

html authentication

Enables HTML authentication.

no html authentication

Disables HTML authentication.

dot1x mandatory authentication

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot1x mandatory authentication

Authentication is mandatory.

no dot1x mandatory authentication

Authentication is not mandatory.

html authentication accounting

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

html authentication accounting

Enables RADIUS accounting.

no html authentication accounting

Disables RADIUS accounting.

html authentication accounting radius profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

html authentication accounting radius profile <name>

Sets RADIUS accounting for HTML users to use the specified RADIUS profile.

no html authentication accounting radius profile

Disables RADIUS accounting RADIUS support for HTML users.

html authentication local

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

html authentication local

Validate HTML logins using the local user list.

no html authentication local

Do not validate HTML logins using the local user list.

html authentication radius

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

html authentication radius

Validate HTML logins using the specified RADIUS profile.

no html authentication radius

Do not validate HTML logins using the specified RADIUS profile.

html authentication radius profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

html authentication radius profile <name>

Validate HTML logins using the specified RADIUS profile.

no html authentication radius profile

Do not validate HTML logins using the specified RADIUS profile.

html authentication request radius cui

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

html authentication request radius cui

Include a request for a CUI in the authentication request.

no html authentication request radius cui

Do not include a request for a CUI in the authentication request.

html authentication timeout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

html authentication timeout *<number>*

Sets the HTML authentication timeout.

active

Supported on:

active

Enable this VAP (virtual network).

no active

Disable this VAP (virtual network).

beacon dtim count

Supported on:

beacon dtim count *<number>*

Defines the DTIM period in the beacon.

Client stations use the DTIM to wake up from low-power mode to receive multicast traffic. The Controller transmits a beacon every 100 ms. The DTIM counts down with each beacon that is sent, therefore if the DTIM is set to 5, then client stations in low-power mode will wake up every 500 ms (.5 second) to receive multicast traffic.

public forwarding

Supported on:

public forwarding (any | 802.1x | none)

Enables support for traffic exchange between wireless client stations.

fast authentication

fast authentication

Enables WPA2 opportunistic key caching.

no fast authentication

Disables WPA2 opportunistic key caching.

layer3 mobility

layer3 mobility

Enables Layer 3 mobility.

no layer3 mobility

Disables Layer 3 mobility.

access lan stations

Supported on:

access lan stations

Permits traffic exchange between wireless and LAN stations.

no access lan stations

Blocks traffic exchange between wireless and LAN stations.

beacon transmit power

Supported on:

beacon transmit power

Advertise the current transmit power setting in the beacon.

no beacon transmit power

Do not advertise the current transmit power setting in the beacon.

data rate maximum

Supported on:

data rate maximum (1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54 | highest)

Sets the maximum transmission rate that clients stations must respect in order to connect with this SSID. Clients stations that attempt to associate at a higher data rate will be refused. Select the Highest option to have the Controller automatically adjust the data rate to its maximum setting based on the wirelessmode being used.

data rate minimum

Supported on:

data rate minimum (lowest | 1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54)

Sets the minimum transmission rate that clients stations must meet in order to connect with this SSID. Client stations that are below this setting will not be able to connect to this SSID. Set the Lowest option to have the Controller automatically adjust the data rate to its minimum setting based on the wirelessmode being used.

add ip-qos profile

Supported on:

```
add ip-qos profile <name>
```

Adds the specified profile to the list of IP QoS profiles in effect for this VAP (virtual network).

<profile-name> **Name of an existing IP QoS profile.**

delete ip-qos profile all

Supported on:

```
delete ip-qos profile all
```

Clears the list of IP QoS profiles currently in effect for this VAP (virtual network).

delete ip-qos profile

Supported on:

```
delete ip-qos profile <name>
```

Removes the specified profile from the list of IP QoS profiles in effect for this VAP (virtual network).

<profile-name> **Name of an existing IP QoS profile currently in the profile list for this VAP (virtual network).**

qos

Supported on:

```
qos ( 802.1p | very-high | high | normal | low | diffsrv | tos | default | vap0 | vap1 | vap2 | vap3)
```

Sets the QoS level for this profile.

```
no qos
```

Disables QoS for this profile.

Four traffic queues are provided based on the WME standard. In order of priority, these queues are:

- **1: Voice traffic**
- **2: Video traffic**
- **3: Best effort data traffic**
- **4: Background data traffic**

Each QoS priority mechanism maps traffic to one of the four traffic queues. Client stations that do not support the QoS mechanism for the profile they are connected to are always assigned to queue 3.

Important: Traffic delivery is based on strict priority (per the WME standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queues 3 and 4.

802.1p	<p>Traffic from 802.1p client stations is classified based on the VLAN priority field present within the VLAN header. When this mechanism is selected, the Controller will advertise WME capabilities, enabling WME clients to associate and take advantage of them. This setting has no effect on legacy clients.</p> <p>Note: To support 802.1p, the wireless profile must have a VLAN assigned to it, which means that client station traffic is forwarded onto the LAN port only.</p>
vap0 to vap3	<p>Allows a specific priority level to be specified for all traffic on a VAP (virtual network) profile. This enables client stations without a QoS mechanism to set traffic priority by connecting to the appropriate SSID.</p> <p>If you enable this priority mechanism, it takes precedence regardless of the priority mechanism supported by associated client stations. For example, if you set SSID-based low priority for a profile, all devices that connect to the profile have their traffic set at this priority</p> <p>Mapping to the traffic queues is as follows: vap0 or very-high=queue 1, vap1 or high=queue 2, vap2 or normal=queue 3, vap3 or low=queue 4</p>
diffsrv	<p>Differential services is a method for defining IP traffic priority on a per-hop basis. The Differential Service bits are defined in RFC2474 and are composed of the six most significant bits of the IP TOS field. These bits define the class selector code points which the CN320 maps to the appropriate traffic queue. (default setting)</p>
tos	<p>The IP TOS (type of service) field can be used to mark prioritization or special handling for IP packets.</p>

upstream diffserv tagging

Supported on:

upstream diffserv tagging

Enables upstream diffserv tagging.

no upstream diffserv tagging

Disables upstream diffserv tagging.

wmm advertising

Supported on:

wmm advertising

Enables WMM information element advertising.

no wmm advertising

Disables WMM information element advertising.

html redirection

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

html redirection

Enables support for HTML logins.

no html redirection

Disables support for HTML logins.

bandwidth

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

bandwidth (very-high | high | normal | low)

Sets the bandwidth level.

bandwidth default rates

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

bandwidth default rates

Enables default bandwidth rates for this VAP (virtual network).

no bandwidth default rates

Disables default bandwidth rates for this VAP (virtual network).

bandwidth default rates maximum

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

bandwidth default rates maximum <max-tx-rate> <max-rx-rate>

Sets the default maximum transmit and receive rates.

radius accounting realms

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius accounting realms

Use RADIUS accounting realms.

no radius accounting realms

Do not use RADIUS accounting realms.

radius authentication realms

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius authentication realms

Use RADIUS authentication realms.

no radius authentication realms

Do not use RADIUS authentication realms.

identify stations by ip only

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

identify stations by ip only

Identify stations based on IP address only.

no identify stations by ip only

Do not identify stations based on address IP only.

location-aware group

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

location-aware group <name>

Sets the specified group name for the access point.

no location-aware group

Deletes the specified group name for the access point.

location-aware called-station-id content

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

location-aware called-station-id content (ssid | group | mac)

Sets the value returned in Called-Station-ID.

dhcp relay

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp relay <primary-ip-address> <[secondary-ip-address]>

Sets the primary and secondary DHCP server for the relay.

no dhcp relay

Resets the primary and secondary DHCP server for the relay.

dhcp relay active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp relay active

The dhcp relay is enabled on the VAP (virtual network).

dhcp relay circuit id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp relay circuit id <string>

Sets the Option 82 circuit ID.

no dhcp relay circuit id

Clears the Option 82 circuit ID.

dhcp relay not active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp relay not active

The dhcp relay is not enabled on the VAP (virtual network).

dhcp relay remote id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp relay remote id <string>

Sets the Option 82 remote ID.

no dhcp relay remote id

Clears the Option 82 remote ID.

dhcp relay subnet

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp relay subnet <ip address>/<mask>

Sets the DHCP relay subnet.

no dhcp relay subnet

Clears the DHCP relay subnet.

dhcp server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp server

The dhcp server is enabled on the VAP (virtual network).

no dhcp server

The dhcp server is not enabled on the VAP (virtual network).

dhcp server dns

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp server dns <ip address>

Sets the domain name server provided to DHCP clients.

no dhcp server dns

Reset the domain name server provided to DHCP clients.

dhcp server gateway

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dhcp server gateway <ip address>

Sets the default gateway provided to DHCP clients.

no dhcp server gateway

Reset the default gateway provided to DHCP clients.

dhcp server range

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`dhcp server range <start-range> <end-range>`

Specify the DHCP server IP address range.

dhcp server subnet

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`dhcp server subnet <ip address>/<mask>`

Sets the DHCP server subnet.

`no dhcp server subnet`

Clears the DHCP server subnet.

radius-framed-protocol-attribute

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`radius-framed-protocol-attribute`

Include the RADIUS Framed-Protocol attribute in Access Request packets. The value for this attribute is PPP (1).

`no radius-framed-protocol-attribute`

Do not include the RADIUS Framed-Protocol attribute in Access Request packets.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`end`

Switches to parent context.

security

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`security (none | wep | 802.1x [wep | static-wep] | wpa (psk | radius) [v1 | v2])`

Sets the current wireless security policy.

Parameters

`none`

No wireless security.

`wep`

This option enables support for wireless users with WEP client software.

`802.1x`

This option enables support for wireless users with 802.1X client software. The Controller supports 802.1x client software that uses EAP-TLS, EAP-TTLS, EAP-SIM, and PEAP.

wep	Enables the use of dynamic WEP keys for all 802.1X sessions. Dynamic key rotation occurs on key 1, which is the broadcast key. Key 0 is the pairwise key. It is automatically generated by the Controller.
static-wep	Support client stations using static WEP keys.
wpa	This option enables support for wireless users with WPA client software.
psk	Enables support for a preshared key:
radius	The Controller obtains the MPPE key from the RADIUS server. This is a dynamic key that changes each time the user logs in and is authenticated. The MPPE key is used to generate the TKIP keys that encrypt the wireless data stream.
v1,v2	Specify which version of WPA to use. None will use both versions (mixed mode).

2.15 VLAN Interface Context

Context path: View > Enable > Config > Internet interface > VLAN interface

View > Enable > Config > LAN interface > VLAN interface

View > Enable > Config > Local mesh > VLAN interface

This context provides commands for configuring Virtual LANs (VLANs). In this context, VLANs can be added or edited.

For example, to create a new VLAN interface named "hongkong" on the LAN port with VLAN id 88, do the following:

```

CLI(config)# interface lan
CLI(if-lan)# interface vlan 88
CLI(if-vlan)# vlan name hongkong
CLI(if-vlan)# ip address mode dhcp
CLI(if-vlan)# no nat
CLI(if-vlan)# end
CLI(if-lan)#

```

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip address <ip address>/<mask>`

Sets a static IP address for the VLAN.

Parameters

`<address>`

IP address.

`</mask>`

Subnet mask in CIDR format. Specifies the number of bits in the mask.

ip address mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip address mode (dhcp | static | none)`

Sets the IP addressing mode for this VLAN interface.

Parameters

dhcp

Dynamic host configuration protocol. The DHCP server will automatically assign an address to the Controller, which functions as a DHCP client.

<code>static</code>	This option enables you to manually assign an IP address to the Controller.
<code>none</code>	This VLAN does not have an IP address.

vlan name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`vlan name <name>`

Change the name of this VLAN interface.

ip default-gateway

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip default-gateway <ip address>`

Sets the default gateway for this VLAN.

`no ip default-gateway`

Removes the default gateway for this VLAN.

ip nat

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip nat`

Enable Network Address translation for this interface.

`no ip nat`

Disable Network Address translation for this interface.

2.16 Local Mesh Context

Context path: View > Enable > Config > Local mesh

This context provides commands for configuring local meshes.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

active

Supported on:

active

Activates the local mesh.

no active

Deactivates the local mesh.

interface

Supported on:

interface (radio1 | radio2 | radio3)

Select the interface to which this local mesh link applies.

no interface (radio1 | radio2 | radio3)

Select the interface to remove for this local mesh link.

local mesh name

Supported on:

local mesh name <name>

Renames the current local mesh link.

remote mac

Supported on:

remote mac <address>

Sets the MAC address of the remote access point.

no remote mac

Deletes the MAC address of the remote access point.

Parameters

<address>

MAC address. Specify 6 pairs of hexadecimal numbers separated by colons, with the values a to f in lowercase. For example: 00:03:52:0a:0f:01

security

Supported on:

security

Enables wireless security.

no security

Disables wireless security.

security mode

Supported on:

security mode (wep | tkip | ccmp)

Set the security mode.

security psk

Supported on:

security psk <secret>

Sets the PSK secret.

no security psk

Clears the PSK secret.

security wep

Supported on:

security wep <key>

Sets the WEP key.

no security wep

Deletes the WEP key.

speed

Supported on:

speed (auto | 1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54)

Sets the speed of the wireless link in Mbps.

interface vlan

Supported on:

interface vlan <id>

Switches to the specified VLAN interface or create a new VLAN interface with the specified Id.

no interface vlan <number>

Removes the specified VLAN interface.

Parameters`<id>`VLAN ID. Range: 1 - 4094.

accept forced links**Supported on:**`accept forced links`**May accept master orders for selection.**`no accept forced links`**ignore master orders for selection.**

allowed downtime**Supported on:**`allowed downtime <number>`**Set the allowed downtime for a connection (or a link) to a peer.**

dynamic local mesh**Supported on:**`dynamic local mesh`**Use dynamic local mesh.**`no dynamic local mesh`**Use static local mesh.**

dynamic mode**Supported on:**`dynamic mode (master | alt-master | slave)`**Selects the dynamic operation mode.**

initial discovery time**Supported on:**`initial discovery time <number>`**Slave: Set the group's initial discovery time in seconds.**

mesh id**Supported on:**`mesh id <id>`**Set the local mesh group id.**

minimum snr

Supported on:

minimum snr *<number>*

Slave: Set the group's minimum SNR.

preserve master link

Supported on:

preserve master link

Preserve master link across reboots.

no preserve master link

Do not preserve master link across reboots.

promiscuous mode

Supported on:

promiscuous mode

Slave: Accept any group.

no promiscuous mode

Slave: Use only the slave's group.

promiscuous mode startup delay

Supported on:

promiscuous mode startup delay *<number>*

Set delay in seconds before promiscuous mode starts (if enabled).

snr cost per hop

Supported on:

snr cost per hop *<number>*

Slave: Set the group's SNR cost per hop.

2.17 RADIUS Context

Context path: View > Enable > Config > RADIUS

This context provides commands for configuring RADIUS profiles.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

radius-server accounting port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server accounting port <number>

Specifies the port to use for RADIUS accounting.

Parameters

<number>

Accounting port number. Range: 1 - 65535.

radius-server alternate hosts

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server alternate hosts

Try last answering RADIUS host first.

no radius-server alternate hosts

Try primary RADIUS host first.

radius-server authentication method

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server authentication method (Controllerhap | chap | Controllerhapv2 | pap | eap-md5)

Sets the authentication method to use when communicating with the RADIUS server.

For 802.1x users, the authentication method is always determined by the 802.1x client software and is not controlled by this setting.

If traffic between the Controller and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or ControllerHAP V2, if supported by your RADIUS Server. (PAP, ControllerHAP V1 and CHAP are less secure protocols.)

radius-server authentication port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server authentication port <number>

Specifies the port to use for RADIUS authentication. By default, RADIUS servers use port 1812.

Parameters

<number> Authentication port number. Range: 1 - 65535

radius-server deadtime

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server deadtime <seconds>

Sets the retry interval for access and accounting requests that time-out.

If no reply is received within this interval, the Controller switches between the primary and secondary RADIUS servers (if defined). If a reply is received after the interval expires, it is ignored.

Parameters

<seconds> Retry interval. Range: 2 - 60 seconds.

radius-server host

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server host <primary>[<secondary>]

Sets the addresses of the primary and secondary RADIUS servers.

Parameters

<primary> IP address of the primary RADIUS server.
<secondary> IP address of the secondary RADIUS server.

radius-server key 2

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server key <primary>[<secondary>]

Enter primary and secondary secrets.

Parameters

<primary> Shared secret for the primary RADIUS server.
<secondary> Shared secret for the secondary RADIUS server.

radius-server message-authenticator

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server message-authenticator

Include the message authenticator attribute in RADIUS packets.

no radius-server message-authenticator

Do not include the message authenticator attribute in RADIUS packets.

radius-server name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server name <name>

Changes the name of the RADIUS profile.

radius-server nasid

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server nasid <id>

Sets the network access server ID you want to use for the Controller.

By default, the serial number of the Controller is used. The Controller includes the NAS-ID attribute in all packets that it sends to the RADIUS server.

radius-server timeout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server timeout

Activates RADIUS timeout.

no radius-server timeout

Disables RADIUS timeout.

radius-server timeout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server timeout <number>

Sets the total timeout for RADIUS requests.

no radius-server timeout

Disables RADIUS timeout.

radius-server force-nas-port-to-vlanid

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server force-nas-port-to-vlanid

Force the NAS-Port attribute to ingress VLAN ID in RADIUS packets.

no radius-server force-nas-port-to-vlanid

Do not force the NAS-Port attribute to ingress VLAN ID in RADIUS packets.

radius-server realm

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server realm (regex | text)

Specifies if realms in list are regular expressions or just plain text.

radius-server realm name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius-server realm name <name>

Adds the specified realm name.

no radius-server realm name <name>

Removes the specified realm name.

2.18 IP_QOS Context

Context path: View > Enable > Config > IP_QOS

This context provides commands for configuring IP QoS profiles.

end

Supported on:

end

Returns to a previous context.

end-port

Supported on:

end-port <number>

Specifies the end port to use for this IP QoS profile.

Parameters

<number>

End port number. Range: 0 - 65535

priority

Supported on:

priority <low | medium | high | very-high>

Sets the priority for this IP QoS profile.

Parameters

<priority>

Available priorities are: low, medium, high and very-high.

profile name

Supported on:

profile name <name>

Changes the name of the IP QoS profile.

protocol

Supported on:

protocol <number>

Specifies the protocol ID use for this IP QoS profile.

Parameters

<number>

Protocol number. Range: 0 - 255.

start-port

Supported on:

`start-port <number>`

Specifies the start port to use for this IP QoS profile.

Parameters

`<number>`

Start port number. Range: 0 - 65535

2.19 DHCP Server Context

Context path: View > Enable > Config > DHCP server

This context lets you configure DHCP server settings.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active

This range is enabled.

no active

This range is not enabled.

gateway

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

gateway *<ip address>*

Sets the default gateway provided to DHCP clients.

no gateway

Reset the default gateway provided to DHCP clients.

range

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

range *<start-range>* *<end-range>*

Specify the DHCP server IP address range.

permanent leases

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

permanent leases *<ip address>* *<macaddr>*

Adds a permanent DHCP lease for this mapping.

no permanent leases *<ip address>* *<macaddr>*

Deletes a permanent DHCP lease for this mapping.

2.20 GRE Interface Context

Context path: View > Enable > Config > GRE interface

Details of the GRE interface.

end force

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`end [force]`

Quits the GRE context.

gre name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`gre name <name>`

Renames the current GRE interface.

ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`ip address <ip address>/<mask>`

Set the local tunnel IP address and mask.

peer ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`peer ip address <ip address>`

Sets the GRE peer IP address.

remote ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

`remote ip address <ip address>`

Sets the remote tunnel IP address.

2.21 IPsec Policy Context

Context path: View > Enable > Config > IPsec policy

This context allows editing of IPsec configuration settings.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active

Enables policy.

no active

Disables policy.

authentication

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

authentication (x509 | psk)

Selects between x509 and psk authentication.

cipher

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

cipher aes

Sets the desired encryption algorithm.

no cipher aes

Do not use this encryption algorithm.

dns domain

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dns domain <names>

Sets the domain name for this policy.

no dns domain <names>

Resets the domain name for this policy.

dns server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dns server (<ip address> | none)

Sets the DNS server for this policy.

no dns server

Resets the DNS server for this policy.

incoming nat

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

incoming nat

Enables NAT for incoming traffic.

no incoming nat

Disables NAT for incoming traffic.

incoming traffic network

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

incoming traffic network <ip address>/<mask>

Sets the Phase 2 incoming network.

interface

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

interface (lan | internet)

Sets the interface this policy applies to.

local id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

local id (ip-address <ip address> | host <name> | email <address> | dn <dn>)

Specify the local id type and value.

mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mode (main | aggressive) (tunnel | transport)

Sets the IPSec mode.

outgoing traffic network

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

outgoing traffic network <ip address>/<mask>

Sets the Phase 2 outgoing network.

peer id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
peer id (ip-address <ip address> | host <name> | email <address> |  
dn <dn>)
```

Specify the peer id type and value.

peer ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
peer ip address (<ip address>| any )
```

Set the peer ip address for this policy.

perfect forward secrecy

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
perfect forward secrecy
```

Enable PFS.

```
no perfect forward secrecy
```

Disable PFS.

preshared key

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
preshared key <secret>
```

Sets the preshared key.

```
no preshared key
```

Removes the preshared key.

2.22 Syslog Destination Context

Context path: View > Enable > Config > Syslog destination

This context provides commands for configuring Syslog destinations.

active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active

Enables logging to the current destination.

no active

Disables logging to the current destination.

logging facility

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

logging facility (local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7)

Sets the facility that is used when logging messages to a syslog server.

Parameters

<facility>

Available facilities are: local0 - local7.

logging host

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

logging host (tcp | udp) <addr> [<number>]

Sets the remote address, the connection protocol and port of current syslog remote destination.

logging prefix

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

logging prefix <string>

Sets the prefix that will be prepended to all syslog messages.

no logging prefix

Removes the prefix that is prepended to all syslog messages.

name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

name <name>

Renames the current syslog destination.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

level

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

level

Enables filtering of the log file by severity level.

no level

Disables filtering of the log file by severity level.

level

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

level (lower | higher) (debug | info | notice | warning | error | critical | alert | emergency)

Defines the severity of messages that will be logged.

no level

Disables filtering of the log file by severity level.

Parameters

debug	Debug-level messages.
info	Informational messages.
notice	Normal, but significant condition.
warning	Warning conditions.
error	Error conditions.
critical	Critical conditions.
alert	Action must be taken immediately.
emergency	System is unusable.

matches

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

matches (any | all) filters

All three log file filters (message, process, and level) are combined to filter the log according to this setting.

message

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

message

Enables filtering of the log file message field.

no message

Disables filtering of the log file message field.

message

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

message (matches | notmatches) <regex>

Use this filter to include log messages. Use a regular expression to define the match criteria for the log file message field.

no message

Disables filtering of the log file message field.

process

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

process

Enables filtering of the log file by process name.

no process

Disables filtering of the log file by process name.

process

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

process (matches | notmatches) <string>

Use this filter to include log messages according to their process name.

no process

Disables filtering of the log file by process name.

2.23 PPTP Client Interface

Context path: View > Enable > Config > PPTP client interface

This is the PPTP client context.

active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active

Sets PPTP client connection to 'up'.

no active

Sets PPTP client connection to 'down'.

pptp client credentials

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pptp client credentials <name> <password>

Sets the PPTP username and password.

pptp client domain name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pptp client domain name <name>

Sets the domain name used by the PPTP client.

pptp client server address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pptp client server address <address>

Sets the IP address to connect to.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

ip nat

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip nat

Enables NAT for the PPTP client.

no ip nat

Disables NAT for the PPTP client.

pptp client auto route discovery

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pptp client auto route discovery

Enables auto-route discovery.

no pptp client auto route discovery

Disables auto-route discovery.

pptp client lcp echo

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

pptp client lcp echo

Enables PPTP LCP echo.

no pptp client lcp echo

Disables PPTP LCP echo.

passive-interface

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

passive-interface

Only listen to RIP, never send.

no passive-interface

Send and listen for RIP.

router rip

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

router rip

Enables RIP for this interface.

no router rip

Disables RIP on this interface.

2.24 Keychain Context

Context path: View > Enable > Config > Keychain

Manage a keychain: a collection of keys.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

End current context.

key

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

key <number>

Enter new key.

no key <number>

Delete key with given ID.

key chain name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

key chain name <name>

Rename current keychain.

2.25 Keys Context

Context path: View > Enable > Config > Keychain > Keys

Edit a key, as part of a keychain.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

End current context.

key-string

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

key-string <name>

Set the authentication string for this key.

no key-string

Remove the authentication string for this key.

2.26 Subscription Plan

Context path: View > Enable > Config > Subscription plan

Details about a subscription plan.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

End current context.

daily restriction

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

daily restriction <from> <to>

Sets the daily restrictions hours.

use daily restriction

Enable daily restrictions.

no use daily restriction

Disable daily restrictions.

end time

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end time <datetime>

Set the account end date and time. "YYYY-MM-DD HH:MM:SS".

use end time

Use account end time.

no use end time

Do not use account end time.

initial login time allocation

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

initial login time allocation <number> (minutes | hours | days)

Sets the amount of time allocated after the first login by a user.

use initial login time allocation

Use the initial login time allocation.

no use initial login time allocation

Do not use the initial login time allocation.

online time limit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

online time limit

Use the online time limit.

online time limit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

online time limit <number> (minutes | hours | days)

Sets the initial online time for an account.

start time

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

start time <datetime>

Set the account start date and time. "YYYY-MM-DD HH:MM:SS".

use start time

Use account start time.

no use start time

Do not use account start time.

subscription plan name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

subscription plan name <newname>

Change the subscription plan name.

2.27 Active Directory Group Context

Context path: View > Enable > Config > Active Directory Group

Contains information about attributes to send when a user is related to an Active Directory group.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

access controlled

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access controlled

Make this user access controlled.

no access controlled

Make this user not access controlled.

access-controlled profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access-controlled profile <name>

Use this session profile for this account.

no access-controlled profile <name>

Do not use this session profile for this account.

use access-controlled profile

Use the Access Controlled profiles.

no use access-controlled profile

Do not use the Access Controlled profiles.

access-controlled virtual ap

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

access-controlled virtual ap <name>

Add to the list of allowed virtual APs.

no access-controlled virtual ap <name>

Remove from the list of allowed virtual APs.

use access-controlled virtual ap

Use only allowed Virtual APs (virtual networks) for this profile.

active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active

Enable this user account.

no active

Disable this user account.

active-directory group name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active-directory group name <name>

Change the name for this user.

egress vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

egress vlan <number>

Set the VLAN tunnel ID.

use egress vlan

Use the VLAN tunnel ID.

no use egress vlan

Do not use the VLAN tunnel ID.

regular profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

regular profile <name>

Apply a non-access-controlled profile.

no regular profile <name>

Remove a non-access-controlled profile.

use regular profile

Use the non-access controlled profiles.

no use regular profile

Do not use the non-access controlled profiles.

regular virtual ap

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

regular virtual ap <name>

Add to the list of allowed virtual APs (virtual networks).

no regular virtual ap <name>

Remove from the list of allowed virtual APs (virtual networks).

use regular virtual ap

Use only allowed Virtual APs (virtual networks) for this profile.

no use regular virtual ap

Use any Virtual AP (virtual network) for this profile.

2.28 Controlled Network AP Context

Context path: View > Enable > Controlled Network AP

Contains commands for controlled network AP configuration.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switches to parent context.

execute action

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

execute action (synchronize | accept-suspicious | accept-product | rediscover)

Execute an action on the entity's devices.

execute system action

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

execute system action (restart | reset | switch-mode)

Execute a system action on the AP.

show config factory

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show config [factory]

Displays the current configuration as a list of CLI commands.

ap group

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ap group <name>

Change the AP group (must Synchronize).

ap name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ap name <name>

Change the current AP name.

config

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

config

Switch to generic configuration context.

contact

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

contact <name>

Modify the contact.

location

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

location <name>

Modify the location.

product type

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

product type (map-320 | map-330 | map-630)

Modify the default product type.

2.29 Controlled Network AP Group Context

Context path: View > Enable > Controlled Network AP Group

Contains commands for controlled network AP Group configuration.

execute action

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

execute action (synchronize | accept-suspicious | accept-product | rediscover)

Execute an action on the entity's devices.

show config factory

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show config [factory]

Displays the current configuration as a list of CLI commands.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

config

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

config

Switch to generic configuration context.

group name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

group name <name>

Change the current group name.

virtual ap binding

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

virtual ap binding <vaprofile>

Create/use a VAP (VSC) binding.

no virtual ap binding <vaprofile>

Delete a VAP (VSC) binding.

2.30 Controlled Network Base Group Context

Context path: View > Enable > Controlled Network Base Group

Contains commands for controlled network Base Group configuration.

execute action

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

execute action (synchronize | accept-suspicious | accept-product | rediscover)

Execute an action on the entity's devices.

show config factory

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

show config [factory]

Displays the current configuration as a list of CLI commands.

config

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

config

Switch to generic configuration context.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

2.31 Controlled Network Context

Context path: View > Enable > Controlled Network AP > Controlled Network

View > Enable > Controlled Network AP Group > Controlled Network

View > Enable > Controlled Network Base Group > Controlled Network

Contains commands for controlled network configuration.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

interface wireless

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

interface wireless (single | dual | triple) <number>

Switch to the wireless interface context.

local mesh group

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

local mesh group <group>

Switch to local mesh group context.

local mesh provisioning group

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

local mesh provisioning group

Switch to local mesh provisioning group context.

provisioning connectivity

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

provisioning connectivity

Switch to provisioning connectivity context.

provisioning discovery

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

provisioning discovery

Switch to provisioning discovery context.

radius profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius profile <profile>

Switch to controlled network radius profile context.

syslog

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

syslog

Switch to syslog context.

sensor server name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

sensor server name <name>

Sets the IP address or hostname of the the RF Manager Server to connect to.

Parameters

Name

Specify the IP address of the the RF Manager Server or its hostname. If a hostname is specified, the Controller must be able to resolve it via DNS, that is, an entry must be created on the network DNS server that points to the IP address of the RF Manager Server.

sensor server id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

sensor server id <id>

Sets the server ID of the the RF Manager Server to connect to.

Parameters

ID

Specify the Server ID of the RF Manager Server to connect to. Set the Server ID to 0 to have the Controller send a discovery request to all active Alvarion InCharge RF Manager Servers. The Controller will connect to the first server that responds to the discovery request.

sensor discovery mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

sensor discovery mode (id | ip)

Sets the method the Controller will use to communicate with the RF Manager Server.

Parameters

id

Connect using the Server ID of the RF Manager Server.

ip

Connect using the IP address or hostname of the RF Manager Server.

Description

For these methods to work, the following must be true:

- **The Controller must be able to reach the RF Manager Server via a network connected to port 1 or port 2. For example, you should be able to ping the RF Manager Server, the IP address from the Controller.**
 - **If there are any firewalls between the Controller and the RF Manager Server, then TCP and UDP ports 3851 must be open bi-directionally.**
 - **If using the hostname option, an entry must be created on the network DNS server that points to the IP address of the RF Manager Server.**
 - **If using the Server ID option, support for multicast traffic must be enabled on all routers and switches connected between the Controller and the RF Manager Server.**
-

sensor network detector

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

sensor network detector

Enable the Network Detector.

no sensor network detector

Disable the Network Detector.

inherit sensor

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit sensor

Inherit sensor settings from parent.

no inherit sensor

Do not inherit sensor settings from parent.

dynamic key

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dynamic key

Enables dynamic key support for 802.1X and WPA.

no dynamic key

Disables dynamic key support for 802.1X and WPA.

dynamic key interval

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dynamic key interval (5m | 10m | 15m | 30m | 1h | 2h | 4h | 8h | 12h)

Specifies how often (in minutes or hours) that the group (broadcast) key is changed for 802.1X and WPA.

dot1x reauth

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot1x reauth

Enable this option to force 802.1X client stations to reauthenticate.

no dot1x reauth

Disables 802.1X reauthentication.

dot1x reauth period

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot1x reauth period (15m | 30m | 1h | 2h | 4h | 8h | 12h)

Sets the 802.1X reauthentication interval. Client stations must reauthenticate when this interval expires.

dot1x reauth terminate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot1x reauth terminate

Enable this option to allow client stations to remain connected during re-authentication. Client traffic is blocked only when re-authentication fails.

no dot1x reauth terminate

Disabled this option to block client traffic during re-authentication and only activate traffic again if authentication succeeds.

dot1x supplicant timeout

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

802.1x supplicant time-out <seconds>

Sets the 802.1X supplicant time-out.

Parameters

<seconds> time-out in seconds.

inherit 8021x

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit 802.1x

Inherit 802.1x settings from parent.

no inherit 802.1x

Do not inherit 802.1x settings from parent.

bridge protocol ieee

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

bridge protocol ieee

Enable the bridge spanning tree protocol to prevent undesirable loops from occurring in the network that may result in decreased throughput.

no bridge protocol ieee

Disable the bridge spanning tree protocol.

inherit untagged stp

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit untagged stp

Inherit untagged spanning tree protocol settings from parent.

no inherit untagged stp

Do not inherit untagged spanning tree protocol settings from parent.

bridge protocol ieee vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

bridge protocol ieee vlan

Enable the bridge spanning tree protocol for VLANs.

no bridge protocol ieee vlan

Disable the bridge spanning tree protocol for VLANs.

inherit vlan stp

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit vlan stp

Inherit vlan spanning tree protocol settings from parent.

no inherit vlan stp

Do not inherit vlan spanning tree protocol settings from parent.

centralized access control

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

centralized access control (auto | enabled | disabled)

Set the centralized access control usage.

inherit access control

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit access control

Inherit Access control settings from parent.

```
no inherit access control
```

Do not inherit access control settings from parent.

inherit local mesh qos

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
inherit local mesh qos
```

Inherit local mesh QoS settings from parent.

```
no inherit local mesh qos
```

Do not inherit local mesh QoS settings from parent.

local mesh ip qos profile

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
local mesh ip qos profile <profile>
```

Add an IP QoS profile to the profile's list.

```
no local mesh ip qos profile <profile>
```

Delete an IP QoS profile from the profile's list.

local mesh qos mechanism

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
local mesh qos mechanism (disabled | 802.1p | very_high | high |  
normal | low | diffsrv | tos | ip_qos)
```

Set the QoS priority mechanism.

inherit service availability

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
inherit service availability
```

Inherit service availability from parent.

```
no inherit service availability
```

Do not inherit service availability from parent.

virtual network services on-failure

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

```
vsc services on-failure
```

Enable wireless services when the Controller is unreachable.

```
no vsc services on-failure
```

Shutdown wireless services when the Controller is unreachable.

inherit l3subnets

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit l3subnets

Inherit L3 subnets from parent.

no inherit l3subnets

Do not inherit L3 subnets from parent.

l3subnet

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

l3subnet <vlanid> <ipsubnet> <ipnetmask>

Add a new l3subnet to the list.

no l3subnet <vlanid> <ipsubnet> <ipnetmask>

Delete an l3subnet from the list.

2.32 Virtual AP Binding Context

Context path: View > Enable > Controlled Network AP Group > Virtual AP Binding

Configuration for VAP Bindings

egress vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

egress vlan

Enable the egress vlan.

no egress vlan

Disable the egress vlan.

egress vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

egress vlan <number>

Set the egress vlan id.

no egress vlan

Disable the egress vlan.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

location aware

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

location aware <name>

Set the location-aware group name.

2.33 Syslog Context

Context path: View > Enable > Controlled Network AP > Controlled Network > Syslog
View > Enable > Controlled Network AP Group > Controlled Network > Syslog
View > Enable > Controlled Network Base Group > Controlled Network > Syslog

Set basic configuration for entity's logging.

message

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

message (matches | notmatches) <regex>

Use this filter to include log messages. Use a regular expression to define the match criteria for the log file message field.

no message

Disables filtering of the log file message field.

message

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

message

Enables filtering of the log file message field.

no message

Disables filtering of the log file message field.

process

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

process (matches | notmatches) <string>

Use this filter to include log messages according to their process name.

no process

Disables filtering of the log file by process name.

process

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

process

Enables filtering of the log file by process name.

no process

Disables filtering of the log file by process name.

level

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

level (lower | higher) (debug | info | notice | warning | error | critical | alert | emergency)

Defines the severity of messages that will be logged.

no level

Disables filtering of the log file by severity level.

Parameters

debug	Debug-level messages.
info	Informational messages.
notice	Normal, but significant condition.
warning	Warning conditions.
error	Error conditions.
critical	Critical conditions.
alert	Action must be taken immediately.
emergency	System is unusable.

level

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

level

Enables filtering of the log file by severity level.

no level

Disables filtering of the log file by severity level.

matches

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

matches (any | all) filters

All three log file filters (message, process, and level) are combined to filter the log according to this setting.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

inherit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit

Inherit settings from parent.

no inherit

Do not inherit setting from parent.

2.34 Provisioning Connectivity Context

Context path: View > Enable > Controlled Network AP > Controlled Network > Provisioning connectivity

View > Enable > Controlled Network AP Group > Controlled Network > Provisioning connectivity

View > Enable > Controlled Network Base Group > Controlled Network > Provisioning connectivity

Set basic configuration for entity's provisioning connectivity.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

inherit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit

Inherit provisioning interface settings from parent.

no inherit

Do not inherit provisioning interface settings from parent.

interface

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

interface (port1 | local-mesh)

Set the provisioning interface.

interface provisioninig

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

interface provisioninig

Enable interface provisioning.

ip assignation

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip assignation (static | dhcp)

Set the ip assignment method.

vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

vlan

Enable use of the provisioning vlan.

no vlan

Disable use of the provisioning vlan.

vlan

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

vlan <id>

Set the provisioning vlan id.

no vlan

Disable use of the provisioning vlan.

ip static

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip static <ip address> <ip address> <ip address>

Set the static IP address.

provisioning local mesh group

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

provisioning local mesh group <id>

Set the local mesh group id.

provisioning local mesh key

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

provisioning local mesh key <key>

Set the local mesh security key.

provisioning local mesh port

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

provisioning local mesh port (radio1 | radio2)

Set the radio used for local mesh .

provisioning local mesh security

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

provisioning local mesh security

Enable the use of local mesh security.

no provisioning local mesh security

Disable the use of local mesh security.

provisioning local mesh security

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

provisioning local mesh security (wep | tkip | ccmp)

Set the local mesh security mode.

no provisioning local mesh security

Disable the use of local mesh security.

provisioning local mesh type

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

provisioning local mesh type (a | b | g | bg)

Set the wireless mode for local mesh .

country code

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

country code <code>

Set the country code for local mesh .

2.35 Provisioning Discovery Context

Context path: View > Enable > Controlled Network AP > Controlled Network > Provisioning discovery

View > Enable > Controlled Network AP Group > Controlled Network > Provisioning discovery

View > Enable > Controlled Network Base Group > Controlled Network > Provisioning discovery

Set basic configuration for entity's provisioning discovery.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

dns name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dns name <name>

Add a DNS name to the list.

no dns name <name>

Delete a DNS name from the list.

dns provisioning

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dns provisioning

Enable DNS provisioning.

no dns provisioning

Disable DNS provisioning.

inherit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit

Inherit provisioning discovery settings from parent.

no inherit

Do not inherit provisioning discovery settings from parent.

dns domain name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dns domain name *<name>*

Set the DNS domain name.

dns server

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dns server *<ip address>*

Add a DNS server to the list.

no dns server *<ip address>*

Delete a DNS server from the list.

discovery provisioning

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

discovery provisioning

Enable discovery provisioning.

no discovery provisioning

Disable discovery provisioning.

ip address

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip address *<ip address>*

Add an IP address to the list.

no ip address *<ip address>*

Delete an IP address from the list.

ip provisioning

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

ip provisioning

Enable IP provisioning.

no ip provisioning

Disable IP provisioning.

2.36 Controlled Mode Wireless Interface Context

Context path: View > Enable > Controlled Network AP > Controlled Network > CN Wireless interface

View > Enable > Controlled Network AP Group > Controlled Network > CN Wireless interface

View > Enable > Controlled Network Base Group > Controlled Network > CN Wireless interface

Configuration for wireless interfaces.

distance

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

distance (small | medium | large)

Sets the distance between access points.

Use this parameter to adjust the receiver sensitivity of the Controller. This parameter should only be changed if:

- **you have more than one wireless access point installed in your location**
- **you are experiencing throughput problems**

In all other cases, use the default setting of Large.

If you have installed multiple Controllers, reducing the receiver sensitivity of the Controller from its maximum will help to reduce the amount of crosstalk between the wireless stations to better support roaming clients. By reducing the receiver sensitivity, client stations will be more likely to connect with the nearest access point.

transmit power

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

transmit power (DB | max)

Sets the maximum transmission power of the wireless radio.

Parameters

<db>

Power is specified in steps of 1dBm. The maximum setting is 18 dBm.

Note: The actual transmit power used may less than the value specified. The Controller determines the power to used based on the settings you made for regulatory domain, wireless mode, and operating frequency.

multicast rate

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

multicast rate (1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54)

Sets the transmit rate for multicast traffic.

This is a fixed rate, which means that if a station is too far away to receive traffic at this rate, then the multicast will not be seen by the station. By raising the multicast rate you can increase overall throughput significantly.

dot11 automatic frequency

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot11 automatic frequency

Enable this option to have the Controller automatically determine the best operating frequency.

no dot11 automatic frequency

Disable automatic frequency selection.

dot11 automatic frequency period

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot11 automatic frequency period (disabled | 1h | 2h | 4h | 8h | 12h | 24h)

Specify how often the frequency setting is re-evaluated when automatic frequency selection is enabled.

dot11 automatic frequency time

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot11 automatic frequency time <time>

Specify when the channel should be re-evaluated.

dot11 automatic transmit-power

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot11 automatic transmit-power

Enables automatic transmit power selection.

no dot11 automatic transmit-power

Disables automatic transmit power selection.

dot11 automatic transmit-power period

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot11 automatic transmit-power period (1h | 2h | 4h | 8h | 12h | 24h)

Sets the interval at which the transmit power setting is re-evaluated when automatic power selection is enabled.

antenna bidirectionnal

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

antenna bidirectionnal (diversity | main | auxiliary)

Sets the antenna to transmit and receive on. Select diversity to transmit and receive on both antennas.

Parameters

diversity	In this mode both antennas are used to transmit and receive. The Controller supports both transmit and receive diversity.
main	Transmit and receive on the main antenna only.
aux	Transmit and receive on the aux antenna only.

autochannel skip

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

autochannel skip <chan>

Adds the specified channel to the list of channels that are not allowed to be selected by the Auto Channel algorithm.

station distance

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

station distance (0km | 5km | 10km | 15km | 20km | 25km | 30km | 35km)

Fine tunes internal timeout settings to account for the distance that wireless links span. For normal operation, the CNx is optimized for links of less than 1 km.

This is a global setting that is useful when creating wireless links to remote sites. However, it also applies to all wireless connection made with the radio, not just for wireless links. Therefore, if you are also using the radio to serve local wireless client stations, adjusting this setting may lower the performance for clients with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)

beacon interval

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

beacon interval <value>

Sets the beacon interval.

Parameters

< value >

Beacon interval value in the range 20 and 500 time units (TU) (1 TU = 1024us).

rts threshold

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

rts threshold <value>

Sets the RTS threshold.

no rts threshold

Deletes the RTS threshold value.

Parameters

< value >

Threshold value in the range 128 and 1540.

Description

Use this parameter to control collisions on the link that can reduce throughput. If the Status Wireless page on the management tool shows increasing values for Tx multiple retry frames or Tx single retry frames, you should adjust this value until the errors clear up. Start with a value of 1024 and then decrease to 512 until errors are reduced or eliminated.

Using a small value for RTS threshold can affect throughput.

If a packet is larger than the threshold, the Controller will hold it and issue a request to send (RTS) message to the client station. Only when the client station replies with a clear to send (CTS) message will the Controller send the packet. Packets smaller than the threshold are transmitted without this handshake.

dot11 mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dot11 mode (monitor | ap+wds | ap-only | wds-only | sensor)

Sets the operating mode for the radio.

radio active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radio active

Enables the radio.

no radio active

Disables the radio.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

inherit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit

Inherit settings from parent.

no inherit

Do not inherit settings from parent.

spectralink view

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

spectralink view

Enable the use of spectralink view.

no spectralink view

Disable the use of spectralink view.

2.37 RADIUS Profile Context

Context path: View > Enable > Controlled Network AP > Controlled Network > RADIUS Profile

View > Enable > Controlled Network AP Group > Controlled Network > RADIUS Profile

View > Enable > Controlled Network Base Group > Controlled Network > RADIUS Profile

Basic per entity RADIUS Profile configuration.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

inherit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit

Inherit settings from parent.

no inherit

Do not inherit settings from parent.

radius nas id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radius nas id <nasid>

Set the radius profile NAS Id.

2.38 Local Mesh Profile Context

Context path: View > Enable > Controlled Network AP > Controlled Network > Local mesh profile

View > Enable > Controlled Network AP Group > Controlled Network > Local mesh profile

View > Enable > Controlled Network Base Group > Controlled Network > Local mesh profile

Configuration for local mesh profiles.

security

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

security

Enables wireless security.

no security

Disables wireless security.

security mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

security mode (wep | tkip | ccmp)

Set the security mode.

security psk

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

security psk <secret>

Sets the PSK secret.

no security psk

Clears the PSK secret.

security wep

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

security wep <key>

Sets the WEP key.

no security wep

Deletes the WEP key.

dynamic mode

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

dynamic mode (master | alt-master | slave)

Selects the dynamic operation mode.

mesh id

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

mesh id <id>

Set the local mesh group id.

allowed downtime

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

allowed downtime <number>

Set the allowed downtime for a connection (or a link) to a peer.

minimum snr

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

minimum snr <number>

Slave: Set the group's minimum SNR.

snr cost per hop

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

snr cost per hop <number>

Slave: Set the group's SNR cost per hop.

initial discovery time

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

initial discovery time <number>

Slave: Set the group's initial discovery time in seconds.

active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

active

Activates the local mesh group.

no active

Deactivates the local mesh group.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

inherit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit

Inherit settings from parent.

no inherit

Do not inherit settings from parent.

name

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

name <name>

Renames the current local mesh group.

radio active

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

radio active (radio1 | radio2)

Enables the radio.

no radio active (radio1 | radio2)

Disables the radio.

2.39 Local Mesh Provisioning Profile Context

Context path: View > Enable > Controlled Network AP > Controlled Network > Local mesh provisioning profile
View > Enable > Controlled Network AP Group > Controlled Network > Local mesh provisioning profile
View > Enable > Controlled Network Base Group > Controlled Network > Local mesh provisioning profile

Configuration for local mesh provisioning profile.

accept connection

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

accept connection

Enable this group to act as alternate master.

no accept connection

Prevent this group from acting as alternate master.

end

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

end

Switch to parent context.

inherit

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

inherit

Inherit settings from parent.

no inherit

Do not inherit settings from parent.

multiple radio

Supported on: Wi²-CTRL-10 Wi²-CTRL-40 Wi²-CTRL-200

multiple radio

On multiple radio products, use all available radios.

no multiple radio

On multiple radio products, do not use all available radios.

